

# SecurITree<sup>®</sup> Version 5.5

Copyright © 2001-2023 Amenaza Technologies Limited  
All Rights Reserved

Amenaza Technologies Limited  
Mailstop 125  
406 - 917 85th St. SW  
Calgary, AB  
Canada T3H 5Z9

Tel: (403) 263-7737  
Fax: (403) 278-8437  
Toll Free: 1-888-949-9797  
International: +1 403 263 7737

[info@amenaza.com](mailto:info@amenaza.com)  
[www.amenaza.com](http://www.amenaza.com)

# Table of Contents

<b>Introduction</b>	<b>11</b>
What Is SecurITree?	11
What are Attack (Threat) Trees?	12
SecurITree Licensing Options	13
Copyright	14
Contact Us	16
<b>Using SecurITree</b>	<b>17</b>
Using SecurITree	17
Using Nodes	18
Using Nodes	18
Add Node	19
Edit Node	22
Delete Node	25
Print Node	26
Insert New Root Node	27
Adopt to Alt Set	28
Deactivate Node/Subtree	29
Using Indicators	30
Using Indicators	30
Add Indicator	33
Edit Indicator	36
Delete Indicator	39
Rename Indicator	40
Attack Scenarios	41
Pruning Attack (Threat) Trees	42
Pruning Attack (Threat) Trees	42
Manual Mode	43
Load Agent Profile Mode	44
Agent Profiles and Pruning Criteria	45
Explanation of Pruning Methods	46
Advanced Analysis	48
Advanced Analysis	48
Overview	49
Attacker and Victim Utility	51
Main Analysis	55
Machine Learning	60
Similarities	61
Attack Scenario Reduction	62
Attack Effectiveness	65
Attack Type and Time Parameters	67
Alternative Sets	68
Libraries vs. Trees	68

Subtree Reuse: Internal Links	70
Countermeasures	77
Attack-Defense Trees	82
Attack Graphs	88
Notes	92
Flags	94
Side Panels	95
Side Panels	95
Node Information	96
Tree Information	97
Toolbars	98
Toolbars	98
Main Toolbar	99
Pruning Trees Toolbar	102
Set Operations on Pruned Trees Toolbar	103
Attack Scenarios Toolbar	104
Advanced Analysis Toolbar	105
Memory Errors	106
Language and Number Format	108
Regular Expressions	109
regex	112

---

**Main Menus** **113**

Main Menus	113
File	114
File Menu	114
New Tree...	115
New Tree from Template...	116
Open Tree...	117
Open Library...	118
Insert Tree...	119
Insert Library...	120
Insert External...	121
Reload External	123
Save Tree	124
Save Tree As...	125
Save Subtree...	126
Save Sanitized Tree	127
Sanitize Subtree	128
Sign Tree	129
Close	130
Basic Reports	131
Advanced Reports	134
Print Tree...	138
Page Layout	139
Tree Properties	140
Node Properties	143

Exit	145
Edit	146
Edit Menu	146
Undo	147
Redo	148
Undo Levels...	149
Cut	150
Copy	151
Paste	152
Paste Special	153
Paste Special	153
Paste as Link	154
Paste as Identical Link	155
Paste as Ganged Link	156
Paste Values	157
Paste Notes	158
Paste Color/Font	159
Paste Tree Structure	160
Break Link	161
Instantiate External Link	162
Instantiate All External Links	163
Add to Scratchpad	164
Nodes	165
Edit Tree in Table Format	166
Change Node Values	167
Set Indicators	168
Define Alternative Sets	171
Define Sensor Defense Pairs	172
Note Types	173
Edit Agent/Victim Profile	174
Edit Profile Weight Map	175
Reduce Subtree	176
Restore Subtree	177
Find	178
View	180
View Menu	180
Zoom...	181
Depth Display Level...	182
Show Legend on Tree	183
Show High Level View of Tree	184
Show Scratchpad	185
Roll Up Subtree	186
Roll Down Subtree	187
Roll Down Subtree 1 Level	188
Roll Down Subtree x Levels...	189
Roll Down Nested Subtrees	190
Display Alternative Sets...	190

Show m of n Combinations	192
Show all enabled bubbles	193
Hide all enabled bubbles	194
Analyze	195
Analyze Menu	195
Calculate Tree	196
Attack Scenarios...	197
Pruning Tree...	198
Set Operations on Pruned Trees...	200
Advanced Analysis...	201
Analyze Subtree	202
Tools	203
Tools Menu	203
Toolbars	204
Panels	205
Show Node Information Panel	206
Show Tree Information Panel	207
Plugins	208
Preferences	209
Preferences	209
Interface	210
Application	213
Tree Properties	215
Auto Calculate	219
Node Info	220
Flags	222
Window	224
Window Menu	224
Advanced Analysis Windows	225
Pruning Windows	226
Set Operations on Pruned Trees	227
Attack Scenario Windows	228
Cascade Windows	229
Close All Analysis Windows	230
Help	231
Help Menu	231
Help Index...	232
Context Sensitive Help	233
Legend	234
About	235

---

**Pruning Menus** **236**

Pruning Menus	236
File	237
File Menu	237
Save Tree	238
Save Tree As...	238

Load Agent Profile	240
Save Agent Profile	241
Print Agent Profile	242
Reports...	243
Print Tree...	246
Page Layout	247
Close	248
Edit	249
Edit Menu	249
Edit Agent Profile...	250
Change Calculation Method...	251
Copy	252
Find...	253
View	255
View Menu	255
Zoom...	256
Depth Display Level...	257
Show Legend on Tree	258
Roll Up Subtree	259
Roll Down Subtree	260
Roll Down Subtree 1 Level	261
Roll Down Subtree x Levels...	262
Roll Down Nested Subtrees	263
Display Pruned Nodes	264
Analyze	265
Analyze Menu	265
Attack Scenarios...	266
Tools	267
Tools Menu	267
Display Toolbar	268
Show Node Information Panel	269
Preferences	270
Help	272
Help Menu	272
Help Index	273
Context Sensitive Help	274
Legend	275
About	276

---

**Set Operations on Pruned Trees Menus** **277**

Set Operations on Pruned Trees Menus	277
File	278
File Menu	278
Save Tree	279
Save Tree As...	280
Reports...	281
Print Tree...	283

Page Layout	285
Close	286
Edit	287
Edit Menu	287
Copy	288
Find...	289
View	291
View Menu	291
Zoom...	292
Depth Display Level...	293
Show Legend on Tree	294
Roll Up Subtree	295
Roll Down Subtree	296
Roll Down Subtree 1 Level	297
Roll Down Subtree x Levels...	298
Roll Down Nested Subtrees	299
Display Flag Columns	300
Display Reduced Names	301
Node Occurrence	302
Show Entire Tree	303
Wrap Cell Text	304
Color Node Names	305
Sort	306
Reset Column Width	307
Tools	308
Tools Menu	308
Display Toolbar	309
Show Node Information Panel	310
Preferences	311
Help	313
Help Menu	313
Help Index	314
Context Sensitive Help	315
Legend	316
About	317

---

**Attack Scenarios Menus** **318**

Attack Scenarios Menus	318
File	319
File Menu	319
Save Tree	320
Save Tree As...	321
Reports...	322
Print Tree...	325
Page Layout	326
Close	327
Edit	327

Edit Menu	328
Copy	329
Find...	330
View	332
View Menu	332
Zoom...	333
Depth Display Level...	334
Show Legend on Tree	335
Roll Up Subtree	336
Roll Down Subtree	337
Roll Down Subtree 1 Level	338
Roll Down Subtree x Levels...	339
Roll Down Nested Subtrees	340
Display Flag Columns	341
Display Reduced Names	342
Node Occurrence	343
Show Entire Tree	344
Wrap Cell Text	345
Color Node Names	346
Filter Scenarios	347
Sort	348
Reset Column Width	349
Tools	350
Tools Menu	350
Display Toolbar	351
Show Node Information Panel	352
Preferences	353
Help	355
Help Menu	355
Help Index	356
Context Sensitive Help	357
Legend	358
About	359

---

## **Advanced Analysis Menus** **360**

Advanced Analysis Menus	360
File	361
File Menu	361
Save Tree	362
Save Tree As...	363
Load Agent Profile	364
Save Agent Profile	365
Print Agent Profile	366
Load Victim Profile	367
Save Victim Profile	368
Print Victim Profile	369
Graphs	369



Reports...	375
Print Tree...	378
Page Layout	379
Close	380
Edit	381
Edit Menu	381
Copy	382
Find...	383
View	385
View Menu	385
Zoom...	386
Depth Display Level...	387
Show Legend on Tree	388
Roll Up Subtree	389
Roll Down Subtree	390
Roll Down Subtree 1 Level	391
Roll Down Subtree x Levels...	392
Roll Down Nested Subtrees	393
Display Flag Columns	394
Display Reduced Names	395
Node Occurrence	396
Show Entire Tree	397
Wrap Cell Text	398
Color Node Names	399
Filter Scenarios	400
Sort	401
Columns	402
Reset Column Order	404
Reset Column Width	406
Cumulative Risk Time Units	407
Analyze	408
Analyze Menu	408
Tools	409
Tools Menu	409
Display Toolbar	410
Show Node Information Panel	411
Show Charts Panel	412
Preferences	413
Help	415
Help Menu	415
Help Index	416
Context Sensitive Help	417
Legend	418
About	419

**Appendix B - License**

**426**

---

**Index**

**441**

---

## What Is SecurITree?

**SecurITree** is a decision support tool that helps organizations understand the risks they and their systems face from both hostile and randomly occurring incidents. It is capable of modeling both physical and electronic (information technology) systems. **SecurITree** is used in commercial, defense, aerospace, health care and critical infrastructure applications. It models threats to systems as a hierarchy of events that could lead to failure. The attack hierarchy is known as an [Attack \(Threat\) Tree](#). Attack Trees decompose the steps needed to compromise a system into a series of goals and sub goals. Mathematical functions indicate what resources (e.g., technical skill, money) are needed to carry out the various attacks. By comparing the resources available to people who are hostile to the organization (known as threat agents) with the resources required to carry out attacks, it is possible to show which threats are most likely to occur.

No model/tool (including Attack Trees/**SecurITree**) can predict what will occur with total accuracy. In many cases it is impossible or impractical to eliminate the risk associated with real computer systems. Proper application of the Attack Tree model can help an organization know which portions of a system are most vulnerable and will provide valuable clues on how risk may be lessened.

## What are Attack (Threat) Trees?

An Attack (Threat) Tree is a graphical model that describes threats to a system. The threat may be a malicious individual intent on damaging the availability, integrity or confidentiality of the system. In other cases, damage may be caused by operator error or environmental events (e.g., a flood). The model must be detailed enough to show the root cause of the failure. Once a model has been created, modelling functions are applied that examine the threat from various perspectives.

## SecurITree Licensing Options

SecurITree has licensing options available for each of the following versions:

1. Full
2. Analyzer
3. Creator
4. Viewer
5. Enterprise

The *Full* version of SecurITree has all features enabled. Attack (Threat) Trees can be created, modified, analyzed and viewed.

The *Analyzer* version of SecurITree has all features of the *Full* version but you cannot save trees, create new trees, or edit existing trees. This version is designed for users who need to view and analyze existing trees that have been created using the *Full* or *Creator* versions of SecurITree.

The *Creator* version of SecurITree has all features of the *Full* version but you cannot perform analysis on the trees. This version is designed for users who only need to create trees for others to analyze in the *Full* or *Analyzer* versions of SecurITree.

The *Viewer* version of SecurITree is designed strictly for viewing only. The advanced features found in the other versions of SecurITree like creating, modifying and analyzing the trees are disabled. This version is ideal for users who only need to view the trees that have been created using the *Full* and *Creator* versions of SecurITree.

The *Enterprise* license consists of a bundle of licenses. You may choose which of the licenses in your bundle will be deployed as "floating" with the remainder being designated as "node-locked". Floating licenses are concurrent usage and are managed by a network license manager at your site. You may install as many copies of SecurITree on your network as you desire. The license manager communicates with the PCs equipped with SecurITree via the corporate network and assigns licenses from a pool. Node-locked licenses are associated with a specific PC and are appropriate for laptops or other systems that may not have network connectivity. Node-locked licenses are always guaranteed to be available.

For more information on these licensing options please contact us at: [sales@amenaza.com](mailto:sales@amenaza.com).

To view the Read Me see [Appendix A - Read Me](#)

To view the End User License Agreement see [Appendix B - License](#)

# Copyright

## SecurITree Version 5.5

Copyright © 2001-2023 Amenaza Technologies Limited.

All rights reserved.

Product of Canada.

This product was developed using Guild software libraries that are Copyright © 757070 Alberta Inc.

All rights reserved. Permission to use, copy and modify this software and to distribute this software in binary form is granted to the user Amenaza Technologies Limited.

This product uses:

Spellex Spell-Checking Engine

Copyright © 2004 Spellex Corporation -  
2000 Wintertree Software Inc.

This product includes software developed by:

Wildcrest Associates (<http://www.wildcrest.com>)

This product includes Jep Java developed by:

Singular Systems (<http://www.singularsys.com>)

This product uses the FreeHEP Java Library (<http://www.freehep.org>). The FreeHEP library is licensed under the terms of the GNU Lesser General Public License (LGPL) - a copy of which is found in FreeHEP LicenseInfoLGPL.rtf (found in the SecurITree installation directory) or at <http://www.gnu.org/copyleft/lesser.html>.

This product is a Java application which executes using a Java Runtime Environment, including runtime components, classes and libraries associated with that environment. The Software has been compiled using the OpenJDK version of Java, a free and open-source implementation of the Java Platform Standard Edition. The OpenJDK Java implementation is licensed under the GNU Public License version 2 with a linking exception (sometimes known as a classpath exception).

Java and OpenJDK are trademarks or registered trademarks of Oracle and its affiliates. The Java components, classes and libraries required to execute the Software are supplied by the Licensor for the convenience of the Licensee.

## Contact Us



Amenaza Technologies Limited  
Suite 125  
406 - 917 85th St. SW  
Calgary, AB  
Canada T3H 5Z9

Tel: (403) 263-7737  
Fax: (403) 278-8437  
Toll Free: 1-888-949-9797  
International: +1 403 263 7737

e-mail: [support@amenaza.com](mailto:support@amenaza.com)  
Web: [www.amenaza.com](http://www.amenaza.com)



## Using SecurITree

The following **SecurITree** topics are described in more detail:

[Using Nodes](#)

[Using Indicators](#)

[Attack Scenarios](#)

[Pruning Attack \(Threat\) Trees](#)

[Advanced Analysis](#)

[Attack Scenario Reduction](#)

[Attack Effectiveness](#)

[Attack Type and Time Parameters](#)

[Alternative Sets](#)

[Libraries vs. Trees](#)

[Subtree Reuse: Internal Links](#)

[Countermeasures](#)

[Attack Graphs](#)

[Notes](#)

[Flags](#)

[Side Panels](#)

[Toolbars](#)

[Memory Errors](#)

[Language and Number Format](#)

## Using Nodes

These actions can be performed on Attack (Threat) Tree nodes:

[Add Node](#)

[Edit Node](#)

[Delete Node](#)

Auto Size Node

[Print Node](#)

[Insert New Root Node](#)

[Adopt to alternative set](#)

[Deactivate Node/Subtree](#)

### To resize nodes:

Click the node to select it, then click the sizing handle (the black spot on the right side of the node) and drag while holding down the mouse button.

To automatically size the node to the size required to show all text, right-click on the node then select "Auto Size Node". Alternatively, click the node to select it then click the toolbar icon for "Auto Size Node", or select **Edit > Nodes > Auto Size Node**.

### To reset node size:

Right-click on the node and select "Reset Node Size".

All nodes on the tree can be "auto-sized" by selecting **Tools > Preferences** then checking "Auto size all nodes on tree" on the *Node Info* tab.

All nodes on the tree can be reset to the standard size by selecting **Tools > Preferences** then clicking on "Reset all nodes to standard size" on the *Node Info* tab.

The tree can be displayed with the default node sizes while retaining the customized sizes by selecting **Tools > Preferences** then clicking on "Display Standard Node Sizes" on the *Interface* tab.

### Navigating the tree:

Every node in the tree can be visited in a depth-first navigation by using the <Page Up> / <Page Down> keys. The arrow keys can also be used to navigate from one node to another.

## Add Node

To **Add** a node to a tree:

1. Select the node that the new node should be added under, i.e. the node that will be the parent for the new node. This will cause the node to be highlighted in yellow.
2. Select **Add** by choosing **Edit > Nodes > Add Node**, clicking on the **Add** button on the left side-panel ([Node Information Panel](#)), by clicking on the **Add** icon on the [toolbar](#), or by using the right mouse button to click the parent node, then select **Add Node** on the pop-up menu.
3. If the *Parent Node Change* dialog box appears, this means that the node you are inserting on is a *LEAF* node and it must be changed to an *AND* or *OR* node. You must select the node type for the parent node, either *AND* or *OR*.
4. The *Add Node* dialog window will be displayed. A status line is displayed at the top of the dialog which informs you of the parent node for this new node. Data must now be entered into the fields in the dialog. Enter the *name* for the node that will appear inside the shape. The *Type* is the type of node which can be either *LEAF*, *AND*, or *OR*.
5. The Internal ID is a unique identifier that is assigned for each node. It cannot be changed. This identifier is used when logging changes to nodes and can be used for synchronization with an external database. The External ID is set by the user. This value can also be used for database synchronization. Please see [Main Menus > Tools > Preferences > Tree Properties](#) for further information.
6. If this tree contains a Behavioral Probability indicator, you must select the Subtype. If this is a *LEAF* node either Capability, Probability, or Countermeasure. If *AND/OR* node, only countermeasure or incident.
7. More on countermeasure nodes: A countermeasure node can only be added under an *AND* node. If the countermeasure node is an *AND/OR* node, only "fault tree" nodes can be added under this node, i.e., *LEAF* nodes can only be Probability nodes.. *AND/OR* countermeasure nodes also need a Countermeasure Type to be selected; Consolidate or Expand countermeasure scenarios. Typically, countermeasure nodes do not have impact values defined.
8. Checking the Deactivate Node/Subtree box will leave the node on the tree, but it will not be used when calculating Attack Scenarios. Nodes can also be deactivated/activated by right-clicking the node and selecting **Nodes > Deactivate Node/Subtree**.
9. Checking Enable Bubble will allow a Bubble to be displayed for this node showing the notes that were defined in **Tools > Preferences > Node Info**. Checking Display Bubble will turn the bubble display on.
10. The **Notes** area is available for notes specific to the node. See [Notes](#) for more information.

**Indicators tab:**

1. If this is a *LEAF* node, values must be entered for all indicators. All calculations on the tree are done using the values entered for *LEAF* nodes. Depending on the type of the indicator, the value must be entered as a numeric, or if it is a Boolean type of indicator, the value TRUE or FALSE must be selected. If this is an *AND* or *OR* node, indicator values are disabled since values for *AND* and *OR* nodes are calculated using the values provided from their *LEAF* nodes.
2. Behavioral and Impact Indicators are split into different areas on the screen.
  1. If this is a LEAF node with subtype Capability, only values for behavioral capability indicators and impact indicators can be entered.
  2. If this is a LEAF node with subtype Probability, only values for the behavioral probability indicator and impact indicators can be entered.
  3. If this is a LEAF node with subtype Countermeasure, only values for the Probability of Fault (or Countermeasure Effectiveness) and Impact indicators can be entered. The value for the Probability indicator is  $1 - \text{Countermeasure Effectiveness}$  and conversely, Countermeasure Effectiveness is  $1 - \text{Probability}$ . Either value can be entered and the other is calculated.
  4. If this is an *AND* or *OR* node and the tree has impact indicators, more fields are displayed on the screen. The "Children's Impact" field is the value calculated for this node using the child values. This field cannot be edited. If the value for the impact indicator is to be overridden, the Impact Operator and Node's Impact fields must be filled in. The Impact Operator must be selected from the pull-down list. The Node's Impact field must be filled in with a value. The Impact Value field cannot be edited. It is the result of impact operation, i.e.,  $\langle \text{Children's Impact} \rangle \text{ apply } \langle \text{Impact Operator} \rangle \text{ to } \langle \text{Node's Impact} \rangle = \langle \text{Impact Value} \rangle$ .
  5. If this is an *AND* node, the *AND* formula can be selected by clicking on the button to open the Formula Selection dialog. In most cases, the Primary *AND* Formula that was defined for the indicator should be used (which is the default). If a Secondary *AND* Formula was defined for the indicator, that selection will be enabled. If Custom *AND* Formula is selected, the formula must be chosen from the list.

**Options tab:**

1. The Attack Effectiveness can be optionally set here. See [Using SecurITree > Attack Effectiveness](#) for more information.

2. The Attack Type and Attack Time parameters can be optionally set here. See [Using SecurITree > Attack Type and Time Parameters](#) for more information.
3. If this is a LEAF node with subtype Capability, the Node Attack Type can be selected. "Use tree default" will use the value that has been set in Tree Properties. See [Tools > Preferences > Tree Properties](#) for further information on node attack type.
4. For AND nodes only, Input Threshold: Enter the number of children required to satisfy AND condition. See Main Menus > View > [Show m of n Combinations](#) for more information.
5. The color of the node and font settings can be changed by clicking the "Change Node Color/Font" button, and then selecting the desired color and font settings on the **Change Node Color/Font** dialog. The node color can be set back to the default color by clicking on the "Reset Node Color/Font" button. All nodes on the tree can be set back to the default color by selecting Tools > Preferences, *Node Info* tab, then clicking on "Reset all node colors to default".
6. An image can be attached to the node by clicking the "Attach Image" button. A name for the image must be entered as well as the file name for the image. When the tree is saved, the image file will be saved with the tree in the \*.rit file. The same image can be attached to multiple nodes by selecting the image name from the pull down. If a node has an attached image, a "camera" icon will be seen on the node. When the node is selected, the camera icon can be clicked to open a dialog showing the image.
7. Select Auto Size Node to make the node be the required size to display the node's name.
8. If any Manually set flags have been defined for this tree, they can be set here.

### Save Changes:

1. Now one of the buttons at the bottom of the screen can be selected to complete the changes.
  - *Save & Exit* will add the node to the tree and the *Add Node* dialog will be dismissed.
  - *Save & Next* will add the node to the tree then bring up the next node on the tree so it can be edited.
  - *Apply & New* will add the node to the tree, but the *Add Node* dialog will remain on your screen. At this point, another node can be added (under the same parent).
  - *Cancel* will dismiss the dialog without adding the node to the tree.
  - *Cancel & Next* will not add the node, but will bring up the next node on the tree so it can be edited.
2. If *Auto Calculate* mode has not been turned off, the tree values will now automatically be re-calculated.

## Edit Node

To **Edit** a node on a tree:

1. Select the node you want to edit by clicking the node. This will cause the node to be highlighted in yellow.
2. Select **Edit** by choosing **Edit > Nodes > Edit Node**, clicking on the **Edit** button on the left side-panel ([Node Information Panel](#)), by clicking the **Edit** icon on the [toolbar](#), clicking **Ctrl-e**, or by using the right mouse button to click the parent node, then select **Edit Node** on the pop-up menu.
3. If the *Parent Node Change* dialog box appears, this means that the node you are inserting on is a *LEAF* node and it must be changed to an *AND* or *OR* node. You must select the node type for the parent node, either *AND* or *OR*.
4. The *Edit Node* dialog window will be displayed. Data values for this node can now be changed. The *Title* is the name for the node that will appear inside the shape. *Type* is the type of node. The choices are: *LEAF*, *AND*, or *OR*.
5. The Internal ID is a unique identifier that is assigned for each node. It cannot be changed. This identifier is used when logging changes to nodes and can be used for synchronization with an external database. The External ID is set by the user. This value can also be used for database synchronization. Please see [Main Menus > Tools > Preferences > Tree Properties](#) for further information.
6. If this tree contains a Behavioral Probability indicator, you must select the Subtype. If this is a *LEAF* node either Capability, Probability, or Countermeasure. If *AND/OR* node, only countermeasure or incident.
7. More on countermeasure nodes: A countermeasure node can only be added under an *AND* node. If the countermeasure node is an *AND/OR* node, only "fault tree" nodes can be added under this node, i.e., *LEAF* nodes can only be Probability nodes. *AND/OR* countermeasure nodes also need a Countermeasure Type to be selected; Consolidate or Expand countermeasure scenarios. Typically, countermeasure nodes do not have impact values defined.
8. Checking the Deactivate Node/Subtree box will leave the node on the tree, but it will not be used when calculating Attack Scenarios. Nodes can also be deactivated/activated by right-clicking the node and selecting *Nodes > Deactivate Node/Subtree*.
9. Checking Enable Bubble will allow a Bubble to be displayed for this node showing the notes that were defined in *Tools > Preferences > Node Info*. Checking Display Bubble will turn the bubble display on.
10. The **Notes** area is available for notes specific to the node. See [Notes](#) for more information.

**Indicators tab:**

1. If this is a *LEAF* node, values must be entered for all indicators. All calculations on the tree are done using the values entered for *LEAF* nodes. Depending on the type of the indicator, the value must be entered as a numeric, or if it is a Boolean type of indicator, the value TRUE or FALSE must be selected. If this is an *AND* or *OR* node, indicator values are disabled since values for *AND* and *OR* nodes are calculated using the values provided from their leaf nodes.
2. Behavioral and Impact Indicators are split into different areas on the screen.
  1. If this is a LEAF node with subtype Capability, only values for behavioral capability indicators and impact indicators can be entered.
  2. If this is a LEAF node with subtype Probability, only values for the behavioral probability indicator and impact indicators can be entered.
  3. If this is a LEAF node with subtype Countermeasure, only values for the Probability of Fault (or Countermeasure Effectiveness) and Impact indicators can be entered. The value for the Probability indicator is  $1 - \text{Countermeasure Effectiveness}$  and conversely, Countermeasure Effectiveness is  $1 - \text{Probability}$ . Either value can be entered and the other is calculated.
  4. If this is an *AND* or *OR* node and the tree has impact indicators, more fields are displayed on the screen. The "Children's Impact" field is the value calculated for this node using the child values. This field cannot be edited. If the value for the impact indicator is to be overridden, the Impact Operator and Node's Impact fields must be filled in. The Impact Operator must be selected from the pull-down list. The Node's Impact field must be filled in with a value. The Impact Value field cannot be edited. It is the result of impact operation, i.e.  $\langle \text{Children's Impact} \rangle \text{ apply } \langle \text{Impact Operator} \rangle \text{ to } \langle \text{Node's Impact} \rangle = \langle \text{Impact Value} \rangle$ .
  5. If this is an *AND* node, the *AND* formula can be selected by clicking on the button to open the Formula Selection dialog. In most cases, the Primary *AND* Formula that was defined for the indicator should be used (which is the default). If a Secondary *AND* Formula was defined for the indicator, that selection will be enabled. If Custom *AND* Formula is selected, the formula must be chosen from the list.

**Options tab:**

1. The Attack Effectiveness can be optionally set here. See [Using SecurITree > Attack Effectiveness](#) for more information.

2. The Attack Type and Attack Time parameters can be optionally set here. See [Using SecurITree > Attack Type and Time Parameters](#) for more information.
3. If this is a LEAF node with subtype Capability, the Node Attack Type can be selected. "Use tree default" will use the value that has been set in Tree Properties. See [Tools > Preferences > Tree Properties](#) for further information on node attack type.
4. For AND nodes only, Input Threshold: Enter the number of children required to satisfy AND condition. See Main Menus > View > [Show m of n Combinations](#) for more information.
5. The color of the node and font settings can be changed by clicking the "Change Node Color/Font" button, and then selecting the desired color and font settings on the **Change Node Color/Font** dialog. The node color can be set back to the default color by clicking on the "Reset Node Color/Font" button. All nodes on the tree can be set back to the default color by selecting Tools > Preferences, *Node Info* tab, then clicking on "Reset all node colors to default".
6. An image can be attached to the node by clicking the "Attach Image" button. A name for the image must be entered as well as the file name for the image. When the tree is saved, the image file will be saved with the tree in the \*.rit file. The same image can be attached to multiple nodes by selecting the image name from the pull down. If a node has an attached image, a "camera" icon will be seen on the node. When the node is selected, the camera icon can be clicked to open a dialog showing the image.
7. Select Auto Size Node to make the node be the required size to display the node's name.
8. If any Manually set flags have been defined for this tree, they can be set here.

### Save Changes:

1. Now one of the buttons at the bottom of the screen can be selected to complete the changes.
  - *Save & Exit* will change the values for this node and the *Edit Node* dialog will be dismissed.
  - *Save & Next* will change the values for this node and bring up the next node on the tree so it can be edited.
  - *Apply* will change the values for this node, but the *Edit Node* dialog will remain on your screen. At this point, more changes can be made to this same node.
  - *Cancel* will dismiss the dialog without changing the node.
  - *Cancel & Next* will not change the node, but will bring up the next node on the tree so it can be edited.
2. If *Auto Calculate* mode has not been turned off, the tree values will now automatically be re-calculated.



## Delete Node

To **Delete** nodes from a tree:

1. Select the node or subtree you want to delete by clicking the node. This will cause the node to be highlighted in yellow.
2. Select **Delete** by choosing **Edit > Nodes > Delete Node**, clicking on the **Delete** button on the left side-panel ( [Node Information Panel](#)), by clicking on the **Delete** icon on the [toolbar](#), or by using the right mouse button to click the node and then select **Delete Node**.
3. The selected node or subtree will be removed from the tree after confirmation.

## Print Node

To **Print** a node on a tree:

1. Select the node you want to print by clicking the node. This will cause the node to be highlighted in yellow.
2. Select **Print**< by choosing **Edit > Nodes > Print Node**, or by using the right mouse button to click the node and then select **Print Node**.
3. A **Print Preview** window will show the node information report.
4. Click on **Print...** to send your report to the printer.

## Insert New Root Node

To **Insert a new root node** for the tree:

1. Select **Edit > Nodes > Insert New Root Node**.
2. The Edit Node window will be displayed. Enter the name for the new root node then select OK.  
See [Edit Node](#) for more information.

## Adopt to Alternative Set

To Adopt a node to an existing alternative set on the tree:

1. Select the node to be adopted. This will cause the node to be highlighted in yellow.
2. Select **Adopt to Alternative Set** by choosing **Edit > Nodes > Adopt to Alternative Set**, or by using the right mouse button to click the node, then select **Adopt to Alternative Set** on the pop-up menu.
3. The *Select Alternative Sets* dialog window will be displayed. All alternative sets defined for this tree which this node does not currently belong to will be displayed. Select the alternative sets this node should belong to.
4. Now one of the buttons at the bottom of the screen can be selected to complete the changes. *OK* will add the node to the selected alternative sets for the tree. *Cancel* will dismiss the dialog without adopting the node to the alternative sets.
5. If *Auto Calculate* mode has not been turned off, the tree values will now automatically be re-calculated.

See [Alternative Sets](#) for further information.

## Deactivate Node/Subtree

To deactivate a node or subtree:

1. Select the node to be deactivated. This will cause the node to be highlighted in yellow.
2. Select **Deactivate Node/Subtree** by choosing **Edit > Nodes > Deactivate Node/Subtree**, or by using the right mouse button to select the node, then click **Deactivate Node/Subtree** on the pop-up menu.
3. When the node/subtree is deactivated, it will remain on the tree but is not included when doing analysis operations.

## Using Indicators

These actions can be performed on Threat Tree indicators:

[Add Indicator](#)

[Edit Indicator](#)

[Delete Indicator](#)

[Rename Indicator](#)

**SecurITree** attack tree models incorporate a feature known as "indicators." Indicators are a property of the attack tree that help the analyst understand how the tree relates to the real world. There is no fixed limit to the number of indicators that can be defined for a tree, but typically three or four indicators are used.

There are two basic types of indicators. Behavioral indicators describe the resources that need to be expended by the attacker in order to reach a particular state or node in the tree. Behavioral indicators include things such as: cost (to the attacker), technical skill, and willingness on the part of the attacker to accept the consequences of their actions. Impact indicators are used to describe the damage or impact on the victim of the attack that is caused by an attacker reaching a given state or node. Setting up impact indicators requires a good understanding of the effect an attack will have on the business in question.

Associated with each indicator is a pair of functions that help determine indicator values for each node in the tree. One member of the indicator function pair is used to calculate the indicator values for *AND* nodes and the other is used for *OR* nodes. It is usually desirable to choose functions that will result in the lowest cost value for a particular node. That is, the calculated value that corresponds to the least costly path from the leaf nodes to intermediate locations in the tree for a particular indicator.

In the case of behavioral indicators the analyst must enter explicit values at the leaf nodes. All node values above the leaves are calculated by the formulas. Behavioral indicators are the core of capability-based analysis. The behavioral indicator node values are compared to the resources available to the various threat agents during pruning operations. States (nodes) in the tree that cannot be attained by a particular threat agent are pruned away.

When using impact indicators, the indicator formulas can be used to compute impact values for intermediate nodes (in the same fashion as with behavioral indicators). Unlike behavioral indicators, it is also possible to override or influence the calculated values for any node in the tree. This allows the analyst to introduce business specific external information into the model (based on interviews with the organization's business people). Impact indicators cannot be used for tree pruning. They are, however, essential in analyzing risk.

Note that indicator values (both behavioral and impact) are calculated independently for each indicator. This means that a set of values at a particular node in a tree may (and probably do) represent distinct traversal paths. The notable exception is when *Attack Scenarios* have been generated. Since each *Attack Scenario* corresponds to a specific path through the tree, the indicator values at a given node then represent the cost for that specific path.

The combination of behavioral and impact indicators come together to provide a complete, risk analysis solution. Capabilities-based pruning on behavioral indicators yields the collection of probable attacks available to a threat agent. Generating a set of *Attack Scenarios* from the capabilities-pruned tree shows which specific paths (attacks) are available to the threat agent. Sorting these *Attack Scenarios* based on impact indicators, yields a risk prioritized list of attacks for a given threat.

### Derived Indicators

Prior to v3.5, there were there were two basic indicator types: *Behavioral* and *Impact*. SecurITree used pre-defined formulas in conjunction with these indicators to determine the *probability* of each attack scenario (based on either the statistical probability or the feasibility and desirability). When *probability* was combined with the *victim impact*, this yielded an estimation of risk. This functionality is sufficient for most, but not all, types of analysis.

In certain cases, analysts wish to derive values based on user defined mathematical expressions that may incorporate other *behavioral* or *impact* indicator values. For example, if a tree had *behavioral* indicators *Cost of Attack* and *Noticeability*, it is possible that an analyst might want to study nodes and scenarios with high (or low) cost and noticeability values. So, they might define a *derived* indicator called *Cost-Noticeability* and use  $Cost\ of\ Attack * Noticeability$  as a *derived* value expression. One can conceive of many scoring systems that could benefit from this type of *derived* value calculation.

Conditional expressions can be defined for the derived indicator. The format is: IF <expression 1> THEN <expression 2> ELSE <expression 3>. Expression 1 must be a boolean expression where the result is either True or False. For example;  $Cost\ of\ Attack \geq 200$ . If the result of Expression 1 is True, the expression defined in Then is used. If the result is False, the Else expression is used.

The *derived* values are calculated on a per node basis. Leaf node derived values are always computed using a user defined expression. AND nodes can aggregate derived values using the standard aggregation formulas available for other indicator types (e.g., Sum of Vertices, Max of Vertices). OR nodes assume their *derived* value based on the value of the child that is selected in a particular scenario. Both AND and OR nodes can override the aggregated values using operators such as *Replace*, *Max Fn*, + (similar to the operators used for *impact* indicators. This allows great flexibility in calculating derived values for individual nodes or for entire scenarios.

The *derived* value feature is intended for experienced customers with complex requirements. Instructions for using these indicators can be found at [Add Indicator](#) and [Edit Indicator](#). Customers wishing to use this feature may wish to consult with Amenaza's Technical Support organization for further advice and information.



## Add Indicator

To Add an Indicator to a tree:

1. Select **Add Indicator** by; choosing **Edit > Set Indicators** from the application menu, or by clicking the **Set Indicators** button in the right side-panel ( [Tree Information Panel](#)), or by using the right mouse button to click the "white space" in the tree display area and then clicking on **Set Indicators** in the pop-up menu. Then click on the **Add** button.
2. The *Add Indicators* dialog window will be displayed. Data must now be entered into the fields in the dialog.
  1. *Indicator Name* is the name for the indicator. You can enter your own name for the indicator or use one of the pre-defined indicators: Breach of Trust, Cost of Attack, Damage Cost, Defender Error, Doable by Outsider, Escapability, Noticeability, Probability of Apprehension, Probability of Occurrence, Technical Ability, or Time to Exploit.
  2. The *Indicator Type* must be selected from the pull-down list - either *Behavioral*, *Impact*, or *Derived*.
  3. The *Indicator Subtype* must be selected from the pull-down list. If a Behavioral indicator type was selected, the choices are *Capability* (default) or *Probability*. If an Impact indicator type was selected, the choices are either *Victim Impact* (default), *Attacker Benefit*, *Dual -Victim Impact & Attacker Benefit*, or *Attacker Detriment*. Derived Indicators do not use a subtype. Note: Only one Behavioral Probability indicator can be defined per tree. The *Dual - Victim Impact & Attacker Benefit* subtype will actually create two indicators, one of each type with "-VI" and "-AB" appended to the indicator name. When editing nodes, only one value is entered and it is saved for both indicators.
  4. The *Argument Type* must be selected from the pull-down list - either *Numeric* or *Boolean*. This choice will determine the indicator values that can be entered and the *AND* Formula that can be used.
  5. If a pre-defined indicator is chosen, the *AND* formula is pre-selected to the typical formula used for the indicator function. This formula may be changed if desired. If you have defined your own name for the indicator, the *AND* formula must be selected. The *AND* Formula is applied to all child nodes of *AND* nodes. This value is selected by choosing a formula from the pull-down list. The *OR* Formula is applied to all child nodes of *OR* nodes. This value is set by default as the *OR* nodes are pass-up values in attack scenarios.
  6. A Secondary *AND* formula may be specified by checking the "Use Secondary *AND* formula" box, then selecting a formula. If this feature is used, you can set an *AND* node to use either the *AND* formula (the default) or the secondary *AND* formula to calculate the node's value.

7. A *Units* field can optionally be entered. This field is only used for display purposes. The exception is for the Behavioral Probability indicator. The units field is used in Advanced Analysis when calculating values.
8. Either a *Value Range* or *Named Values* can be specified for the indicator.
  - *Value Range* - This field is preset if a pre-defined indicator is used. If the check box for *no lower bound* or *no upper bound* is selected, any numeric value can be entered in *LEAF* nodes for this indicator. If the check box is not selected, a range value can be entered so edit checking will be performed when values are entered for *LEAF* nodes. If the *Argument Type* and *AND* formula are of type *Boolean*, the range values are set to 0-1.
  - *Named Values* - If this is selected, specified name/value pairs can be defined for the indicator. Only these values can be selected when entering *LEAF* node values. Click the **Edit** button to define the name/value pairs.
9. Notes can be entered to describe this indicator in the *Notes* area.
10. You can choose to apply a default value to all leaf nodes that currently exist for this tree. This may be desirable to ensure the tree will continue to calculate after this indicator is added. The values for each *LEAF* node can be changed as desired at a later time. If the *Argument Type* and *AND* formula are of type *Boolean*, the value True or False can be chosen for the default value. If *Named Values* were defined, a named value can be selected. Otherwise, a numeric value must be entered.
11. You can also choose to set a default value that will be used when a new *LEAF* node is created. This is specified in a similar way as described above.
12. If the Type of *Derived* is selected, some of the above fields are not available. Instead, "Computed Value Expressions" can be entered for the different node types. Clicking on the **Edit** button beside the node type will open a window where the expression can be entered. A valid "Computed Value Expression" can be any mathematical expression including indicators (Note: indicator names must be delimited with " " [double-quotes].) A test value can be entered for any indicators that are used in the expression in order to check that it is valid. Click on **Compute** to check the expression. If there is an error, the expression field will turn light red and an error message will be displayed.

Global values can be defined and can be used in all derived formula expressions. The entered expression is the default that will be used for all nodes of that type on the tree. A different expression can be used for a specific node by editing the node. See [Using Indicators](#) for a further description on the use of Derived Indicators.
3. Now one of the buttons at the bottom of the screen can be selected to complete the changes. *OK* will add the indicator to the tree and the *Add Indicators* dialog will be dismissed. *Cancel* will dismiss the dialog without adding the indicator to the tree.

4. You will be returned to the **Set Indicators** window. At this point, other indicators can be modified. If modifications have been made to indicators and the *Cancel* button is selected, all modifications will be reverted.
5. If *Auto Calculate* mode has not been turned off, the tree values will be automatically re-calculated if a default value was set for this indicator function.

## Edit Indicator

To Edit an Indicator for a tree:

1. Select **Edit Indicator** by; choosing **Edit > Set Indicators** from the application menu, or by clicking the **Set Indicators** button in the right side-panel ( [Tree Information Panel](#)), or by using the right mouse button to click the "white space" in the tree display area and then clicking on **Set Indicators** in the pop-up menu. Select the indicator to be edited in the "Defined Indicators" area, then click on the **Edit** button.
2. The *Edit Indicators* dialog window will be displayed. Data values for indicator functions can now be changed.
  1. You must select the *Indicator Name* that you want to change.
  2. The *Indicator Type* must be selected from the pull-down list - either *Behavioral* or *Impact*.
  3. The *Indicator Subtype* can be selected from the pull-down list. If a Behavioral indicator type was selected, the choices are *Capability* (default) or *Probability*. If an Impact indicator type was selected, the choices are either *Victim Impact* (default), *Attacker Benefit* or *Attacker Detriment*. Note: Only one Behavioral Probability indicator can be defined per tree. The *Dual - Victim Impact & Attacker Benefit* subtype will actually create two indicators, one of each type with "-VI" and "-AB" appended to the indicator name. When editing nodes, only one value is entered and it is saved for both indicators.
  4. The *Argument Type* can be selected from the pull-down list - either *Numeric* or *Boolean*. This choice will determine the indicator values that can be entered and the *AND* Formula that can be used.
  5. The *AND* formula is set to the current formula defined for the indicator function. This formula may be changed if desired. The *AND* Formula is applied to all child nodes of *AND* nodes. This value is selected by choosing a formula from the pull-down list. The *OR* Formula is applied to all child nodes of *OR* nodes. This value is set by default as the *OR* nodes are pass-up values in attack scenarios.
  6. A Secondary *AND* formula may be specified by checking the "Use Secondary *AND* formula" box, then selecting a formula. If this feature is used, you can set an *AND* node to use either the *AND* formula (the default) or the secondary *AND* formula to calculate the node's value.
  7. A *Units* field can optionally be entered. This field is only used for display purposes. The exception is for the Behavioral Probability indicator. The units field is used in Advanced Analysis when calculating values.
  8. Either a *Value Range* or *Named Values* can be specified for the indicator.

- *Value Range* - If the check box for *no lower bound* or *no upper bound* is selected, any numeric value can be entered in *LEAF* nodes for this indicator. If the check box is not selected, a range value can be entered so edit checking will be performed when values are entered for *LEAF* nodes. If the *Argument Type* and *AND* formula are of type *Boolean*, the range values are set to 0-1. Current values will not be edit checked if the *Value Range* is changed. Each node must be edited to determine if the value falls between the new allowable range.
- *Named Values* - If this is selected, specified name/value pairs can be defined for the indicator. Only these values can be selected when entering *LEAF* node values. Click the **Edit** button to define the name/value pairs. If a named value is edited and the value is changed, you will have the option to have all nodes with the old value set to the new value. If you choose to change the node values, you must apply the indicator change. Otherwise the values for the nodes on the tree will not match the named values.

9. Notes can be entered to describe this indicator in the *Notes* area.

10. You can choose to apply a default value to all *LEAF* nodes that currently exist for this tree. This is probably not desirable since *LEAF* nodes should already contain values. The only time this might be done would be if the formula was changed from one requiring numeric data to Boolean data (or vice versa). If the *Argument Type* and *AND* formula are of type *Boolean*, the value True or False can be chosen for the default value. If *Named Values* were defined, a named value can be selected. Otherwise, a numeric value must be entered.

11. You can also choose to set a default value that will be used when a new *LEAF* node is created. This is specified in a similar way as described above.

12. If the Type of *Derived* is selected, some of the above fields are not available. Instead, "Computed Value Expressions" can be entered for the different node types. Clicking on the **Edit** button beside the node type will open a window where the expression can be entered. A valid "Computed Value Expression" can be any mathematical expression including indicators (Note: indicator names must be delimited with " " [double-quotes].) A test value can be entered for any indicators that are used in the expression in order to check that it is valid. Click on **Compute** to check the expression. If there is an error, the expression field will turn light red and an error message will be displayed.

Global values can be defined and can be used in all derived formula expressions.

The entered expression is the default that will be used for all nodes of that type on the tree.

A different expression can be used for a specific node by editing the node. See [Using Indicators](#) for a further description on the use of Derived Indicators.

3. Now one of the buttons at the bottom of the screen can be selected to complete the changes. *OK* will change the indicator for the tree and the *Edit Indicators* dialog will be dismissed. *Cancel* will dismiss the dialog without changing the indicator for the tree.

4. You will be returned to the **Set Indicators** window. At this point, other indicators can be modified. If modifications have been made to indicators and the *Cancel* button is selected, all modifications will be reverted.
5. If *Auto Calculate* mode has not been turned off, the tree values will be automatically re-calculated if a default value was set for this indicator function.

## Delete Indicator

To Delete an Indicator from a tree:

1. Select **Delete Indicator** by; choosing **Edit > Set Indicators** from the application menu, or by clicking the **Set Indicators** button in the right side-panel ([Tree Information Panel](#)), or by using the right mouse button to click the "white space" in the tree display area and then clicking on **Set Indicators** in the pop-up menu. Select the indicator to be deleted in the "Defined Indicators" area, then click on the **Delete** button.
2. After confirming the delete operation, you will be returned to the **Set Indicators** window. At this point, other indicators can be modified. If modifications have been made to indicators and the *Cancel* button is selected, all modifications will be reverted.

## Rename Indicator

To Rename an Indicator for a tree:

1. Select **Rename Indicator** by; choosing **Edit > Set Indicators** from the application menu, or by clicking the **Set Indicators** button in the right side-panel ( [Tree Information Panel](#)), or by using the right mouse button to click the "white space" in the tree display area and then clicking on **Set Indicators** in the pop-up menu. Select the indicator to be renamed in the "Defined Indicators" area, then click on the **Rename** button.
2. Type in the new name for the indicator. Click *OK* to complete change or *Cancel* to abort the change.
3. You will be returned to the **Set Indicators** window. At this point, other indicators can be modified. If modifications have been made to indicators and the *Cancel* button is selected, all modifications will be reverted.



## Attack Scenarios

An Attack (Threat) Tree represents a set of possible attacks that will achieve the overall goal represented by the tree's root node. An [Attack Scenario](#) represents a particular member of the set.

That is, an *Attack Scenario* consists of the particular activities (represented by leaf nodes) that an attacker would perform to achieve the root goal. These leaf level attacks would, of course, activate intermediate nodes along the path to the root goal. Strictly speaking, the intermediate nodes are not part of the *Attack Scenario* but are shown in the graphical representation so as to make it clear how the attack will take place.

An *Attack Scenario* can be used as the basis for an early warning system that will detect when a particular attack is underway.

## Pruning Attack (Threat) Trees

To prune trees you must first [initiate](#) the tree pruning process and have a pruning window open. An Attack (Threat) Tree can be evaluated using several methods:

[Manual Mode](#)

[Load Agent Profile Mode](#)

See [Agent Profiles and Pruning Criteria](#) for more information on the differences between these two concepts.

For a more detailed explanation of the differences between the pruning modes and the methods of calculation, see the [Explanation of Pruning Methods](#) section.

## Manual Mode

Select each indicator you are interested in and specify the value for the nodes that should remain on the tree. All nodes with values outside of the range that is specified are pruned from the tree. See [Edit Agent Profile](#) for further explanation.

## Load Agent Profile Mode

- You can load an [Agent Profile](#) that was previously created. This is done by selecting **File > Load Agent Profile**, or by clicking the **Load Agent Profile** icon on the [toolbar](#).
- A warning message is given if there are existing *Pruning Criteria* since they will be overwritten.
- If a file already exists with the same name as the name of this *Pruning Window*, it is pre-selected in the **File > Load Save Profile** dialog. You can also save *Agent Profiles* by clicking the **Save Agent Profile** icon on the [toolbar](#). *Agent Profile* files end with the extension .agt.
- After the file is selected, the *Pruning Criteria* is applied to the base tree.
- A message will be displayed above the tree display area which informs you of the number of nodes removed during the application of this *Pruning Criteria*.
- The *Agent Profile Pruning Criteria* area now contains the evaluators that were loaded from the file. The *Pruning Criteria* for the *Agent Profile* can be edited by selecting **Edit > Edit Agent Profile**, or by clicking the **Edit Agent Profile** icon on the [toolbar](#).

## Agent Profiles and Pruning Criteria

### **The Difference Between An Agent Profile And Pruning Criteria**

A Threat Agent is a group of people or a random situation likely to cause harm to a system. e.g., hackers, industrial spies, disgruntled employees, Mother Nature. Threat Agents are constrained by their capabilities or the resources available to them. If these limitations are known, it is possible to prune an Attack (Threat) Tree to show only the attacks achievable by a particular threat agent. This is done by applying *Pruning Criteria*.

*Pruning Criteria* are a set of qualifying conditions that act as a filter to remove nodes from the Attack Tree that fail to meet the specified conditions. For example, one member of such a set might be "attacks costing < \$1000".

Knowing the characteristics of various threat agents, it is possible to associate a set of pruning criteria with each agent. Thus, each threat agent has a characteristic set of pruning criteria known as a "profile". While it would be possible to manually re-enter the pruning criteria for each threat agent in every **SecurITree** session, this would quickly become tedious and error prone. To make it easier, **SecurITree** allows the *Agent Profile* for threat agents to be defined, saved and reloaded as needed.

## Explanation of Pruning Methods

There are two basic approaches to tree pruning. Node value-based and scenario-based.

### **NODE VALUE-BASED PRUNING**

Node value-based pruning examines the set of behavioral indicator values associated with each node.

If the set of resources at a node do not match the conditions specified in the Threat Agent Profile then the node is removed or "pruned".

Node value-based tree pruning is very fast and gives good, but not perfectly accurate results. The problem is that each member of the set of values associated with each node is derived in isolation. A given indicator value is computed using the indicator formulas applied to a particular (usually minimal) path through the tree. The path taken to determine the value of one indicator may be (and usually is) different from the paths used to compute the node values for other indicators.

Node value-based pruning should only be used for rough calculations or when Scenario-based pruning computations would be time prohibitive. As improvements to processing power occur node value-based pruning will likely be deprecated.

### **SCENARIO-BASED PRUNING**

A second, more accurate approach to pruning is based upon attack scenarios. Provided that your estimates of the resources required to exploit system vulnerabilities are accurate, and your assumptions about the capabilities of your adversary are valid, attack scenario-based pruning will show exactly which attacks are within the adversary's reach.

When performing attack scenario-based pruning, **SecurITree** will first perform a pre-pass of node-based pruning. Then with the nodes remaining on the tree, all viable paths through the tree are calculated to get the list of scenarios. The behavioral indicator formulas are used to compute the resource cost for each attack (i.e. path or minimal set of paths that lead to the root goal). It then compares the resource requirements of each attack to the capabilities of the adversary and deletes all attacks that are impossible. **SecurITree** then combines (takes the union of) the nodes from all of the remaining attack scenarios. The resulting tree contains only those nodes which will be traversed in one or more of the attack scenarios within the adversary's grasp.

Attack scenario-based pruning is highly accurate, but slow to compute. It may take several minutes to generate a pruning window for a moderately large tree. Memory requirements can also be significant. Amenaza recommends that all final reports be based on attack scenario-based pruning. Node value pruning is more appropriate for "what-if" brainstorming sessions.

## Advanced Analysis

### [Overview](#)

### [Attacker and Victim Utility Functions](#)

Curve Definitions

How to Define Curves

How to Define Boolean Values

### [Main Analysis Window](#)

Indicator and Utility Function Columns

Feasibility

Desirability

Propensity

Pain Factor

Risk Metric

### [Machine Learning](#)

### [Similarities](#)



## Overview

This document is meant to be a quick, how-to guide to advanced analysis. For more detailed information please read Amenaza's white paper "*Attack Tree-based Risk Analysis*" which can be found in the Documents folder where you installed Amenaza **SecurITree**. The file name is "AttackTree AllRisks-January2010.pdf".

Every day, people are faced with far more choices than they are able to pursue. One model for explaining people's choices suggests that one activity is chosen over another because it has a superior cost-benefit ratio. Costs dissuade people from making a choice whereas benefits increase their motivation.

The decisions adversaries make follow the same rules. For this to be more than a useful theory, we need to understand and quantify the costs and benefits that adversaries encounter. Doing so will allow us predict attackers' behavior.

Differing values and circumstances cause different people to perceive the same absolute quantity of a resource differently. **SecurITree's** Advanced Analysis takes this into account by considering the particular characteristics of each adversary. Easy attacks are those that require an adversary to expend only a small fraction of their resources, or combinations of resources that they do not consider valuable. Desirable attacks are those that yield benefits the attacker perceives as valuable. Attacks that are both easy and desirable are highly probable.

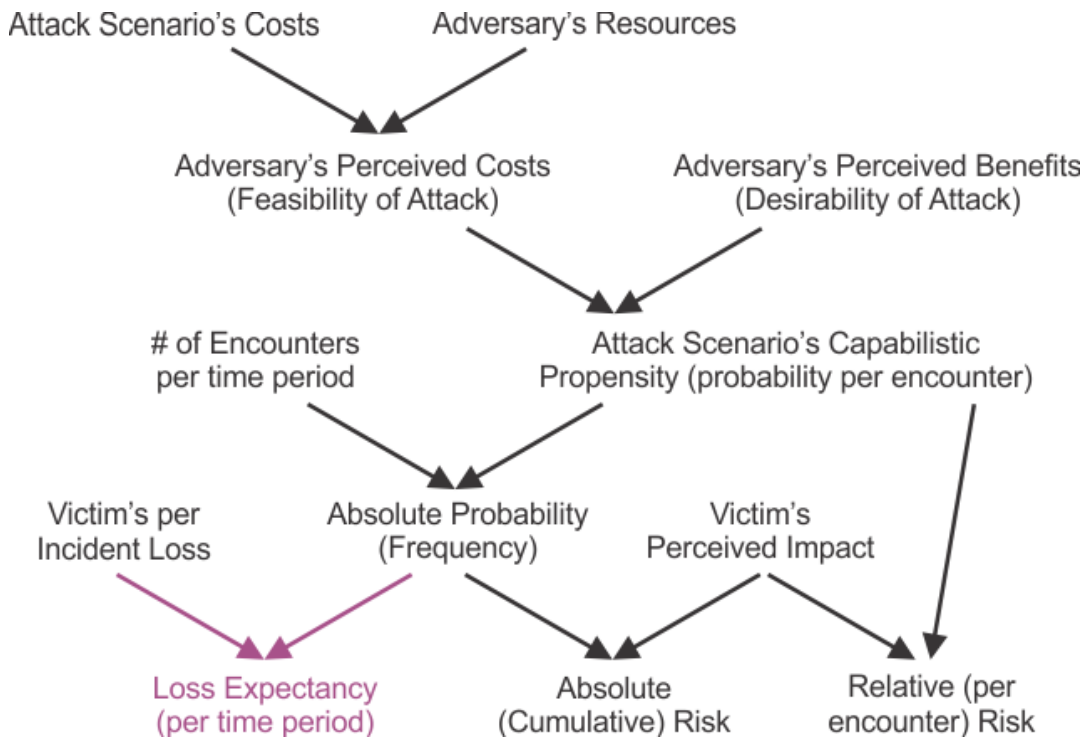
Given that

$$\text{Attack Risk} = \text{Attack Probability} \times \text{Attack Impact}$$

predicting the probability of an attacker's actions is an important step in understanding risk. **SecurITree's** *Advanced Analysis* allows the analyst to define utility functions that describe the value the adversary places on the resources they will spend in performing the attack and the rewards they will obtain as a result. This truly makes it possible to "think like an attacker". The utility functions are used to calculate a *propensity value* for each attack scenario. The *propensity* value represents the likelihood that, given an encounter between the specified threat agent and the system, they will chose to execute the attack scenario. It is analogous to the *relative frequency* or *relative probability* term used in statistics. The absolute likelihood (or frequency) of attacks depends on both the propensity and the number of encounters between adversaries and the system. Additional information about the number of adversaries must be added to the model in order to determine the absolute probability.

Calculating the risk associated with an attack scenario also requires that we understand the attack's impact. Analysts create additional curves representing the perceived injury experienced by the victim based on the losses they will experience. Attack scenario probability and impact are combined to provide a metric of risk.

This process can be summarized in the following flowchart:



## Attacker and Victim Utility Functions

Utility functions are graphical descriptions of the value that attackers and victims place on the costs and benefits associated with attacks. There are three general types of utility functions:

1) **Attacker Resource Affinity Utility Functions** - These functions describe the capability and willingness of an adversary to deliver the resources required for a given attack. Money, time, willingness to be noticed and technical ability are all examples of adversarial capabilities. The output of the utility function for a specific resource is 1 if none of the resource is required to perform an attack. The utility function drops as the amount of the utility increases, eventually reaching 0 when the capability of the adversary is exceeded. The shape of the curve describing the decrease reflects the value that the adversary places on the resource. Adversaries that are highly risk averse will have steeply decreasing, concave curves. Risk tolerant adversaries will usually have convex curves.

2) **Attacker Benefit Utility Functions** - Functions that show the interest an adversary has in accumulating a particular benefit. The interest is 0 if none of the benefit is obtained through an attack. The attacker's interest and perceived benefit rises as more of the resource is gained. In many cases the attacker's appetite for the commodity is satiated at some point and the interest levels off at 1.

The types of benefits that can be mapped include money, fame, enjoyment of the victim's discomfiture, etc.

3) **Victim Impact Utility Functions** - A curve that indicates the amount of discomfort experienced by the victim as losses increase or unpleasant effects occur. When the loss is 0 the impact is also 0.

Impact rises to 1 as the amount of loss increases. The shape of the curve, and the amount of loss required to drive the impact to 1, reflect the sensitivity of the victim to this type of loss.

Note that an adversary can be dissuaded from performing an attack if even one of the necessary resources is very valuable to them. To represent this, the overall adversarial cost is calculated by taking the product of the Attacker Resource Affinity Utility functions.

The overall benefits obtained by an adversary and the overall losses experienced by a victim are determined by taking a weighted sum of the attacker benefit utility functions and the victim impact utility functions.

## Curve Definitions

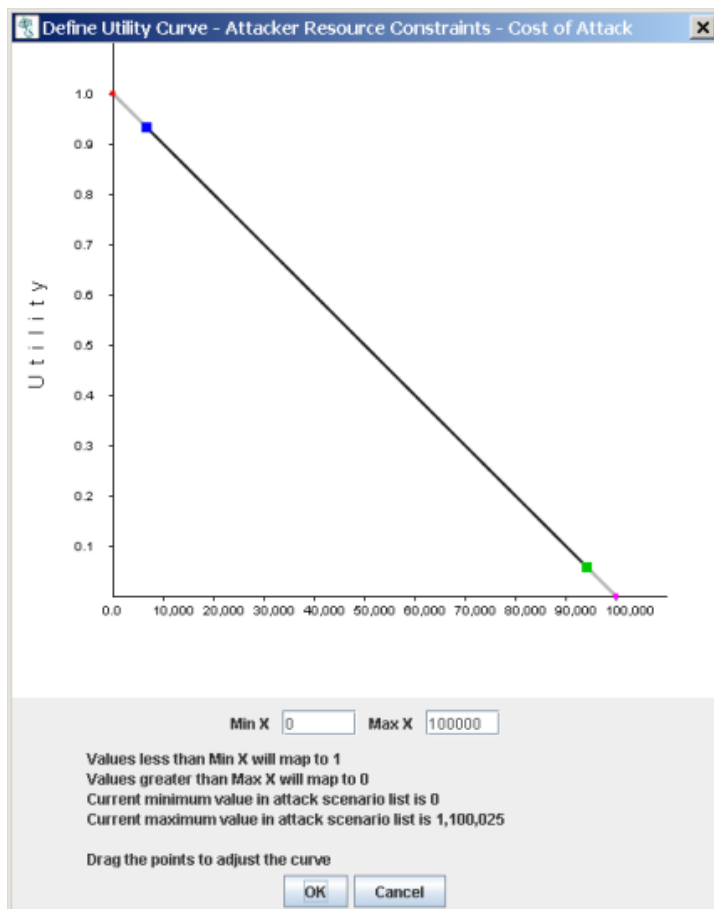
To perform Advanced Analysis, you first must define an attacker resource affinity utility curve for each behavioral indicator function. This curve shows how attached the adversary is to the resource and their limit of the resource.

## How to Define Curves

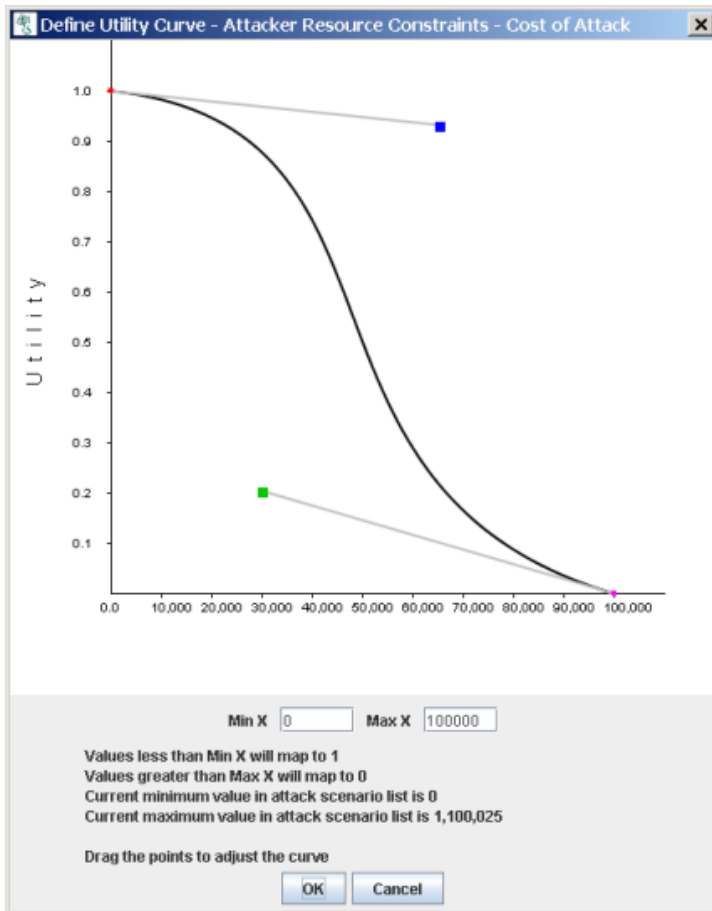
Before you can perform advanced analysis on a tree, you need to define at least one indicator for the tree, just as you would for traditional pruning. You can then click on Advanced Analysis in the Analyze menu. Give the analysis window a name, and continue on to the next screen.

At this point, you can define the curves for a particular threat agent / victim combination. The threat agent indicators are listed at the top of the window, with the victim profile below. Along the right side of the window are a column of buttons, labeled as "Define Curve" and "Define Mapping". These are the buttons you press to enter the adversary's capabilities and motivations.

To define a curve for a particular resource, benefit, or impact, click on the appropriate button. A screen like the following will display showing the default curve (a straight line at a 45 degree angle).



By then dragging the blue and green dots, you can modify the curve as you see fit, to match the profile of the attacker:



You can perform the same steps on other indicators to define how your adversary's abilities and resources are bound.

## How to Define Boolean Values

The astute reader will have noticed that, while proving excellent for ranged indicators, this approach does not work for functions with boolean indicators. With booleans, the analyst is essentially turning flags on or off: Is the attacker an insider? Do we allow that the defender could have made some mistake? Depending on the exact meaning of the indicator, the mapping to the utility function will differ.

To allow for this arbitrary mapping, **SecurITree** allows analysts to fine-tune the function. When defining the utility function for a boolean function, you are presented with the following screen:



While initially this screen may seem rather confusing, it is really quite simple. The easiest way to think of it is, "Given an attack for which this boolean indicator value is true (or false), can the attacker accomplish the attack?" For instance, in the house burglary example, we assume that the youth is not a trusted individual (such as a friend of the home owner), therefore, any attacks which require a breach of trust to accomplish cannot be performed. Thus, when Breach of Trust is True,  $f(\text{Breach of Trust})$  (in other words, the utility function) is false.

Suppose we wanted to model another attacker, identical in all other ways to our other troubled friend, except this young man knows and trusts the owner of the house. Obviously, some attacks are now possible which were not possible before (assume that the youth had been given a key to water plants during the homeowner's vacation, and had made a copy of the key); however, the original attacks which were possible by the untrusted attacker are still possible now. To model this, we would change both values of the utility function to True:



You should perform these same steps for all defined indicators, including Attacker Resource Constraints, Attacker Benefits, and Victim Impacts. Once you are finished, click OK at the bottom of the window.

## Main Analysis

After defining the attackers' resources and benefits, and the defender's impact, the main Advanced Analysis screen is displayed. Each row in the main table indicates one distinct [attack scenario](#), along with the different indicators, utility functions, and calculated metrics associated with that scenario. We will now discuss each column in more detail.

## Indicator and Utility Function Columns

The indicator columns (for instance, Cost of Attack, Technical Ability, etc.) show the aggregation of all values for that particular attack scenario. This indicates the raw amount of resources needed to perform a particular attack, and is no different than the values found in traditional pruning.

The associated Utility Function columns (for instance,  $f(\text{Cost of Attack})$ ,  $f(\text{Technical Ability})$ , etc.) show the willingness of the attacker to part with the resources required by the attack scenario (in the case of behavioral indicators), or the desire of the attacker to acquire the resources they expect to gain by performing the attack scenario (in the case of attacker benefit impact indicators). These values range between 0 and 1, with 0 meaning the attacker is not at all willing to spend the required resources, and 1 meaning the attacker is fully willing to spend them.

## Feasibility

*Feasibility* is a metric describing the overall ease with which the attacker can carry out the attack, based on all the attacker's behavioral indicator values and associated utility functions.

The resource utility functions (curves) created by the analyst define a specific threat agent's willingness to part with scarce resources over a range of attack costs. For very low amounts of a resource the resource utility curves yield an output value of 1, showing that an attacker is completely unconstrained by the resource. Like everyone else, they like things that are free. As the amount of resource required to perform the attack increases, so does the adversary's willingness to spend it. At the point that the attack's resource cost exceeds the amount of resource possessed by the adversary their willingness drops to 0.

From an adversary's perspective, an attack is easy if the perceived value of all of the resources required to perform the attack is low. If the value of any of the required resources is high, then the attack can no longer be considered easy.

A convenient mathematical way to model the easiness of a particular attack scenario to a given threat agent is to use the resource affinity functions to map the various raw attack resource costs to the

particular threat agent's willingness to part with each of the resources. This will yield a set of values ranging from 0 (unable or unwilling) to 1 (completely willing) and then multiplying those values together to compute a *feasibility* metric. If even one of the resource utility functions' output values is low then the result of the multiplication will be near 0. Only if the threat agent is completely able and willing to spend all of the required resources will the product yield a value approaching 1.

One minor problem with this strategy is that the *feasibility* values will drop as the number of indicators in the tree increases. Consider a tree with three behavioral resource indicators. Suppose, for a particular attack scenario and threat agent that the adversary is very willing (0.95) to spend each of the three resources. This would yield a *feasibility* value of 0.85. If the model were altered by adding three additional indicators, each of which the adversary was similarly willing to spend, then the *feasibility* value would drop to 0.735. A good way to normalize this tendency is by taking the *n*th root of the product, where *n* is the number of behavioral resource indicators in the tree.

The formula to use for calculating Feasibility can be selected by going to [Tools > Preferences > Tree Properties](#) tab. The choices are:

$\prod_{i=1}^n f_i(I)$  product of resource affinity functions or  $\sqrt[n]{\prod_{i=1}^n f_i(I)}$  *n*th root of the product of resource affinity functions.

## Desirability

*Desirability* represents a metric of all the attacker benefits, weighted together as defined in the indicator curves window. This value is meant to approximate how much the attacker wants to perform this particular attack; like the other values, it is a value between 0 and 1. The value is obtained by summing the weighted values of each attacker benefit utility function:

$$(w1 * f1) + (w2 * f2) + \dots + (wn * fn)$$

## Capabilistic Propensity (or relative probability)

Propensity combines an attack scenario's *Desirability* and *Feasibility* values to provide a metric of the likelihood the attack will occur given an encounter between the threat agent and the target system. It is a measure of "bang for buck" or cost-benefit to the attacker. Propensity is analogous to the relative frequency concept found in statistics. It is the relative probability that an attack will occur as a result of an encounter between the attacker and the system.

## Stochastic Probability



If the tree is using a Probability Indicator and the attack scenario has a probabilistic event (i.e., a node with a subtype of Probability), this column will contain the stochastic probability value.

## # Hostile Encounters

There are three primary factors that determine the number of encounters that a system will undergo with a specific class of threat agents in a period of time:

1. The number of adversaries who have plausible access to the defender's system. For physical attacks this generally means the attackers and the target are within the same geographic region. For electronic attacks it implies some degree of mutual network connectivity (Internet, dial-up lines).
2. The number of targets (within the region) competing for the attention of the defender.
3. The period of time for which the number of encounters will be estimated.

Additional factors that influence the number of encounters include:

- The nature of the attacker and the fraction of the time they dedicate to attacks.
- The characteristics of the exploit:
  - Will performing the exploit permanently deplete the attacker's resources?
  - Does the nature of the exploit constrain the attacker to performing only one attack at a time? These attacks are referred to as single-shot attacks.
  - How long does it take for the attacker to do the attack and then regroup for another attack? We call these attacks single threaded or sequential attacks.
  - Can an attacker attempt to attack multiple targets concurrently? Multi-threaded attacks are very common in electronic (computer) attacks.

For each type of exploit, the number of encounters in a given time period can be estimated by

$$\# \text{ Single shot encounters} = \frac{\# \text{ Adversaries}}{\# \text{ Targets}}$$

$$\# \text{ Single threaded encounters} = \frac{(\# \text{ Adversaries}) (\text{Duty Factor})}{(\text{Attack Time} + \text{Recovery Time}) (\# \text{ Targets})}$$

$$\# \text{ Multi-threaded encounters} = \frac{(\# \text{ Adversaries}) (\text{Thread Factor}) (\text{Duty Factor})}{(\text{Attack Time} + \text{Recovery Time}) (\# \text{ Targets})}$$

These formulae are approximations.

## Scenario Frequency or Rate of Occurrence (RO)

The number of times a particular attack scenario will occur in a given time period is proportional to the scenario's propensity (relative frequency) and the number of encounters that occur in the time period. That is

$$\text{Rate of Occurrence} = \text{propensity} \times \# \text{ encounters (per time period)}$$

If the time period chosen is one year, then the frequency is known as the Annual Rate of Occurrence (ARO). This term is widely used in conventional risk analysis.

## Loss Expectancy per Time period for each Impact Indicator

The Scenario Frequency multiplied by the raw impact indicator values will give the loss expectancy for the time period for each impact indicator.

## Pain Factor

Just as the *Desirability* metric is an indication of the degree of motivation an adversary will have to execute a scenario, the *Pain Factor* represents the discomfort the defender will feel if it occurs. Basically, it evaluates how much a particular attack is going to hurt. Like *desirability*, it is evaluated by computing the weighted sum of all victim impact utility functions.

## Relative Risk

As stated earlier, risk is a combination of both probability and impact. If propensity is used as the probability term, and pain factor is used as the impact term in the risk equation, the result is a measure of the risk associated with an encounter between the defender's system and a particular threat agent. We call this relative risk because it is calculated relative to each encounter between the system and the attacker.

## **Absolute Risk**

The absolute risk associated with a particular attack scenario to a system defender will depend on the scenario's propensity (the relative frequency for each encounter) and pain factor, and the number of encounters that will take place in a given time period. This is a more accurate representation of the risk faced by a defender than is relative risk.

## Machine Learning

After Advanced Analysis has been performed on the tree, further analysis can be done to better understand the results.

Machine learning classifies attack scenarios into groups that have similar characteristics. You need to specify the number of groups, the criteria used for evaluation and the range of attack scenarios to be considered.

The clustering algorithm iteratively works to perform the grouping. In most cases, **SecurITree** will determine a good number of iterations automatically. However, you can override this if desired.

The criteria used for evaluation are chosen from the various indicator functions. Although any number of criteria can be selected, increasing the number greatly increases the number of calculations that must be performed! It is recommended to start with basic parameters such as feasibility, desirability and victim impact. Avoid selecting criteria that overlap. For example., Technical Ability is used to estimate Feasibility, so selecting both of those may not make sense.

The machine learning algorithm that clusters the scenarios is an iterative process. The algorithm makes an initial guess as to which scenarios belong to each of the specified number of clusters. The initial guess at groupings is seldom optimal, but serves as a starting point for the algorithm. The algorithm then attempts to improve on the cluster groupings by moving scenarios between groups based on similarity of the user's selected criteria. The learning algorithm may require numerous iterations to successfully cluster the scenarios into groups of similar characteristics. Generally, fewer scenarios will move on each successive iteration as clustering improves. Clustering is considered successful when the number of scenarios moved drops below a specified threshold.

**SecurITree** allows the analyst to specify the threshold value used to consider clustering to have been successful (default is 1%). Depending on the data set and the criteria chosen it is possible (though rare) that the number of scenarios moving between clusters will never drop below the specified threshold. That is, scenarios will endlessly move back and forth between clusters. To prevent the algorithm from iterating forever, **SecurITree** limits the number iterations to a maximum value (default is 25). If the maximum number of iterations is reached before the percentage of scenarios moving between clusters falls below the threshold value, **SecurITree** will give the user the opportunity to perform additional iterations and manually decide whether the algorithm is converging or not.

## Similarities

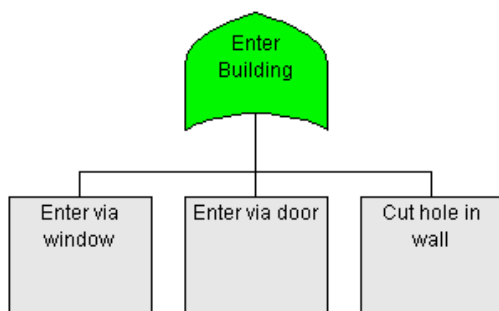
After Advanced Analysis has been performed on the tree, further analysis can be done to better understand the results.

Select an attack scenario on the Advanced Analysis Table, then select Analyze > Show Similarities. The table will include a "Similarity Index" column which gives the number of similar nodes between the selected scenario and all the other scenarios. The table is sorted showing the scenarios with the most similarities to the least. A different scenario can be selected on the Advanced Analysis Table and the Similarities table will be automatically updated.

## Attack Scenario Reduction

A minimal set of leaf node activities in an attack tree that result in the attainment of the root node is known as an attack scenario. In the case of complex attack trees, there may be thousands of distinct attack scenarios. The large number of scenarios can require excessive amounts of time and computing power to analyse. Not all of the scenarios are equally significant.

For example, consider a simple attack tree representing a number of different ways an intruder could enter a building.

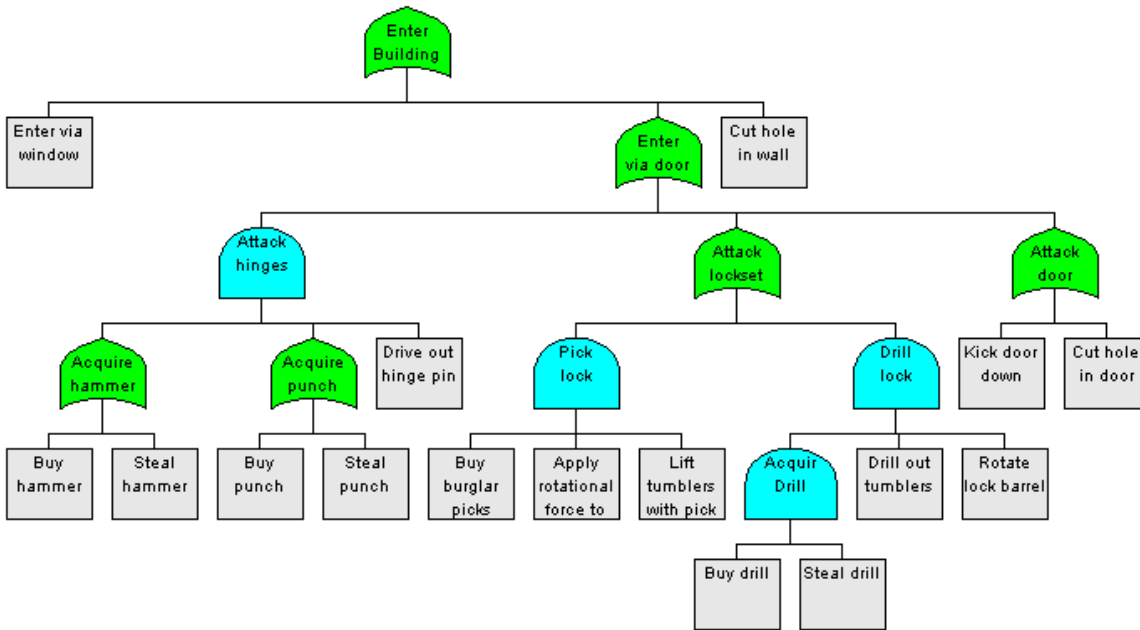


This attack tree has only three attack scenarios associated with it.

Row	Scenario	Scenario Type	Attack Scenario	Cost of Attack	Technical Ability
1	1	C	{Enter via window}	0	5
2	2	C	{Enter via door}	100	30
3	3	C	{Cut hole in wall}	300	40

The analyst has associated a set of values with each leaf node that attempts to represent the challenge an adversary will face in *Entering via window*, *Entering via door* or *Cutting a hole in wall*.

The leaf nodes in the figure do not describe any of the details of the activities. Suppose the analyst determines that greater detail is required to adequately model the ways in which an adversary might enter via a door. This leads to the more elaborate tree shown below.



This tree expands the single *Enter via door* attack scenario shown before into eight separate attack scenarios (scenarios 2 through 9) for a total of ten in the entire tree.

Row	Scenario	Attack Scenario	Cost of Attack	Technical Ability
1	1	{Enter via window}	0	5
2	2	{Buy hammer, Buy punch, Drive out hinge pin}	50	10
3	3	{Buy hammer, Steal punch, Drive out hinge pin}	26	15
4	4	{Steal hammer, Buy punch, Drive out hinge pin}	26	15
5	5	{Steal hammer, Steal punch, Drive out hinge pin}	2	15
6	6	{Buy burglar picks, Apply rotational force to lock barrel, Lift tumble...	250	50
7	7	{Buy drill, Steal drill, Drill out tumblers, Rotate lock barrel}	100	35
8	8	{Kick door down}	0	20
9	9	{Cut hole in door}	100	35
10	10	{Cut hole in wall}	300	40

If all the analyst is interested in knowing is whether or not a particular adversary can *Enter via door*, then it is often possible to eliminate certain scenarios because they are redundant. A quick perusal of the *Enter via door* scenarios (scenario 2 through 9) shows that some scenarios are as easy or easier, in every way, than other scenarios. For instance, scenario #5 (Cost of Attack = \$2, Technical Ability = 15) is easier than scenarios #3 and #4 (which have the same technical ability rating but a higher monetary cost). So, if there is an adversary capable of performing scenarios #3 or #4, then they can also perform #5. The list of attack scenarios can be *reduced* by eliminating scenarios 3 and 4 without jeopardizing our ability to say whether a particular adversary could do a door attack.

Of course, the adversary's capability to perform an attack scenario is not the only thing that determines whether they will perform it. It is also necessary to consider the desirability of the

scenario. When deciding whether to reduce or eliminate a scenario we must also check that the easier scenario provides at least as many benefits (in all senses) to the attacker. The scenario with the lower resource requirements cannot act as a representative of the more costly scenario because, despite its easiness, it might not provide a sufficient incentive to induce the adversary to perform it. The more costly scenario must remain because the adversary may perform it if they have the necessary resources in order to attain the more lucrative benefits.

Since the risk equation involves both the probability of the attack scenario and its impact on the victim, the impact must also be taken into account when determining if a scenario can be eliminated. A scenario targeted for elimination (harder, less beneficial to the adversary) must also be less damaging to the victim. Otherwise, it should be kept. Even though it is less likely to occur the higher damage may make it a higher risk (so it cannot be eliminated).

There are two other factors that can impede scenario reduction. If the scenarios being compared contain booleans then both boolean values must be the same. There is no algorithmic way to determine whether *TRUE* or *FALSE* is the more restrictive or higher impact condition. For instance, one analyst might define a behavioral boolean *Doable only by Insider* whereas another might set up *Doable by Anyone*. So, the only safe elimination is when the boolean values match.

Finally, the absolute probability of a scenario (and its overall impact) is affected by the number of encounters between the adversary and the defender's system. The expected number of encounters is defined by the mode of attack parameters (single shot, single threaded or multithreaded). Given two otherwise identical attack scenarios, the scenario with the higher number of encounters will have the highest absolute probability and risk (and is the scenario that should be preserved during reduction). Normally, the multi-threaded parameters generate more encounters than single threaded, and single threaded parameters generate more encounters than single shot. This *aggressive* assumption is normally used by **SecurITree**. In some unusual cases that order of precedence might not apply and **SecurITree** can be told to use a *conservative* strategy - reducing only those scenarios with matching attack modes.

To reduce the attack scenarios, starting at the selected node, to the minimum set, use the [Reduce Subtree](#) command.

The reduction algorithm to use can be selected by going to [Tools > Preferences > Tree Properties](#) tab.



## Attack Effectiveness

Sometimes an attacker's capabilistic actions (at both leaf and intermediate node levels) are not purely deterministic. It is as if, after an adversary applies the requisite resources to execute an attack, they then must roll a dice to see whether the outcome will be successful. The adversary creates the event but is not completely in charge of the outcome. We will call these capabilistic events that have random factors, *probabilistic outcomes*. *Probabilistic outcomes* can occur at any node in the tree that has a capabilistic component.

To capture this random component, beginning in **SecurITree** v3.3, capabilistic nodes can be assigned an attribute called *attack effectiveness (AE)*. The *attack effectiveness* is input as a value between 0 and 1 that specifies the likelihood the application of the resources will cause the node to succeed. The user can specify one of two ways in which the *attack effectiveness* term can be applied.

### *Encounter-based AE:*

If the adversary is naive (or optimistic) they may expect that their actions will always have a 100% success rate. They do not discount the value of an attack operation that has an uncertain outcome. They find it as desirable as if it were guaranteed to succeed (provided that they supply the required resources). Thus, *relative risk* remains unchanged by the *AE*. (This is correct if it is assumed that victim impact occurs even if the attack is unsuccessful - if victim impact only occurs in successful attacks then *relative risk* is overestimated.) However, the fraction of encounters that result in a attempted scenario occurring successfully must be reduced by the *AE* factor to yield a lower effective *scenario frequency*. This also reduces the *cumulative risk* by the *AE* factor.

### *Attacker Benefit-based AE:*

If the adversary is astute they will recognize that certain steps in a node or attack scenario have a likelihood of failure that is beyond their control. This will devalue the *attacker benefits* that they would otherwise expect to attain. Since the attacker's motivation is proportional to the perceived benefits they hope to receive, the devaluation must be applied to the raw benefits before they are translated via their respective utility functions. Depending on the shape of the utility functions, this may result in a reduction of benefit that is greater or lesser than the *AE* factor. We call this *attacker benefit-based AE*.

For any given scenario the *attacker benefit-based AEs* and the *encounter-based AE* terms are accumulated separately for each node traversed in the scenario. The former will be multiplied together to get an *overall attacker benefit-based AE* which will reduce the attacker benefits before they are transformed by the utility functions. The latter will be multiplied together and used to compute an overall *effective # of encounters* term.

In both cases, the *cumulative risk* will be decreased for any attack scenario that has components with *AE* values  $< 1$ .

NOTE: Attack Effectiveness cannot be set for Probability or Countermeasure nodes.

## Attack Type and Time Parameters

In a given encounter between an adversary and the target, the *propensity* that they will perform an attack scenario depends on their capabilities and goals. However, to understand the actual frequency that the scenario will occur requires that we estimate the number of encounters between the adversary and the target. The number of encounters that will be experienced by the defender's system is determined by both the characteristics of the threat agent and the nature of the attack scenario.

The relevant characteristics of the threat agent are defined in the *threat agent profile* and include:

- the number of adversaries in the threat agent class
- the fraction of time that is spent working on attacks
- the number of attacks that the adversary can perform simultaneously
- the number of targets competing for the attention of the threat agent

Parameters that deal with the nature of the scenario are associated with the leaf level operations required for the attack. The operations may be:

1. Single shot - able to be performed only once by a given threat agent. Execution of the attack permanently depletes all of the attacker's resources.
2. Single threaded - able to be performed multiple times, but consecutively. Each time the operation is performed it takes a specified amount of time followed by a recovery time during which the adversary prepares for another attempt.
3. Multi-threaded - able to be performed multiple times, concurrently (limited by the attacker's resources).

These parameters can be set for each leaf node in the tree. This can be labor intensive. In many trees, most of the leaf nodes share similar attack types (single shot, single threaded, multi-threaded) and attack time/recovery time parameters. If this is the case, it may be useful to set default values for each attack type in Tools > Preferences > Tree Properties (tab). It is also possible to set a default attack type for leaf nodes that will apply unless overridden.

## Alternative Sets

Models may represent systems at a conceptual phase, systems as actually implemented, or actual systems that include one or more proposed changes. The differences between these models is often small. For example, an analyst may want to compare the performance of an "as-built" system with a similar system that has been enhanced with a countermeasure. The analyst could make a copy of the original "as-built" system model and modify the copy, but it would then be tedious to maintain the synchronization in common portions of the models. **SecurITree** makes it possible to create a single model which captures all of the variations.

When a new tree is created, the nodes in the tree are members of a set that is known as the *Base Tree* alternative set. At some point it may become necessary to create a new model based on the original. The analyst then defines a new alternative set. For example, the *Countermeasure #1* alternative set. The nodes in the original *Base Tree* alternative set are given membership in the new *Countermeasure #1* set -- they belong to both alternatives (which are initially identical).

The analyst can select which alternative set is *active*, i.e. which alternative set they wish to view/manipulate. Generally speaking, creations of new nodes and deletions of existing nodes apply only to the active alternative set. Modifications to nodes that are members of more than one alternative set will be reflected in all of the sets to which they belong. Where ambiguities exist, **SecurITree** will prompt you for clarification. The user interface does allow the user to manage node set membership directly if necessary.

Analytic, print and file export operations apply to only the members of the active alternative set. Only files stored in .RIL or .RIT formats preserve the multiple alternative sets.

## Libraries vs. Trees

The difference between libraries (.ril) and trees (.rit) is that libraries are just a special type of Attack (Threat) Tree file. Libraries are threat tree template files that are used to create Attack Trees. They can be used as the starting point for creating a new tree or they can be inserted into an existing Attack Tree. They can only be modified by the user using the **File > Save Tree As...** command.

Amenaza Technologies has included several library files with **SecurITree** which model major technologies that are in use today. These files are updated on a regular basis and these updates are provided to all customers who have our maintenance support package.

## Subtree Reuse: Internal Links

Analysts sometimes notice that the identical subtree may be repeated in multiple locations within a tree model. This situation commonly arises when a similar defensive technology appears in different parts of a system's architecture. For example, a facility may use the same type of doors and lock sets everywhere. Opening one door may lead to a completely different location than another, but the procedure for breaking the door's security (e.g., pick lock, force door) is identical in all cases. *Internal links* are for convenience where the procedure is identical but the logical state achieved by carrying out a given set of steps is different.

*Internal links* allow an analyst to keep one copy of a subtree in memory, but reference it multiple times. The indicator values, notes and tree structure of all nodes within all instances of the *internal link* (i.e. that share the same *link number*) are identical. Any edits made to one instance will be instantly applied to all other linked instances. However, for purposes of analysis, SecurITree treats each instance as separate and distinct. From an analytical perspective it is as if the linked subtrees were unrelated copies. Because linked nodes share the same labels this may cause the illusion of redundant scenarios in an attack scenario listing. That is, depending on the structure of the model, a particular combination of leaf level events may appear multiple times. This ambiguity can easily be resolved by enabling *View > Display Node Information* before generating the attack scenario listing (which will show that the node identifiers are distinct despite the label being the same). *Internal links* are widely used and can greatly reduce the effort of building attack tree models.

### (Normal) links vs. Identical links

SecurITree's *Link* feature (for both *Internal* and *External* links) allows multiple instances of a node or subtree to be placed throughout the tree. If any one of these instances is edited (either directly, in the case of *internal* links, or in a reference file, in the case of *external* links), all other instances will also be modified. *Links* have existed in SecurITree since version 1 and *External links* since version 2. Beginning in SecurITree version 4, a new type of *link* is being introduced. To avoid confusion, the longstanding *link* feature (both *internal* and *external*) will be referred to as *normal* links, or simply, *links*. The new type of *link* will be identified as an *identical link*

Normal links are used to represent ways of attacking similar (but different) components. As a simple example, a facility may use the same type of door everywhere. So, the various techniques of breaching the door (crowbars, lock picks, stolen keys) would be the same for all doors. However, it is important to understand that the various instances of the linked *open door* subtree represent different doors that presumably lead to different parts of the building. Similarly, a subtree could represent attacks against a particular type of computer operating system. A *normal link* to the *compromise operating system* subtree would be used to represent attacks against a different computer (that had the same type of operating system). Again, the possible attacks would be the same but the benefits to the attacker and the impacts on the victim might be very different. The benefit of using a link (instead of

just copying the subtree) is that improvements or changes to any instance of the linked subtree result in all other instances being updated as well.

*Identical* links are a feature provided to deal with certain special cases in attack trees. They should be used sparingly and with great consideration. The following discussion will help you understand when *identical links* are appropriate.

Attack trees are a special type of Boolean logic trees. Note that it is possible to create many alternate logic trees that yield the same logical output (represented by the root node) for a given set of (identical) inputs (represented by leaf level events). Prior to v4.0, this was not a concern because it was impossible to place two identical leaf nodes in the tree, even using normal links. Normal links represent nodes that are distinct and different but for whom the logical states and exploit procedures are similar - but not identical.

Beginning in **SecurITree** v4.0 and the introduction of *identical links*, multiple instances of an identical node (denoted by "=") become possible in a tree. An example of an *identical link* is shown in figure 1. In this case, *Exploit 2* acts as a single event or input. If *Exploit 2* occurs at all, it must be applied to both the *Procedure 1* and *Procedure 2 AND* nodes. The attack scenario list would include {(Exploit 1, Exploit 2), (Exploit 3, Exploit 2)}.

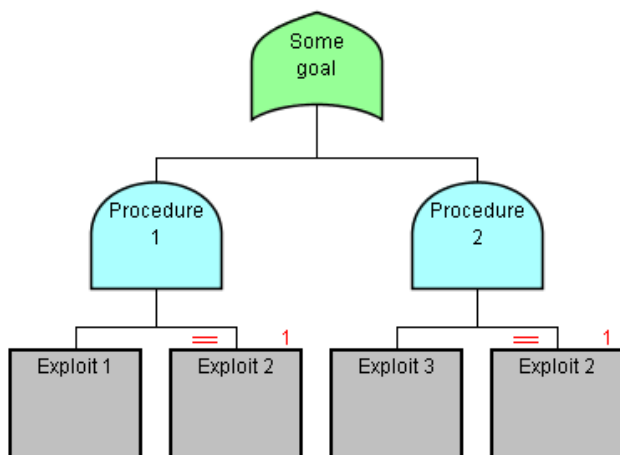


Figure 1

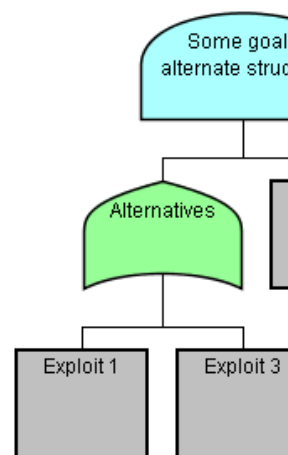


Figure 2

Note that this attack scenario list is identical to that produced by the more concise Figure 2 attack tree - in a Boolean logic sense, the two trees are completely equivalent. However, in the first representation, it was necessary to show that *Exploit 2* was the identical operation and operates against the exact same target component (as depicted by the red = sign).

Since it can be seen that Figure 2 is arguably a more concise and easily understood representation of the Boolean logic, it is fair to wonder why *identical links* are even necessary. In most cases, they are not and most analysts did not feel their lack in pre-v4.0 versions of SecurITree. However, there are two reasons why allowing the first representation can be useful. First, it may simply be more convenient and intuitive. The analyst may have spent considerable time creating a tree whose intermediate *AND* and *OR* nodes represent states that are easily understood by humans. Significant effort might be required to modify the tree to the second representation. Beginning with SecurITree v4 and *identical links*, this restriction is lifted and analysts are free to use the most natural and convenient structure.

Aside from convenience, there is a more fundamental reason for *identical links*. Attack trees, as implemented in Amenaza's SecurITree software, are not simple Boolean logic trees. They have been enhanced to allow modeling of impacts (benefits to the attacker, damages to the victim) at all levels of the tree. Unlike a simple Boolean logic tree (which are only concerned with which set of leaf level inputs will trigger the root level output) Amenaza's attack trees distinguish between paths taken to the root node. Although several sets of leaf level events may result in the attainment of the root goal, the impacts to the victim and the benefits to the adversary may be very different. This results in different risk values for the various scenarios. In order to capture these differences the analyst may need to structure the tree in a particular way so that the impacts can be injected appropriately. This, in turn, makes necessary the use of linked subtrees that are identical.

Another example of this requirement is

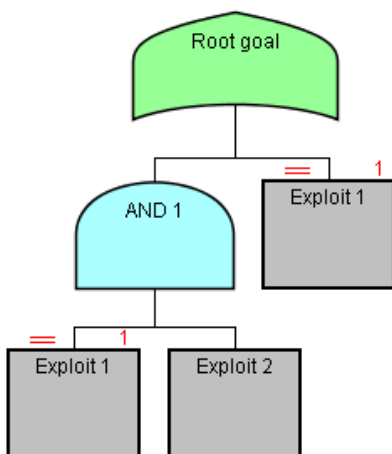


Figure 3

with attack scenarios { (Node 1, Node 2), (Node 1) }



At first glance, one might wonder why any adversary would ever perform the more complex scenario (Node 1, Node 2) if they could achieve the root goal simply by doing (Node 1). Why would they ever do two operations (with presumably a higher total resource expenditure) if performing only one would suffice?

If the impacts of both scenarios (benefits to the attacker and damages to the victim) are the same, then there is no valid reason for doing the more complicated scenario. It is always true (but not helpful) that any number of non-useful tasks can be performed in addition to the tasks required to reach root. So, in many cases, the more complex scenario could be removed from the scenario list because it is non-minimal.

However, if attainment of *AND 1* brought certain, unique benefits to the attacker, that would make the attack scenario (Node 1, Node 2) much more desirable than (Node 1) by itself. The greater desirability would affect the probability of the scenario and therefore increase the risk. Similarly, *AND 1* might contain a greater impact to the victim (which would also increase the risk of the complex scenario). In this case, the complex scenario should be retained in the scenario list (despite the fact that it is non-minimal from a leaf node perspective).

In SecurITree's preferences (Tools>Preferences), SecurITree allows the analyst to choose whether to

- a) see all scenarios (whether non-minimal or not)
- b) remove only those non-minimal scenarios whose impacts differ
- c) remove all non-minimal scenarios

It must be stressed that cases where the use of *identical links* is appropriate are usually quite restricted. Inappropriate use of *identical links* can result in confusion, and in some case, a logical paradox. For example,

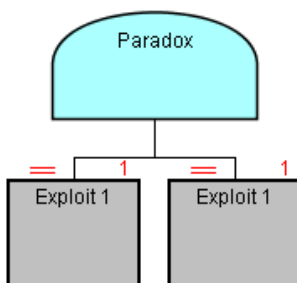


Figure 4

It is very difficult to understand what this subtree means. The attack scenario produced from such a structure is {(Exploit 1, Exploit1)}. It shows two operations being required, yet says they are the identical operation. Since the resource expenditures of leaf nodes under an *AND* node are usually aggregated (in accordance with the indicator definitions) it becomes very unclear how this calculation should be performed.

This is just one simple case and even more confusing structures are easily constructed. Since an unambiguously correct result is unclear, **SecurITree** attempts to prevent the user from creating such structures. In some cases a user may be able to create an illegal structure that is not immediately detected. In this case **SecurITree** will detect the illegal structure when analysis is attempted.

### **Ganged links**

*Ganged* links are a variant on *Normal Links* but used in very specific cases.

It is not uncommon for defenders to deploy the same technology in multiple areas of their systems. Depending on the attack, the adversary may have to defeat two or more instances of some particular technology. *Gangs* are used to show that the attacker's choices for each instance are dependent on previous choices. The *gang* metaphor is taken from the field of electronics, where multiple capacitors, resistors or inductors are mechanically ganged so as to move together.

A very simple example is a door. Generally speaking, most of the doors in a particular building are very similar in their construction. Although a variety of methods can be used to open the door (pick lock, use crowbar, trick access card system) it is likely that an attacker who finds it necessary to pass through a series of doors to reach their target will use the same exploit on each one.

Similarly, in the network security world, it is common for networks to be broken into multiple security zones. Each zone is separated from its adjacent zone(s) by some type of firewall technology. Frequently, the same type of firewall is used in all locations. The least secure zone may be the Internet, which is separated from the business network by a firewall. The company may also have created a highly secure network zone (for the company's information jewels) that is again separated from the business network by a firewall. Just as in the case of the door, there may be a variety of different exploits and attacks available to an adversary for traversing a firewall boundary. However, since the company uses the same firewall technology in all locations, then once the adversary has chosen a particular strategy to make it past the first firewall, they will likely use the same strategy on subsequent firewalls. Knowing this significantly reduces the number of scenarios that need to be evaluated.

The diagram below shows a very simple attack tree for a three zone network architecture: Internet, Business Network, Secure Network. The model shows how an attacker might start from the Internet, compromise the Internet firewall to gain a presence on the business network, then attack the firewall protecting the secure network segment. The number of scenarios in the *Compromise Firewall* subtree is 10 and the scenario count of *Compromise Windows 10 / Server 2016* is 820. Without ganged links the number of scenarios that must be evaluated is therefore 90,200. By *ganging* the two *Compromise Firewall* subtrees together, the number of scenarios drops to 16,400.

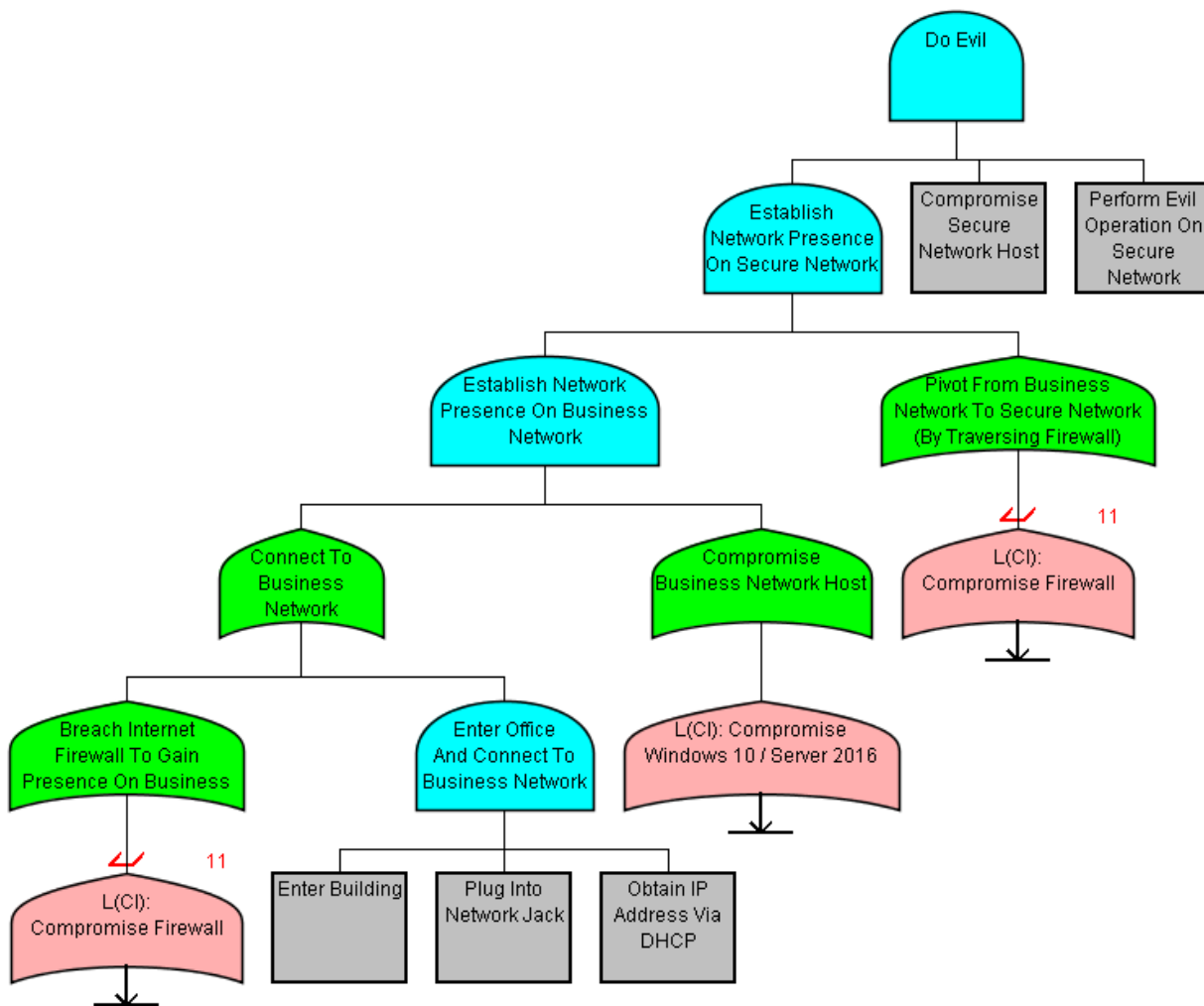


Figure 5

See Also:

- [Paste as Link](#)
- [Paste as Identical Link](#)
- [Paste as Ganged Link](#)

[Subtree Links and Attack Graphs](#)

## Countermeasures

Prior to **SecurITree** v4.0, countermeasures and controls could be depicted in three ways:

1. The capability resource requirements associated with a leaf node could be increased to reflect an improvement in the component the attacker was attempting to exploit. For example, if an inexpensive, hollow core door (with a cheap lockset) was replaced with a high quality, solid core door (equipped with top grade hardware) then battering through or prying open the door would become more difficult. The technical ability rating and the cost of the equipment required to overcome the door would increase for the *Penetrate door* leaf node.
2. Changes could be made to the defender's system to make an attack more complex and challenging. In cases where an attack required a series of steps (depicted by an *AND* node), then additional children could be added beneath the *AND* node representing the new activities, which would be chosen by the defender to be as difficult as possible. For instance, if an attack scenario for obtaining electronic information involved the steps of: entering a computer room, stealing a data tape, and reading the tape then the attack could be made much more difficult by encrypting all data on tapes. The revised attack scenario would then be: enter computer room, steal data tape, read tape, break encryption on information. Hopefully, the *break encryption* step would be very challenging for the attacker. The *break encryption* procedure could be a single leaf node or, more typically, a subtree describing various approaches to breaking encryption. In cases where an *AND* node was not already present in the undefended tree, a new *AND* node could be created and the original attack step (leaf node) placed beneath it, along with the new additional attack step.
3. The clever use of Boolean capability indicators and attacker capabilities could be used to describe defenses. For instance, certain leaf level activities in a tree might be technically straightforward and low cost, but only feasible for a trusted, authorized insider. These operations would have a *Breach of Trust* indicator value of *True*. The threat agent profile for an insider would reflect the insider's capability to perform these privileged operations whereas an outsider would not. So, if an organization implemented procedures to eliminate hostile insiders (background checks, regular polygraph examinations, procedures to ensure that critical activities are always performed by two randomly chosen personnel) then the countermeasure would be represented by setting the attacker's *Breach of Trust* capability to be *False*.

These three techniques have proven to be effective in a wide variety of circumstances. However, they are implicit and may not be recognized as countermeasures by someone reviewing the model. It would be useful to be able to represent controls in a more direct fashion.

A variety of academic papers have been published describing extensions to the attack tree model. Of particular interest is the 2011 paper published by Roy, Kim and Trivedi (ACT: Towards unifying the constructs of attack and defense trees, Arpan Roy, Dong Seong Kim and Kishor S Trivedi, Security

and Communication Networks, 2011; 3:1-15). In the paper, Roy et al discuss an extended tree model they call an *attack countermeasure tree*.

Beginning with **SecurITree** version 4.0, Amenaza has implemented a *countermeasure* feature. It takes inspiration from academic papers (such as the one cited), Amenaza's own research and development, and feedback from customers.

Seen from an attacker's point of view, a countermeasure is an additional obstacle that has been added to an attack procedure by the defender. Since procedures are depicted in an attack tree as *AND* nodes, it follows that a countermeasure must always fall beneath an *AND* node. In most cases, the *AND* node already exists (as the parent of the original attack steps). If the attack previously had only a single step (represented by a leaf node) then an *AND* node parent must be introduced and the leaf node and the countermeasure placed beneath.

From the defender's point of view, a good countermeasure is a system (or machine) that operates correctly and fulfills its mission as much of the time as possible. Ideally, machines should operate perfectly 100% of the time. However, no real world systems achieve this level of performance. For example, X-ray scanners (or the humans operating them) sometimes miss dangerous items in passengers' luggage at airport security checkpoints. Similarly, network intrusion detection systems fail to identify malicious packets a certain fraction of the time. In both cases a 98% success rating would be considered very good. Nonetheless, this does mean that malicious payloads are getting past the control 2% of the time.

Most of the failures in a countermeasure are due to technical limitations, non-hostile human error or other random factors. The failures are not due to the actions of the adversary. If this assumption is correct then the different failure modes in a countermeasure can be represented using a probability-based fault tree. To create a countermeasure, construct a fault tree that represents the various ways in which the countermeasure can fail due to random factors. The leaf level events in this fault tree are assumed to be independent events, so the standard statistical formulae apply.

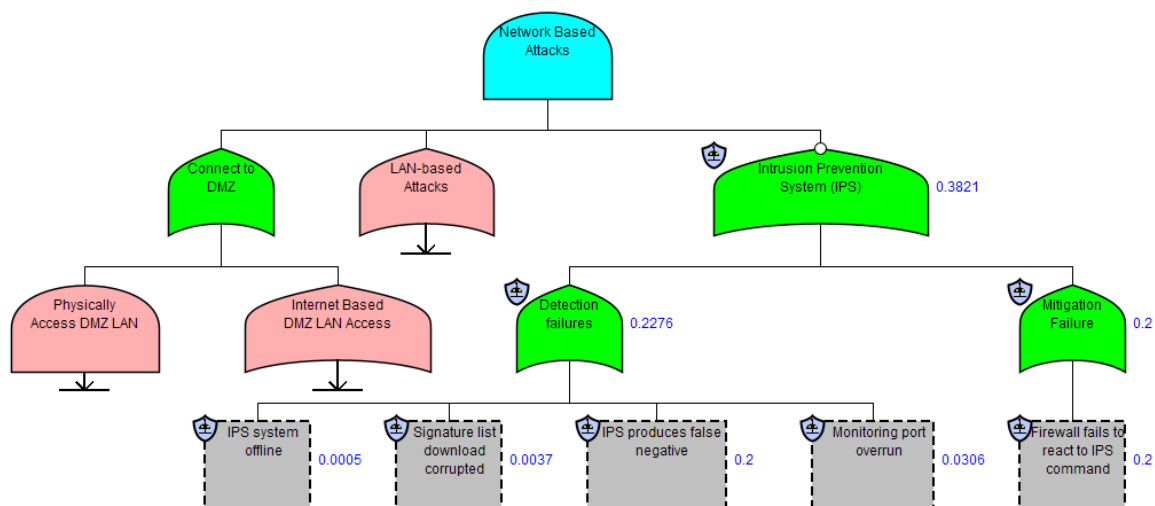
Prior to version 4.0, it was certainly possible to use the probabilistic functions in **SecurITree** to construct a fault tree. However, there were certain limitations that limited their usefulness for representing countermeasures. First, all of the paths in the failure subtree would be expanded in conjunction with other capabilities components of the attack scenarios. While this is not wrong, it does not allow the analyst to see the overall effectiveness of the countermeasure system acting as a unit. What is needed is the ability to compute the overall probability of the countermeasure failing (from any and all causes) and to show the effect of the failure on a deliberate attack.

Beginning in version 4.0, a new *countermeasure* node subtype is available. The *countermeasure* subtree must be placed directly beneath an *AND* node. All nodes that form part of the countermeasure node have a unique symbology denoted by a blue shield emblazoned with a tiny robot. The shield conveys the idea that this is a defense node and the robot that it is a type of automaton. The topmost node in the *countermeasure* subtree (i.e., the *root* of the *countermeasure*) has a small circle on top,

conveying to the mind that the attack only succeeds when the countermeasure fails. (The *not* symbol is for symbolic purposes only and does not reflect any change to the underlying mathematics).

By default, the *countermeasure* subtree will act in *consolidated* mode. That is, a single probability value will be computed for the countermeasure as a whole and only the root node of the countermeasure subtree will appear in attack scenario lists. Alternately, the analyst can select the *expand* mode in the subtree's root which will expand the paths in the *countermeasure* subtree (and calculate a probability of each path).

It is hoped that this abstraction is general enough to accommodate many of the schemes proposed in the literature for representing countermeasures. For instance, one of the proposed mechanisms for modeling countermeasure failures involves a *detection* step and a *mitigation* step. To represent this, a countermeasure tree is placed beneath an *AND* node. The countermeasure subtree root could be an *OR* node, with branches representing the countermeasure's failure to detect or mitigate hostile events. An network intrusion prevention system (IPS) provides an excellent example.



This example (extracted from a larger attack tree) shows that, in order to carry out a *Network Based Attack* on a host located on a DMZ the attacker will need to perform three steps:

1. Connect to the DMZ (through either physical access or some type of Internet connectivity - the details are not shown)
2. Perform an attack against the host on the LAN (i.e., send malicious packets)
3. Hope that the IPS fails for some random reason

The first two steps are driven by the attacker. The last step depends on the periodic failure of the countermeasure.

In the example above, the probabilities of the various leaf level events are shown as well as the probabilities of the *OR* nodes above them (calculated using standard fault tree statistical formulas). We see that the IPS system is offline 0.0005 of the time - not likely a major cause of failure. However, the model also shows that the IPS fails to identify a malicious packet as harmful 0.2 of the time (probably because the IPS doesn't have a signature or heuristic capable of deducing the nature of the packet). Using statistical formulas, by the time we get to the *Intrusion Prevention System (IPS)* countermeasure root node we find the countermeasure fails 0.3821 of the time.

Often when we consider the reliability of machines we talk about a machine's "uptime". In this example, the IPS has an uptime of 0.6179. However, we are more interested in the fraction of time that the control is ineffective - 0.3821. SecurITree's symbology attempts to convey this by placing a ° symbol at the top of the countermeasure's root node.

The way this affects the overall probability of the attack is by opening a window of opportunity for the attacker. The way to think about this is to consider what the probability of a given attack scenario would be if the countermeasure didn't exist. For sake of argument, suppose that there were no countermeasure and some scenario involving the *Connect to DMZ* and *LAN-based attack* steps has a capabilistic propensity of 0.4. The absence of the countermeasure is equivalent to the countermeasure being present, but failing 100% of the time. But in the example, the countermeasure is present but fails 0.3821 of the time. When the countermeasure is operational attacks will fail. The countermeasure's failure to perform opens a window of opportunity for the attacker. The overall probability of the hypothetical scenario is  $0.4 \times 0.3821 = 0.1528$ .

Impacts (attacker benefits/detriments and victim impacts) can be injected into nodes in a countermeasure subtree, just as with any other node in the tree. However, the way the impact values are handled differs depending on whether the subtree is in *consolidated* or *expanded* mode.

In *expanded* mode, the impacts for each scenario within the countermeasure tree are calculated as per normal. In *consolidated* mode, a single value is derived to represent all the scenarios in the tree. As mentioned earlier, this is straightforward for probabilistic values and standard statistical formulas are used. The situation is more complex for impact values and there is arguably no approach that is correct for all situations.

Where an *AND* node appears in a countermeasure subtree, the method of calculating impacts is straightforward because all of the children must occur to satisfy the logic. So, whatever *AND* function is defined for the impact indicator (typically sum or maximum) will be used to compute the impact.

Situations involving an *OR* node are more complex. Any non-null subset of the *OR* node's children could occur, and might have an impact. Since each of the children's probability is independent from its siblings, there is no requirement that the probabilities of the *OR*'s children tally to 1 - and, in fact, they usually do not. The approach taken by SecurITree is to use a form of Monte Carlo analysis to roll the dice and see which children become active on a given trial. Then, of the subset of children that are active, further analysis is used to determine which child's impact will be chosen as that of the



trial. In a sense, SecurITree is taking the view that when, in a given cycle, several children become active, they would not (in the real world) all become active at the same instant in time - one would be first and that is the one that would cause the impact. Monte Carlo analysis determines which of the active children is most likely to occur first based on the active children's relative probabilities. Choosing the first active child's impact is not necessarily correct in all situations, but it seems reasonable in most situations. As experience with this analysis grows, other options may be provided based on user feedback. One way of avoiding these issues is to simply place all impacts in the countermeasure subtree's root node. Indeed, in many cases the impact of a countermeasure failure will be the same regardless of how it fails, so this would be a good default choice. At the very least, the analyst should be aware that inserting impacts in countermeasure subtrees beneath *OR* nodes will trigger SecurITree to use Monte Carlo analysis. This is computationally expensive and, if used excessively, will degrade performance.

Note that, typically, countermeasure nodes do not have impact values defined.

## Attack-Defense Trees

### Introduction to Attack-Defense Trees

Attack tree models have existed since the 1990s (or possibly even the late 1980s). They have proven to be extremely useful for exploring how adversaries might attack systems.

Attack trees are a bit like the *Mouse Trap* board game - a Rube Goldberg-like mouse catching device - wherein once the machine is set in motion a complex sequence of events occur that ultimately leads to the capture of a mouse. Of course, in the real world, the mouse might well notice movement in the machine and deduce that it was being attacked (before the mouse catching basket should drop). This might allow it to quickly take defensive action and protect itself by placing a stick in one of the machine's gears. A classic attack tree would not capture the dynamic interplay between the attacker (the mouse trap machine) and the defender (the mouse).

Academic researchers have recognized this shortcoming and criticized the static nature of attack trees. Various researchers have proposed extensions to the attack tree metaphor and called the result *attack-defense trees*. It should be noted there seem to be as many different views of exactly what comprises an attack-defense tree as there are researchers. One of the most lucid descriptions is found in a 2011 paper by Roy, Kim and Trivedi, "ACT: Towards unifying the constructs of attack and defense trees", published in the Security and Communication Networks Journal.

### Attack-Defense Trees in SecurITree

#### Overview

Support for attack-defense trees in **SecurITree** will begin with version 5.1 (August 2020). It should be noted that Amenaza's implementation of attack-defense trees does not attempt to mimic any particular academic paper description, although it takes inspiration from them.

Three elements are used to depict an attack-defense tree (or subtree) in Amenaza's version of attack-defense trees. The top of any attack-defense tree must always be an AND node. In a normal AND node, all of the AND's child nodes (or subtrees) must be completed in order for the AND condition to be satisfied. The difference with an attack-defense AND node is that some of the child operations are conditional.

Each subtree beneath the attack-defense AND node depicts a set of attack scenarios (or, in the case of a probability-based countermeasure, fault tree cut-sets). **SecurITree** models follow the convention that, if order is important, the AND's children should be arranged from left to right.

The various leaf node combinations that satisfy the logic of AND's subtrees correspond to paths through the subtrees. In the real world, the leaf nodes correspond to actions by the attacker and the AND and OR nodes above to states achieved by the combinations of LEAF nodes. A clever defender might identify that successful attacks might require the attacker to pass through certain of these nodes. In that case, the defender might place sensors in the real world locations corresponding to those nodes. For instance, if a series of attacks required the adversary to pass through a door, then a sensor could be placed at the door. In the case of network attacks against critical servers, an intrusion detection system might monitor a network segment. Those attack scenarios that traverse a sensor node would cause the sensor to be *tripped* or *triggered* and the defender alerted to the presence of the attacker.

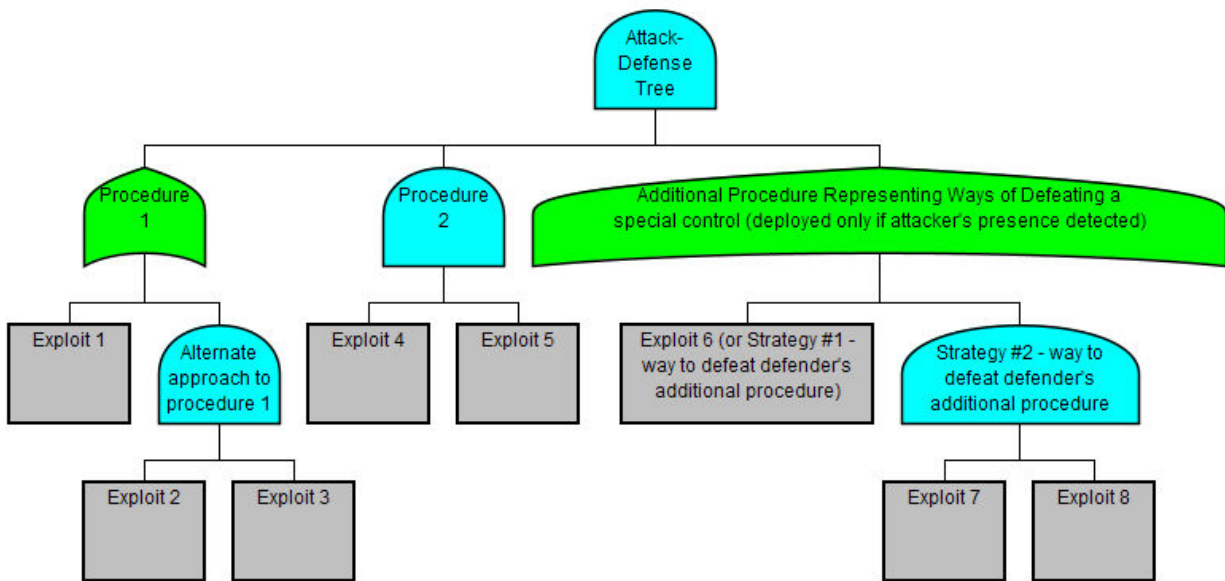
Once the defender is aware that an attack is underway, they would respond appropriately. In the case of the door alarm being triggered, a security guard might be dispatched to investigate. Note that the guard might not normally patrol that area, but the security alert would generate a special response.

That response would occur after the event was detected. The response would be depicted as either an additional attack subtree describing a sequence of events the attacker would have to overcome to defeat the additional capabilistic countermeasure (e.g., knock out the security guard) or, if the countermeasure were probabilistic in nature, hope that the countermeasure would fail of its own accord.

**Both the subtree containing the sensor and the additional countermeasure subtree (whether capabilistic or probabilistic in nature) must be located directly beneath the attack-defense AND node, and according to our conventions of ordering activities from left to right, the response countermeasure subtree must always appear to the right of the subtree containing the sensor.**

### Creating an Attack-Defense Tree

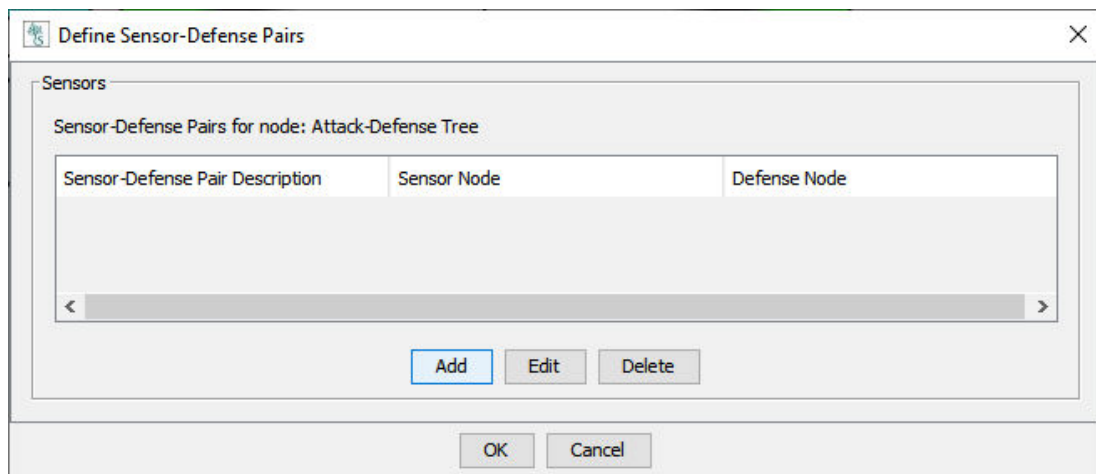
To create an *attack-defense* tree (or, more usually, subtree) in **SecurITree** the analyst first identifies (or creates) the AND node that will be the attack-defense tree's parent - the *Attack- Defense AND node* (or simply, *A-D AND node*). In most regards, this AND node is similar to ordinary AND nodes in the tree. However, it differs in that it contains a list of *sensor-defense pairs* that describe the relationships between sensors and the defender's responses when a particular sensor is tripped. Consider the tree in **Figure 1** below.



**Figure 1** - Evolving an attack tree into an attack-defense tree

As drawn, all three of the subtrees below *Attack-Defense Tree* need to be achieved in order for the top root node to be fulfilled. But suppose the right-most subtree, *Additional Procedure*, was expensive and the defender didn't want to deploy it unless they felt they were under attack. Analysis might show that the adversary would be most likely to complete *Procedure 1* by using the *Alternate approach to procedure 1* (involving *Exploit 2* and *Exploit 3*). It would therefore make sense for the defender to install a sensor that would tell themselves if the adversary had managed to perform the *Alternate approach to procedure 1*. The defender would respond by deploying an additional control - a control that would require the adversary to traverse the *Additional Procedure* subtree.

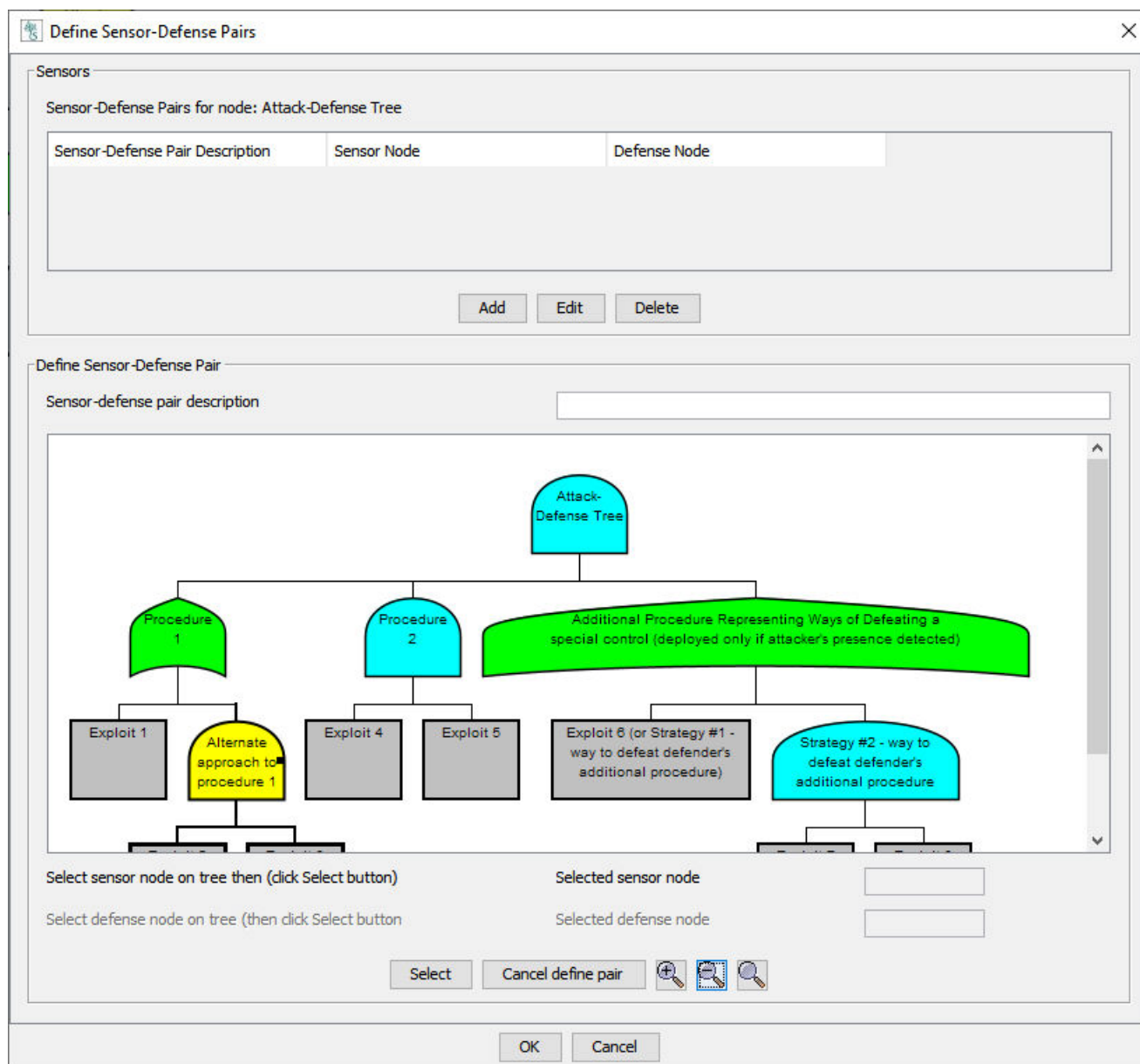
To define the sensor in the model the analyst would right-click on *Attack-Defense Tree* and select the *Define Sensor-Defense Pairs* option. A dialog would then open and they would click **Add** (**Figure 2**).



**Figure 2 - Sensor-Defense Pair List Creation**

A new window would appear showing the *AD-AND* node and the subtrees beneath it. Begin by entering the *Sensor-defense pair description*.

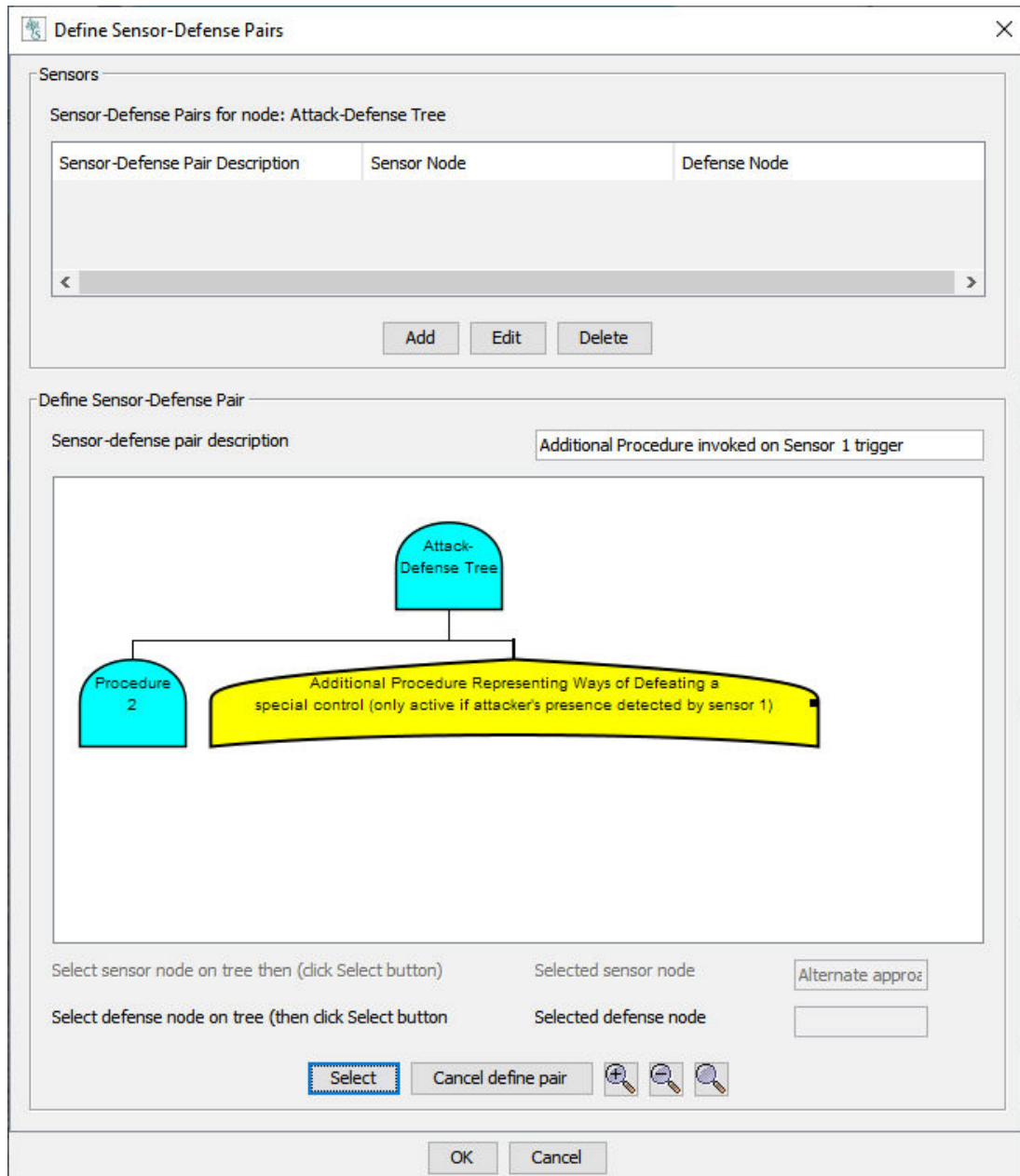
Note that only subtrees containing nodes eligible to be *sensor* nodes are displayed. For instance, subtrees that are part of links are excluded. The analyst would then select *Alternate approach to procedure 1* and click *Select* ( **Figure 3**)



**Figure 3 - Sensor placement on a node**

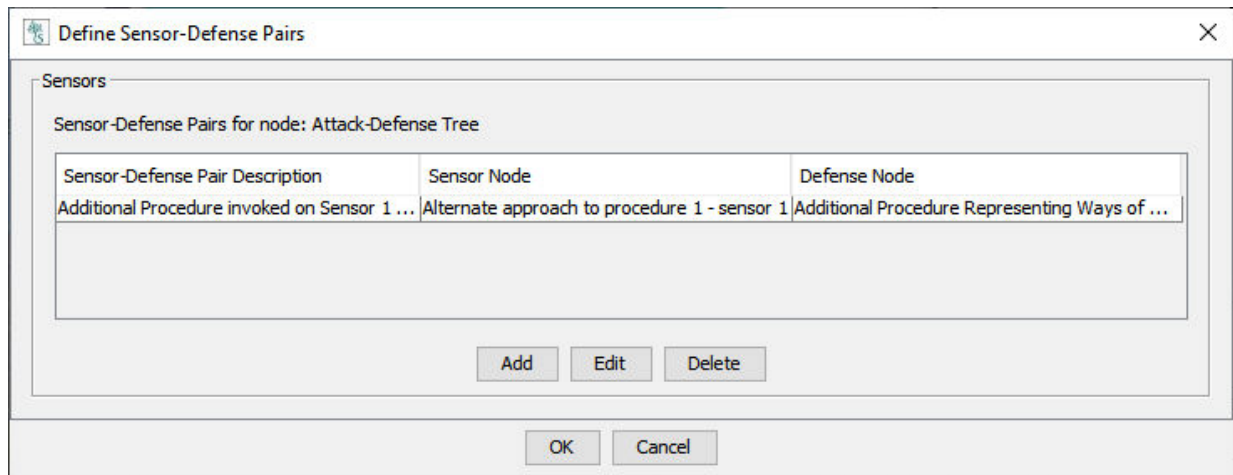
The analyst must now specify which countermeasure subtree will be invoked if the previously selected sensor is traversed in an attack scenario. In this example ( **Figure 4** ) the *Additional Procedure...* subtree has been selected.

In order for a defense subtree to be eligible to be selected (and displayed to the user) it needs to be to the right of the sensor node and immediately beneath the *AD-AND* node. The user is prompted to enter the sensor-defense pair description if it was not entered previously and, upon clicking *OK* the sensor-defense pair is added to the list.



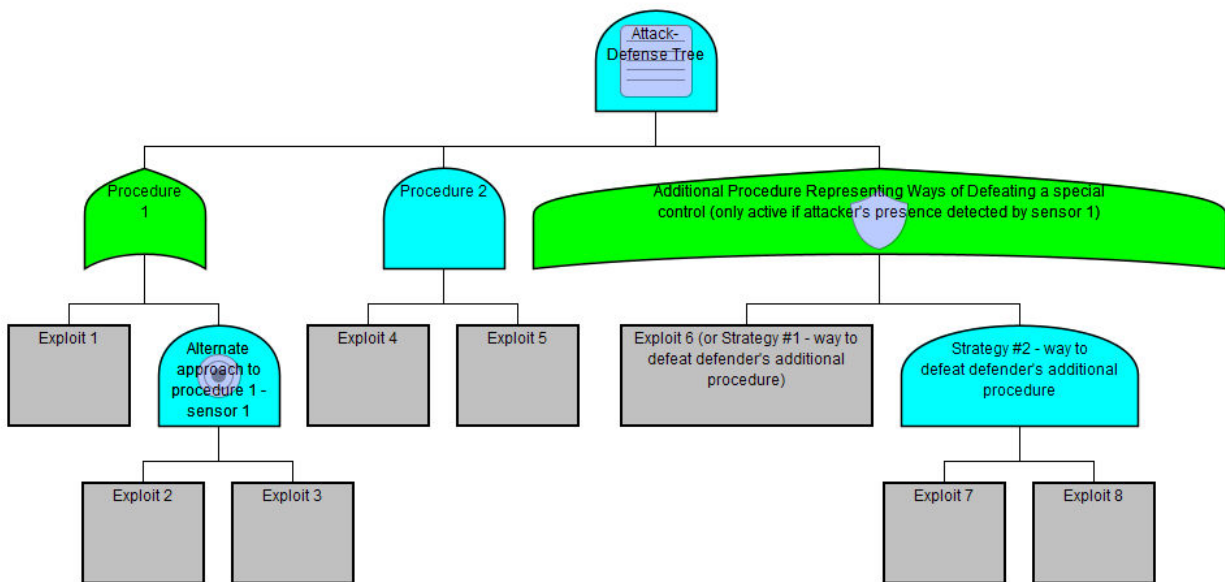
**Figure 4** - Defense subtree selection

The user then completes the creation of the sensor-pair definition in the A-D List node by clicking *OK* (**Figure 5**).



**Figure 5** - Completion of S-D pair

The completed A-D tree now appears (**Figure 6**).



**Figure 6** - Completed Attack-Defense tree

The following are the attack scenarios (**Figure 7**).

Row (of 4)	Scenario	Scenario Type	Attack Scenario
1	1	C	{Exploit 1, Exploit 4, Exploit 5, Exploit 6 (or Strategy #1 - way to defeat defender's additional procedure)}
2	2	C	{Exploit 1, Exploit 4, Exploit 5, Exploit 7, Exploit 8}
3	3	C	{Exploit 2, Exploit 3, Exploit 4, Exploit 5, Exploit 6 (or Strategy #1 - way to defeat defender's additional procedure)}
4	4	C	{Exploit 2, Exploit 3, Exploit 4, Exploit 5, Exploit 7, Exploit 8}

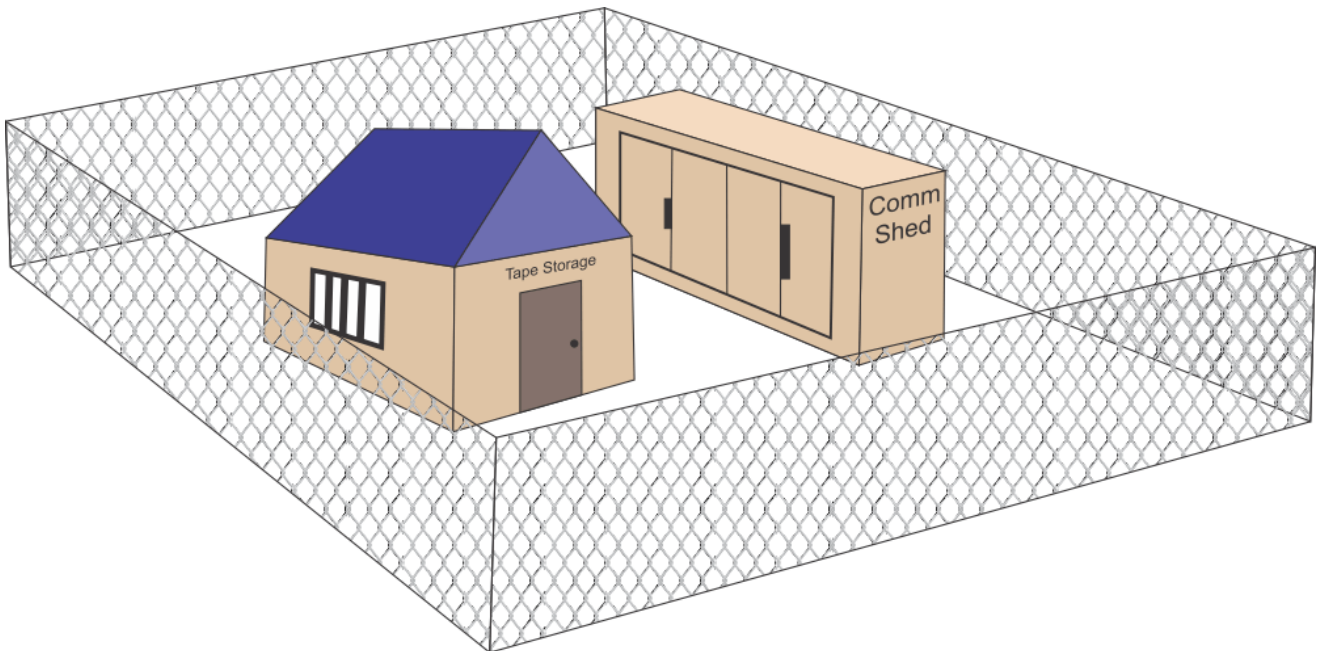
**Figure 7** - Attack scenario list for A-D tree

## Subtree Links and Attack Graphs

Even a cursory review of academic material on attack trees will reveal another, similar construct called *attack graphs*. Some researchers feel that attack graphs remove some of the limitations inherent in attack trees. So, if attack graphs are superior, why doesn't **SecurITree** do attack graph analysis? Or, does it?

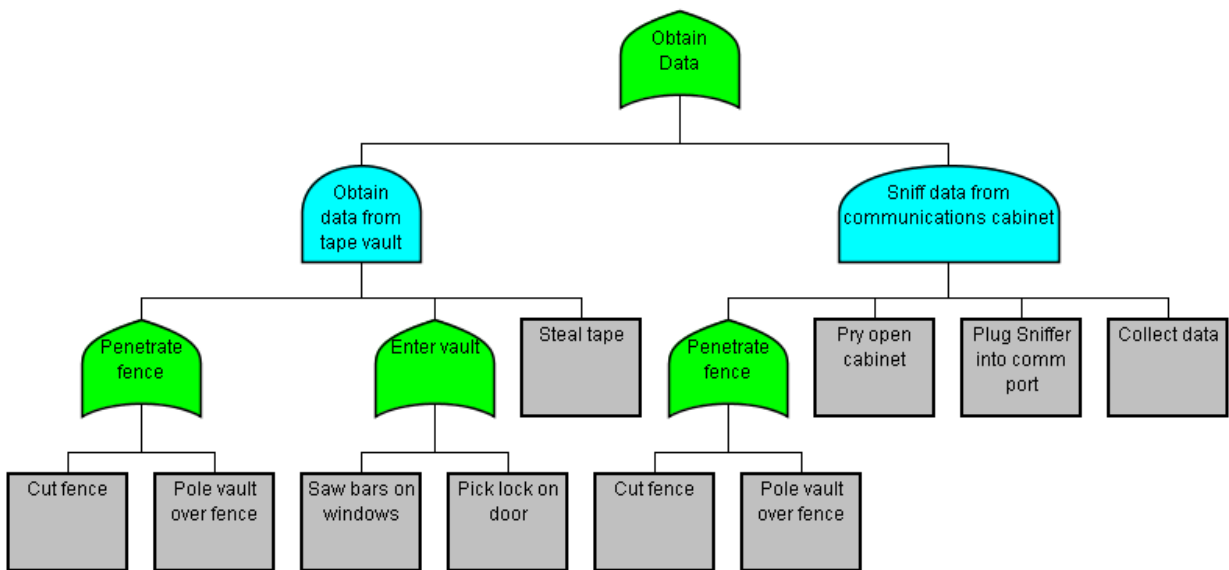
Part of the challenge in comparing attack trees to attack graphs is that there is no universally agreed upon definition of either term. However, the ambiguity seems particularly pronounced in the area of attack graphs. It does seem universally agreed that attack trees are hierarchical in nature (each node has exactly one parent) whereas attack graphs are not (a given node may have multiple parents).

One valid complaint about attack trees is that even simple situations can require very verbose trees, with significant duplication. Consider the following example.



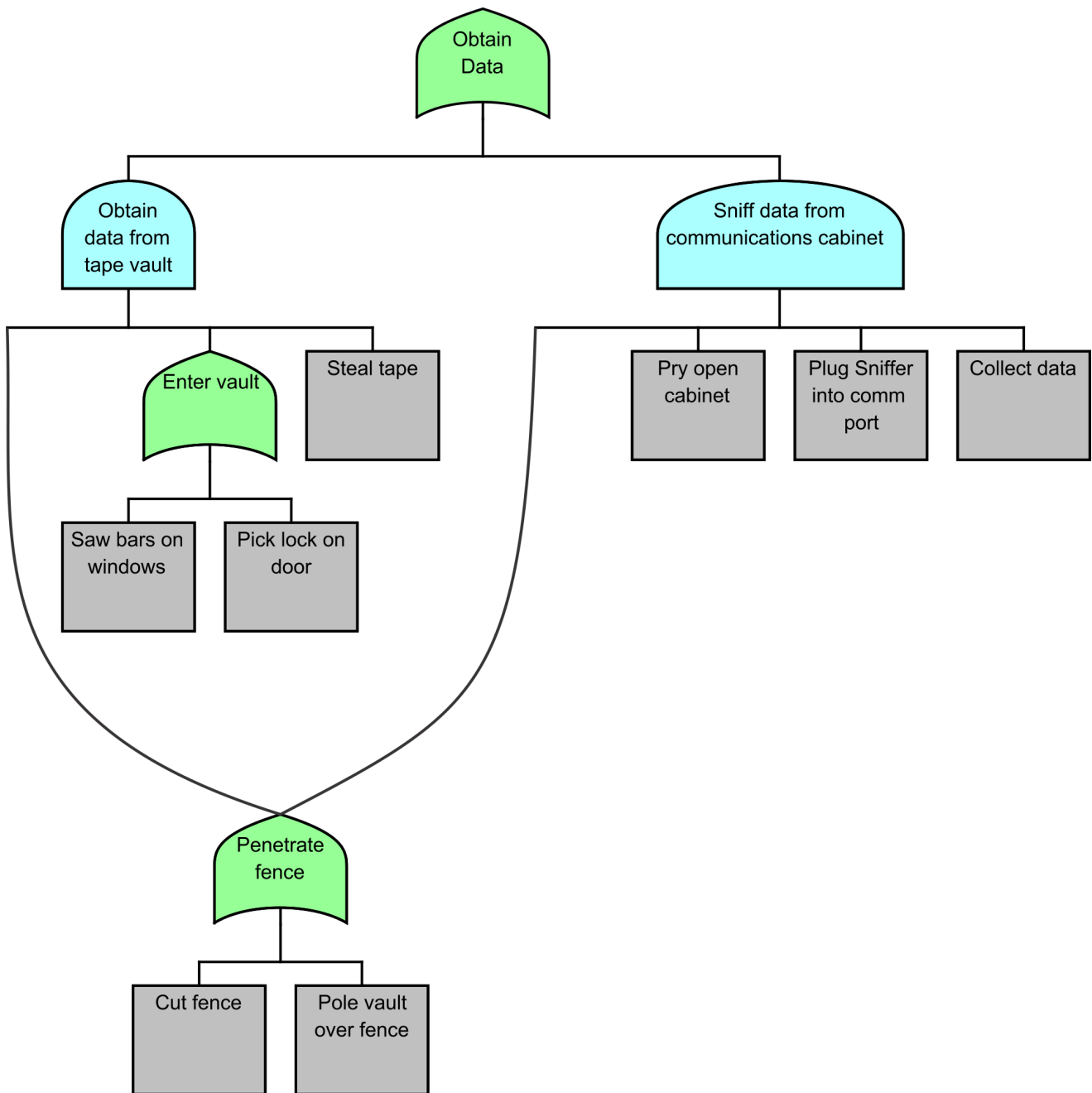
A certain facility contains data that is of interest to an attacker (see figure 1). There are (in this very simple example) two ways for the attacker to obtain the desired data. They could enter a tape storage vault and steal a backup tape containing the data. Alternately, they could break into a communications cabinet and plug a cable into a communications device to collect the data by eavesdropping. The facility is surrounded by a chain link fence.





An attack tree representing the possible attack scenarios is shown in figure 2. Notice that, whether the attacker decides to steal a tape, or to collect the data through communications eavesdropping, the initial steps of the attack (*Penetrate fence*) are the same. This requires that the *Penetrate fence* subtree be duplicated in the attack tree.

Figure 3 shows an alternate, attack graph representation. Notice how the duplication of the *Penetrate fence* subtree has been eliminated. In this simple situation, there wasn't much difference in the size of the diagrams, but in other cases the duplication might be many times greater, making the attack tree appear much larger!



However, moving to an attack graph representation introduces another problem that may not be immediately obvious. In this simple example, there was only one subtree that had multiple parents. In a more general case, there might be many different subtrees that all had multiple parents. Drawing such complex situations can be very complicated. In general, either the lines connecting the subtrees to their parents have to cross, or the lines must follow very circuitous paths to avoid crossing (and even that may not always be possible). Rather than providing visual simplification, the attack graph representation may actually make the situation worse!

**SecurITree** offers an alternative (that is admittedly a compromise). **SecurITree** allows analysts to create *links*. *Links* allow a given subtree to be the child of multiple parents. Editing any one of the

subtrees causes all instances of the subtree to be simultaneously updated. This happens because, internally, the data structures inside **SecurITree** are representing the linked subtree as an attack graph. However, the visual representation is rendered as an attack tree (for clarity). Analysis is performed on the equivalent attack tree structure.

In **SecurITree** there are two types of links: *normal* links and *identical* links. *Normal* links (or simply, *links*) are used to represent subtrees whose steps are identical, but whose goal takes you to different logical states. For instance, if the tape vault and communications cabinet in the previous example were in separate locations, and surrounded by similar (but different) chain link fences, then a *normal* link would be used. In the case above, both the vault and the cabinet are surrounded by the exact same fence, so an *identical* link would be the correct choice. When *identical* links are used, the underlying representation and interpretation of the model is essentially that of an attack graph.

## Notes

When you *Add* a new node or *Edit* an existing node on a threat tree you will notice there is a section on both of these windows for *Notes*. There is also a section for Notes on the [Node Information](#) side panel.

Notes are used to add information to your threat tree which helps users describe different aspects of the tree, its nodes, and its indicators. In this way you can provide detailed documentation for your threat trees as well as adding useful insight into how and why your trees have been built in a particular way.

The **Note Type** can be selected by clicking on the tab for the note type (located just above the **Notes** area). There are three default note types: *Node*, *Subtree* and *Exploits*. You can add your own custom note types by selecting **Edit > Note Types**.

Below the **Note Type** tabs is the **Notes** field. This is where you write the text for a particular **Note Type**. Once you have added text in the **Notes** field for a **Note Type**, an asterisk (\*) will appear to the right of that **Note Type** on the tab. In this way you can easily see which note types have text associated with them.

Spell checking is performed while you enter the note data. You can also check the spelling for the entire selected note area by clicking "Check Spelling". Changes to the note can be undone by clicking Undo or <ctrl>z and can be redone by clicking Redo or <ctrl>y.

### Bubble Notes

Notes for a node can be displayed on the tree by using "Bubble Notes". To use this feature, Bubbles must first be defined for the tree, then the Bubble must be enabled for the nodes where required, then the Bubble must be displayed. Here is how to do this:

- Define:

Choose **Tools > Preferences**, then select the **Node Info** tab. In the "Notes to Display in Bubble" section, check all notes that should be included in the bubble.

- Enable:

Edit the node where a Bubble should be displayed. Near the top of the window, check "Enable Bubble".

- Display:

Edit the node where a Bubble should be displayed. Near the top of the window, check "Display Bubble". Or, click on the bubble symbol found on the bottom right corner of the node.

All Bubbles that have been enabled for nodes on the tree can be shown or hidden by using the Toolbar icons or in **Tools > Preferences** select **Node Info** tab, then in the "Notes to Display in Bubble" section, click Show or Hide. Or use View > Show all enabled bubbles / View > Hide all enabled bubbles from the application menu.

## Flags

Sometimes it is useful to set a visual indicator on a node. For instance, you may want to be able to tell at a glance which nodes are edited by a particular person, deal with a particular issue, or have been edited. **SecurITree** provides six visual markers (known as flags) for this purpose. Depending on how flags are configured, they may appear under explicit user control or automatically when certain events (such as editing) occurs. When a flag is set it appears as a small colored flag directly beneath the node.

**Flags** can be created by selecting **Tools > Preferences** from the application menu, then choosing the [Flags](#) tab.

## Side Panels

The main application screen has two side panels. The left side panel contains [Node Information](#). The right side panel displays [Tree Information](#). The **Tools > Panels > Show Node Information Panel** and **Tools > Panels > Show Tree Information Panel** commands allow you to hide or display the side panels as you desire.

## Node Information

The *Node Information Panel* contains information on the currently selected node. The node can be edited by clicking on the Add, Edit or Delete buttons on this panel. See "[Using Nodes](#)" for more information.

The *Note Type* that is displayed for the selected node can be changed by selecting the tab for the note type. See [Notes](#) for more information.

This panel can be shown or hidden by clicking **Tools > Panels > Show Node Information Panel** or by pressing **Ctrl-I** or by clicking the **Show Node Information Panel** icon on the toolbar.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".



## Tree Information

The *Tree Information Panel* contains:

- A legend describing the node types on trees.
- A list of the indicator functions for the current tree.

The indicator functions can be edited by clicking on the **Set Indicators** button on this panel. See "[Using Indicators](#)" for more information.

This panel can be shown or hidden by clicking **Tools > Panels > Show Tree Information Panel** or by pressing **Ctrl-T** or by clicking the **Show Tree Information Panel** icon on the toolbar.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".

## Toolbars

[Main Toolbar](#)

[Pruning Trees Toolbar](#)

[Set Operations on Pruned Trees Toolbar](#)

[Attack Scenarios Toolbar](#)

[Advanced Analysis Toolbar](#)

## Main Toolbar

The following icons are located on the **Main Toolbar**:



[New Tree](#)



[Open Tree](#)



[Save Tree](#)



[Save Tree As](#)



[Print](#)



[Undo](#)



[Redo](#)



[Cut](#)



[Copy](#)



[Paste](#)



[Paste as Link](#)























[Paste as Identical Link](#)



[Paste as Ganged Link](#)



[Break Link](#)

-  [Add to Scratchpad](#)
-  [Show Scratchpad](#)
-  [Show Node Information Panel](#)
-  [Show Tree Information Panel](#)
-  [Show Thumbnail of Tree](#)
-  [Find](#)
-  [Zoom In](#)
-  [Zoom Out](#)
-  [Zoom to Fit](#)
-  [Help \(Help Index\)](#)
-  [Add Node](#)
-  [Edit Node](#)
-  [Delete Node](#)
-  [Auto Size Node](#)
-  [Auto Calculate](#)
-  [Attack Scenarios](#)
-  [Pruning Tree](#)
-  [Advanced Analysis](#)
-  [Analyze Subtree](#)
-  [Show all enabled bubbles](#)



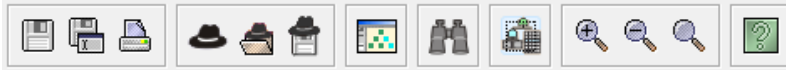
[Hide all enabled bubbles](#)



[Plugin](#)

## Pruning Trees Toolbar

The following icons are located on the **Pruning Trees Toolbar**:



[Save Tree](#)



[Save Tree As](#)



[Print](#)



[Edit Agent Profile](#)



[Load Agent Profile](#)



[Save Agent Profile](#)



[Show Node Information Panel](#)



[Find](#)



[Attack Scenarios](#)



[Zoom In](#)



[Zoom Out](#)



[Zoom to Fit](#)



[Help \(Help Index\)](#)

## Set Operations on Pruned Trees Toolbar

The following icons are located on the **Set Operations on Pruned Trees Toolbar**:



[Save Tree](#)



[Save Tree As](#)



[Print](#)



[Show Node Information Panel](#)



[Find](#)



[Sort](#)



[Zoom In](#)



[Zoom Out](#)



[Zoom to Fit](#)



[Help \(Help Index\)](#)

## Attack Scenarios Toolbar

The following icons are located on the **Attack Scenarios Toolbar**:



[Save Tree](#)



[Save Tree As](#)



[Print](#)



[Show Node Information Panel](#)



[Find](#)



[Sort](#)



[Filter Scenarios](#)



[Zoom In](#)



[Zoom Out](#)



[Zoom to Fit](#)



[Help \(Help Index\)](#)



## Advanced Analysis Toolbar

The following icons are located on the **Advanced Analysis Toolbar**:



[Save Tree](#)



[Save Tree As](#)



[Print](#)



[Define Indicator Curves](#)



[Machine Learning](#)



[Similarities](#)



[Show Node Information Panel](#)



[Show Charts Panel](#)



[Find](#)



[Sort](#)



[Filter Scenarios](#)



[Zoom In](#)



[Zoom Out](#)



[Zoom to Fit](#)



[Help \(Help Index\)](#)

## Memory Errors

A memory error can occur while working on very large attack trees in SecurITree. If you receive the error message:

"Operation caused an Out of Memory condition"

It is probably necessary to increase the amount of memory available to the SecurITree application.

To do this:

- Locate the file SecurITree.ini in the directory where SecurITree was installed.
- Make a backup copy of this file.
- Edit SecurITree.ini
  - o Find the parameter: Virtual Machine Parameters=-Xms128m -Xmx512m (these values may be different than displayed here).
  - o Increase the values to the desired values.
  - o Do not exceed the memory available on your computer or SecurITree will not execute.
  - o If this parameter does not exist in the file, it can be added.
  - o Note 1: -Xms specifies the minimum heap size, -Xmx specifies the maximum heap size.
  - o Note 2: The m suffix may be replaced by g to measure in gigabytes, e.g., -Xms1g -Xmx1g
  - o Note 3: Setting these parameters to the same value avoids being conservative, and will often improve startup time.

Instructions for changing memory size for OS X:

- Go to the SecurITree directory (default:/Applications/Amenaza/SecurITree).
- Right click on the SecurITree application, and click on 'Show Package Contents'.
- Double click on the Contents folder.
- Double click on the Info.plist file.
- Click on the black triangle next to the 'Root' property list, to show sub folders. Do the same with the triangle next to the 'Java' property list. Do the same to the triangle next to VMOptions under the Java node.
- You will see two String values: - Xms2M and -Xmx64M (the numbers might vary). These represent the minimum and maximum amount of memory dedicated to the Java Virtual Machine. Change these according to the guidelines specified above.

- When you are finished, hit Cmd-S to save the file, and exit.

If you require assistance with this change, please contact Amenaza Technical Support at:

1-888-949-9797 or (403) 263-7737 or  
[http://www.amenaza.com/request\\_support.php](http://www.amenaza.com/request_support.php) or  
[support@amenaza.com](mailto:support@amenaza.com)

## Language and Number Format

The language to use for displaying the menus and messages for **SecurITree** can be set. See Language for more information.

The current choices for Language are:

en - English  
 fr - French (Français)  
 de - German (Deutsch)

The format for displaying numbers can also be set. This usually corresponds to the language that has been selected.

This is the format for numbers:

Country Code		Format
US or CA	North American	1,234,567.89
FR	France	1 234 567,89
DE	Germany	1.234.567,89

It is possible to display numbers in a format that does not correspond to the language. In order to do this, you must edit the file "SecurITree\_locale.properties" which can be found in your home directory.

For example, to set the language to English and numbers to be displayed in the German format, these two lines should be in the "SecurITree\_locale.properties" file:

```
LANGUAGE=en
COUNTRY=DE
```

NOTE 1: The language must be lowercase and the country must be uppercase.

NOTE 2: If the Language is changed using the Language menu, the default country (and, therefore, number format) will be set. You must exit **SecurITree**, edit the "SecurITree\_locale.properties" file, then restart **SecurITree** if you need to use settings other than the default.

The "SecurITree\_locale.properties" file normally does not need to be edited. This is only necessary under special circumstances.

## Regular Expressions

Sources for more information on regular expressions include: <https://www.regular-expressions.info/>

or: <https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html>

Excerpt from javadocs:

### Summary of regular-expression constructs

Construct	Matches
<b>Characters</b>	
x	The character x
\\	The backslash character
\\0n	The character with octal value 0n (0 <= n <= 7)
\\uhhhh	The character with hexadecimal value 0xhhhh
\\t	The tab character ('\\u0009')
\\n	The newline (line feed) character ('\\u000A')
\\r	The carriage-return character ('\\u000D')
\\f	The form-feed character ('\\u000C')
\\a	The alert (bell) character ('\\u0007')
\\e	The escape character ('\\u001B')
\\cx	The control character corresponding to x
<b>Character classes</b>	
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)

[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z](subtraction)
<b>Predefined character classes</b>	
.	Any character (may or may not match line terminators)
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\h	A horizontal whitespace character: [ \t\xA0\u1680\u180e\u2000-\u200a\u202f\u205f\u3000]
\H	A non-horizontal whitespace character: [^\h]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\v	A vertical whitespace character: [\n\x0B\f\r\x85\u2028\u2029]
\V	A non-vertical whitespace character: [^\v]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]
<b>POSIX character classes (US-ASCII only)</b>	
\p{Lower}	A lower-case alphabetic character: [a-z]
\p{Upper}	An upper-case alphabetic character:[A-Z]

\p{ASCII}	All ASCII:[\x00-\x7F]
\p{Alpha}	An alphabetic character:[\p{Lower}\p{Upper}]
\p{Digit}	A decimal digit: [0-9]
\p{Alnum}	An alphanumeric character:[\p{Alpha}\p{Digit}]
\p{Punct}	Punctuation: One of !"#\$%&'()*+,-./:;<=>?@[\\^_`{ }~
\p{Graph}	A visible character: [\p{Alnum}\p{Punct}]
\p{Print}	A printable character: [\p{Graph}\x20]
\p{Blank}	A space or a tab: [ \t]
\p{Cntrl}	A control character: [\x00-\x1F\x7F]
\p{XDigit}	A hexadecimal digit: [0-9a-fA-F]
\p{Space}	A whitespace character: [ \t\n\x0B\f\r]
\p{Sc}	A currency symbol
<b>Boundary matchers</b>	
^	The beginning of a line
\$	The end of a line
\b	A word boundary
\B	A non-word boundary
\A	The beginning of the input
\G	The end of the previous match
\Z	The end of the input but for the final terminator, if any
\z	The end of the input

\R	Any Unicode linebreak sequence, is equivalent to [\u000D\u000A [\u000A\u000B\u000C\u000D\u0085\u2028\u2029]
<b>Quantifiers</b>	
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times
<b>Logical operators</b>	
XY	X followed by Y
X Y	Either X or Y
(X)	X, as a capturing group
<b>Quotation</b>	
\	Nothing, but quotes the following character
\Q	Nothing, but quotes all characters until \E
\E	Nothing, but ends quoting started by \Q

One source for more information on regular expressions: <http://www.regular-expressions.info/>



## Main Menu

**SecurITree** has the following Menu:

[File](#)

[Edit](#)

[View](#)

[Analyze](#)

[Tools](#)

[Window](#)

[Help](#)

## File Menu

The following options are available under the **File** menu:

- [New Tree...](#)
- [New Tree From Template...](#)
- [Open Tree...](#)
- [Open Library...](#)
- [Insert Tree...](#)
- [Insert Library...](#)
- [Insert External...](#)
- [Reload External](#)
- [Save Tree](#)
- [Save Tree As...](#)
- [Save Subtree...](#)
- [Save Sanitized Tree](#)
- [Sanitize Subtree](#)
- [Sign Tree](#)
- [Close](#)
- Reports
  - [Basic Reports](#)
  - [Advanced Reports](#)
- [Print Tree...](#)
- [Page Layout](#)
- [Tree Properties](#)
- [Node Properties](#)
- Open Recent
- [Exit](#)

## New Tree...

This command is used to create a new Attack (Threat) Tree:

1. Select the **File > New Tree...** command from the application menu, or click on the **New Tree** icon on the [toolbar](#).
2. You will be asked to enter a name for your new Attack (Threat) Tree, this will be the root node. Nodes can now be added to the tree.

## New Tree from Template...

This command is used to create a new Attack (Threat) Tree using a previously created tree as a template. These attributes will be copied from the template tree to the new tree:

- Indicator functions
- Note types
- Flags
- Watermarks
- Print settings

1. Select the **File > New Tree from Template...** command from the application menu.
2. You will be asked to enter a name for your new Attack (Threat) Tree, this will be the name of the root node.
3. Now you must choose the file to use as the template file. Select the file then click on *Open*.
4. Nodes can now be added to the tree.

## Open Tree...

This command is used to open an existing Attack (Threat) Tree file. By default, Attack Tree files are located in a sub-directory called "Data" which is created automatically in the directory where you installed **SecurITree**. This default will change automatically to the directory where you last opened or saved a tree if it is different from the default location.

1. Select the **File > Open Tree...** command from the application menu, or click on the **Open Tree** icon on the [toolbar](#).
2. Select the .rit file that you want to open and it will appear in the *File name:* window. Then click on the *Open* button to open the file. Alternatively, double click on the file name and the file will open.

### **NOTE:**

You may receive the following message while opening a file:

*A checkpoint file was found. Do you want to use this file?*

A checkpoint file is created when a file is opened in order to automatically save changes (every 10 minutes) in case the program is exited abnormally and the file that was being worked on was not saved properly.

Therefore, you may want to use the checkpoint file as it will probably contain information that was not saved in the original file. If so, click on the *Yes* button. If you determine that you do not want to use this file and want to revert back to the original file, simply **Close** the file and when asked *Do you want to save the tree?*, click on the *No* button. Now you can open the original file.

If a checkpoint file is found but you want to use the original file, click on the *No* button.

## Open Library...

This command is used to open an existing Attack (Threat) Tree library file. By default, Attack Tree library files are located in a sub-directory called "Library" which is created automatically in the directory where you installed **SecurITree**. This default will change automatically to the directory where you last opened or saved a library tree if it is different from the default location.

1. Select the **File > Open Library...** command from the application menu.
2. Select the .ril file that you want to open and it will appear in the *File name:* window. Then click on the *Open* button to open the file. Alternatively, double click on the file name and the file will open.
3. The working filename will be changed to <filename>.rit to minimize the chances of overwriting the library file. The first time you try to save the file, you will be automatically given the default sub-directory "Data" and be given the chance to enter a new name for the file with the default extension .rit.

See [Libraries vs. Trees](#) for more information.

## Insert Tree...

The **Insert Tree** command is used to insert an existing Attack (Threat) Tree file into the active Attack Tree you are currently working on.

1. Select the node that you want to use as the insertion point by clicking on the node.
2. Use the **File > Insert Tree...** command from the application menu or right-click the selected node and choose **Insert Tree...** from the pop-up menu.
3. If the *Parent Node Change* dialog box appears, this means that the node you are inserting on is a *LEAF* node and it must be changed to an *AND* or *OR* node. You must select the node type for the parent node, either *AND* or *OR*.
4. You will get the **Open** dialog box. You will be positioned at your default "Data" directory. Select the file to be inserted, then click on the *Open* button to select the file. Alternatively, double click on the file name and the file will be selected.
5. The tree to be inserted is checked to make sure the indicator functions it contains match the indicator functions in the base tree. If the tree does not have an indicator that is in the base tree, you will get the *Enter Default Node Value* dialog box and will have the opportunity to enter a default value for the nodes in the tree.
6. If a default value is entered, it is only applied to the leaf nodes in the tree that is being inserted. If a default value is not entered, you will have to enter a value for each leaf node in the tree after it has been added to the base tree. The tree cannot be calculated until every leaf node has a value for every indicator.
7. If the tree contains an indicator that is not in the base tree, the *Enter Default Node Value* dialog box will ask if the indicator should be added to the base tree and a default value should be set for all leaf nodes. If you select *No*, the values for the indicator that were in the nodes in the tree will be lost. The original tree file will not be altered.
8. The selected Attack Tree is then added at the node you have selected.

## Insert Library...

The **Insert Library** command is used to insert an existing Attack (Threat) Tree library file into the active Threat Tree you are currently working on.

1. Select the node that you want to use as the insertion point by clicking on the node.
2. Use the **File > Insert Library...** command from the application menu or right-click the selected node and choose **Insert Library...** from the pop-up menu.
3. If the *Parent Node Change* dialog box appears, this means that the node you are inserting on is a *LEAF* node and it must be changed to an *AND* or *OR* node. You must select the node type for the parent node, either *AND* or *OR*.
4. You will get the **Open** dialog box. You will be positioned at your default "Library" directory. Select the file to be inserted, then click on the *Open* button to select the file. Alternatively, double click on the file name and the file will be selected.
5. The library to be inserted is checked to make sure the indicator functions it contains match the indicator functions in the base tree. If the library does not have an indicator that is in the base tree, you will get the *Enter Default Node Value* dialog box and will have the opportunity to enter a default value for the nodes in the tree.
6. If a default value is entered, it is only applied to the leaf nodes in the library that is being inserted. If a default value is not entered, you will have to enter a value for each leaf node in the tree after it has been added to the base tree. The tree cannot be calculated until every leaf node has a value for every indicator.
7. If the library contains an indicator that is not in the base tree, the *Enter Default Node Value* dialog box will ask if the indicator should be added to the base tree and a default value should be set for all leaf nodes. If you select *No*, the values for the indicator that were in the nodes in the tree will be lost. The original tree file will not be altered.
8. The selected Attack Tree library is then added at the node you have selected.



## Insert External...

The **Insert External** command is used to insert an existing Attack (Threat) Tree file into the active Attack Tree you are currently working on. It is similar to the **Insert Tree** and **Insert Library** facility with an important difference - a copy of the externally linked subtree is stored in the active attack tree along with a reference to the external subtree it was copied from. The external subtree is graphically depicted in the tree by nodes outlined in red (instead of black).

Every time the tree is opened, the external subtrees are checked. If an externally linked tree has been modified, you will be given the option to update the copy that is saved in your attack tree.

You cannot make any changes to nodes within the external subtree. If you attempt to modify a node in an external subtree, you will be given the option to make the subtree internal to the current tree it is in, then the nodes may be updated. You can make changes to externally linked trees. The only way to do this is to edit the tree in the external file. The next time you open a tree that contains that external link, you will have the option to bring it up-to-date or convert the nodes to internal nodes on the tree.

1. Select the node that you want to use as the insertion point by clicking on the node.
2. Use the **File > Insert External...** command from the application menu or right-click the selected node and choose **Insert External...** from the pop-up menu.
3. If the *Parent Node Change* dialog box appears, this means that the node you are inserting on is a *LEAF* node and it must be changed to an *AND* or *OR* node. You must select the node type for the parent node; either *AND* or *OR*.
4. There are two choices for the way an external link can be added to your tree. Either:
  - an absolute path name can be used - which means the file to be inserted will always be found in the directory that is selected, or
  - the `EXTTREETPATH` can be used to find the filename specified. With this option, the `EXTTREETPATH` is searched until the filename is found. The file can move from one directory to another within the `EXTTREETPATH` and still be found. It is important to remember the file is used from the directory in the path where it first occurs. Please see `Tools > Preferences > Interface > Path for Externally Linked Trees` for information on updating the path.
5. You will get the **Open** dialog box. If *absolute path name* was selected, you will be positioned at your default "Data" directory. If *Use EXTTREETPATH* was selected, you will be given a list of all available filenames found in all directories on the path. Select the file to be inserted, then

click on the *Open* button to select the file. Alternatively, double click on the file name and the file will be selected.

6. The tree to be inserted is checked to make sure the indicator functions it contains match the indicator functions in the base tree. If the tree does not have an indicator that is in the base tree, you will not be allowed to insert this tree as an externally linked tree.
7. If the tree contains an indicator that is not in the base tree, the *Enter Default Node Value* dialog box will ask if the indicator should be added to the base tree and a default value should be set for all leaf nodes. If a default value is entered, it is only applied to the leaf nodes in the base tree. If you select *No*, the values for the indicator that were in the nodes in the tree will be lost. The original tree file will not be altered.
8. The selected Attack Tree is then added as an internal link at the node you have selected.

## Reload External

The **Reload External** command is used to update any existing external links that are currently in the active Attack Tree you are working on. It is used if an externally linked has been changed after you have opened the current attack tree. If an externally linked tree has been modified, you will be given the option to update the copy that is saved in your attack tree.

See [Insert External...](#) for further information on External links.

1. Use the **File > Reload External** command from the application menu to reload any external files that have changed.

## Save Tree

Use the **File > Save Tree** command to save your file to disk. It is recommended that files be saved on a regular basis during a **SecurITree** session and especially after significant changes have been made.

1. Select the **File > Save Tree** command from the application menu, or click on the **Save Tree** icon on the [toolbar](#).
2. If this is a new Attack (Threat) Tree that was not previously saved, the **Save** dialog box will be displayed. Select the folder you want to save the file in, type in a name for this file and click on the *Save* button.
3. If this tree was previously saved or was opened from disk, it will automatically be saved using the same filename.

## Save Tree As...

Use the **File > Save Tree As...** command to save your file to disk with a new name. It is recommended that files be saved on a regular basis during a **SecurITree** session, and especially after significant changes have been made.

1. Select the **File > Save Tree As...** command from the application menu, or click on the **Save Tree As** icon on the [toolbar](#).
2. The [Save](#) dialog box will be displayed. Select the folder you want to save the file in, enter a new file name if required, and click on the *Save* button to save your file with a new name.
3. Files can also be saved in different formats. If you would like to save the tree as you see it on the screen as an image file, you can choose either PNG, JPG, or SVG format. The *Files of type:* field has a pull-down list. If you choose *PNG Files (\*.png)*, *JPG Files (\*.jpg)*, or *SVG Files (\*.svg)* your tree will be saved as an image. You should use a matching extension in the *File name:* field or do not specify an extension and the correct extension will be added for you.

This command allows you to *Save Attack (Threat) Tree* files into the following file formats:

File Types	Format / Purpose
.rit	to save the file with a new name (similar to using <b>File &gt; Save As...</b> )
.ril	to save the file as a <b>SecurITree</b> library
.png	to save the file as a Portable Network Graphics image
.jpg	to save the file as a JPEG (Joint Photographic Experts Group) image
.svg	to save the file as an SVG (Scalable Vector Graphics) image
.atml	to save the file in Attack Tree Markup Language - xml format
.gxl	to save the file in Graph eXchange Language

## Save Subtree...

To save part of an Attack (Threat) Tree in the main window as a separate file, use the **File > Save Subtree...** command.

1. Select the Root (topmost) Node of the tree that you want to save.
2. Select the **File > Save Subtree...** command from the application menu.
3. The [Save](#) dialog box will be displayed. Select the folder you want to save the file in. Make sure that you enter a new filename so that you do not overwrite your current file. Click on the *Save* button to save your file with a new name.

## Save Sanitized Tree

The File > Save Sanitized Tree command will take a copy of your tree, "sanitize" it, then save your tree to the file name you specify. The reason for doing this is so that a tree containing sensitive or confidential data can be sent to Amenaza for support purposes, or to any other party, and the sensitive data will not be disclosed.

To "sanitize" the tree;

1. The indicator names will be changed.
2. Indicator notes will be removed.
3. Node names will be changed.
4. Node notes will be removed.

1. Select the **File > Save Sanitized Tree** command from the application menu.
2. The **Save** dialog box will be displayed. Select the folder you want to save the file in, type in a name for this file and click on the *Save* button.
3. The file can now be shared safely.

## Sanitize Subtree

To sanitize a portion of an Attack Tree, use the **File > Sanitize Subtree** command.

1. Select the Root (topmost) node of the subtree you want to sanitize.
2. Select the **File > Sanitize Subtree** command from the application menu.
3. All nodes at the selected node and below will now be sanitized.



## Sign Tree

This feature can only be used with a special "Tree Signing" license. It is used to digitally sign a tree and save it to disk. The signed tree file can then be opened when using a Demo license with a public key matching the signing license.

1. Select the **File > Sign Tree** command from the application menu.
2. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name, and click on the *Save* button to save your file with a digital signature.

## Close

This command is used to **Close** the active Attack (Threat) Tree file. If the Attack Tree file has changes that have not been saved, you will be asked if you want to save them before closing the file.

## Basic Reports

The **File > Reports > Basic Reports** command allows you to view the Attack (Threat) Tree you are working on in a tabular format. The following Reports are available:

- **All Nodes** - All nodes on the tree are displayed in the report.
- **Only Leaf Nodes** - Only LEAF nodes are included in the report.
- **Complete Node Information** - All indicator values and notes are included in the report.
- **Complete Node Information - LEAF nodes only** - All indicator values and notes are included in the report.
- **Complete Node Information + Scenarios per Node** - The number of times the node occurs in scenarios is calculated and included in the report. Clicking on a node in the table will display a table showing all scenarios where this node is found. Clicking on a scenario will show the tree for the scenario.
- **Attack Scenarios** - A listing of all Attack Scenarios. This report is only available in an Attack Scenario window or in an Advanced Analysis window.
- **Agent Profile Cross-Reference** - This report is only available if pruning windows have been created. The report indicates which agent profiles are capable of performing an attack by placing an "X" under the appropriate pruning window name. If a node was removed from a tree during pruning operations, it will not have an "X" in that column.
- **Pruning Sensitivity** - This report is only available in a pruning window if the node-based method of pruning was used. The report provides a list of all pruning criteria and whether or not nodes were eliminated from the tree. If a node was removed on a particular pruning criterion, an "X" is placed in the column. The total number of criteria that caused the node to be pruned (removed) is also displayed.

The delta column for each pruning criteria is colored. This is the explanation of the color coding:

- Pink/(Red) represent attacks that are within/(well within) the capability of the threat agent.
- Light Yellow/(Dark Yellow) represent attacks that are nearly within/(just within) the capability of the threat agent.
- Light Green/(Green) represent attacks beyond/(well beyond) the capability of the threat agent.
- Numeric indicator values express the resources required to carry out the attack.
- # indicator values show the resources available to the attacker minus resources required to carry out the attack.
- Negative values indicate the attacker had a shortfall of the resources required for the attack.

This report provides a useful guide of the confidence level of the analysis. In general, a higher number of criteria used to eliminate an attack indicates a stronger assurance that an attack is

beyond the capabilities of an attacker. In other words, it would be necessary for the analyst to misjudge the capabilities of the attacker in multiple ways for the result to be incorrect.

- **Scenario Sensitivity** - This report is only available in a pruning window if the scenario based method of pruning was used. This report shows if an attack scenario was removed based on the pruning criterion. See the Pruning Sensitivity report for more information on the usage of this report.
- **Advanced Analysis** - The Advanced Analysis table. This report is only available in an Advanced Analysis window.
- **Potential Choke Points** - This report has information for each node in the tree. Each time a node is found in an attack scenario, the value for these columns in the attack scenario are accumulated; Capabilistic Propensity, Impact, Relative Risk and Cumulative Risk. This can be used to determine which nodes in the tree contribute the greatest risk or impact. This report is only available in an Advanced Analysis window.

The first two reports can be saved to a file. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for these report files is .txt.

The reports in table format can also be saved. This option can be used to save the tree information to a file in a format so it can be used in a spreadsheet program such as Microsoft Excel. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. Now you will get the *Report Setup* dialog. You must choose either CSV Format (comma separated values) or Delimited Format. If you choose Delimited, you must now choose a character from the pull-down list that will be used to delimit the fields in the node information. If the character that was chosen is found in the text of the node information, you will receive the message: *Column delimiter was found in tree data. File will not be properly delimited.* This means data that should be in one column will be split across more than one column in the spreadsheet. You must also decide if new line characters should be removed from the note areas. If these note areas contain *new line characters* and they are not removed, the note area will go to the next line in the spreadsheet.

3. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for report files in CSV Format is .csv and in Delimited Format is .rpt.
4. After the file has been saved, you can open it in a spreadsheet program. If you are using Excel, it is best to first start Excel then open the report file you created. This will cause the "Text Import Wizard" to start which will ask about the character that is used to delimit the data. Select "Delimited", then choose "Other" and enter the character that you used as a delimiter (the default is "|"). The data should now be in columns in the spreadsheet.

The reports **Attack Scenarios** and **Advanced Analysis** allow another save option. You can choose to save the tree image for each scenario (from the specified start row through the specified end row) to a separate file. The directory where the files are saved defaults to the directory that was used to open this tree. You can specify a different directory by clicking on **Change**. The images are saved as png files with the name *scenarioXX.png* where XX is the scenario number (not the row number). If there is already a file by that name in the directory it will be overwritten.

All of the reports can be printed. To print a report:

1. Select the report format you want. Note, for reports in table format you may need to adjust the column dividers to ensure that the columns are the correct width for viewing as they are printed using WYSIWYG (what you see is what you get).
2. Click on **Page Layout** to set page margins, print orientation, and header and footer settings.
3. Click on the **Print...** button or select **File > Print...** from the menu on the *Reports* window.
4. Alternatively, if this is a table-type report, you can click on **Print Custom**. You will be given further options such as specifying the start and end row, and if the report should be shrunk to fit the page horizontally. If this is the Advanced Analysis table, the additional options to create a detailed report, include tree images and print the tree in black and white or color are also given.
5. A **Print Preview** window will show your report.
6. Click on **Print...** to send your report to the printer.

## Advanced Reports

### Risk Summary Reports

There are a number of graphical reports available in **SecurITree** to show the overall risk to a target system from multiple threats. These reports are available from the main **SecurITree** window under **File > Reports > Advanced Reports**. These reports differ from those available from the *Advanced Analysis* window (which focus on the risk from a single threat).

In theory, determining the total, overall risk to a target system requires that the analyst add the risk from every potential threat. This could be a formidable task since there may be no end to the complete set of threats to a system. Fortunately, a reasonable approximation can be made by examining only the most important threats.

Threats may be human threat agents, who are deliberately trying to attack a system. As long as the various threat agents are operating independently, the risk from each of the threat agents is added to produce an overall value. However, the caveat that the agents must be operating independently means it is not appropriate to combine the risk contributed by various "flavors" of the same adversary. For example, an analyst may have defined an *organized crime syndicate* type of threat agent. Two versions of this threat agent may exist, one with the capability of carrying out insider attacks and the other lacking that ability. Normally, only one of these threat agents can exist at a given time. Before producing a risk graph that displays or uses a total, overall risk value, **SecurITree** requires that the user confirm that all major threat agents have been identified and that they are operating independently. Random events, if relevant, also contribute to the total risk value and are included in the total.

### Cumulative Risk Graph

The *Cumulative Risk graph* shows the cumulative risk vs the number of scenarios with that level of risk for each adversary-target pair specified by the analyst. This allows easy comparison of the risk contributed by different adversaries and also demonstrates whether or not proposed controls are effective.

Each curve in the graph is similar to a histogram chart. A perfectly secure system would show a horizontal line superimposed over the x-axis, describing a system with no scenarios with non-zero risk. More typically, there will be a number of scenarios with a high level of risk. This is manifest by a spike close to the y-axis. The higher the spike, the worse the risk of the set of risky scenarios. The broader the spike, the more scenarios that must be dealt with to reduce the overall risk.

From a defender's point of view, a narrow, high spike generally represents an unacceptable situation, but one that is straightforward to resolve. The defender can focus on mitigating the risk associated with a small number of scenarios. On the other hand a wide, high pulse can be problematic because there may be a large number of high risk attack vectors. Unless an architectural solution can be found

wherein a small set of controls will mitigate the risk of a large number of high risk scenarios, the system may prove impossible to secure. This requires an architectural solution that, at the attack tree level, typically involves introducing an AND node with at least one child activity that is difficult for the adversary to perform. If the high risk scenarios are comprised of OR nodes, and no way can be found to introduce a blocking AND node, then it may be infeasible to secure the system.

## Relative Risk Graph

The *Relative Risk graph* is similar to the Cumulative Risk graph (above) except that the Relative risk values are used to create the report.

## Feasibility Graph

This graph shows the percentage of scenarios with more than a given Feasibility.

## Desirability Graph

This graph shows the percentage of scenarios with more than a given Desirability.

## Capabilistic Propensity Graph

This graph shows the percentage of scenarios with more than a given Capabilistic Propensity.

## Total Propensity Graph

This graph shows the percentage of scenarios with more than a given Total Propensity.

## Pain Factor Graph

This graph shows the percentage of scenarios with more than a given Pain Factor.

## Advanced Analysis Summary

A report with one tabular chart for each *alternative set* included in the analysis. The report highlights information extracted from the highest risk scenario for each threat agent.

## Pie Chart

One *pie chart* is displayed for each *alternative set* (which usually corresponds to real or proposed system configurations). The *pie* is divided into different areas showing the relative contribution of each *threat agent* and from random factors. Caution should be used in comparing one *pie chart* with another. Although the pies are visually the same size, they may represent quite different total amounts of risk.

The highest value used for the Segment Values is the Cumulative Risk value of the highest Total Propensity that is not a Probability scenario.

## Bar Chart

One *bar chart* is displayed for each *alternative set*. Each bar represents the risk contributed by a top risk scenario for a given adversary-target pair. The scale is the same for all of the charts so meaningful comparisons between them are possible and useful.

## Scatter Charts

Two *scatter charts* are displayed for each adversary-target pair, one related to *relative risk* and the other to *cumulative risk*. In both charts, the *x* axis indicates the *victim impact* and the *y* axis indicates *probability* or *frequency* respectively. Each attack scenario has a point plotted on the chart reflecting its *probability* (or *frequency*) and *impact*. Since the product of these two terms is *risk*, the level of risk can be read from the chart. For convenience in reading the charts, equi-risk contours are displayed.

Where a point appears on the scatter chart is important. For example, consider a *relative risk* scatter graph showing a point (A) with high probability and low impact. It may have exactly the same *relative risk* as a second point (B) that has low probability and high impact. In the case of point A, its corresponding scenario is almost certain **if there are any encounters between the adversary and the target**. Point B will happen rarely, but when it does it will have catastrophic consequences.

Similarly, if a *cumulative risk* scatter graph showed two other points (C and D) in similar locations, we could be almost certain that event C would happen regularly (but with low impact per event). It might be acceptable to ignore the risk of scenario C until the model's predictions are confirmed through actual experience. The damage would be low and controls put in place before it accumulated to a serious level. Measures would be required to prepare for event D since if it occurred it would be too late to do anything about it.

Comparing the two scatter graphs is also useful. If the *relative risk* scatter graph showed a number of scenarios with high probability, but the *cumulative risk* scatter graph showed the same scenarios at a lower probability, then it could be concluded that the main reason why those scenarios are not being



realized is due to a lack of encounters with adversaries. Essentially, they are safe because no one is actively trying to attack them. If an adversary emerged, the target system would be a sitting duck.

## **Pareto Charts**

One *pareto chart* is produced for each *alternative set* specified. The *Pareto charts* show the portion of total risk contributed by each *threat agent*.

## Print Tree...

The **File > Print Tree...** command allows you to print the current Attack (Threat) Tree.

1. Select the **File > Print Tree...** command from the application menu, or click on the **Print Tree** icon on the [toolbar](#).
2. The **Print Options** dialog will appear. Change the settings as required.
  - The size of the printout can be set. If *Default Size* is selected, the tree will be printed in a size similar to that seen on the screen. If *Fit to page* is selected, the tree will be printed so that it fits on one page. If *Resize* is selected, the *Scale Factor* can be specified where 1 is the default size, 0.5 is half the size and 2.0 is twice as big. You can specify the scale factor you require.
  - You can specify a Main Title and Sub Title for the printout.
  - Trees can be printed in color or black and white.
  - The font size for the text in the nodes can be specified.

Note: These Print Options are saved with the tree. If you open a new tree, the settings will be different.

- The *Page Layout* button will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.
  - Select **Print...** to continue with printing or **Close** to cancel out of printing.
3. If you select **Print...**, you will now see a preview of how the tree will be printed. If all looks good, click **Print...** (at the top of the window) to select your printer and send the printout to the printer.

## Page Layout

The **File > Page Layout** command will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.

## Tree Properties

To display this window, choose **Tools > Preferences** from the application menu then select the **Tree Properties** tab, or select **File > Tree Properties**, or use the right mouse button to click the "white space" in the tree display area and then click on **Tree Properties** in the pop-up menu.

The **Tree Properties** window displays information about when the tree was created and modified. It also allows up to two watermarks to be specified for the tree.

The [Automatically Calculate Tree](#) option will toggle the auto calculate function.

## File Protection

The file can be marked as "protected" by clicking on the Edit button. In the File Protection Settings window;

1. Select Yes in the Protected: field.
2. Enter a Password.
3. Information about when the protection was set is displayed;
  - Date
  - Set By Name - user's name
  - Set By License - the license that was used when setting the protection.
4. The type of protection can be selected by checking one or more of the following:
  - Tree Structure - can't create/delete/move nodes or change node type
  - Indicator values
  - Note Data
  - Indicator Definitions
5. The file protection can only be removed or changed when the correct password is provided.
6. The protection can be bypassed by doing a *Save As* (which will create an identical, unprotected file).

## Tree Logging and Database Synchronization

This feature is still in the developmental stage. If you are interested in using this feature, please contact Amenaza Technologies. Log file format and DB sync functionality may change in the future. Please be aware of this before using this feature.

Click on the Edit button to make changes. In the Tree Logging and DB Sync window:

- To turn on tree logging, check the "Log tree changes to file" checkbox and enter a file name where the log entries should be written, by typing in the name or by browsing to the file and selecting the file.
- To synchronize with a database, check the box "Define programs to synchronize with database". Now enter the names of your Java classes that will be called when each of the activities occurs. Every activity must have a class defined, but the same class can be used for multiple activities.

More information on how to define your DB sync classes:

Make a Java class that implements SecurITreeDBSyncInterface. Then compile it using the command:

```
javac -classpath SecurITree.jar <directory>\<dbsync_program>.java.
```

You need to set classpath to be SecurITree.jar to include the references for custom exceptions, interfaces, etc. Now enter this program name in the DB Sync dialog using <directory>.<dbsync\_program> (no backslash after directory name, no .java or .class after program name).

## Subtree Reduction Algorithm

The algorithm to use when calculating the minimal set of attack scenarios under a node that has been set as reduced can be selected. The choices are:

- Aggressive
- Conservative

See [Using SecurITree > Attack Scenario Reduction](#) for more information.

## Feasibility

The formula to use for calculating Feasibility can be selected. The choices are:

$\prod_{i=1}^n f_i(x)$  product of resource affinity functions or  $\sqrt[n]{\prod_{i=1}^n f_i(x)}$  nth root of the product of resource affinity functions.

See [Using SecurITree > Advanced Analysis > Main Analysis Feasibility](#) for more information.

## Default Attack Type

The *Default leaf node attack type* can be selected. The choices are:

- Single Shot Attack
- Single Threaded Attack
- Multi-Threaded Attack

The nature of a leaf node operation determines whether an adversary can perform the activity once (single shot), repeatedly, but sequentially (single threaded), or repeatedly and concurrently (multi-threaded). This is known as the *attack type*.

An *attack type* must be defined for each leaf node in the tree. However, in many cases most of the leaf nodes will have the same attack type. For example, trees with mostly physical attacks will have a lot of *single threaded* leaf nodes whereas trees with many automated, electronic exploits would predominantly have leaf nodes that were *multi-threaded*. For convenience, you can set a default attack type that will apply to all leaf nodes in the tree except those for which you have overridden the default and explicitly set the *attack type*.

The *Default attack time parameters for each attack type* can be set for the tree.

Strictly speaking, since each leaf node in the tree represents a different attacker activity, each node should have a unique attack time and recovery time. However, for leaf nodes of the same attack type, the time parameters are often very similar. For convenience, default values for each attack type can be defined that will apply unless overridden by setting custom values in particular leaf nodes. Choose defaults that closely match the characteristics of the majority of each attack type of leaf nodes in the tree.

## Time Units

Choose the unit of time to be used in Advanced Analysis for the cumulative risk related columns on the table. This value is saved for use with the currently opened tree.

## **Global Values**

Global values used with Derived Indicators can be edited here.

## **Notes**

Notes about the tree can be specified here.

## Node Properties

To display this window, select **File > Node Properties**, or use the right mouse button to click on a node and then click on **Node Properties** in the pop-up menu.

The **Node Properties** window displays information about the node such as the number of nodes and the number of attack scenarios in the subtree starting at this node, whether or not this node has been marked as Reduced (see [Using SecurITree > Attack Scenario Reduction](#) for more information), and Attack Type and Attack Parameters settings for the node.



## Exit

This command is used to **Exit** out of the **SecurITree** program completely. If any Attack (Threat) Tree files are open and have changes that have not been saved, you will be asked if you want to save them before exiting the program.

## Edit Menu

The following options are available under the **Edit** menu:

- [Undo](#)
- [Redo](#)
- [Undo Levels...](#)
- [Cut](#)
- [Copy](#)
- [Paste](#)
- [Paste Special](#)
- [Break Link](#)
- [Instantiate External Link](#)
- [Instantiate All External Links](#)
- [Add to Scratchpad](#)
- [Nodes](#)
- [Edit Tree in Table Format](#)
- [Change Node Values](#)
- [Set Indicators](#)
- [Define Alternative Sets...](#)
- [Define Sensor Defense Pairs](#)
- [Note Types](#)
- Maintenance
  - [Edit Agent/Victim Profile](#)
  - [Edit Profile Weight Map](#)
- [Reduce Subtree](#)
- [Restore Subtree](#)
- [Find...](#)

## Undo

This command is used to **Undo** the 10 most recent tree editing actions that have taken place in the current Attack (Threat) Tree file. Select **Edit > Undo** in order to do this.

## Redo

This command is used to **Redo** the 10 most recent undo actions that have taken place in the current Attack (Threat) Tree file. Select **Edit > Redo** in order to do this.

## Undo Levels...

The **Undo Levels...** command is used to set the number of levels of Undo allowed while editing the tree.

- To change the number of undo levels, choose **Edit > Undo Levels...** from the application menu. Select the number of levels you would like to allow from the pull-down list, then click *OK*.
- The default is 10 levels of undo.
- If zero (0) is selected, undo will be disabled.

## Cut

To **Cut** nodes from a tree:

1. Select the node or subtree you want to cut by clicking the node. This will cause the node to be highlighted in yellow.
2. Select **Cut** by choosing **Edit > Cut**; clicking on the **Cut** icon from the [toolbar](#); or by using the right mouse button to click the selected node, then clicking on **Cut**.
3. The selected node or subtree will be copied then removed from the tree.
4. At this point, you can [Paste](#) the node or subtree into a new location in the tree. You can also [Paste as Link](#) and make it an internal link.

## Copy

This command is used to **Copy** nodes on a tree. The copied subtree is saved so it can be used internally within the tree and is also saved onto the system clipboard. The copy can be performed on the entire tree or a subtree.

1. Select the node or subtree you want to copy by clicking the node. This will cause the node to be highlighted in yellow. If you do not select a node on the tree, the entire tree will be copied. Select **Copy** by choosing **Edit > Copy**, clicking on the **Copy** icon from the [toolbar](#), or by using the right mouse button to click the selected node and then selecting **Copy**.
2. The selected node or subtree will be copied.
3. At this point, you can [Paste](#) the node or subtree into a new location in the tree. You can also [Paste as Link](#) and make it an internal link. The values for all indicators can be pasted to another node by selecting [Paste Special > Paste Values](#) and all notes can be copied to another node by selecting [Paste Special > Paste Notes](#).
4. The system clipboard now contains the subtree in several different formats: raster image, vector image, pdf, and in the tree structure format.
  - The image of the tree can be pasted into another application such as a word processor. In Word, use Paste Special, then select the required format.
  - The node or subtree can be pasted into a new location in the currently opened tree, or it can be pasted into another instance of **SecurITree** that is running on the same workstation by using [Paste Special > Paste Tree Structure From Clipboard](#).

## Paste

To **Paste** nodes into a tree:

1. You must first [Cut](#) or [Copy](#) a node or subtree on the tree.
2. Select the node that will be the parent of the node or subtree that was **Cut** or **Copied** by clicking the node. This will cause the node to be highlighted in yellow.
3. Select **Paste** by choosing **Edit > Paste**, clicking on the **Paste** icon from the [toolbar](#), or by using the right mouse button to click the selected node, then clicking on **Paste**.
4. The node or subtree that was previously **Cut** or **Copied** will be pasted at this location on the tree.



## Paste Special

Nodes can be copied then pasted using the [Paste](#) feature. It is also possible to perform special paste functions by using:

[Paste as Link](#)

[Paste as Identical Link](#)

[Paste as Ganged Link](#)

[Paste Values](#)

Paste All Values

Paste Indicator Values

Paste Attack Type Values

[Paste Notes](#)

[Paste Color/Font](#)

[Paste Tree Structure From Inter-App Clipboard](#)

## Paste as Link

To **Paste** internal links into a tree:

1. You must first [Cut](#) or [Copy](#) a node or subtree on the tree.
2. Select the node that will be the parent of the node or subtree that is to be pasted as an internal link by clicking the node. This will cause the node to be highlighted in yellow.
3. Select **Paste as Link** by choosing **Edit > Paste Special > Paste as Link**, clicking on the **Paste as Link** icon from the [toolbar](#), or by using the right mouse button to click the selected node, then clicking on **Paste Special > Paste as Link**.
4. The node or subtree that was previously **Cut** or **Copied** will be pasted at this location on the tree as an internal link.

An *internal link* is a special subtree. It is distinguishable by a *chainlink* icon above all of the nodes in the subtree and is identified by a **red link number** positioned to the right of the chainlink symbol on the topmost node of the internally linked subtree. All links with the same number belong to the same internal link. Only one copy of the linked subtree exists in memory. All instances of a linked subtree are references to the same data in memory. Any changes made to a node in a linked subtree will be reflected in the corresponding node of all the linked instances; i.e., in all of the *internal links* which share the same *link number*.

When only one copy of an internal link exists (i.e. all other internal links have been cut or deleted from the tree), the internal link symbol will be removed from all nodes on the remaining internal link subtree.

See also:

[Subtree Reuse: Internal Links](#)

## Paste as Identical Link

To Paste identical links into a tree:

1. You must first [Cut](#) or [Copy](#) a node or subtree on the tree.
2. Select the node that will be the parent of the node or subtree that is to be pasted as an identical link by clicking the node. This will cause the node to be highlighted in yellow.
3. Select **Paste as Identical Link** by choosing **Edit > Paste Special > Paste as Identical Link**, clicking on the **Paste as Identical Link** icon from the [toolbar](#), or by using the right mouse button to click the selected node, then clicking on **Paste Special > Paste as Identical Link**.
4. The node or subtree that was previously **Cut** or **Copied** will be pasted at this location on the tree as an identical link.

An *identical link* is a special subtree. It is distinguishable by a red equal sign icon at the top left of all of the nodes in the subtree and is identified by a **red link number** positioned at the top right of the topmost node of the identical link subtree. All links with the same number belong to the same identical link. Only one copy of the linked subtree exists in memory. All instances of a linked subtree are references to the same data in memory. Any changes made to a node in a linked subtree will be reflected in the corresponding node of all the linked instances; i.e., in all of the *identical links* which share the same *link number*.

When only one copy of an identical link exists (i.e. all other identical links have been cut or deleted from the tree), the identical link symbol will be removed from all nodes on the remaining identical link subtree.

See also:

[Subtree Reuse: Internal Links](#)

## Paste as Ganged Link

To Paste ganged links into a tree:

1. You must first [Cut](#) or [Copy](#) a node or subtree on the tree.
2. Select the node that will be the parent of the node or subtree that is to be pasted as a ganged link by clicking the node. This will cause the node to be highlighted in yellow.
3. Select **Paste as Ganged Link** by choosing **Edit > Paste Special > Paste as Ganged Link**, clicking on the **Paste as Ganged Link** icon from the [toolbar](#), or by using the right mouse button to click the selected node, then clicking on **Paste Special > Paste as Ganged Link**.
4. The node or subtree that was previously **Cut** or **Copied** will be pasted at this location on the tree as a ganged link.

A *ganged link* is a special subtree. It is distinguishable by a red icon at the top left of all of the nodes in the subtree and is identified by a **red link number** positioned at the top right of the topmost node of the ganged link subtree. All links with the same number belong to the same ganged link. Only one copy of the linked subtree exists in memory. All instances of a linked subtree are references to the same data in memory. Any changes made to a node in a linked subtree will be reflected in the corresponding node of all the linked instances; i.e., in all of the *ganged links* which share the same *link number*.

When only one copy of a ganged link exists (i.e. all other ganged links have been cut or deleted from the tree), the ganged link symbol will be removed from all nodes on the remaining ganged link subtree.

br>

See also:

[Subtree Reuse: Internal Links](#)

## Paste Values

To **paste values** from one node to another node:

1. You must first [copy](#) a LEAF node on the tree.
2. Select the target LEAF node by clicking the node. This will cause the node to be highlighted in yellow.
3. You can choose to paste only indicator values, or only attack type values, or all indicator and attack type values.
4. Make your selection by choosing **Edit > Paste Special > Paste All Values** or **Paste Indicator Values** or **Paste Attack Type Values** or right-click the target node then choose **Paste Special > Paste All Values** or **Paste Indicator Values** or **Paste Attack Type Values** from the pop-up menu.
5. The indicator values/attack type values for the node that was previously **copied** will be used as the values for this node.

## Paste Notes

To **paste notes** from one node to another node:

1. You must first [copy](#) a node on the tree.
2. Select the target node by clicking the node. This will cause the node to be highlighted in yellow.
3. Select **Paste Notes** by choosing **Edit > Paste Special > Paste Notes** or right-click the target node then choose **Paste Special > Paste Notes** from the pop-up menu.
4. The notes for the node that was previously **copied** will be pasted to this node. If the target node already contains notes, the pasted notes will be appended after the existing notes.

## Paste Color/Font

To paste the color and font settings of one node to another node:

1. You must first [copy](#) a node on the tree.
2. Select the target node by clicking the node. This will cause the node to be highlighted in yellow.
3. Select **Paste Color/Font** by choosing **Edit > Paste Special > Paste Color/Font** or right-click the target node then choose **Paste Special > Paste Color/Font** from the pop-up menu.
4. The color of the node that was previously **copied** will be set for this node as well as any changes to font..

## Paste Tree Structure From Clipboard

To Paste into the tree from the clipboard:

1. You must first **Copy** from this tree or another instance of **SecurITree**.
2. Select the node that will be the parent of the node or subtree that was **Copied** by clicking the node. This will cause the node to be highlighted in yellow.
3. Select **Paste** by choosing **Edit > Paste Special > Paste Tree Structure From Clipboard**, or by using the right mouse button to click the selected node, then clicking on **Paste Special > Paste Tree Structure From Clipboard**.
4. The node or subtree that was previously **Copied** will be pasted at this location on the tree.



## Break Link

An internal link is a special subtree. It is identified with the *chainlink* icon over all nodes contained in the subtree and a red number on the top right of the root node of the internal link subtree. Only one copy of the linked subtree is actually stored in memory. All representations of the subtree are references to the copy in memory. Any changes made to a node in the internal link subtree will be made to that node in all occurrences of the internal link on the tree.

The **Break Link** function can be used to change a subtree from a link to a regular subtree. This is equivalent to doing a cut and paste on the subtree.

1. Select the linked node or subtree you want to convert to a regular node or subtree by clicking the node. This will cause the node to be highlighted in yellow. You must select the root node of the link.
2. Select **Break Link** by choosing **Edit > Break Link**, clicking on the **Break Link** icon from the [toolbar](#), or by using the right mouse button to click the selected node and then selecting **Break Link**.
3. If this is a ganged link or an identical link, you will be given the choice to set the link to a regular link.
4. The selected node or subtree will be converted from a link to regular nodes.

## Instantiate External Link

An external link is a special subtree. It is identified with a red outline around all nodes contained in the subtree. Changes cannot be made to any nodes in the externally linked subtree since they are a representation of the actual subtree from another file. See [File > Insert External...](#) for more information about externally linked subtrees.

The **Instantiate External Link** function can be used to change a subtree from a reference to a tree in another file to regular nodes in the current tree.

1. Select the root node of the externally linked node or subtree you want to convert to a regular node or subtree by clicking the node. This will cause the node to be highlighted in yellow.
2. Select **Instantiate External Link** by choosing **Edit > Instantiate External Link**.
3. The selected node or subtree will be converted from an external link to regular nodes.

## Instantiate All External Links

An external link is a special subtree. It is identified with a red outline around all nodes contained in the subtree. Changes cannot be made to any nodes in the externally linked subtree since they are a representation of the actual subtree from another file. See [File > Insert External...](#) for more information about externally linked subtrees.

The **Instantiate All External Links** function can be used to change all externally linked subtrees from a reference to a tree in another file to regular nodes in the current tree.

1. Select **Instantiate All External Links** by choosing **Edit > Instantiate All External Links**.
2. All nodes or subtrees that are externally linked will be converted to regular nodes.

## Add to Scratchpad

The **Edit > Add to Scratchpad** command allows you to save subtrees to a scratchpad area so they can be conveniently copied or moved around the tree. This feature can also be activated by using the right mouse button to click the selected node, then click on **Add to Scratchpad**.

To view or hide the scratchpad, select **View > Show Scratchpad**.

## Using Nodes

These actions can be performed on Attack (Threat) Tree nodes:

[Add Node](#)

[Edit Node](#)

[Delete Node](#)

Auto Size Node

[Print Node](#)

[Insert New Root Node](#)

[Adopt to alternative set](#)

[Deactivate Node/Subtree](#)

### To resize nodes:

Click the node to select it, then click the sizing handle (the black spot on the right side of the node) and drag while holding down the mouse button.

To automatically size the node to the size required to show all text, right-click on the node then select "Auto Size Node". Alternatively, click the node to select it then click the toolbar icon for "Auto Size Node", or select **Edit > Nodes > Auto Size Node**.

### To reset node size:

Right-click on the node and select "Reset Node Size".

All nodes on the tree can be "auto-sized" by selecting **Tools > Preferences** then checking "Auto size all nodes on tree" on the *Node Info* tab.

All nodes on the tree can be reset to the standard size by selecting **Tools > Preferences** then clicking on "Reset all nodes to standard size" on the *Node Info* tab.

The tree can be displayed with the default node sizes while retaining the customized sizes by selecting **Tools > Preferences** then clicking on "Display Standard Node Sizes" on the *Interface* tab.

### Navigating the tree:

Every node in the tree can be visited in a depth-first navigation by using the <Page Up> / <Page Down> keys. The arrow keys can also be used to navigate from one node to another.

## Edit Tree in Table Format

The tree can be edited in a table format. This is an alternative to clicking on and editing each node individually. It may be useful, for example, when changing the Leaf node values for an indicator.

This facility has limited functionality which may be expanded in the future. Please contact Amenaza Technologies if you have any suggestions or comments on this feature.

To start this function, select the **Edit > Edit Tree in Table Format** command from the application menu. At this time the only fields that can be changed are:

- Node names
- Leaf node values for Behavioral Capability and Impact indicators.

While editing the tree in table format, other changes to the tree are not allowed. Clicking on *Save Changes and Close* will apply changes to all nodes that have been altered. *Cancel* will discard all changes and the tree will not be altered.

## Change Node Values

This feature can be used to do a tree-wide change of a particular indicator value for all nodes. This is an alternative to clicking on and editing each node individually.

To start this function, select the **Edit > Change Node Values** command from the application menu.

- Select the indicator name for values to be changed
- Replace Value Matches:
  - o Only values matching the entered value will be changed.
  - o Enter the old value
  - o Enter the new value
- Replace All:
  - o A mathematical expression can be entered to change all values for this indicator. The keyword "value" is used for the current value of the node. For example, "value \* 2" will multiply the current value by 2.

All matching LEAF node values and matching AND/OR impact values will be changed from the old to the new value.

## Using Indicators

These actions can be performed on Threat Tree indicators:

[Add Indicator](#)

[Edit Indicator](#)

[Delete Indicator](#)

[Rename Indicator](#)

**SecurITree** attack tree models incorporate a feature known as "indicators." Indicators are a property of the attack tree that help the analyst understand how the tree relates to the real world. There is no fixed limit to the number of indicators that can be defined for a tree, but typically three or four indicators are used.

There are two basic types of indicators. Behavioral indicators describe the resources that need to be expended by the attacker in order to reach a particular state or node in the tree. Behavioral indicators include things such as: cost (to the attacker), technical skill, and willingness on the part of the attacker to accept the consequences of their actions. Impact indicators are used to describe the damage or impact on the victim of the attack that is caused by an attacker reaching a given state or node. Setting up impact indicators requires a good understanding of the effect an attack will have on the business in question.

Associated with each indicator is a pair of functions that help determine indicator values for each node in the tree. One member of the indicator function pair is used to calculate the indicator values for *AND* nodes and the other is used for *OR* nodes. It is usually desirable to choose functions that will result in the lowest cost value for a particular node. That is, the calculated value that corresponds to the least costly path from the leaf nodes to intermediate locations in the tree for a particular indicator.

In the case of behavioral indicators the analyst must enter explicit values at the leaf nodes. All node values above the leaves are calculated by the formulas. Behavioral indicators are the core of capability-based analysis. The behavioral indicator node values are compared to the resources available to the various threat agents during pruning operations. States (nodes) in the tree that cannot be attained by a particular threat agent are pruned away.

When using impact indicators, the indicator formulas can be used to compute impact values for intermediate nodes (in the same fashion as with behavioral indicators). Unlike behavioral indicators, it is also possible to override or influence the calculated values for any node in the tree. This allows the analyst to introduce business specific external information into the model (based on interviews with the organization's business people). Impact indicators cannot be used for tree pruning. They are, however, essential in analyzing risk.



Note that indicator values (both behavioral and impact) are calculated independently for each indicator. This means that a set of values at a particular node in a tree may (and probably do) represent distinct traversal paths. The notable exception is when *Attack Scenarios* have been generated. Since each *Attack Scenario* corresponds to a specific path through the tree, the indicator values at a given node then represent the cost for that specific path.

The combination of behavioral and impact indicators come together to provide a complete, risk analysis solution. Capabilities-based pruning on behavioral indicators yields the collection of probable attacks available to a threat agent. Generating a set of *Attack Scenarios* from the capabilities-pruned tree shows which specific paths (attacks) are available to the threat agent. Sorting these *Attack Scenarios* based on impact indicators, yields a risk prioritized list of attacks for a given threat.

### Derived Indicators

Prior to v3.5, there were there were two basic indicator types: *Behavioral* and *Impact*. SecurITree used pre-defined formulas in conjunction with these indicators to determine the *probability* of each attack scenario (based on either the statistical probability or the feasibility and desirability). When *probability* was combined with the *victim impact*, this yielded an estimation of risk. This functionality is sufficient for most, but not all, types of analysis.

In certain cases, analysts wish to derive values based on user defined mathematical expressions that may incorporate other *behavioral* or *impact* indicator values. For example, if a tree had *behavioral* indicators *Cost of Attack* and *Noticeability*, it is possible that an analyst might want to study nodes and scenarios with high (or low) cost and noticeability values. So, they might define a *derived* indicator called *Cost-Noticeability* and use  $Cost\ of\ Attack * Noticeability$  as a *derived* value expression. One can conceive of many scoring systems that could benefit from this type of *derived* value calculation.

Conditional expressions can be defined for the derived indicator. The format is: IF <expression 1> THEN <expression 2> ELSE <expression 3>. Expression 1 must be a boolean expression where the result is either True or False. For example;  $Cost\ of\ Attack \geq 200$ . If the result of Expression 1 is True, the expression defined in Then is used. If the result is False, the Else expression is used.

The *derived* values are calculated on a per node basis. Leaf node derived values are always computed using a user defined expression. AND nodes can aggregate derived values using the standard aggregation formulas available for other indicator types (e.g., Sum of Vertices, Max of Vertices). OR nodes assume their *derived* value based on the value of the child that is selected in a particular scenario. Both AND and OR nodes can override the aggregated values using operators such as *Replace*, *Max Fn*, + (similar to the operators used for *impact* indicators. This allows great flexibility in calculating derived values for individual nodes or for entire scenarios.

The *derived* value feature is intended for experienced customers with complex requirements. Instructions for using these indicators can be found at [Add Indicator](#) and [Edit Indicator](#). Customers wishing to use this feature may wish to consult with Amenaza's Technical Support organization for further advice and information.

## Define Alternative Sets

Define Alternative Sets is used to create, rename and delete alternative sets for the tree. To learn more, see Using SecurITree / [Alternative Sets](#).

1. To start the function, select the **Edit > Define Alternative Sets** command from the application menu.
2. To create a new alternative set, type the name in the Create area. If this is the first alternative set being created, it must be based on the Base Tree. If other alternative sets have been defined, select the set to base this new set on. Click on *Create*.
3. To rename or delete an existing alternative set, select the set name from the list in the Edit area then click the *Rename* or *Delete* button.
4. When all define alternative set operations have been completed, click *Close* to dismiss the dialog.

## Define Sensor Defense Pairs

Define Sensor Defense Pairs is used to build an Attack-Defense tree. To learn more, see Using SecurITree / [Attack-Defense trees](#).

Sensor Defense Pairs can only be defined on AND nodes.

## Note Types

Use this menu to create, rename and delete note types for the tree. To learn more, see Using SecurITree / [Notes](#).

1. To start the function, select the **Edit > Note Types** command from the application menu.
2. To create a note type, enter the name for the note in the *New Note Type Name* area, then click the *Create* button. This note type is now available to be used to write notes for every node in the tree.
3. To rename or delete an existing note type, select the name from the pull-down list in the Edit area. There are now three choices:
  1. "Delete note type and delete existing notes" will complete remove the note type and all existing notes.
  2. "Delete note type and append notes to note type:" will allow you to select another note type, then all notes of the type to be deleted will be appended to the end of the selected note type.  
At least one note type must exist for the tree, so the last note type cannot be removed.
3. To rename, enter the new name for the note type.
4. Now press the "OK" button to confirm the action.
5. Notes can be reordered by selecting a note name in the "Note Type Reorder" area, then clicking on the "Move Up" or "Move Down" buttons.
6. If there are any note types on the tree that do not contain any notes, you can choose to automatically remove the note types or retain them by selecting/deselecting the checkbox in the "Note Type Cleanup" area.
7. When all note type operations have been completed, click *Close* to dismiss the dialog.

## Edit Agent/Victim Profile

Agent or Victim Profiles can be edited by opening this window. This is an alternative to making changes to agent profiles while pruning the tree or changing agent or victim profiles while doing Advanced Analysis.

To start this function, select the **Edit > Maintenance > Edit Agent/Victim Profile** command from the application menu. Click on *Load Profile* to load an Agent Profile (.agt file) or Victim Profile (.vip file).

At this time these are the changes that can be made:

- Indicators can be renamed or deleted.
- Basic pruning evaluators can be changed.
- Utility mappings can be changed for Attacker Resources, Attacker Benefits, Attacker Detriments and Victim Impacts.
- Attacker Encounter parameters can be changed.
- Notes can be altered.

Clicking on *Save Profile* will apply all changes that have been made. Click *Print Profile* to open the print window. *Close* will dismiss the window.

## Edit Profile Weight Map

To start this function, select the **Edit > Maintenance > Edit Profile Weight Map** command from the application menu.

The use of this tool is not normally necessary - **SecurITree** should maintain the Profile Weight Map information automatically. However, if threat agent and/or victim profiles have been moved or renamed outside of **SecurITree** (using a file Explorer) it is possible that weighting information will have been lost. This facility gives you the opportunity to recover that information and to clean up stale table entries.

When a threat agent or victim profile is used to analyze an attack tree, the analyst specifies the weighting values a threat agent (or victim) associate with the impact indicators in that tree. Since the weighting values for a given threat agent (or victim) may differ depending on the tree being analyzed, **SecurITree** cannot simply store the weights with the profile. Instead, it keeps a list of profiles applied to the tree and the weights that were used and stores this information in the attack tree (.RIT) file.

When an analyst applies a profile to a tree, **SecurITree** checks through the tree's Profile Weight Map to see if the profile has been used previously with the active tree. If an entry is found in the Profile Weight Map with the same path and profile name then the previously defined weighting values are re-used. Unfortunately, if the profile has been moved or renamed no match will be found and the weighting information will not be loaded.

The Edit Profile Weight Map dialog allows users to view entries to see what weighting values were used and to manually recover them if necessary. Stale entries can also be deleted.

The Edit Profile Weight Map dialog will become more sophisticated in future releases.

## Reduce Subtree

The **Reduce Subtree** command is used to reduce the attack scenarios, starting at the selected node, to the minimum set. For further information on minimizing attack scenarios, see [Using SecurITree > Attack Scenario Reduction](#).

1. Select the topmost node of the subtree to be reduced. This will cause the node to be highlighted in yellow.
2. Choose **Edit > Reduce Subtree** from the application menu, or alternately, use the right mouse button to click the selected node, then click **Reduce Subtree** on the pop-up menu.
3. The node will be rolled-up and any analysis functions requiring attack scenarios will be performed on the minimum set that is calculated for this subtree. The subtree cannot be rolled-down. The only way to see the nodes in the subtree under this node is to [Restore Subtree](#).



## Restore Subtree

The **Restore Subtree** command can be used on nodes that have been set to use reduced attack scenario calculation. For further information on minimizing attack scenarios, see [Using SecurITree > Attack Scenario Reduction](#).

1. Select the reduced node. This will cause the node to be highlighted in yellow.
2. Choose **Edit > Restore Subtree** from the application menu, or alternately, use the right mouse button to click the selected node, then click **Restore Subtree** on the pop-up menu.
3. The entire list of attack scenarios will now be calculated for this subtree when performing attack scenario analysis functions.

## Find...

The find feature can be used to search for text strings within nodes.

1. To start the **Find** function, select the **Edit > Find...** command from the application menu, or click on the **Find** icon on the [toolbar](#).
2. In the "Find What:" box, either:
  - type in the search string, or choose a previous search string from the drop-down list. If the search string should be saved for future use, the list of search strings can be edited by clicking the button. See also **Tools > Preferences > Interface**.

or select:

- Nodes with empty note fields
  - Nodes with undefined values
  - Root of links
  - Nodes with indicator values: and select the Indicator, Operator and Value.
  - Single Shot Attack
  - Single Threaded Attack
  - Multi-Threaded Attack
  - Reduced Nodes
  - Benefit-based Attack Effectiveness
  - Encounter-based Attack Effectiveness
  - SAND or Custom AND defined
3. If "Search String" was selected in the "Find What:" area, select the areas that should be searched by checking the fields in the "Look In:" area. You can choose "Node Name" and/or any notes that have been defined for the tree. Internal and External ID can also be searched.
  4. The "Match:" area allows you to control the options for the search.
    - Case: Find text matching the specified pattern of uppercase and lowercase letters.
    - Whole words: Find occurrences of the text as whole words.
    - [Regular expression](#): Specify the search string in the form of a regular expression. [See Using SecurITree > Regular Expressions](#) for more information.
  5. The scope for the search can be either:

- the entire tree or
  - the subtree starting at the currently selected node or
  - only *LEAF* nodes
6. After clicking on Search, the results of the search are displayed. You can click on a node in the result list, which will cause the node to be selected. If you double-click the node, the Edit Node window will open which will allow you to edit the node. All occurrences of the search string will be highlighted in yellow.
  7. If the node is part of a sub-tree that has been rolled-up, the button "Roll Down" will show in the Action column. Clicking on that button will cause the subtree to be rolled down.
  8. A Replace can be performed based on the search criteria that has been used. Select either "Replace All" or "Replace Selected" (after selecting one or more entries in the search results area). A dialog window will open which will allow you to enter the new value.
    - When the replace function is used with "Search String", it will replace text found in Node names or Notes.
    - When used with "Nodes with indicator values:", all matching LEAF node values and AND/OR impact values will be changed.
  9. The search results list can be printed by clicking the "Print Results" button.
  10. The table of search results can be saved by clicking the "Save As" button. See the section on saving table reports in [Basic Reports](#) for more information.
  11. A node or multiple nodes can be deleted by selecting the node/s in the table. All highlighted nodes will be deleted after confirmation.

## View Menu

The following options are available under the **View** menu:

[Zoom...](#)

[Depth Display Level...](#)

[Show Legend on Tree](#)

[Show High Level View of Tree](#)

[Show Scratchpad](#)

[Roll Down Subtree](#)

[Roll Down Subtree 1 Level](#)

[Roll Down Subtree x Levels...](#)

[Roll Down Nested Subtrees](#)

[Display Alternative Sets...](#)

[Show m of n Combinations](#)

[Show all enabled bubbles](#)

[Hide all enabled bubbles](#)

## Zoom...

The **Zoom** command is used to enlarge or reduce the size of the nodes in the application window. To change the node size:

1. Click either the + (**Zoom In**) or - (**Zoom Out**) or (**Zoom to Fit**) magnifying glass icon on the [toolbar](#). The view of the tree changes immediately.
2. Choose **View > Zoom...** from the application menu. You will get the *Zoom* dialog box where the node size can be specified. You can either select one of the preset zoom percentages by clicking on a radio button, or you can enter a percentage in the box on the bottom of the dialog for a custom setting. In both cases, the new node size is shown in the preview window. Once the desired zoom setting is arrived at, click *OK* to apply it to the view of the tree.

## Depth Display Level...

The **Depth Display Level...** command is used for viewing the tree to the desired depth of detail making it easy to summarize the tree you are working on.

- To hide or display nodes in the application window choose **View > Depth Display Level...** from the application menu. Select the number of levels you would like to see from the pull-down list, then click *OK*.
- If you would like to display all nodes on the tree, select *All* from the pull-down list.
- The status line (at the bottom of the screen) will be updated to inform you of the number of levels in the tree that are displayed.

## Show Legend on Tree

The **View > Show Legend on Tree** command allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

This information can be set by selecting **Tools > Preferences** from the application menu, then choosing the **Node Info** tab to set indicator values to be displayed, or the **Flags** tab to define flags.

## Show High Level View of Tree

When the **View > Show High Level View of Tree** checkbox is selected, a small window will be displayed which shows a miniature version of the tree. A blue box in the window shows the portion of the tree that is currently displayed in the main window. This will help in determining the part of the tree that is showing on the screen.



## Show Scratchpad

The **View > Show Scratchpad** command allows you to display or hide the scratchpad area. Subtrees can be saved to a scratchpad area so they can be conveniently copied or moved around the tree. To add to the scratchpad, select **Edit > Add to Scratchpad**.

## Roll Up Subtree

The **Roll Up Subtree** command is used to hide all nodes under the selected node making it easier to view the area of the tree you are working on.

1. Select the topmost node you still want to see by clicking the node. This will cause the node to be highlighted in yellow.
2. To hide all nodes beneath the selected node, choose **View > Roll Up Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Up Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-U** or **Ctrl-<up arrow key>**.
4. The node color will change and a down pointing arrow will be added to indicate there are more nodes under this one that are currently not being displayed.

## Roll Down Subtree

The **Roll Down Subtree** command is used to show all nodes under the selected node if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. To show all nodes beneath the selected node, choose **View > Roll Down Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-D** or **Ctrl-<down arrow key>**.
4. The node will change to its normal colour and all nodes under this one will be displayed.

## Roll Down Subtree 1 Level

The **Roll Down Subtree 1 Level** command is used to show all nodes one level under the selected node.

1. Select a node on the tree by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree 1 Levels** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree 1 Level** on the pop-up menu. Or, click on the node then press **Ctrl-Shift-D**.
4. One level of nodes below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Subtree x Levels

The **Roll Down Subtree x Levels** command is used to show all nodes under the selected node (to the desired depth) if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree x Levels...** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree x Levels...** on the pop-up menu.
4. You will be asked to enter the number of levels to be rolled down. That number of levels below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Nested Subtrees

The **Roll Down Nested Subtrees** command is used to show all nodes under the selected node.

1. Select a node that is to be the start of the subtree to be rolled down by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Nested Subtrees** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Nested Subtrees** on the pop-up menu.
4. To roll down the entire tree, select the root node.

## Display Alternative Sets

Display Alternative Sets is used to change the active alternative set for the tree. To learn more, see Using SecurITree / [Alternative Sets](#).

1. To change the active alternative set, select the **View > Display Alternative Sets** command from the application menu, or click the desired alternative set in the pull-down on the Toolbar.
2. If the "Display all alternative sets on tree" box is selected, all nodes that are not found on the currently active alternative set will be shown on the tree as "outline" images. Analysis functions cannot be performed when all alternative sets are displayed.
3. Click *OK* to dismiss the dialog.

## Show m of n Combinations

The input values needed to trigger (satisfy) normal *AND* and *OR* nodes can be thought of as being on opposite ends of a spectrum. Normal *AND* nodes require all of their children to be active while *OR* nodes are activated if even a single child is active. In certain cases an analyst may need a logic node that triggers at a threshold somewhere in between the two extremes. That is, a node that activates if  $m$  of the node's  $n$  children are active. **SecurITree** allows the analyst to set this threshold value in *AND* nodes. Note that internally, **SecurITree** implements this by creating a complex graph of (normal) *AND* and *OR* nodes that replicate this behavior.

Excessive use of this feature may generate trees with very large attack scenario spaces.

The **Show m of n Combinations** command is used to open a new window which will expand the tree showing all the combinations for the *AND* node.

To set a value, edit an *AND* node, select the Options tab, then select an Input Threshold value that is less than the number of child nodes for this *AND* node.



## Show all enabled bubbles

The **Show all enabled bubbles** command is used to show a "bubble" containing notes for all nodes on the tree which have been set to have bubbles enabled. See **Using SecurITree > Notes** for more information.

## Hide all enabled bubbles

The **Hide all enabled bubbles** command is used to hide "bubbles" containing notes for all nodes on the tree which have been set to have bubbles enabled. See **Using SecurITree > Notes** for more information.

## Analyze Menu

The following options are available under the **Analyze** menu:

[Calculate Tree](#)

[Attack Scenarios...](#)

[Pruning Tree...](#)

[Set Operations on Pruned Trees...](#)

[Advanced Analysis...](#)

[Analyze Subtree](#)

## Calculate Tree

To calculate the values for all nodes on the tree:

- Select **Analyze > Calculate Tree**.
- All nodes are calculated by applying the appropriate formula for the indicator function and using the current value in the *LEAF* node.
- This function is mostly performed when [Auto Calculate](#) has been turned off and the manual mode for calculating nodes is required.

## Attack Scenarios...

To initiate the **Attack Scenarios...** process you select **Analyze > Attack Scenarios...** from the main menu. An *Attack Scenarios* window is then displayed for the *Base Tree*.

The top portion of the window has a table which lists all the *Attack Scenarios* for the *Base Tree*. Clicking on any of the *Attack Scenarios* listed will change the tree displayed so that it represents that particular scenario. Clicking on any of the column headings in the table will sort the table in ascending/descending order based on the items in that column.

See [Attack Scenarios](#) for more information on this subject.

## Pruning Tree...

To initiate the **Tree Pruning** process:

1. Select **Analyze > Pruning Tree...**
2. You will be prompted to enter a name for the [Pruning Window](#). This name should be that of a particular threat agent. For example, if you are attempting to reflect attacks that could be performed by a hacker then you would enter "Hacker".
3. By default, the calculation method is set to "**Scenario-based**". If you prefer, the method can be set to "**Node-Based**" by clicking on the radio button. Further information on this subject is provided below.
4. An *Agent Profile* by the same name as the name entered for the *Pruning Window* can automatically be applied to the tree. The *Agent Profile* must have previously been created and saved. Select the "*Apply Agent Profile ...*" radio button in the *Pruning Action* area to do this.
5. Once the name is specified and the calculation mode is set appropriately, click *OK* (or simply hit *Enter*) to generate a *Pruning Window*.
6. Within the pruning window you are able to prune the tree based on criteria applied against the indicator values.

NOTE:

1. Duplicate prune screen names are not allowed.
2. Once a [Pruning Window](#) is opened, the application enters *Analysis Mode* and many of the functions on the main screen are disabled. This ensures no changes are made to the base tree while prune processing is in progress. This message appears on the main screen above the tree display area: *Tree changes are not allowed when Analysis windows are open*. When all Analysis screens have been closed, Analysis mode is turned off and tree changes are allowed again.
3. **SecurITree** supports a number of different ways of creating a pruning tree. These are selectable via the radio buttons in the dialog box. The default method, "**Scenario-based**", is highly accurate but slow. It determines which parts of the tree are inaccessible to the adversary by comparing the attacker's resources with each and every possible attack scenario. Creating a "**Scenario-based**" pruning window may take several minutes for a large tree.

The "**Node-Based**" pruning method is an approximation that determines whether to delete nodes by comparing a node's set of values to the adversary's capabilities. This is quick but not perfectly accurate.

For detailed information on the differences in pruning methods, see [Explanation of Pruning Methods](#).

Amenaza recommends using "**Scenario-based**" pruning wherever possible and certainly for final reports. It may be necessary to use "**Node-Based**" pruning when dealing with very large trees or during "what-if" brainstorming sessions where speed of computation is essential.

## Set Operations on Pruned Trees

To initiate the **Set Operations on Pruned Trees** process:

1. Select **Analyze > Set Operations on Pruned Trees**.
2. A new window is displayed where the set operations on pruned trees can be performed.
3. The "Define Set Equation" button is used to perform the set operation functions.
4. The pruned trees and operator of *Intersection*, *Union* or *Difference* can now be selected.
5. A message is displayed to inform you of the number of nodes of the base tree that remain.
6. This process can be performed as many times as required.

See [Set Operations on Pruned Trees Menus](#) for more options on this window.



## Advanced Analysis...

To initiate the **Advanced Analysis** process:

1. Select **Analyze > Advanced Analysis...** from the main menu.
2. You will be prompted to Load an Agent Profile and Victim Profile to automatically apply the profile values or you can simply enter a name for the [Analysis Window](#). Once the profiles and/or name is specified, click *OK* (or simply hit *Enter*) to continue.
3. You will now be presented with the *Define Indicator Utility Functions window*. At this point you can load a predefined Agent Profile or Victim Profile, or you can manually define the Utility Mapping for each indicator. See [Attacker and Victim Utility Functions](#).
4. Once the indicators you want to analyze have been defined, click *OK* to generate an *Advanced Analysis Window*.
5. The top portion of the window has a table which lists all the *Attack Scenarios* for the *Base Tree*. Clicking on any of the *Attack Scenarios* listed will change the tree displayed so that it represents that particular scenario. Clicking on any of the column headings in the table will sort the table in ascending/descending order based on the items in that column. See [Attack Scenarios](#) for more information on this subject.

See [Advanced Analysis](#) for more information.

### NOTE:

1. Duplicate window names are not allowed.
2. Once an [Advanced Analysis Window](#) is opened, the application enters *Analysis Mode* and many of the functions on the main screen are disabled. This ensures no changes are made to the base tree while analysis is in progress. This message appears on the main screen above the tree display area: *Tree changes are not allowed when Analysis windows are open*. When all Analysis screens have been closed, Analysis mode is turned off and tree changes are allowed again.

## Analyze Subtree

To initiate analysis using a subtree of the main tree:

1. Select the node that is the root of the subtree you want to analyze by clicking the node. This will cause the node to be highlighted in yellow.
2. Select **Analyze > Analyze Subtree** from the main menu.
3. A new **SecurITree** session will open for analysis of a copy of the selected subtree. The current **SecurITree** session will be minimized. The original **SecurITree** session will resume when the subtree analysis session ends.
4. Changes made to the subtree in the new session will be lost upon return. If you wish to preserve the changes, save the subtree before exiting the Analyze Subtree session and import the modified subtree into your master tree.

## Tools Menu

The following options are available under the **Tools** menu:

[Toolbars](#)

[Panels](#)

[Plugins](#)

[Preferences](#)

## Toolbars

The **Toolbars** menu is used to hide or display the entire application toolbar or subsets of the toolbar. Choose **Tools > Toolbars** from the application menu and you will be given a list of the available toolbars.

The **Toggle All Toolbars** checkbox will toggle the [toolbar](#) from being displayed or hidden. Every other toolbar checkbox will toggle subsets of the toolbar from being displayed or hidden.

The **Reorder Toolbars** item will order the toolbar subsets into the default order if they have been moved around.

## Panels

The main application screen has two side panels. The left side panel contains [Node Information](#). The right side panel displays [Tree Information](#). The **Tools > Panels > Show Node Information Panel** and **Tools > Panels > Show Tree Information Panel** commands allow you to hide or display the side panels as you desire.

[Show Node Information Panel](#)

[Show Tree Information Panel](#)

## Show Node Information Panel

The **Tools > Panels > Show Node Information Panel** command allows you to display or hide the [Node Information](#) side panel. The panel can also be displayed or hidden by pressing **Ctrl-i** or by clicking the **Show Node Information Panel** icon on the toolbar.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".

## Show Tree Information Panel

The **Tools > Panels > Show Tree Information Panel** command allows you to display or hide the [Tree Information](#) side panel. The panel can also be displayed or hidden by pressing **Ctrl-t** or by clicking the **Show Tree Information Panel** icon on the toolbar.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".

## Plugins

This is a feature with external documentation. Please contact Amenaza Technical Support at:

1-888-949-9797 or (403) 263-7737 or

[http://www.amenaza.com/request\\_support.php](http://www.amenaza.com/request_support.php) or  
[support@amenaza.com](mailto:support@amenaza.com)

for further information.



## Preferences

The **Preferences** option is used to define your choices and settings. Choose **Tools > Preferences** from the application menu and the Preferences window will appear. There are several tabs on this window you can choose from.

[Interface](#)

[Application](#)

[Tree Properties](#)

[Node Info](#)

[Flags](#)

Click on *OK* once you have defined the preferences you wish to set. If you do not want to save the changes you have made, click on *Cancel* and your settings will not be changed.

## Interface

Choose **Tools > Preferences** from the application menu then select the **Interface** tab to display this window.

The Interface option will allow you to change the following settings:

## Look and Feel

The Look and Feel selection will change the look of the components on the screen. The choices for Look and Feel are:

Native OS, Metal, Windows, Windows Classic

## Scroll the Viewport by Dragging

Enable or disable Viewport dragging for the application. If Viewport dragging is enabled, the tree display area can be moved using the "hand" cursor. To do this, click and hold the mouse button when the mouse is positioned over the white area on the tree display. Dragging the mouse will move the tree display along with the "hand" cursor.

## Language

Select the Language for the menus and messages. The Language choice can only be selected when no trees are opened.

The choices for Language are:

English  
French (Français)  
German (Deutsch)

## Node Style

Select the style for drawing nodes. The choices for Node Style are:

Original  
Boolean

The **Change Default Node Colors/Fonts** button can be selected to alter the colors used for displaying nodes. Each node type can be changed and the **Use Default Colors** button can be selected to reset the colors back to the defaults.

The font for nodes can be changed setting the color, type, size and style. If Autosize is selected, the font size dynamically changes when you use Zoom. If you select a different font size this will be static, even if Zoom is used. The **Use Default Font** button can be selected to reset the font back to default.

If nodes on the tree have been resized, they can be displayed using the standard sizes by checking the **Display Standard Node Sizes** box. The customized sizes will be retained.

**Display indicator values on node tooltip** can be selected to give an expanded information box when the mouse is hovering over nodes.

When **Highlight Subtree** is selected, a darker border is drawn around all nodes in the subtree of the node which is currently selected on the tree.

**Capitalize New Node Name** will capitalize the first character of each word of the node name only when adding new nodes.

**Texture Node** will give a faded color to the nodes.

## Background Color

The Background Color can be specified by selecting the desired color from the palette. The color that is chosen is saved and will be used each time the application is run.

## Spelling Options

Used to make changes to the spelling options for the application. Click on the **Edit User Dictionary** button to add or remove words from the user dictionary. The user dictionary is saved at `$userhome\Application Data\Amenaza\SecurITree\userdict.tlx`

Click on **Spelling Options** to set the preferences for spell checking.

## Search Options

Click on the **Edit Search Strings** button to add or delete strings that can be used for searching in the **Edit > Find** dialog. After changes have been made, be sure to click the Save button before closing the window. The list of strings is customized for the user and is saved at \$userhome\Application Data\Amenaza\SecurITree\SecurITree\_search.txt

## Application

Choose Tools > Preferences from the application menu then select the **Application** tab to display this window.

The Application option will allow you to change the following settings:

## Action for Non-Minimal Scenarios with Identical Link Nodes

There are three choices for handling Attack Scenarios when identical link nodes are present in the tree. Non-minimal scenarios can occur. The action to use for these scenarios can be:

- Retain
- Eliminate
- Eliminate when identical impact values

For information on how to create Identical Link nodes, see [Main Menus > Edit > Paste Special > Paste as Identical Link](#).

## Edit Path for Externally Linked Trees

The **Edit Path for Externally Linked Trees** option is used to set the path variable used when inserting an externally linked subtree.

The EXTTREEPATH must contain full path names of all directories to look in for external links separated by semicolons (;), or a directory can be specified with "..\" which is the directory above where the current file is found, or "." where it is a subdirectory under the current file.

When looking for an externally linked subtree that was saved in the tree using the EXTTREEPATH option, the directories are searched in the order they are found in the EXTTREEPATH field. The file is selected from the first directory in which it is found.

See [File > Insert External...](#) for more information about inserting externally linked subtrees.

## Insert Subtree Action

When subtrees are inserted into a tree, the indicators are checked to determine if there is a match. If the indicators do match, it is possible the notes area for the indicator is different. You can choose the default action to take when this occurs. You can either:

- Ignore the indicator notes in the subtree being inserted.
- Append the notes to the end of existing notes.
- Prompt for the action to take when indicator notes do not match.

## Check Point

While a tree file is open in **SecurITree**, a checkpoint file is saved every x minutes. If **SecurITree** ends unexpectedly, the next time the tree file is opened, the checkpoint file can be used to recover any changes that were made between the last time the file was saved until the time of the last checkpoint save. The time interval can be set to be between 0 - 60 minutes. If 0 is entered, checkpoint files will not be saved.

## Tree Properties

To display this window, choose **Tools > Preferences** from the application menu then select the **Tree Properties** tab, or select **File > Tree Properties**, or use the right mouse button to click the "white space" in the tree display area and then click on **Tree Properties** in the pop-up menu.

The **Tree Properties** window displays information about when the tree was created and modified. It also allows up to two watermarks to be specified for the tree.

The [Automatically Calculate Tree](#) option will toggle the auto calculate function.

## File Protection

The file can be marked as "protected" by clicking on the Edit button. In the File Protection Settings window;

1. Select Yes in the Protected: field.
2. Enter a Password.
3. Information about when the protection was set is displayed;
  - Date
  - Set By Name - user's name
  - Set By License - the license that was used when setting the protection.
4. The type of protection can be selected by checking one or more of the following:
  - Tree Structure - can't create/delete/move nodes or change node type
  - Indicator values
  - Note Data
  - Indicator Definitions
5. The file protection can only be removed or changed when the correct password is provided.
6. The protection can be bypassed by doing a *Save As* (which will create an identical, unprotected file).

## Tree Logging and Database Synchronization

This feature is still in the developmental stage. If you are interested in using this feature, please contact Amenaza Technologies. Log file format and DB sync functionality may change in the future. Please be aware of this before using this feature.

Click on the Edit button to make changes. In the Tree Logging and DB Sync window:

- To turn on tree logging, check the "Log tree changes to file" checkbox and enter a file name where the log entries should be written, by typing in the name or by browsing to the file and selecting the file.

- To synchronize with a database, check the box "Define programs to synchronize with database". Now enter the names of your Java classes that will be called when each of the activities occurs. Every activity must have a class defined, but the same class can be used for multiple activities.

More information on how to define your DB sync classes:

Make a Java class that implements SecurITreeDBSyncInterface. Then compile it using the command:

```
javac -classpath SecurITree.jar <directory>\<dbsync_program>.java.
```

You need to set classpath to be SecurITree.jar to include the references for custom exceptions, interfaces, etc. Now enter this program name in the DB Sync dialog using <directory>.<dbsync\_program> (no backslash after directory name, no .java or .class after program name).

## Subtree Reduction Algorithm

The algorithm to use when calculating the minimal set of attack scenarios under a node that has been set as reduced can be selected. The choices are:

- Aggressive
- Conservative

See [Using SecurITree > Attack Scenario Reduction](#) for more information.

## Feasibility



The formula to use for calculating Feasibility can be selected. The choices are:

$\prod_{i=1}^n f_i(x)$  product of resource affinity functions or  $\sqrt[n]{\prod_{i=1}^n f_i(x)}$  nth root of the product of resource affinity functions.

See [Using SecurITree > Advanced Analysis > Main Analysis Feasibility](#) for more information.

## Default Attack Type

The *Default leaf node attack type* can be selected. The choices are:

- Single Shot Attack
- Single Threaded Attack
- Multi-Threaded Attack

The nature of a leaf node operation determines whether an adversary can perform the activity once (single shot), repeatedly, but sequentially (single threaded), or repeatedly and concurrently (multi-threaded). This is known as the *attack type*.

An *attack type* must be defined for each leaf node in the tree. However, in many cases most of the leaf nodes will have the same attack type. For example, trees with mostly physical attacks will have a lot of *single threaded* leaf nodes whereas trees with many automated, electronic exploits would predominantly have leaf nodes that were *multi-threaded*. For convenience, you can set a default attack type that will apply to all leaf nodes in the tree except those for which you have overridden the default and explicitly set the *attack type*.

The *Default attack time parameters for each attack type* can be set for the tree.

Strictly speaking, since each leaf node in the tree represents a different attacker activity, each node should have a unique attack time and recovery time. However, for leaf nodes of the same attack type, the time parameters are often very similar. For convenience, default values for each attack type can be defined that will apply unless overridden by setting custom values in particular leaf nodes. Choose defaults that closely match the characteristics of the majority of each attack type of leaf nodes in the tree.

## Time Units

Choose the unit of time to be used in Advanced Analysis for the cumulative risk related columns on the table. This value is saved for use with the currently opened tree.

## **Global Values**

Global values used with Derived Indicators can be edited here.

## **Notes**

Notes about the tree can be specified here.

## Auto Calculate

The **Auto Calculate** option will toggle the auto calculate function.

Choose **Tools > Preferences > Tree Properties > Automatically Calculate Tree** from the application menu to toggle this function.

- The current value for the Auto Calculate function is shown at the bottom of the screen in the status area. If Auto Calculate has been disabled and the tree is printed, a message will be printed at the top of the tree.
- When Auto Calculate is turned on (the default), the tree node values will automatically be re-calculated when changes are made to values in leaf nodes.
- When Auto Calculate is turned off, the tree node values must be manually re-calculated when changes are made to values in *LEAF* nodes and when nodes are added and removed.
- The benefit of having the auto calculate function turned off is realized when trees are being built. When *AND* and *OR* nodes are added to a tree, and before their *LEAF* nodes are added, error messages will be generated since the tree cannot be properly calculated without valid values in the (non-existent) *LEAF* nodes.
- Another benefit is when an indicator is added to the tree. The tree cannot be calculated until a value for the new indicator is added to every *LEAF* node.

## Node Info

Choose **Tools > Preferences** from the application menu, then select the **Node Info** tab to display this window.

**Display Indicator Values** is used to display the indicator values for the nodes on the tree.

Choose Values to Display:

- Select one or more of the indicators you would like displayed by clicking the check boxes.
- A legend will appear in the top left corner of the application window and the selected indicator values will then be displayed beside the nodes.
- The color the indicator value is displayed in corresponds to the color used to display the name of the indicator function in the legend.

The *Show Legend on Tree* checkbox allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

The legend can also be set by selecting **View > Show Legend on Tree** from the application menu.

Click on *OK* once you have chosen the values to display. The Node Information that was selected will now be displayed on the tree.

**NOTE:** A total of five (5) Indicator Values can be displayed at one time.

The **Node Display Settings** section has controls that can be used to change the way nodes are displayed for the tree. These settings are saved with the tree and are not saved as user defined settings.

- The **Display Node ID** setting is used to display the node IDs beside the node name inside every node in the tree.
- The **Reset all node colors to default** button can be selected to change any nodes that were individually changed to different colors. If this action is selected, it cannot be cancelled or undone with the **Undo** function.
- **Auto size all nodes on tree** is used to set all node sizes so that the node name fits into the node box.

- **Reset all nodes to standard size** will reset any nodes that were individually changed to a different size and/or set to auto-size. If this action is selected, it cannot be cancelled or undone with the **Undo** function.

**NOTE:** The tree can be displayed with the default node sizes while retaining customized sizes by selecting the Interface tab then clicking on "Display Standard Node Sizes".

The **Notes to Display in Bubble** section is used to select which note types should be shown in bubbles. See **Using SecurITree > Notes** for more information.

## Flags

The **Flags** window is used to set up flags to use with the tree.

Choose **Tools > Preferences** from the application menu, then choose the **Flags** tab and the *Flags* dialog box will appear.

- There are six predefined flag colors that will display under the nodes in specific locations when the flag for that node has been set.
- The flag name can be specified and should reflect how that flag is being used in the tree.
- The *Display* checkbox allows you to decide if the flags should be displayed on the tree. If this is turned off, the flags will still be set for the nodes but will not display. This feature is useful if, for example, you do not want to show flags on printed output.
- There are several settings for flags that can be chosen.
  - o Disabled - the flag will be reset for all nodes on the tree.
  - o Manual - the flag can be set manually when the node is edited.
  - o Last Edit - only one node on the tree will be set, showing that it was the last node to be edited.
  - o Content Edit - this flag will be automatically set whenever a node's values or notes are edited.
  - o New Node - this flag will be automatically set whenever a new node is added to the tree.
  - o Undefined Value - this flag will be automatically set whenever a node has an indicator with an undefined value.
  - o Indicator Value - when this setting is selected, you must click on the "Edit" button to enter the indicator, operator and value to be used as the criteria for setting the flag.
  - o Note Value - when this setting is selected, you must click on the "Edit" button to enter the note and value to be used as the criteria for setting the flag. If "All Notes" is selected, all notes are searched for the value entered in the value field. If Regular Expression is selected, the value can be specified using a regular expression.
  - o Attacker Benefit - this flag will be automatically set whenever a node has an Attacker Benefit type indicator with a value defined.
  - o Attacker Detriment - this flag will be automatically set whenever a node has an Attacker Detriment type indicator with a value defined.
  - o Victim Impact - this flag will be automatically set whenever a node has a Victim Impact type indicator with a value defined.

- o Any Impact - this flag will be automatically set whenever a node has any type of impact indicator with a value defined (either an Attacker Benefit or Victim Impact type indicator).
  - o Single Shot Attack - this flag will be automatically set whenever a node has the Attack Type set to Single Shot Attack.
  - o Single Threaded Attack - this flag will be automatically set whenever a node has the Attack Type set to Single Threaded Attack.
  - o Multi-Threaded Attack - this flag will be automatically set whenever a node has the Attack Type set to Multi-Threaded Attack.
- When a flag's setting is changed from one type to another, you will be given the option to retain values that were previously set for nodes on the tree. This does not apply when changing the setting to *disabled*.
  - The *Clear Flag* button can be used to clear the flag from all nodes.
  - If a tree containing flags is inserted into another tree, the flags for the tree to be inserted will be reset on the inserted instance. They will not be reset on the original version of the tree being inserted.

The *Show Legend on Tree* checkbox allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

The legend can also be set by selecting **View > Show Legend on Tree** from the application menu.

Click on *OK* once you have defined the values for the flags you wish to set. The flags you have set are now ready to use.

See [Using SecurITree > Flags](#) for more information.

## Window Menu

The following options are available under the **Window** menu:

[Attack Scenario Windows](#)

[Pruning Windows](#)

[Set Operations on Pruned Trees](#)

[Advanced Analysis Windows](#)

[Cascade Windows](#)

[Close All Analysis Windows](#)



## Advanced Analysis Windows

The **Advanced Analysis Windows** command is used to display the *Advanced Analysis Windows* that are associated with the current tree. This is a fast and convenient way to switch between windows, especially if you have several different windows open.

1. Choose **Window > Advanced Analysis Windows** from the application menu.
2. Select the *Advanced Analysis Window* that you wish to see.
3. To close the *Advanced Analysis Window*, use the **File > Close** command on the *Advanced Analysis Window* menu.

## Pruning Windows

The **Pruning Windows** command is used to display the *Pruning Windows* that are associated with the current tree. This is a fast and convenient way to switch between windows, especially if you have several different windows open.

1. Choose **Window > Pruning Windows** from the application menu.
2. Select the *Pruning Window* that you wish to see.
3. To close the *Pruning Window*, use the **File > Close** command on the *Pruning Window* menu.

## Set Operations on Pruned Trees

The **Set Operations on Pruned Trees** command is used to display the *Set Operations on Pruned Trees Window* for the current tree. This is a fast and convenient way to switch between windows, especially if you have several different windows open.

1. Choose **Window > Set Operations on Pruned Trees** from the application menu.
2. To close the *Set Operations on Pruned Trees Window*, use the **File > Close** command on the *Set Operations on Pruned Trees Window* menu.

## Attack Scenario Windows

The **Attack Scenario Windows** command is used to display the *Attack Scenario Windows* that are associated with the current tree. This is a fast and convenient way to switch between windows, especially if you have several different windows open.

1. Choose **Window > Attack Scenario Windows** from the application menu.
2. Select the *Attack Scenario Window* that you wish to see.
3. To close the *Attack Scenario Window*, use the **File > Close** command on the *Attack Scenario Window* menu.

## Cascade Windows

The **Cascade Windows** command is used to cascade all open **SecurITree** windows on the screen.

## Close All Analysis Windows

The **Close All Analysis Windows** command is used to close all the *Analysis Windows* that are open for the current Attack (Threat) Tree. The tree will no longer be in *Analysis Mode* and changes can now be made to the base tree.

## Help Menu

The following options are available under the **Help** menu:

[Help Index](#)

[Context Sensitive Help](#)

[Legend](#)

[About](#)

## Help Index

The **Help > Help Index** command is used to access these help files.



## Context Sensitive Help

The **Context Sensitive Help** command is used to directly access help on menu, toolbar, and side panel items by clicking on them.

1. Choose **Help > Context Sensitive Help** from the application menu. The mouse pointer will change from a *Normal Select* (just an arrow) to a *Help Select* (an arrow with a ?) pointer.
2. Move the mouse pointer to the desired menu, toolbar, and side panel item that you require help with and click on it.
3. If there is **Context Sensitive Help** the *Help Index* window will appear with the proper help topic displayed. If there is no **Context Sensitive Help** then the mouse pointer will revert back to *Normal Select*.

## Legend

The **Help > Legend** command opens a window which displays a legend describing the node types on trees. It will also show Tree Setting information including Flags and Indicator information.

## About

Displays the following information about the product:

- Current **SecurITree** Version and Build Numbers
- Contact Information
- Copyright Information

If you click on the **License** button, the *License* window will open which contains the following information:

- Type of License
- Who it is Licensed to
- License Expiration Date
- End User License Agreement (EULA)

If you click on the **JavaVM** button, the JavaVM window will open which will show:

- The Java Version that is being used for **SecurITree**
- The Total Memory available to use and the current Free Memory. To make changes to the memory available for the application, see [Memory Errors](#).

The **Properties** button will show:

- The location of the SecurITree\_console.txt file and SecurITree.cfg file.
- A listing of the Java properties.

The **Console** button will display:

- The contents of the SecurITree\_console.txt file which may contain error messages.

The **Splash** button will display the splash screen.

## Pruning Menus

The Pruning Window has the following Menus:

[File](#)

[Edit](#)

[View](#)

[Analyze](#)

[Tools](#)

[Help](#)

## File Menu

The following options are available under the **File** menu:

[Save Tree](#)

[Save Tree As...](#)

[Load Agent Profile](#)

[Save Agent Profile](#)

[Print Agent Profile](#)

[Reports...](#)

[Print Tree...](#)

[Page Layout](#)

[Close](#)

## Save Tree

Use the **File > Save Tree** command to save your file to disk. It is recommended that files be saved on a regular basis during a **SecurITree** session and especially after significant changes have been made.

1. Select the **File > Save Tree** command from the application menu, or click on the **Save Tree** icon on the [toolbar](#).
2. If this is a new Attack (Threat) Tree that was not previously saved, the **Save Tree** dialog box will be displayed. Select the folder you want to save the file in, type in a name for this file and click on the *Save* button.
3. If this tree was previously saved or was opened from disk, it will automatically be saved using the same filename.

## Save Tree As...

Use the **File > Save Tree As...** command to save your file to disk with a new name. It is recommended that files be saved on a regular basis during a **SecurITree** session, and especially after significant changes have been made.

1. Select the **File > Save Tree As...** command from the application menu, or click on the **Save Tree As** icon on the [toolbar](#).
2. The [Save](#) dialog box will be displayed. Select the folder you want to save the file in, enter a new file name if required, and click on the *Save* button to save your file with a new name.
3. Files can also be saved in different formats. If you would like to save the tree as you see it on the screen as an image file, you can choose either PNG, JPG, or SVG format. The *Files of type:* field has a pull-down list. If you choose *PNG Files (\*.png)*, *JPG Files (\*.jpg)*, or *SVG Files (\*.svg)* your tree will be saved as an image. You should use a matching extension in the *File name:* field or do not specify an extension and the correct extension will be added for you.

This command allows you to *Save Attack (Threat) Tree* files into the following file formats:

File Types	Format / Purpose
.rit	to save the file with a new name (similar to using <b>File &gt; Save As...</b> )
.ril	to save the file as a <b>SecurITree</b> library
.png	to save the file as a Portable Network Graphics image
.jpg	to save the file as a JPEG (Joint Photographic Experts Group) image
.svg	to save the file as an SVG (Scalable Vector Graphics) image
.atml	to save the file in Attack Tree Markup Language - xml format
.gxl	to save the file in Graph eXchange Language

## Load Agent Profile

- You can load an [Agent Profile](#) that was previously created. This is done by selecting **File > Load Agent Profile**, or by clicking the **Load Agent Profile** icon on the [toolbar](#).
- A warning message is given if there are existing *Pruning Criteria* since they will be overwritten.
- If a file already exists with the same name as the name of this *Pruning Window*, it is pre-selected in the **File > Load Agent Profile** dialog. You can also save *Agent Profiles* by clicking the **Save Agent Profile** icon on the [toolbar](#). *Agent Profile* files end with the extension .agt.
- After the file is selected, the *Pruning Criteria* is applied to the base tree.
- A message will be displayed above the tree display area which informs you of the number of nodes removed during the application of this *Pruning Criteria*.
- The *Agent Profile Pruning Criteria* area now contains the evaluators that were loaded from the file. The *Pruning Criteria* for the *Agent Profile* can be edited by selecting **Edit > Edit Agent Profile**, or by clicking the **Edit Agent Profile** icon on the [toolbar](#).



## Save Agent Profile

The *Pruning Criteria* area can be saved and used for future evaluations on this tree or any other tree with matching indicator functions. Select **File > Save Agent Profile** to save the *Pruning Criteria* to a file. *Agent Profile* files end with an extension of .agt.

## Print Agent Profile

The **File > Print Agent Profile** command allows you to print the currently loaded Agent Profile.

1. Select the **File > Print Agent Profile** command from the application menu.
2. You will now see a preview of your printout. If all looks good, click **Print...** (at the top of the window) to select your printer and send the printout to the printer.

## Reports...

The **File > Reports > Basic Reports** command allows you to view the Attack (Threat) Tree you are working on in a tabular format. The following Reports are available:

- **All Nodes** - All nodes on the tree are displayed in the report.
- **Only Leaf Nodes** - Only LEAF nodes are included in the report.
- **Complete Node Information** - All indicator values and notes are included in the report.
- **Complete Node Information - LEAF nodes only** - All indicator values and notes are included in the report.
- **Complete Node Information + Scenarios per Node** - The number of times the node occurs in scenarios is calculated and included in the report. Clicking on a node in the table will display a table showing all scenarios where this node is found. Clicking on a scenario will show the tree for the scenario.
- **Attack Scenarios** - A listing of all Attack Scenarios. This report is only available in an Attack Scenario window or in an Advanced Analysis window.
- **Agent Profile Cross-Reference** - This report is only available if pruning windows have been created. The report indicates which agent profiles are capable of performing an attack by placing an "X" under the appropriate pruning window name. If a node was removed from a tree during pruning operations, it will not have an "X" in that column.
- **Pruning Sensitivity** - This report is only available in a pruning window if the node-based method of pruning was used. The report provides a list of all pruning criteria and whether or not nodes were eliminated from the tree. If a node was removed on a particular pruning criterion, an "X" is placed in the column. The total number of criteria that caused the node to be pruned (removed) is also displayed.

The delta column for each pruning criteria is colored. This is the explanation of the color coding:

- Pink/(Red) represent attacks that are within/(well within) the capability of the threat agent.
- Light Yellow/(Dark Yellow) represent attacks that are nearly within/(just within) the capability of the threat agent.
- Light Green/(Green) represent attacks beyond/(well beyond) the capability of the threat agent.
- Numeric indicator values express the resources required to carry out the attack.
- # indicator values show the resources available to the attacker minus resources required to carry out the attack.
- Negative values indicate the attacker had a shortfall of the resources required for the attack.

This report provides a useful guide of the confidence level of the analysis. In general, a higher number of criteria used to eliminate an attack indicates a stronger assurance that an attack is

beyond the capabilities of an attacker. In other words, it would be necessary for the analyst to misjudge the capabilities of the attacker in multiple ways for the result to be incorrect.

- **Scenario Sensitivity** - This report is only available in a pruning window if the scenario based method of pruning was used. This report shows if an attack scenario was removed based on the pruning criterion. See the Pruning Sensitivity report for more information on the usage of this report.
- **Advanced Analysis** - The Advanced Analysis table. This report is only available in an Advanced Analysis window.
- **Potential Choke Points** - This report has information for each node in the tree. Each time a node is found in an attack scenario, the value for these columns in the attack scenario are accumulated; Capabilistic Propensity, Impact, Relative Risk and Cumulative Risk. This can be used to determine which nodes in the tree contribute the greatest risk or impact. This report is only available in an Advanced Analysis window.

The first two reports can be saved to a file. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for these report files is .txt.

The reports in table format can also be saved. This option can be used to save the tree information to a file in a format so it can be used in a spreadsheet program such as Microsoft Excel. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. Now you will get the *Report Setup* dialog. You must choose either CSV Format (comma separated values) or Delimited Format. If you choose Delimited, you must now choose a character from the pull-down list that will be used to delimit the fields in the node information. If the character that was chosen is found in the text of the node information, you will receive the message: *Column delimiter was found in tree data. File will not be properly delimited.* This means data that should be in one column will be split across more than one column in the spreadsheet. You must also decide if new line characters should be removed from the note areas. If these note areas contain *new line characters* and they are not removed, the note area will go to the next line in the spreadsheet.

3. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for report files in CSV Format is .csv and in Delimited Format is .rpt.
4. After the file has been saved, you can open it in a spreadsheet program. If you are using Excel, it is best to first start Excel then open the report file you created. This will cause the "Text Import Wizard" to start which will ask about the character that is used to delimit the data. Select "Delimited", then choose "Other" and enter the character that you used as a delimiter (the default is "|"). The data should now be in columns in the spreadsheet.

The reports **Attack Scenarios** and **Advanced Analysis** allow another save option. You can choose to save the tree image for each scenario (from the specified start row through the specified end row) to a separate file. The directory where the files are saved defaults to the directory that was used to open this tree. You can specify a different directory by clicking on **Change**. The images are saved as png files with the name *scenarioXX.png* where XX is the scenario number (not the row number). If there is already a file by that name in the directory it will be overwritten.

All of the reports can be printed. To print a report:

1. Select the report format you want. Note, for reports in table format you may need to adjust the column dividers to ensure that the columns are the correct width for viewing as they are printed using WYSIWYG (what you see is what you get).
2. Click on **Page Layout** to set page margins, print orientation, and header and footer settings.
3. Click on the **Print...** button or select **File > Print...** from the menu on the *Reports* window.
4. Alternatively, if this is a table-type report, you can click on **Print Custom**. You will be given further options such as specifying the start and end row, and if the report should be shrunk to fit the page horizontally. If this is the Advanced Analysis table, the additional options to create a detailed report, include tree images and print the tree in black and white or color are also given.
5. A **Print Preview** window will show your report.
6. Click on **Print...** to send your report to the printer.

## Print Tree...

The **File > Print Tree...** command allows you to print the current Attack (Threat) Tree.

1. Select the **File > Print Tree...** command from the application menu, or click on the **Print Tree** icon on the [toolbar](#).
2. The **Print Options** dialog will appear. Change the settings as required.
  - The size of the printout can be set. If *Default Size* is selected, the tree will be printed in a size similar to that seen on the screen. If *Fit to page* is selected, the tree will be printed so that it fits on one page. If *Resize* is selected, the *Scale Factor* can be specified where 1 is the default size, 0.5 is half the size and 2.0 is twice as big. You can specify the scale factor you require.
  - You can specify a Main Title and Sub Title for the printout.
  - Trees can be printed in color or black and white.
  - The font size for the text in the nodes can be specified.

Note: These Print Options are saved with the tree. If you open a new tree, the settings will be different.

- The *Page Layout* button will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.
  - Select **OK** to save the settings, **Print...** to continue with printing or **Cancel** to cancel out of printing.
3. If you select **Print...**, you will now see a preview of how the tree will be printed. If all looks good, click **Print...** (at the top of the window) to select your printer and send the printout to the printer.

## Page Layout

The **File > Page Layout** command will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.

## Close

This command is used to **Close** the active *Pruning Window*. When all *Pruning Windows* have been closed, the main tree will no longer be in *Pruning Mode*. An alternate way to close all *Pruning Windows* is by selecting **Analyze > Close Pruning Windows** from the application menu.



## Edit Menu

The following options are available under the **Edit** menu:

[Edit Agent Profile...](#)

[Change Calculation Method...](#)

[Copy](#)

[Find...](#)

## Edit Agent Profile...

Selecting **Edit > Edit Agent Profile...**, or clicking on the **Edit Agent Profile** icon on the [toolbar](#) will open the *Edit Agent Profile - Specify Pruning Criteria - <pruning window name>* dialog. You can Add, Edit, or Delete the *Pruning Criteria* for the *Agent Profile*. After changes have been made, the *Pruning Criteria* will be applied to the base tree. Any nodes with values outside of the range of the evaluator will be pruned. For example, if the evaluator was "Cost of Attack  $\leq$  2000", any nodes with values greater than 2000 will be pruned.

A message will be displayed above the tree display area which informs you of the number of nodes removed during the application of the pruning criteria.

The process of adding and editing *Pruning Criteria* can continue using any of the indicators that are required to reflect the threat agent attack this pruning is simulating. It is very simple to modify the value for the indicators to reflect the resources available to the *Threat Agent* that is being modeled.

See [Agent Profiles and Pruning Criteria](#) for more information on the differences between these two concepts.

### **Editing** *Pruning Criteria* for the *Agent Profile*:

1. Select the *Indicator Name* by choosing from the pull-down list.
2. Select the *Operator* from the pull-down list.
3. Enter the *Value* for the *Pruning Criteria*. If the indicator is Boolean then *True* or *False* can be chosen, otherwise, a numeric value must be entered.
4. If you want to delete the *Pruning Criteria* for an indicator, select the operator "*Undefined*" and the *Pruning Criteria* will be removed from the *Agent Profile* list.
5. Click the *Apply* button to apply the *Pruning Criteria* to the tree.
6. You can continue refining the *Operators* and *Values* for each *Pruning Criteria*.
7. Click the *Close* button when you are finished using the *Edit Agent Profile* window.

### **Notes** for the *Agent Profile*:

*Notes* can be added for the *Agent Profile* to explain your rationale for choosing the values for your *Pruning Criteria*.

## Change Calculation Method...

The **Change Calculation Method...** command is used to change the method of calculation that is used while pruning the tree. Select either "**Scenario Based**", "**Node-Based**", or "**Scenario and Node Based**" by clicking on the radio buttons. For those who would like to understand the computational differences between the pruning modes, see [Explanation of Pruning Methods](#).

## Copy

This command is used to **Copy** the tree image to the system clipboard. The copy can be performed on the entire tree or a subtree.

1. Select the node or subtree you want to copy by clicking the node. This will cause the node to be highlighted in yellow. If you do not select a node on the tree, the entire tree will be copied. Select **Copy** by choosing **Edit > Copy** or by using the right mouse button to click the selected node and then selecting **Copy**.
2. The selected node or subtree will be copied.
3. The system clipboard now contains the subtree in several different formats: raster image, vector image, pdf, and in the tree structure format.

The image of the tree can be pasted into another application such as a word processor. In Word, use Paste Special, then select the required format.

## Find...

The find feature can be used to search for text strings within nodes.

1. To start the **Find** function, select the **Edit > Find...** command from the application menu, or click on the **Find** icon on the [toolbar](#).
2. In the "Find What:" box, either:
  - type in the search string, or choose a previous search string from the drop-down list. If the search string should be saved for future use, the list of search strings can be edited by clicking the button. See also **Tools > Preferences > Interface**.

or select:

- Nodes with empty note fields
  - Nodes with undefined values
  - Root of links
  - Nodes with indicator values: and select the Indicator, Operator and Value.
  - Single Shot Attack
  - Single Threaded Attack
  - Multi-Threaded Attack
  - Reduced Nodes
  - Benefit-based Attack Effectiveness
  - Encounter-based Attack Effectiveness
  - SAND or Custom AND defined
3. If "Search String" was selected in the "Find What:" area, select the areas that should be searched by checking the fields in the "Look In:" area. You can choose "Node Name" and/or any notes that have been defined for the tree. Internal and External ID can also be searched.
  4. The "Match:" area allows you to control the options for the search.
    - Case: Find text matching the specified pattern of uppercase and lowercase letters.
    - Whole words: Find occurrences of the text as whole words.
    - [Regular expression](#): Specify the search string in the form of a regular expression. [See Using SecurITree > Regular Expressions](#) for more information.
  5. The scope for the search can be either:
    - the entire tree or

- the subtree starting at the currently selected node or
  - only *LEAF* nodes
6. After clicking on Search, the results of the search are displayed. You can click on a node in the result list, which will cause the node to be selected. If you double-click the node, the Edit Node window will open which will allow you to edit the node. All occurrences of the search string will be highlighted in yellow.
  7. If the node is part of a sub-tree that has been rolled-up, the button "Roll Down" will show in the Action column. Clicking on that button will cause the subtree to be rolled down.
  8. A Replace can be performed based on the search criteria that has been used. Select either "Replace All" or "Replace Selected" (after selecting one or more entries in the search results area). A dialog window will open which will allow you to enter the new value.
    - When the replace function is used with "Search String", it will replace text found in Node names or Notes.
    - When used with "Nodes with indicator values:", all matching LEAF node values and AND/OR impact values will be changed.
  9. The search results list can be printed by clicking the "Print Results" button.
  10. The table of search results can be saved by clicking the "Save As" button. See the section on saving table reports in [Reports](#) for more information.
  11. A node or multiple nodes can be deleted by selecting the node/s in the table. All highlighted nodes will be deleted after confirmation.

## View Menu

The following options are available under the **View** menu:

[Zoom...](#)

[Depth Display Level...](#)

[Show Legend on Tree](#)

[Roll Up Subtree](#)

[Roll Down Subtree](#)

[Roll Down Subtree 1 Level](#)

[Roll Down Subtree x Levels...](#)

[Roll Down Nested Subtrees](#)

[Display Pruned Nodes](#)

## Zoom...

The **Zoom** command is used to enlarge or reduce the size of the nodes in the application window. To change the node size:

1. Click either the + (**Zoom In**) or - (**Zoom Out**) or (**Zoom to Fit**) magnifying glass icon on the [toolbar](#). The view of the tree changes immediately.
2. Choose **View > Zoom...** from the application menu. You will get the *Zoom* dialog box where the node size can be specified. You can either select one of the preset zoom percentages by clicking on a radio button, or you can enter a percentage in the box on the bottom of the dialog for a custom setting. In both cases, the new node size is shown in the preview window. Once the desired zoom setting is arrived at, click *OK* to apply it to the view of the tree.



## Depth Display Level...

The **Depth Display Level...** command is used for viewing the tree to the desired depth of detail making it easy to summarize the tree you are working on.

- To hide or display nodes in the application window choose **View > Depth Display Level...** from the application menu. Select the number of levels you would like to see from the pull-down list, then click *OK*.
- If you would like to display all nodes on the tree, select *All* from the pull-down list.
- The status line (at the bottom of the screen) will be updated to inform you of the number of levels in the tree that are displayed.

## Show Legend on Tree

The **View > Show Legend on Tree** command allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

This information can be set by selecting **Tools > Preferences** from the application menu, then choosing the **Node Info** tab to set indicator values to be displayed, or the **Flags** tab to define flags.

## Roll Up Subtree

The **Roll Up Subtree** command is used to hide all nodes under the selected node making it easier to view the area of the tree you are working on.

1. Select the topmost node you still want to see by clicking the node. This will cause the node to be highlighted in yellow.
2. To hide all nodes beneath the selected node, choose **View > Roll Up Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Up Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-U** or **Ctrl-<up arrow key>**.
4. The node color will change and a down pointing arrow will be added to indicate there are more nodes under this one that are currently not being displayed.

## Roll Down Subtree

The **Roll Down Subtree** command is used to show all nodes under the selected node if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. To show all nodes beneath the selected node, choose **View > Roll Down Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-D** or **Ctrl-<down arrow key>**.
4. The node will change to its normal colour and all nodes under this one will be displayed.

## Roll Down Subtree 1 Level

The **Roll Down Subtree 1 Level** command is used to show all nodes one level under the selected node.

1. Select a node on the tree by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree 1 Levels** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree 1 Level** on the pop-up menu. Or, click on the node then press **Ctrl-Shift-D**.
4. One level of nodes below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Subtree x Levels

The **Roll Down Subtree x Levels** command is used to show all nodes under the selected node (to the desired depth) if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree x Levels...** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree x Levels...** on the pop-up menu.
4. You will be asked to enter the number of levels to be rolled down. That number of levels below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Nested Subtrees

The **Roll Down Nested Subtrees** command is used to show all nodes under the selected node.

1. Select a node that is to be the start of the subtree to be rolled down by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Nested Subtrees** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Nested Subtrees** on the pop-up menu.
4. To roll down the entire tree, select the root node.

## Display Pruned Nodes

The **View > Display Pruned Nodes** command allows you to display or hide the nodes that are pruned after applying the agent profile pruning criteria. The pruned nodes are displayed with dimmed colors.



## Analyze Menu

The following options are available under the **Analyze** menu:

[Attack Scenarios...](#)

## Attack Scenarios...

To initiate the **Attack Scenarios...** process, select **Analyze > Attack Scenarios...** from the main pruning menu. An *Attack Scenarios* window is then displayed for the *Pruning Tree*.

The top portion of the window has a table which lists all the *Attack Scenarios* for the *Base Tree*. Clicking on any of the *Attack Scenarios* listed will change the tree displayed so that it represents that particular scenario. Clicking on any of the column headings in the table will sort the table in ascending/descending order based on the items in that column.

See [Attack Scenarios](#) for more information on this subject.

## Tools Menu

The following options are available under the **Tools** menu:

[Display Toolbars](#)

[Show Node Information Panel](#)

[Preferences](#)

## Display Toolbar

The **Display Toolbar** command is used to hide or display the application toolbar. Choose **Tools > Display Toolbar** from the application menu and the [toolbar](#) will toggle from being displayed or hidden.

## Show Node Information Panel

The **Tools > Show Node Information Panel** command allows you to display or hide the [Node Information](#) side panel. The panel can also be displayed or hidden by pressing **Ctrl-i**.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".

## Preferences

The **Preferences** option is used to define your choices and settings. Choose **Tools > Preferences** from the menu and the Preferences window will appear. The only tab available in this mode is Node Info.

Changes to Node Info settings can be made in this window.

**Display Indicator Values** is used to display the indicator values for the nodes on the tree.

Choose Values to Display:

- Select one or more of the indicators you would like displayed by clicking the check boxes.
- A legend will appear in the top left corner of the application window and the selected indicator values will then be displayed beside the nodes.
- The color the indicator value is displayed in corresponds to the color used to display the name of the indicator function in the legend.

The *Show Legend on Tree* checkbox allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

The legend can also be set by selecting **View > Show Legend on Tree** from the application menu.

**NOTE:** A total of five (5) Indicator Values can be displayed at one time.

The **Node Display Settings** section has controls that can be used to change the way nodes are displayed for the tree. These settings are saved with the tree and are not saved as user defined settings.

- The **Display Node ID** setting is used to display the node IDs beside the node name inside every node in the tree.
- The **Reset all node colors to default** button can be selected to change any nodes that were individually changed to different colors. If this action is selected, it cannot be cancelled or undone with the **Undo** function.
- **Auto size all nodes on tree** is used to set all node sizes so that the node name fits into the node box.
- **Reset all nodes to standard size** will reset any nodes that were individually changed to a different size and/or set to auto-size. If this action is selected, it cannot be cancelled or undone with the **Undo** function.

**NOTE:** The tree can be displayed with the default node sizes while retaining customized sizes by selecting the Interface tab then clicking on "Display Standard Node Sizes".

Click on *OK* once you have chosen the values to display. The Node Information that was selected will now be displayed on the tree.

## Help Menu

The following options are available under the **Help** menu:

[Help Index](#)

[Context Sensitive Help](#)

[Legend](#)

[About](#)



## Help Index

The **Help > Help Index** command is used to access these help files.

## Context Sensitive Help

The **Context Sensitive Help** command is used to directly access help on menu, toolbar, and side panel items by clicking on them.

1. Choose **Help > Context Sensitive Help** from the application menu. The mouse pointer will change from a *Normal Select* (just an arrow) to a *Help Select* (an arrow with a ?) pointer.
2. Move the mouse pointer to the desired menu, toolbar, and side panel item that you require help with and click on it.
3. If there is **Context Sensitive Help** the *Help Index* window will appear with the proper help topic displayed. If there is no **Context Sensitive Help** then the mouse pointer will revert back to *Normal Select*.

## Legend

The **Help > Legend** command opens a window which displays a legend describing the node types on trees. It will also show Tree Setting information including Flags and Indicator information.

## About

Displays the following information about the product:

- Current **SecurITree** Version and Build Numbers
- Contact Information
- Copyright Information

If you click on the **License** button, the *License* window will open which contains the following information:

- Type of License
- Who it is Licensed to
- License Expiration Date
- End User License Agreement (EULA)

If you click on the **JavaVM** button, the JavaVM window will open which will show:

- The Java Version that is being used for **SecurITree**
- The Total Memory available to use and the current Free Memory. To make changes to the memory available for the application, see [Memory Errors](#).

The **Properties** button will show:

- The location of the SecurITree\_console.txt file and SecurITree.cfg file.
- A listing of the Java properties.

The **Console** button will display:

- The contents of the SecurITree\_console.txt file which may contain error messages.

The **Splash** button will display the splash screen.

## Set Operations on Pruned Trees Menus

The Set Operations on Pruned Trees Window has the following Menus:

[File](#)

[Edit](#)

[View](#)

[Tools](#)

[Help](#)

Associated with an attack tree is a set of *attack scenarios* which describe different ways in which the root goal of the attack tree could hypothetically be achieved. The main attack tree can be *pruned* based on the capabilities of particular threat agents. The pruning operations remove nodes from the main tree that are not usable by the threat agent in their quest for the root node. Unless the threat agent is capable of performing every possible scenario this means that the *attack scenarios* for a pruned tree are a subset of the scenarios for the main tree.

It is often useful to compare and analyze the various attack scenario subsets associated (by pruning) with the various threat agents. For instance, an analyst might study two adversaries that are identical in all capabilities except that one has insider access (i.e., the ability to breach trust). The analyst might use pruning to identify the scenarios that could be performed by each adversary. The outsider pruned tree would identify the scenarios available to the outsider. The insider pruned tree would identify all scenarios available to the insider. Note that this would include the outsider scenarios since there is nothing to preclude an insider from performing an outsider attack. It would not be immediately obvious which scenarios were unique to the insider. However, this would be easy to determine using a *set difference* operation.

{Set of all insider attack scenarios} - {Set of outsider attack scenarios} = {Set of attack scenarios unique to insider}

Many useful analytic activities are possible using *set operations*.

Note that an earlier form of *set operations* (Leaf node-based evaluation) is now deprecated and will be removed in the next release of SecurITree.

## File Menu

The following options are available under the **File** menu:

[Save Tree](#)

[Save Tree As...](#)

[Reports...](#)

[Print Tree...](#)

[Page Layout](#)

[Close](#)

## Save Tree

Use the **File > Save Tree** command to save your file to disk. It is recommended that files be saved on a regular basis during a **SecurITree** session and especially after significant changes have been made.

1. Select the **File > Save Tree** command from the application menu, or click on the **Save Tree** icon on the [toolbar](#).
2. If this is a new Attack (Threat) Tree that was not previously saved, the **Save Tree** dialog box will be displayed. Select the folder you want to save the file in, type in a name for this file and click on the *Save* button.
3. If this tree was previously saved or was opened from disk, it will automatically be saved using the same filename.

## Save Tree As...

Use the **File > Save Tree As...** command to save your file to disk with a new name. It is recommended that files be saved on a regular basis during a **SecurITree** session, and especially after significant changes have been made.

1. Select the **File > Save Tree As...** command from the application menu, or click on the **Save Tree As** icon on the [toolbar](#).
2. The [Save](#) dialog box will be displayed. Select the folder you want to save the file in, enter a new file name if required, and click on the *Save* button to save your file with a new name.
3. Files can also be saved in different formats. If you would like to save the tree as you see it on the screen as an image file, you can choose either PNG, JPG, or SVG format. The *Files of type:* field has a pull-down list. If you choose *PNG Files (\*.png)*, *JPG Files (\*.jpg)*, or *SVG Files (\*.svg)* your tree will be saved as an image. You should use a matching extension in the *File name:* field or do not specify an extension and the correct extension will be added for you.

This command allows you to *Save Attack (Threat) Tree* files into the following file formats:

File Types	Format / Purpose
.rit	to save the file with a new name (similar to using <b>File &gt; Save As...</b> )
.ril	to save the file as a <b>SecurITree</b> library
.png	to save the file as a Portable Network Graphics image
.jpg	to save the file as a JPEG (Joint Photographic Experts Group) image
.svg	to save the file as an SVG (Scalable Vector Graphics) image
.atml	to save the file in Attack Tree Markup Language - xml format
.gxl	to save the file in Graph eXchange Language



## Reports...

The **File > Reports > Basic Reports** command allows you to view the Attack (Threat) Tree you are working on in a tabular format. The following Reports are available:

- **All Nodes** - All nodes on the tree are displayed in the report.
- **Only Leaf Nodes** - Only LEAF nodes are included in the report.
- **Complete Node Information** - All indicator values and notes are included in the report.
- **Complete Node Information - LEAF nodes only** - All indicator values and notes are included in the report.
- **Complete Node Information + Scenarios per Node** - The number of times the node occurs in scenarios is calculated and included in the report. Clicking on a node in the table will display a table showing all scenarios where this node is found. Clicking on a scenario will show the tree for the scenario.
- **Attack Scenarios** - A listing of all Attack Scenarios. This report is only available in an Attack Scenario window or in an Advanced Analysis window.
- **Agent Profile Cross-Reference** - This report is only available if pruning windows have been created. The report indicates which agent profiles are capable of performing an attack by placing an "X" under the appropriate pruning window name. If a node was removed from a tree during pruning operations, it will not have an "X" in that column.
- **Pruning Sensitivity** - This report is only available in a pruning window if the node-based method of pruning was used. The report provides a list of all pruning criteria and whether or not nodes were eliminated from the tree. If a node was removed on a particular pruning criterion, an "X" is placed in the column. The total number of criteria that caused the node to be pruned (removed) is also displayed.

The delta column for each pruning criteria is colored. This is the explanation of the color coding:

- Pink/(Red) represent attacks that are within/(well within) the capability of the threat agent.
- Light Yellow/(Dark Yellow) represent attacks that are nearly within/(just within) the capability of the threat agent.
- Light Green/(Green) represent attacks beyond/(well beyond) the capability of the threat agent.
- Numeric indicator values express the resources required to carry out the attack.
- # indicator values show the resources available to the attacker minus resources required to carry out the attack.
- Negative values indicate the attacker had a shortfall of the resources required for the attack.

This report provides a useful guide of the confidence level of the analysis. In general, a higher number of criteria used to eliminate an attack indicates a stronger assurance that an attack is

beyond the capabilities of an attacker. In other words, it would be necessary for the analyst to misjudge the capabilities of the attacker in multiple ways for the result to be incorrect.

- **Scenario Sensitivity** - This report is only available in a pruning window if the scenario based method of pruning was used. This report shows if an attack scenario was removed based on the pruning criterion. See the Pruning Sensitivity report for more information on the usage of this report.
- **Advanced Analysis** - The Advanced Analysis table. This report is only available in an Advanced Analysis window.
- **Potential Choke Points** - This report has information for each node in the tree. Each time a node is found in an attack scenario, the value for these columns in the attack scenario are accumulated; Capabilistic Propensity, Impact, Relative Risk and Cumulative Risk. This can be used to determine which nodes in the tree contribute the greatest risk or impact. This report is only available in an Advanced Analysis window.

The first two reports can be saved to a file. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for these report files is .txt.

The reports in table format can also be saved. This option can be used to save the tree information to a file in a format so it can be used in a spreadsheet program such as Microsoft Excel. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. Now you will get the *Report Setup* dialog. You must choose either CSV Format (comma separated values) or Delimited Format. If you choose Delimited, you must now choose a character from the pull-down list that will be used to delimit the fields in the node information. If the character that was chosen is found in the text of the node information, you will receive the message: *Column delimiter was found in tree data. File will not be properly delimited.* This means data that should be in one column will be split across more than one column in the spreadsheet. You must also decide if new line characters should be removed from the note areas. If these note areas contain *new line characters* and they are not removed, the note area will go to the next line in the spreadsheet.

3. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for report files in CSV Format is .csv and in Delimited Format is .rpt.
4. After the file has been saved, you can open it in a spreadsheet program. If you are using Excel, it is best to first start Excel then open the report file you created. This will cause the "Text Import Wizard" to start which will ask about the character that is used to delimit the data. Select "Delimited", then choose "Other" and enter the character that you used as a delimiter (the default is "|"). The data should now be in columns in the spreadsheet.

The reports **Attack Scenarios** and **Advanced Analysis** allow another save option. You can choose to save the tree image for each scenario (from the specified start row through the specified end row) to a separate file. The directory where the files are saved defaults to the directory that was used to open this tree. You can specify a different directory by clicking on **Change**. The images are saved as png files with the name *scenarioXX.png* where XX is the scenario number (not the row number). If there is already a file by that name in the directory it will be overwritten.

All of the reports can be printed. To print a report:

1. Select the report format you want. Note, for reports in table format you may need to adjust the column dividers to ensure that the columns are the correct width for viewing as they are printed using WYSIWYG (what you see is what you get).
2. Click on **Page Layout** to set page margins, print orientation, and header and footer settings.
3. Click on the **Print...** button or select **File > Print...** from the menu on the *Reports* window.
4. Alternatively, if this is a table-type report, you can click on **Print Custom**. You will be given further options such as specifying the start and end row, and if the report should be shrunk to fit the page horizontally. If this is the Advanced Analysis table, the additional options to create a detailed report, include tree images and print the tree in black and white or color are also given.
5. A **Print Preview** window will show your report.
6. Click on **Print...** to send your report to the printer.

## Print Tree...

The **File > Print Tree...** command allows you to print the current Attack (Threat) Tree.

1. Select the **File > Print Tree...** command from the application menu, or click on the **Print Tree** icon on the [toolbar](#).
2. The **Print Options** dialog will appear. Change the settings as required.
  - The size of the printout can be set. If *Default Size* is selected, the tree will be printed in a size similar to that seen on the screen. If *Fit to page* is selected, the tree will be printed so that it fits on one page. If *Resize* is selected, the *Scale Factor* can be specified where 1 is the default size, 0.5 is half the size and 2.0 is twice as big. You can specify the scale factor you require.
  - You can specify a Main Title and Sub Title for the printout.
  - Trees can be printed in color or black and white.
  - The font size for the text in the nodes can be specified.

Note: These Print Options are saved with the tree. If you open a new tree, the settings will be different.

- The *Page Layout* button will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.
  - Select **OK** to save the settings, **Print...** to continue with printing or **Cancel** to cancel out of printing.
3. If you select **Print...**, you will now see a preview of how the tree will be printed. If all looks good, click **Print...** (at the top of the window) to select your printer and send the printout to the printer.

## Page Layout

The **File > Page Layout** command will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.

## Close

This command is used to **Close** the active *Set Operations on Pruned Trees Window*.

## Edit Menu

The following options are available under the **Edit** menu:

[Copy](#)

[Find...](#)

## Copy

This command is used to **Copy** the tree image to the system clipboard. The copy can be performed on the entire tree or a subtree.

1. Select the node or subtree you want to copy by clicking the node. This will cause the node to be highlighted in yellow. If you do not select a node on the tree, the entire tree will be copied. Select **Copy** by choosing **Edit > Copy** or by using the right mouse button to click the selected node and then selecting **Copy**.
2. The selected node or subtree will be copied.
3. The system clipboard now contains the subtree in several different formats: raster image, vector image, pdf, and in the tree structure format.

The image of the tree can be pasted into another application such as a word processor. In Word, use Paste Special, then select the required format.



## Find...

The find feature can be used to search for text strings within nodes.

1. To start the **Find** function, select the **Edit > Find...** command from the application menu, or click on the **Find** icon on the [toolbar](#).
2. In the "Find What:" box, either:
  - type in the search string, or choose a previous search string from the drop-down list. If the search string should be saved for future use, the list of search strings can be edited by clicking the button. See also **Tools > Preferences > Interface**.

or select:

- Nodes with empty note fields
  - Nodes with undefined values
  - Root of links
  - Nodes with indicator values: and select the Indicator, Operator and Value.
  - Single Shot Attack
  - Single Threaded Attack
  - Multi-Threaded Attack
  - Reduced Nodes
  - Benefit-based Attack Effectiveness
  - Encounter-based Attack Effectiveness
  - SAND or Custom AND defined
3. If "Search String" was selected in the "Find What:" area, select the areas that should be searched by checking the fields in the "Look In:" area. You can choose "Node Name" and/or any notes that have been defined for the tree. Internal and External ID can also be searched.
  4. The "Match:" area allows you to control the options for the search.
    - Case: Find text matching the specified pattern of uppercase and lowercase letters.
    - Whole words: Find occurrences of the text as whole words.
    - [Regular expression](#): Specify the search string in the form of a regular expression. [See Using SecurITree > Regular Expressions](#) for more information.
  5. The scope for the search can be either:
    - the entire tree or

- the subtree starting at the currently selected node or
  - only *LEAF* nodes
6. After clicking on Search, the results of the search are displayed. You can click on a node in the result list, which will cause the node to be selected. If you double-click the node, the Edit Node window will open which will allow you to edit the node. All occurrences of the search string will be highlighted in yellow.
  7. If the node is part of a sub-tree that has been rolled-up, the button "Roll Down" will show in the Action column. Clicking on that button will cause the subtree to be rolled down.
  8. A Replace can be performed based on the search criteria that has been used. Select either "Replace All" or "Replace Selected" (after selecting one or more entries in the search results area). A dialog window will open which will allow you to enter the new value.
    - When the replace function is used with "Search String", it will replace text found in Node names or Notes.
    - When used with "Nodes with indicator values:", all matching LEAF node values and AND/OR impact values will be changed.
  9. The search results list can be printed by clicking the "Print Results" button.
  10. The table of search results can be saved by clicking the "Save As" button. See the section on saving table reports in [Reports](#) for more information.
  11. A node or multiple nodes can be deleted by selecting the node/s in the table. All highlighted nodes will be deleted after confirmation.

## View Menu

The following options are available under the **View** menu:

[Zoom...](#)

[Depth Display Level...](#)

[Show Legend on Tree](#)

[Roll Up Subtree](#)

[Roll Down Subtree](#)

[Roll Down Subtree 1 Level](#)

[Roll Down Subtree x Levels...](#)

[Roll Down Nested Subtrees](#)

[Display Flag Columns](#)

[Display Reduced Names](#)

[Show # of times node occurs in scenarios](#)

[Show Entire Tree](#)

[Wrap Cell Text](#)

[Color Node Names](#)

[Sort](#)

[Reset Column Width](#)

## Zoom...

The **Zoom** command is used to enlarge or reduce the size of the nodes in the application window. To change the node size:

1. Click either the + (**Zoom In**) or - (**Zoom Out**) or (**Zoom to Fit**) magnifying glass icon on the [toolbar](#). The view of the tree changes immediately.
2. Choose **View > Zoom...** from the application menu. You will get the *Zoom* dialog box where the node size can be specified. You can either select one of the preset zoom percentages by clicking on a radio button, or you can enter a percentage in the box on the bottom of the dialog for a custom setting. In both cases, the new node size is shown in the preview window. Once the desired zoom setting is arrived at, click *OK* to apply it to the view of the tree.

## Depth Display Level...

The **Depth Display Level...** command is used for viewing the tree to the desired depth of detail making it easy to summarize the tree you are working on.

- To hide or display nodes in the application window choose **View > Depth Display Level...** from the application menu. Select the number of levels you would like to see from the pull-down list, then click *OK*.
- If you would like to display all nodes on the tree, select *All* from the pull-down list.
- The status line (at the bottom of the screen) will be updated to inform you of the number of levels in the tree that are displayed.

## Show Legend on Tree

The **View > Show Legend on Tree** command allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

This information can be set by selecting **Tools > Preferences** from the application menu, then choosing the **Node Info** tab to set indicator values to be displayed, or the **Flags** tab to define flags.

## Roll Up Subtree

The **Roll Up Subtree** command is used to hide all nodes under the selected node making it easier to view the area of the tree you are working on.

1. Select the topmost node you still want to see by clicking the node. This will cause the node to be highlighted in yellow.
2. To hide all nodes beneath the selected node, choose **View > Roll Up Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Up Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-U** or **Ctrl-<up arrow key>**.
4. The node color will change and a down pointing arrow will be added to indicate there are more nodes under this one that are currently not being displayed.

## Roll Down Subtree

The **Roll Down Subtree** command is used to show all nodes under the selected node if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. To show all nodes beneath the selected node, choose **View > Roll Down Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-D** or **Ctrl-<down arrow key>**.
4. The node will change to its normal colour and all nodes under this one will be displayed.



## Roll Down Subtree 1 Level

The **Roll Down Subtree 1 Level** command is used to show all nodes one level under the selected node.

1. Select a node on the tree by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree 1 Levels** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree 1 Level** on the pop-up menu. Or, click on the node then press **Ctrl-Shift-D**.
4. One level of nodes below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Subtree x Levels

The **Roll Down Subtree x Levels** command is used to show all nodes under the selected node (to the desired depth) if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree x Levels...** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree x Levels...** on the pop-up menu.
4. You will be asked to enter the number of levels to be rolled down. That number of levels below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Nested Subtrees

The **Roll Down Nested Subtrees** command is used to show all nodes under the selected node.

1. Select a node that is to be the start of the subtree to be rolled down by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Nested Subtrees** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Nested Subtrees** on the pop-up menu.
4. To roll down the entire tree, select the root node.

## Display Flag Columns

The **View > Display Flag Columns** command allows you to display or hide columns for the flags defined for the tree. The column will show an "X" in the row if the attack scenario contains a node with that flag set. If there are no nodes with the flag set in the attack scenario, the cell will be blank.

The columns will only be displayed if there are flags defined for the tree.

## Display Reduced Names

The **View > Display Reduced Names** command allows you to decide how the leaf node names are displayed for the attack scenario.

If **Display Reduced Names** is selected, all leaf nodes are displayed. If it is not selected, the nodes under any subtrees that have been set as *reduced* will not be displayed. Instead, the name of the reduced subtree will be used.

## Show # times node occurs in scenarios

The **View > Show # times node occurs in scenarios** command allows you to toggle the visual display of node occurrence.

If **Show # times node occurs in scenarios** is selected, the lines joining nodes are shown as a light line for nodes that do not occur frequently, whereas nodes that occur in many scenarios will have a heavy line. The variable width line basically shows the influence of sections of the tree.

The actual number of times the node occurs in all scenarios is displayed on the right side of the node.

If indicator values are set to be displayed, the values will not be shown while this checkbox is selected. If it is not selected, the tree will be drawn with normal connecting lines.

## Show Entire Tree

The **View > Show Entire Tree** command allows you to toggle if all nodes on the tree should be displayed.

If **Show Entire Tree** is selected, all nodes are displayed but nodes that are not on the path for the selected attack scenario are shown dimly. If the checkbox is not selected, only the nodes on the path for the selected attack scenario are shown.

## Wrap Cell Text

The **View > Wrap Cell Text** command allows you to toggle the wrapping of text in the Attack Scenario column in the table.

If **Color Node Names** has been selected, selecting **Wrap Cell Text** will cause **Color Node Names** to be deselected.



## Color Node Names

The **View > Color Node Names** command allows you to toggle the coloring of node names in the Attack Scenario column in the table. If a node color is changed from the default node color (in the main window), that same color will be used in the table.

If **Wrap Cell Text** has been selected, **Color Node Names** cannot be selected.

## Sort

The sort feature can be used to sort a table on multiple columns.

1. To start the **Sort** function, select the **View > Sort** command from the menu, or click on the **Sort** icon on the [toolbar](#).
2. Choose a column name from the drop-down list, then select "Add". The column can be sorted in Ascending or Descending order.
3. To sort on secondary columns, choose additional columns then click "Add' again.
4. Click the "X" button to remove a sort criterion.
5. Click **OK** to sort the table.
6. Clicking on a column header on the table will cause the table to be sorted by that column and will override the choices in the Sort dialog.

## Reset Column Width

If column widths in the Attack Scenario table are changed, the widths will be remembered until the tree is closed. The **View > Reset Column Width** command will set widths back to the default, which is the width of the column header.

## Tools Menu

The following options are available under the **Tools** menu:

[Display Toolbars](#)

[Show Node Information Panel](#)

[Preferences](#)

## Display Toolbar

The **Display Toolbar** command is used to hide or display the application toolbar. Choose **Tools > Display Toolbar** from the application menu and the [toolbar](#) will toggle from being displayed or hidden.

## Show Node Information Panel

The **Tools > Show Node Information Panel** command allows you to display or hide the [Node Information](#) side panel. The panel can also be displayed or hidden by pressing **Ctrl-i**.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".

## Preferences

The **Preferences** option is used to define your choices and settings. Choose **Tools > Preferences** from the menu and the Preferences window will appear. The only tab available in this mode is Node Info.

Changes to Node Info settings can be made in this window.

**Display Indicator Values** is used to display the indicator values for the nodes on the tree.

Choose Values to Display:

- Select one or more of the indicators you would like displayed by clicking the check boxes.
- A legend will appear in the top left corner of the application window and the selected indicator values will then be displayed beside the nodes.
- The color the indicator value is displayed in corresponds to the color used to display the name of the indicator function in the legend.

The *Show Legend on Tree* checkbox allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

The legend can also be set by selecting **View > Show Legend on Tree** from the application menu.

**NOTE:** A total of five (5) Indicator Values can be displayed at one time.

The **Node Display Settings** section has controls that can be used to change the way nodes are displayed for the tree. These settings are saved with the tree and are not saved as user defined settings.

- The **Display Node ID** setting is used to display the node IDs beside the node name inside every node in the tree.
- The **Reset all node colors to default** button can be selected to change any nodes that were individually changed to different colors. If this action is selected, it cannot be cancelled or undone with the **Undo** function.
- **Auto size all nodes on tree** is used to set all node sizes so that the node name fits into the node box.
- **Reset all nodes to standard size** will reset any nodes that were individually changed to a different size and/or set to auto-size. If this action is selected, it cannot be cancelled or undone with the **Undo** function.

**NOTE:** The tree can be displayed with the default node sizes while retaining customized sizes by selecting the Interface tab then clicking on "Display Standard Node Sizes".

Click on *OK* once you have chosen the values to display. The Node Information that was selected will now be displayed on the tree.



## Help Menu

The following options are available under the **Help** menu:

[Help Index](#)

[Context Sensitive Help](#)

[Legend](#)

[About](#)

## Help Index

The **Help > Help Index** command is used to access these help files.

## Context Sensitive Help

The **Context Sensitive Help** command is used to directly access help on menu, toolbar, and side panel items by clicking on them.

1. Choose **Help > Context Sensitive Help** from the application menu. The mouse pointer will change from a *Normal Select* (just an arrow) to a *Help Select* (an arrow with a ?) pointer.
2. Move the mouse pointer to the desired menu, toolbar, and side panel item that you require help with and click on it.
3. If there is **Context Sensitive Help** the *Help Index* window will appear with the proper help topic displayed. If there is no **Context Sensitive Help** then the mouse pointer will revert back to *Normal Select*.

## Legend

The **Help > Legend** command opens a window which displays a legend describing the node types on trees. It will also show Tree Setting information including Flags and Indicator information.

## About

Displays the following information about the product:

- Current **SecurITree** Version and Build Numbers
- Contact Information
- Copyright Information

If you click on the **License** button, the *License* window will open which contains the following information:

- Type of License
- Who it is Licensed to
- License Expiration Date
- End User License Agreement (EULA)

If you click on the **JavaVM** button, the JavaVM window will open which will show:

- The Java Version that is being used for **SecurITree**
- The Total Memory available to use and the current Free Memory. To make changes to the memory available for the application, see [Memory Errors](#).

The **Properties** button will show:

- The location of the SecurITree\_console.txt file and SecurITree.cfg file.
- A listing of the Java properties.

The **Console** button will display:

- The contents of the SecurITree\_console.txt file which may contain error messages.

The **Splash** button will display the splash screen.

## Attack Scenarios Menus

The Attack Scenarios Window has the following Menus:

[File](#)

[Edit](#)

[View](#)

[Tools](#)

[Help](#)

## File Menu

The following options are available under the **File** menu:

[Save Tree](#)

[Save Tree As...](#)

[Reports...](#)

[Print Tree...](#)

[Page Layout](#)

[Close](#)

## Save Tree

Use the **File > Save Tree** command to save your file to disk. It is recommended that files be saved on a regular basis during a **SecurITree** session and especially after significant changes have been made.

1. Select the **File > Save Tree** command from the application menu, or click on the **Save Tree** icon on the [toolbar](#).
2. If this is a new Attack (Threat) Tree that was not previously saved, the **Save Tree** dialog box will be displayed. Select the folder you want to save the file in, type in a name for this file and click on the *Save* button.
3. If this tree was previously saved or was opened from disk, it will automatically be saved using the same filename.



## Save Tree As...

Use the **File > Save Tree As...** command to save your file to disk with a new name. It is recommended that files be saved on a regular basis during a **SecurITree** session, and especially after significant changes have been made.

1. Select the **File > Save Tree As...** command from the application menu, or click on the **Save Tree As** icon on the [toolbar](#).
2. The [Save](#) dialog box will be displayed. Select the folder you want to save the file in, enter a new file name if required, and click on the *Save* button to save your file with a new name.
3. Files can also be saved in different formats. If you would like to save the tree as you see it on the screen as an image file, you can choose either PNG, JPG, or SVG format. The *Files of type:* field has a pull-down list. If you choose *PNG Files (\*.png)*, *JPG Files (\*.jpg)*, or *SVG Files (\*.svg)* your tree will be saved as an image. You should use a matching extension in the *File name:* field or do not specify an extension and the correct extension will be added for you.

This command allows you to *Save Attack (Threat) Tree* files into the following file formats:

File Types	Format / Purpose
.rit	to save the file with a new name (similar to using <b>File &gt; Save As...</b> )
.ril	to save the file as a <b>SecurITree</b> library
.png	to save the file as a Portable Network Graphics image
.jpg	to save the file as a JPEG (Joint Photographic Experts Group) image
.svg	to save the file as an SVG (Scalable Vector Graphics) image
.atml	to save the file in Attack Tree Markup Language - xml format
.gxl	to save the file in Graph eXchange Language

## Reports...

The **File > Reports > Basic Reports** command allows you to view the Attack (Threat) Tree you are working on in a tabular format. The following Reports are available:

- **All Nodes** - All nodes on the tree are displayed in the report.
- **Only Leaf Nodes** - Only LEAF nodes are included in the report.
- **Complete Node Information** - All indicator values and notes are included in the report.
- **Complete Node Information - LEAF nodes only** - All indicator values and notes are included in the report.
- **Complete Node Information + Scenarios per Node** - The number of times the node occurs in scenarios is calculated and included in the report. Clicking on a node in the table will display a table showing all scenarios where this node is found. Clicking on a scenario will show the tree for the scenario.
- **Attack Scenarios** - A listing of all Attack Scenarios. This report is only available in an Attack Scenario window or in an Advanced Analysis window.
- **Agent Profile Cross-Reference** - This report is only available if pruning windows have been created. The report indicates which agent profiles are capable of performing an attack by placing an "X" under the appropriate pruning window name. If a node was removed from a tree during pruning operations, it will not have an "X" in that column.
- **Pruning Sensitivity** - This report is only available in a pruning window if the node-based method of pruning was used. The report provides a list of all pruning criteria and whether or not nodes were eliminated from the tree. If a node was removed on a particular pruning criterion, an "X" is placed in the column. The total number of criteria that caused the node to be pruned (removed) is also displayed.

The delta column for each pruning criteria is colored. This is the explanation of the color coding:

- Pink/(Red) represent attacks that are within/(well within) the capability of the threat agent.
- Light Yellow/(Dark Yellow) represent attacks that are nearly within/(just within) the capability of the threat agent.
- Light Green/(Green) represent attacks beyond/(well beyond) the capability of the threat agent.
- Numeric indicator values express the resources required to carry out the attack.
- # indicator values show the resources available to the attacker minus resources required to carry out the attack.
- Negative values indicate the attacker had a shortfall of the resources required for the attack.

This report provides a useful guide of the confidence level of the analysis. In general, a higher number of criteria used to eliminate an attack indicates a stronger assurance that an attack is

beyond the capabilities of an attacker. In other words, it would be necessary for the analyst to misjudge the capabilities of the attacker in multiple ways for the result to be incorrect.

- **Scenario Sensitivity** - This report is only available in a pruning window if the scenario based method of pruning was used. This report shows if an attack scenario was removed based on the pruning criterion. See the Pruning Sensitivity report for more information on the usage of this report.
- **Advanced Analysis** - The Advanced Analysis table. This report is only available in an Advanced Analysis window.
- **Potential Choke Points** - This report has information for each node in the tree. Each time a node is found in an attack scenario, the value for these columns in the attack scenario are accumulated; Capabilistic Propensity, Impact, Relative Risk and Cumulative Risk. This can be used to determine which nodes in the tree contribute the greatest risk or impact. This report is only available in an Advanced Analysis window.

The first two reports can be saved to a file. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for these report files is .txt.

The reports in table format can also be saved. This option can be used to save the tree information to a file in a format so it can be used in a spreadsheet program such as Microsoft Excel. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. Now you will get the *Report Setup* dialog. You must choose either CSV Format (comma separated values) or Delimited Format. If you choose Delimited, you must now choose a character from the pull-down list that will be used to delimit the fields in the node information. If the character that was chosen is found in the text of the node information, you will receive the message: *Column delimiter was found in tree data. File will not be properly delimited.* This means data that should be in one column will be split across more than one column in the spreadsheet. You must also decide if new line characters should be removed from the note areas. If these note areas contain *new line characters* and they are not removed, the note area will go to the next line in the spreadsheet.

3. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for report files in CSV Format is .csv and in Delimited Format is .rpt.
4. After the file has been saved, you can open it in a spreadsheet program. If you are using Excel, it is best to first start Excel then open the report file you created. This will cause the "Text Import Wizard" to start which will ask about the character that is used to delimit the data. Select "Delimited", then choose "Other" and enter the character that you used as a delimiter (the default is "|"). The data should now be in columns in the spreadsheet.

The reports **Attack Scenarios** and **Advanced Analysis** allow another save option. You can choose to save the tree image for each scenario (from the specified start row through the specified end row) to a separate file. The directory where the files are saved defaults to the directory that was used to open this tree. You can specify a different directory by clicking on **Change**. The images are saved as png files with the name *scenarioXX.png* where XX is the scenario number (not the row number). If there is already a file by that name in the directory it will be overwritten.

All of the reports can be printed. To print a report:

1. Select the report format you want. Note, for reports in table format you may need to adjust the column dividers to ensure that the columns are the correct width for viewing as they are printed using WYSIWYG (what you see is what you get).
2. Click on **Page Layout** to set page margins, print orientation, and header and footer settings.
3. Click on the **Print...** button or select **File > Print...** from the menu on the *Reports* window.
4. Alternatively, if this is a table-type report, you can click on **Print Custom**. You will be given further options such as specifying the start and end row, and if the report should be shrunk to fit the page horizontally. If this is the Advanced Analysis table, the additional options to create a detailed report, include tree images and print the tree in black and white or color are also given.
5. A **Print Preview** window will show your report.
6. Click on **Print...** to send your report to the printer.

## Print Tree...

The **File > Print Tree...** command allows you to print the current Attack (Threat) Tree.

1. Select the **File > Print Tree...** command from the application menu, or click on the **Print Tree** icon on the [toolbar](#).
2. The **Print Options** dialog will appear. Change the settings as required.
  - The size of the printout can be set. If *Default Size* is selected, the tree will be printed in a size similar to that seen on the screen. If *Fit to page* is selected, the tree will be printed so that it fits on one page. If *Resize* is selected, the *Scale Factor* can be specified where 1 is the default size, 0.5 is half the size and 2.0 is twice as big. You can specify the scale factor you require.
  - You can specify a Main Title and Sub Title for the printout.
  - Trees can be printed in color or black and white.
  - The font size for the text in the nodes can be specified.

Note: These Print Options are saved with the tree. If you open a new tree, the settings will be different.

- The *Page Layout* button will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.
  - Select **OK** to save the settings, **Print...** to continue with printing or **Cancel** to cancel out of printing.
3. If you select **Print...**, you will now see a preview of how the tree will be printed. If all looks good, click **Print...** (at the top of the window) to select your printer and send the printout to the printer.

## Page Layout

The **File > Page Layout** command will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.

## Close

This command is used to **Close** the active Attack Scenario Window.

## Edit Menu

The following options are available under the **Edit** menu:

[Copy](#)

[Find...](#)



## Copy

This command is used to **Copy** the tree image to the system clipboard. The copy can be performed on the entire tree or a subtree.

1. Select the node or subtree you want to copy by clicking the node. This will cause the node to be highlighted in yellow. If you do not select a node on the tree, the entire tree will be copied. Select **Copy** by choosing **Edit > Copy** or by using the right mouse button to click the selected node and then selecting **Copy**.
2. The selected node or subtree will be copied.
3. The system clipboard now contains the subtree in several different formats: raster image, vector image, pdf, and in the tree structure format.

The image of the tree can be pasted into another application such as a word processor. In Word, use Paste Special, then select the required format.

## Find...

The find feature can be used to search for text strings within nodes.

1. To start the **Find** function, select the **Edit > Find...** command from the application menu, or click on the **Find** icon on the [toolbar](#).
2. In the "Find What:" box, either:
  - type in the search string, or choose a previous search string from the drop-down list. If the search string should be saved for future use, the list of search strings can be edited by clicking the button. See also **Tools > Preferences > Interface**.

or select:

- Nodes with empty note fields
  - Nodes with undefined values
  - Root of links
  - Nodes with indicator values: and select the Indicator, Operator and Value.
  - Single Shot Attack
  - Single Threaded Attack
  - Multi-Threaded Attack
  - Reduced Nodes
  - Benefit-based Attack Effectiveness
  - Encounter-based Attack Effectiveness
  - SAND or Custom AND defined
3. If "Search String" was selected in the "Find What:" area, select the areas that should be searched by checking the fields in the "Look In:" area. You can choose "Node Name" and/or any notes that have been defined for the tree. Internal and External ID can also be searched.
  4. The "Match:" area allows you to control the options for the search.
    - Case: Find text matching the specified pattern of uppercase and lowercase letters.
    - Whole words: Find occurrences of the text as whole words.
    - [Regular expression](#): Specify the search string in the form of a regular expression. [See Using SecurITree > Regular Expressions](#) for more information.
  5. The scope for the search can be either:
    - the entire tree or

- the subtree starting at the currently selected node or
  - only *LEAF* nodes
6. After clicking on Search, the results of the search are displayed. You can click on a node in the result list, which will cause the node to be selected. If you double-click the node, the Edit Node window will open which will allow you to edit the node. All occurrences of the search string will be highlighted in yellow.
  7. If the node is part of a sub-tree that has been rolled-up, the button "Roll Down" will show in the Action column. Clicking on that button will cause the subtree to be rolled down.
  8. A Replace can be performed based on the search criteria that has been used. Select either "Replace All" or "Replace Selected" (after selecting one or more entries in the search results area). A dialog window will open which will allow you to enter the new value.
    - When the replace function is used with "Search String", it will replace text found in Node names or Notes.
    - When used with "Nodes with indicator values:", all matching LEAF node values and AND/OR impact values will be changed.
  9. The search results list can be printed by clicking the "Print Results" button.
  10. The table of search results can be saved by clicking the "Save As" button. See the section on saving table reports in [Reports](#) for more information.
  11. A node or multiple nodes can be deleted by selecting the node/s in the table. All highlighted nodes will be deleted after confirmation.

## View Menu

The following options are available under the **View** menu:

[Zoom...](#)

[Depth Display Level...](#)

[Show Legend on Tree](#)

[Roll Up Subtree](#)

[Roll Down Subtree](#)

[Roll Down Subtree 1 Level](#)

[Roll Down Subtree x Levels...](#)

[Roll Down Nested Subtrees](#)

[Display Flag Columns](#)

[Display Reduced Names](#)

[Show # of times node occurs in scenarios](#)

[Show Entire Tree](#)

[Wrap Cell Text](#)

[Color Node Names](#)

[Filter Scenarios](#)

[Sort](#)

[Reset Column Width](#)

## Zoom...

The **Zoom** command is used to enlarge or reduce the size of the nodes in the application window. To change the node size:

1. Click either the + (**Zoom In**) or - (**Zoom Out**) or (**Zoom to Fit**) magnifying glass icon on the [toolbar](#). The view of the tree changes immediately.
2. Choose **View > Zoom...** from the application menu. You will get the *Zoom* dialog box where the node size can be specified. You can either select one of the preset zoom percentages by clicking on a radio button, or you can enter a percentage in the box on the bottom of the dialog for a custom setting. In both cases, the new node size is shown in the preview window. Once the desired zoom setting is arrived at, click *OK* to apply it to the view of the tree.

## Depth Display Level...

The **Depth Display Level...** command is used for viewing the tree to the desired depth of detail making it easy to summarize the tree you are working on.

- To hide or display nodes in the application window choose **View > Depth Display Level...** from the application menu. Select the number of levels you would like to see from the pull-down list, then click *OK*.
- If you would like to display all nodes on the tree, select *All* from the pull-down list.
- The status line (at the bottom of the screen) will be updated to inform you of the number of levels in the tree that are displayed.

## Show Legend on Tree

The **View > Show Legend on Tree** command allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

This information can be set by selecting **Tools > Preferences** from the application menu, then choosing the **Node Info** tab to set indicator values to be displayed, or the **Flags** tab to define flags.

## Roll Up Subtree

The **Roll Up Subtree** command is used to hide all nodes under the selected node making it easier to view the area of the tree you are working on.

1. Select the topmost node you still want to see by clicking the node. This will cause the node to be highlighted in yellow.
2. To hide all nodes beneath the selected node, choose **View > Roll Up Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Up Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-U** or **Ctrl-<up arrow key>**.
4. The node color will change and a down pointing arrow will be added to indicate there are more nodes under this one that are currently not being displayed.



## Roll Down Subtree

The **Roll Down Subtree** command is used to show all nodes under the selected node if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. To show all nodes beneath the selected node, choose **View > Roll Down Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-D** or **Ctrl-<down arrow key>**.
4. The node will change to its normal colour and all nodes under this one will be displayed.

## Roll Down Subtree 1 Level

The **Roll Down Subtree 1 Level** command is used to show all nodes one level under the selected node.

1. Select a node on the tree by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree 1 Levels** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree 1 Level** on the pop-up menu. Or, click on the node then press **Ctrl-Shift-D**.
4. One level of nodes below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Subtree x Levels

The **Roll Down Subtree x Levels** command is used to show all nodes under the selected node (to the desired depth) if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree x Levels...** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree x Levels...** on the pop-up menu.
4. You will be asked to enter the number of levels to be rolled down. That number of levels below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Nested Subtrees

The **Roll Down Nested Subtrees** command is used to show all nodes under the selected node.

1. Select a node that is to be the start of the subtree to be rolled down by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Nested Subtrees** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Nested Subtrees** on the pop-up menu.
4. To roll down the entire tree, select the root node.

## Display Flag Columns

The **View > Display Flag Columns** command allows you to display or hide columns for the flags defined for the tree. The column will show an "X" in the row if the attack scenario contains a node with that flag set. If there are no nodes with the flag set in the attack scenario, the cell will be blank.

The columns will only be displayed if there are flags defined for the tree.

## Display Reduced Names

The **View > Display Reduced Names** command allows you to decide how the leaf node names are displayed for the attack scenario.

If **Display Reduced Names** is selected, all leaf nodes are displayed. If it is not selected, the nodes under any subtrees that have been set as *reduced*< will not be displayed. Instead, the name of the reduced subtree will be used.

## Show # times node occurs in scenarios

The **View > Show # times node occurs in scenarios** command allows you to toggle the visual display of node occurrence.

If **Show # times node occurs in scenarios** is selected, the lines joining nodes are shown as a light line for nodes that do not occur frequently, whereas nodes that occur in many scenarios will have a heavy line. The variable width line basically shows the influence of sections of the tree.

The actual number of times the node occurs in all scenarios is displayed on the right side of the node.

If indicator values are set to be displayed, the values will not be shown while this checkbox is selected. If it is not selected, the tree will be drawn with normal connecting lines.

## Show Entire Tree

The **View > Show Entire Tree** command allows you to toggle if all nodes on the tree should be displayed.

If **Show Entire Tree** is selected, all nodes are displayed but nodes that are not on the path for the selected attack scenario are shown dimly. If the checkbox is not selected, only the nodes on the path for the selected attack scenario are shown.



## Wrap Cell Text

The **View > Wrap Cell Text** command allows you to toggle the wrapping of text in the Attack Scenario column in the table.

If **Color Node Names** has been selected, selecting **Wrap Cell Text** will cause **Color Node Names** to be deselected.

## Color Node Names

The **View > Color Node Names** command allows you to toggle the coloring of node names in the Attack Scenario column in the table. If a node color is changed from the default node color (in the main window), that same color will be used in the table.

If **Wrap Cell Text** has been selected, **Color Node Names** cannot be selected.

## Filter Scenarios

The **Filter Scenarios** feature can be used to remove scenarios from the table based on defined criteria.

- To start the **Filter Scenarios** function, select the **View > Filter Scenarios** command from the menu, or click on the **Filter Scenarios** icon on the [toolbar](#).
- Choose a column name from the drop-down list, then select "Add".
- Now the criteria for filtering must be defined by specifying an operator and value.
- To filter on secondary columns, choose additional columns then click "Add" again.
- Select a criteria in the list then click the "Remove" button to remove a filter criteria
- Select a criteria in the list then click the "Edit" button to make changes to a filter criteria.
- The choice can be made to match any or match all criteria that have been defined.
- Click **OK** to filter the table. Only attack scenarios matching the criteria defined will be shown in the table.

## Sort

The sort feature can be used to sort a table on multiple columns.

1. To start the **Sort** function, select the **View > Sort** command from the menu, or click on the **Sort** icon on the [toolbar](#).
2. Choose a column name from the drop-down list, then select "Add". The column can be sorted in Ascending or Descending order.
3. To sort on secondary columns, choose additional columns then click "Add' again.
4. Click the "X" button to remove a sort criterion.
5. Click **OK** to sort the table.
6. Clicking on a column header on the table will cause the table to be sorted by that column and will override the choices in the Sort dialog.

## Reset Column Width

If column widths in the Attack Scenario table are changed, the widths will be remembered until the tree is closed. The **View > Reset Column Width** command will set widths back to the default, which is the width of the column header.

## Tools Menu

The following options are available under the **Tools** menu:

[Display Toolbars](#)

[Show Node Information Panel](#)

[Preferences](#)

## Display Toolbar

The **Display Toolbar** command is used to hide or display the application toolbar. Choose **Tools > Display Toolbar** from the application menu and the [toolbar](#) will toggle from being displayed or hidden.

## Show Node Information Panel

The **Tools > Show Node Information Panel** command allows you to display or hide the [Node Information](#) side panel. The panel can also be displayed or hidden by pressing **Ctrl-i**.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".



## Preferences

The **Preferences** option is used to define your choices and settings. Choose **Tools > Preferences** from the menu and the Preferences window will appear. The only tab available in this mode is Node Info.

Changes to Node Info settings can be made in this window.

**Display Indicator Values** is used to display the indicator values for the nodes on the tree.

Choose Values to Display:

- Select one or more of the indicators you would like displayed by clicking the check boxes.
- A legend will appear in the top left corner of the application window and the selected indicator values will then be displayed beside the nodes.
- The color the indicator value is displayed in corresponds to the color used to display the name of the indicator function in the legend.

The *Show Legend on Tree* checkbox allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

The legend can also be set by selecting **View > Show Legend on Tree** from the application menu.

**NOTE:** A total of five (5) Indicator Values can be displayed at one time.

The **Node Display Settings** section has controls that can be used to change the way nodes are displayed for the tree. These settings are saved with the tree and are not saved as user defined settings.

- The **Display Node ID** setting is used to display the node IDs beside the node name inside every node in the tree.
- The **Reset all node colors to default** button can be selected to change any nodes that were individually changed to different colors. If this action is selected, it cannot be cancelled or undone with the **Undo** function.
- **Auto size all nodes on tree** is used to set all node sizes so that the node name fits into the node box.
- **Reset all nodes to standard size** will reset any nodes that were individually changed to a different size and/or set to auto-size. If this action is selected, it cannot be cancelled or undone with the **Undo** function.

**NOTE:** The tree can be displayed with the default node sizes while retaining customized sizes by selecting the Interface tab then clicking on "Display Standard Node Sizes".

Click on *OK* once you have chosen the values to display. The Node Information that was selected will now be displayed on the tree.

## Help Menu

The following options are available under the **Help** menu:

[Help Index](#)

[Context Sensitive Help](#)

[Legend](#)

[About](#)

## Help Index

The **Help > Help Index** command is used to access these help files.

## Context Sensitive Help

The **Context Sensitive Help** command is used to directly access help on menu, toolbar, and side panel items by clicking on them.

1. Choose **Help > Context Sensitive Help** from the application menu. The mouse pointer will change from a *Normal Select* (just an arrow) to a *Help Select* (an arrow with a ?) pointer.
2. Move the mouse pointer to the desired menu, toolbar, and side panel item that you require help with and click on it.
3. If there is **Context Sensitive Help** the *Help Index* window will appear with the proper help topic displayed. If there is no **Context Sensitive Help** then the mouse pointer will revert back to *Normal Select*.

## Legend

The **Help > Legend** command opens a window which displays a legend describing the node types on trees. It will also show Tree Setting information including Flags and Indicator information.

## About

Displays the following information about the product:

- Current **SecurITree** Version and Build Numbers
- Contact Information
- Copyright Information

If you click on the **License** button, the *License* window will open which contains the following information:

- Type of License
- Who it is Licensed to
- License Expiration Date
- End User License Agreement (EULA)

If you click on the **JavaVM** button, the JavaVM window will open which will show:

- The Java Version that is being used for **SecurITree**
- The Total Memory available to use and the current Free Memory. To make changes to the memory available for the application, see [Memory Errors](#).

The **Properties** button will show:

- The location of the SecurITree\_console.txt file and SecurITree.cfg file.
- A listing of the Java properties.

The **Console** button will display:

- The contents of the SecurITree\_console.txt file which may contain error messages.

The **Splash** button will display the splash screen.

## Advanced Analysis Menus

The Advanced Analysis Window has the following Menus:

[File](#)

[Edit](#)

[View](#)

[Analyze](#)

[Tools](#)

[Help](#)



## File Menu

The following options are available under the **File** menu:

[Save Tree](#)

[Save Tree As...](#)

Agent Profile

[Load Agent Profile](#)

[Save Agent Profile](#)

[Print Agent Profile](#)

Victim Profile

[Load Victim Profile](#)

[Save Victim Profile](#)

[Print Victim Profile](#)

[Graphs](#)

[Reports...](#)

[Print Tree...](#)

[Page Layout](#)

[Close](#)

## Save Tree

Use the **File > Save Tree** command to save your file to disk. It is recommended that files be saved on a regular basis during a **SecurITree** session and especially after significant changes have been made.

1. Select the **File > Save Tree** command from the application menu, or click on the **Save Tree** icon on the [toolbar](#).
2. If this is a new Attack (Threat) Tree that was not previously saved, the **Save Tree** dialog box will be displayed. Select the folder you want to save the file in, type in a name for this file and click on the *Save* button.
3. If this tree was previously saved or was opened from disk, it will automatically be saved using the same filename.

## Save Tree As...

Use the **File > Save Tree As...** command to save your file to disk with a new name. It is recommended that files be saved on a regular basis during a **SecurITree** session, and especially after significant changes have been made.

1. Select the **File > Save Tree As...** command from the application menu, or click on the **Save Tree As** icon on the [toolbar](#).
2. The [Save](#) dialog box will be displayed. Select the folder you want to save the file in, enter a new file name if required, and click on the *Save* button to save your file with a new name.
3. Files can also be saved in different formats. If you would like to save the tree as you see it on the screen as an image file, you can choose either PNG, JPG, or SVG format. The *Files of type:* field has a pull-down list. If you choose *PNG Files (\*.png)*, *JPG Files (\*.jpg)*, or *SVG Files (\*.svg)* your tree will be saved as an image. You should use a matching extension in the *File name:* field or do not specify an extension and the correct extension will be added for you.

This command allows you to *Save Attack (Threat) Tree* files into the following file formats:

File Types	Format / Purpose
.rit	to save the file with a new name (similar to using <b>File &gt; Save As...</b> )
.ril	to save the file as a <b>SecurITree</b> library
.png	to save the file as a Portable Network Graphics image
.jpg	to save the file as a JPEG (Joint Photographic Experts Group) image
.svg	to save the file as an SVG (Scalable Vector Graphics) image
.atml	to save the file in Attack Tree Markup Language - xml format
.gxl	to save the file in Graph eXchange Language

## Load Agent Profile

- You can load an [Agent Profile](#) that was previously created. This is done by selecting **File > Agent Profile > Load Agent Profile**, or by clicking the **Load Agent Profile** button found on the *Define Indicator Utility Functions* window.
- A warning message is given if there are existing *Utility Functions* since they will be overwritten.
- If a file already exists with the same name as the name of this *Advanced Analysis Window*, it is pre-selected in the **File > Agent Profile > Load Agent Profile** dialog. You can also save *Agent Profiles* by clicking the **Save Agent Profile** button. *Agent Profile* files end with the extension .agt.
- After the file is selected, the *Define Indicator Utility Functions window* is opened (if it was not already opened).
- The *Utility Functions* for the *Agent Profile* can be edited by clicking on the buttons under the *Utility Mapping* heading on the right side of the window.
- When the *Utility Functions* you want to analyze have been entered, click on OK and they will be applied to the attack scenario table.

## Save Agent Profile

The *Indicator Utility Functions* can be saved and used for future evaluations on this tree or any other tree with matching indicator functions. Select **File > Agent Profile > Save Agent Profile** to save the *Indicator Utility Functions* to a file. *Agent Profile* files end with an extension of .agt.

## Print Agent Profile

The **File > Agent Profile > Print Agent Profile** command allows you to print the currently loaded Agent Profile.

1. Select the **File > Agent Profile > Print Agent Profile** command from the application menu.
2. You will now see a preview of your printout. If all looks good, click **Print...** (at the top of the window) to select your printer and send the printout to the printer.

## Load Victim Profile

- You can load a [Victim Profile](#) that was previously created. This is done by selecting **File > Victim Profile > Load Victim Profile**, or by clicking the **Load Victim Profile** button found on the *Define Indicator Utility Functions* window.
- A warning message is given if there are existing *Utility Functions* since they will be overwritten.
- If a file already exists with the same name as the name of this *Advanced Analysis Window*, it is pre-selected in the **File > Victim Profile > Load Victim Profile** dialog. You can also save *Victim Profiles* by clicking the **Save Victim Profile** button. *Victim Profile* files end with the extension .vip.
- After the file is selected, the *Define Indicator Utility Functions window* is opened (if it was not already opened).
- The *Utility Functions* for the *Victim Profile* can be edited by clicking on the buttons under the *Utility Mapping* heading on the right side of the window.
- When the *Utility Functions* you want to analyze have been entered, click on OK and they will be applied to the attack scenario table.

## Save Victim Profile

The *Indicator Utility Functions* can be saved and used for future evaluations on this tree or any other tree with matching indicator functions. Select **File > Victim Profile > Save Victim Profile** to save the *Indicator Utility Functions* to a file. *Victim Profile* files end with an extension of *.vip*.



## Print Victim Profile

The **File > Victim Profile > Print Victim Profile** command allows you to print the currently loaded Victim Profile.

1. Select the **File > Victim Profile > Print Victim Profile** command from the application menu.
2. You will now see a preview of your printout. If all looks good, click **Print...** (at the top of the window) to select your printer and send the printout to the printer.

## Graphs

The following are available under the **Graphs** menu:

Cumulative Risk Graph

Relative Risk Graph

Feasibility Graph

Desirability Graph

Capabilistic Propensity Graph

Total Propensity Graph

Pain Factor Graph

Advanced Analysis Summary

Pie Chart

Bar Chart

Scatter Charts

Pareto Chart

The graphs can be printed by clicking on the **Print...** button. They can also be incorporated in other documents or applications by clicking the **Copy graph to clipboard** button, then pasting the image into the application.

## Advanced Analysis Graphs

Each *advanced analysis* session examines the interaction between a given threat agent and the target system. We sometimes refer to this as the *adversary-target pair*. There are usually a number of *attack scenarios* that the adversary can pursue to achieve their objectives of compromising the defender. The *feasibility*, *desirability* and *propensity* for each scenario are computed based on the model's parameters that have been set by the analyst. From the attacker's point of view, whether or not an attack has a negative impact on the victim has no influence on their behavior. Or, better said, if one of the attacker's goals is to cause a negative impact on the victim then that should be explicitly

defined as an *attacker benefit* in the model. Otherwise, the model assumes that causing a victim to suffer is not a goal of the adversary.

During the creation of the scenario table, each *attack scenario* is examined independently, as if it were the only attack considered by the adversary. However, in a real encounter between adversary and target, the various possible scenarios compete for the attacker's choice. If the adversary performs one attack (successfully), that generally eliminates the other attack scenarios from consideration. If the model is perfect, then the scenario with the highest *propensity* will be the only one ever chosen by the specified threat agent. Of course, models are not perfect. There is uncertainty in the description of both the adversary and the target. This means that it would be wise for the defender to prepare to deal with any and all *attack scenarios* with *propensity* values close to the maximum.

Not all of the *attack scenarios* with similar likelihoods will have the same impact on the victim. Some may have little effect whereas others may be devastating. This means that the level of risk (to the defender) may vary considerably over the likely scenarios. Since uncertainties in our model make it impossible to predict with certainty which of the likely scenarios will be chosen, the most prudent approach for predicting overall risk is to identify the preferred scenario with the highest risk. Within the set of the preferred scenarios with similar *propensity* values, the risk value is mostly dependent on the *victim impact*. Arguably this may overstate the overall risk if the lower impact scenarios are chosen often, but it is best to err on the side of caution.

**SecurITree** provides a number of graphs and charts to describe the output of *advanced analysis models*.

## Cumulative Risk Graph

The *Cumulative Risk graph* shows the cumulative risk vs the number of scenarios with that level of risk. The graph is similar to a histogram chart. A perfectly secure system would show a horizontal line superimposed over the x-axis, describing a system with no scenarios with non-zero risk. More typically, there will be a number of scenarios with a high level of risk. This is manifest by a spike close to the y-axis. The higher the spike, the worse the risk of the set of risky scenarios. The broader the spike, the more scenarios that must be dealt with to reduce the overall risk.

From a defender's point of view, a narrow, high spike generally represents an unacceptable situation, but one that is straightforward to resolve. The defender can focus on mitigating the risk associated with a small number of scenarios. On the other hand a wide, high pulse can be problematic because there may be a large number of high risk attack vectors. Unless an architectural solution can be found wherein a small set of controls will mitigate the risk of a large number of high risk scenarios, the system may prove impossible to secure. This requires an architectural solution that, at the attack tree level, typically involves introducing an AND node with at least one child activity that is difficult for the adversary to perform. If the high risk scenarios are comprised of OR nodes, and no way can be found to introduce a blocking AND node, then it may be infeasible to secure the system.

## Relative Risk Graph

The *Relative Risk graph* is similar to the Cumulative Risk graph (above) except that the Relative risk values are used to create the report.

## Feasibility Graph

This graph shows the percentage of scenarios with more than a given Feasibility.

## Desirability Graph

This graph shows the percentage of scenarios with more than a given Desirability.

## Capabilistic Propensity Graph

This graph shows the percentage of scenarios with more than a given Capabilistic Propensity.

## Total Propensity Graph

This graph shows the percentage of scenarios with more than a given Total Propensity.

## Pain Factor Graph

This graph shows the percentage of scenarios with more than a given Pain Factor.

## Pie Chart

The pie chart is an alternate representation of the *risk graph*. It shows the portion of the total number of scenarios that have different risk ranges. Obviously, it is a good thing if the greatest portion of the pie represents low risk scenarios. However, caution should be used in comparing the pie chart from one adversary-target combination with another. The actual range of risk values may be very different for each combination. Yet because the size of the pie is the same it is easy to be misled. For example, a particular adversary-target combination might have a pie chart with half the pie in its highest risk category. Another pie chart might have only 1/10 of the area in the highest risk category for its adversary-target combination - but the actual risk values could be substantially higher for that

1/10 than those in the previous chart's 1/2 size area. Comparisons between *advanced analysis* pie charts is therefore difficult.

The highest value used for the Segment Values is the Cumulative Risk value of the highest Total Propensity that is not a Probability scenario.

## Bar Chart

The bar chart is particularly useful if there are a small number of high risk scenarios that need to be addressed. It allows a visual comparison of the risk between highest risk scenarios. The accompanying table makes it obvious which types of attacks are of highest concern.

## Scatter Charts

Two scatter charts are displayed for each adversary-target analysis, one related to *relative risk* and the other to *cumulative risk*. In both charts, the *x* axis indicates the *victim impact* and the *y* axis indicates *probability* or *frequency* respectively. Each attack scenario has a point plotted on the chart reflecting its probability (or *frequency*) and *impact*. Since the product of these two terms is *risk*, the level of risk can be read from the chart. For convenience in reading the charts, equi-risk contours are displayed.

Where a point appears on the scatter chart is important. For example, consider a *relative risk* scatter graph showing a point (A) with high probability and low impact. It may have exactly the same *relative risk* as a second point (B) that has low probability and high impact. In the case of point A, its corresponding scenario is almost certain **if there are any encounters between the adversary and the target**. Point B will happen rarely, but when it does it will have catastrophic consequences.

Similarly, if a *cumulative risk* scatter graph showed two other points (C and D) in similar locations, we could be almost certain that event C would happen regularly (but with low impact per event). It might be acceptable to ignore the risk of scenario C until the model's predictions are confirmed through actual experience. The damage would be low and controls put in place before it accumulated to a serious level. Measures would be required to prepare for event D since if it occurred it would be too late to do anything about it.

Comparing the two scatter graphs is also useful. If the *relative risk* scatter graph showed a number of scenarios with high probability, but the *cumulative risk* scatter graph showed the same scenarios at a lower probability, then it could be concluded that the main reason why those scenarios are not being realized is due to a lack of encounters with adversaries. Essentially, they are safe because no one is actively trying to attack them. If an adversary emerged, the target system would be a sitting duck.

## Pareto Charts

One *pareto chart* is produced for each *alternative set* specified. The *Pareto charts* show the portion of total risk contributed by each *threat agent*.

## Reports...

The **File > Reports > Basic Reports** command allows you to view the Attack (Threat) Tree you are working on in a tabular format. The following Reports are available:

- **All Nodes** - All nodes on the tree are displayed in the report.
- **Only Leaf Nodes** - Only LEAF nodes are included in the report.
- **Complete Node Information** - All indicator values and notes are included in the report.
- **Complete Node Information - LEAF nodes only** - All indicator values and notes are included in the report.
- **Complete Node Information + Scenarios per Node** - The number of times the node occurs in scenarios is calculated and included in the report. Clicking on a node in the table will display a table showing all scenarios where this node is found. Clicking on a scenario will show the tree for the scenario.
- **Attack Scenarios** - A listing of all Attack Scenarios. This report is only available in an Attack Scenario window or in an Advanced Analysis window.
- **Agent Profile Cross-Reference** - This report is only available if pruning windows have been created. The report indicates which agent profiles are capable of performing an attack by placing an "X" under the appropriate pruning window name. If a node was removed from a tree during pruning operations, it will not have an "X" in that column.
- **Pruning Sensitivity** - This report is only available in a pruning window if the node-based method of pruning was used. The report provides a list of all pruning criteria and whether or not nodes were eliminated from the tree. If a node was removed on a particular pruning criterion, an "X" is placed in the column. The total number of criteria that caused the node to be pruned (removed) is also displayed.

The delta column for each pruning criteria is colored. This is the explanation of the color coding:

- Pink/(Red) represent attacks that are within/(well within) the capability of the threat agent.
- Light Yellow/(Dark Yellow) represent attacks that are nearly within/(just within) the capability of the threat agent.
- Light Green/(Green) represent attacks beyond/(well beyond) the capability of the threat agent.
- Numeric indicator values express the resources required to carry out the attack.
- # indicator values show the resources available to the attacker minus resources required to carry out the attack.
- Negative values indicate the attacker had a shortfall of the resources required for the attack.

This report provides a useful guide of the confidence level of the analysis. In general, a higher number of criteria used to eliminate an attack indicates a stronger assurance that an attack is

beyond the capabilities of an attacker. In other words, it would be necessary for the analyst to misjudge the capabilities of the attacker in multiple ways for the result to be incorrect.

- **Scenario Sensitivity** - This report is only available in a pruning window if the scenario based method of pruning was used. This report shows if an attack scenario was removed based on the pruning criterion. See the Pruning Sensitivity report for more information on the usage of this report.
- **Advanced Analysis** - The Advanced Analysis table. This report is only available in an Advanced Analysis window.
- **Potential Choke Points** - This report has information for each node in the tree. Each time a node is found in an attack scenario, the value for these columns in the attack scenario are accumulated; Capabilistic Propensity, Impact, Relative Risk and Cumulative Risk. This can be used to determine which nodes in the tree contribute the greatest risk or impact. This report is only available in an Advanced Analysis window.

The first two reports can be saved to a file. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for these report files is .txt.

The reports in table format can also be saved. This option can be used to save the tree information to a file in a format so it can be used in a spreadsheet program such as Microsoft Excel. To create the file:

1. Click on the *Save As* button or select **File > Save As...** from the application menu on the *Reports* window.
2. Now you will get the *Report Setup* dialog. You must choose either CSV Format (comma separated values) or Delimited Format. If you choose Delimited, you must now choose a character from the pull-down list that will be used to delimit the fields in the node information. If the character that was chosen is found in the text of the node information, you will receive the message: *Column delimiter was found in tree data. File will not be properly delimited.* This means data that should be in one column will be split across more than one column in the spreadsheet. You must also decide if new line characters should be removed from the note areas. If these note areas contain *new line characters* and they are not removed, the note area will go to the next line in the spreadsheet.



3. The **Save** dialog box will be displayed. Select the folder you want to save the file in, enter a file name and click on the *Save* button. The default file extension for report files in CSV Format is .csv and in Delimited Format is .rpt.
4. After the file has been saved, you can open it in a spreadsheet program. If you are using Excel, it is best to first start Excel then open the report file you created. This will cause the "Text Import Wizard" to start which will ask about the character that is used to delimit the data. Select "Delimited", then choose "Other" and enter the character that you used as a delimiter (the default is "|"). The data should now be in columns in the spreadsheet.

The reports **Attack Scenarios** and **Advanced Analysis** allow another save option. You can choose to save the tree image for each scenario (from the specified start row through the specified end row) to a separate file. The directory where the files are saved defaults to the directory that was used to open this tree. You can specify a different directory by clicking on **Change**. The images are saved as png files with the name *scenarioXX.png* where XX is the scenario number (not the row number). If there is already a file by that name in the directory it will be overwritten.

All of the reports can be printed. To print a report:

1. Select the report format you want. Note, for reports in table format you may need to adjust the column dividers to ensure that the columns are the correct width for viewing as they are printed using WYSIWYG (what you see is what you get).
2. Click on **Page Layout** to set page margins, print orientation, and header and footer settings.
3. Click on the **Print...** button or select **File > Print...** from the menu on the *Reports* window.
4. Alternatively, if this is a table-type report, you can click on **Print Custom**. You will be given further options such as specifying the start and end row, and if the report should be shrunk to fit the page horizontally. If this is the Advanced Analysis table, the additional options to create a detailed report, include tree images and print the tree in black and white or color are also given.
5. A **Print Preview** window will show your report.
6. Click on **Print...** to send your report to the printer.

## Print Tree...

The **File > Print Tree...** command allows you to print the current Attack (Threat) Tree.

1. Select the **File > Print Tree...** command from the application menu, or click on the **Print Tree** icon on the [toolbar](#).
2. The **Print Options** dialog will appear. Change the settings as required.
  - The size of the printout can be set. If *Default Size* is selected, the tree will be printed in a size similar to that seen on the screen. If *Fit to page* is selected, the tree will be printed so that it fits on one page. If *Resize* is selected, the *Scale Factor* can be specified where 1 is the default size, 0.5 is half the size and 2.0 is twice as big. You can specify the scale factor you require.
  - You can specify a Main Title and Sub Title for the printout.
  - Trees can be printed in color or black and white.
  - The font size for the text in the nodes can be specified.

Note: These Print Options are saved with the tree. If you open a new tree, the settings will be different.

- The *Page Layout* button will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.
  - Select **OK** to save the settings, **Print...** to continue with printing or **Cancel** to cancel out of printing.
3. If you select **Print...**, you will now see a preview of how the tree will be printed. If all looks good, click **Print...** (at the top of the window) to select your printer and send the printout to the printer.

## Page Layout

The **File > Page Layout** command will open the **Page Layout and Decorators** dialog box. This will allow you to set page margins, print orientation, and header and footer settings before printing your tree.

## Close

This command is used to **Close** the active Attack Scenario Window.

## Edit Menu

The following options are available under the **Edit** menu:

[Copy](#)

[Find...](#)

## Copy

This command is used to **Copy** the tree image to the system clipboard. The copy can be performed on the entire tree or a subtree.

1. Select the node or subtree you want to copy by clicking the node. This will cause the node to be highlighted in yellow. If you do not select a node on the tree, the entire tree will be copied. Select **Copy** by choosing **Edit > Copy** or by using the right mouse button to click the selected node and then selecting **Copy**.
2. The selected node or subtree will be copied.
3. The system clipboard now contains the subtree in several different formats: raster image, vector image, pdf, and in the tree structure format.

The image of the tree can be pasted into another application such as a word processor. In Word, use Paste Special, then select the required format.

## Find...

The find feature can be used to search for text strings within nodes.

1. To start the **Find** function, select the **Edit > Find...** command from the application menu, or click on the **Find** icon on the [toolbar](#).
2. In the "Find What:" box, either:
  - type in the search string, or choose a previous search string from the drop-down list. If the search string should be saved for future use, the list of search strings can be edited by clicking the button. See also **Tools > Preferences > Interface**.

or select:

- Nodes with empty note fields
  - Nodes with undefined values
  - Root of links
  - Nodes with indicator values: and select the Indicator, Operator and Value.
  - Single Shot Attack
  - Single Threaded Attack
  - Multi-Threaded Attack
  - Reduced Nodes
  - Benefit-based Attack Effectiveness
  - Encounter-based Attack Effectiveness
  - SAND or Custom AND defined
3. If "Search String" was selected in the "Find What:" area, select the areas that should be searched by checking the fields in the "Look In:" area. You can choose "Node Name" and/or any notes that have been defined for the tree. Internal and External ID can also be searched.
  4. The "Match:" area allows you to control the options for the search.
    - Case: Find text matching the specified pattern of uppercase and lowercase letters.
    - Whole words: Find occurrences of the text as whole words.
    - [Regular expression](#): Specify the search string in the form of a regular expression. [See Using SecurITree > Regular Expressions](#) for more information.
  5. The scope for the search can be either:

- the entire tree or
  - the subtree starting at the currently selected node or
  - only *LEAF* nodes
6. After clicking on Search, the results of the search are displayed. You can click on a node in the result list, which will cause the node to be selected. If you double-click the node, the Edit Node window will open which will allow you to edit the node. All occurrences of the search string will be highlighted in yellow.
  7. If the node is part of a sub-tree that has been rolled-up, the button "Roll Down" will show in the Action column. Clicking on that button will cause the subtree to be rolled down.
  8. A Replace can be performed based on the search criteria that has been used. Select either "Replace All" or "Replace Selected" (after selecting one or more entries in the search results area). A dialog window will open which will allow you to enter the new value.
    - When the replace function is used with "Search String", it will replace text found in Node names or Notes.
    - When used with "Nodes with indicator values:", all matching LEAF node values and AND/OR impact values will be changed.
  9. The search results list can be printed by clicking the "Print Results" button.
  10. The table of search results can be saved by clicking the "Save As" button. See the section on saving table reports in [Reports](#) for more information.
  11. A node or multiple nodes can be deleted by selecting the node/s in the table. All highlighted nodes will be deleted after confirmation.



## View Menu

The following options are available under the **View** menu:

[Zoom...](#)

[Depth Display Level...](#)

[Show Legend on Tree](#)

[Roll Up Subtree](#)

[Roll Down Subtree](#)

[Roll Down Subtree 1 Level](#)

[Roll Down Subtree x Levels...](#)

[Roll Down Nested Subtrees](#)

[Display Flag Columns](#)

[Display Reduced Names](#)

[Show # of times node occurs in scenarios](#)

[Show Entire Tree](#)

[Wrap Cell Text](#)

[Color Node Names](#)

[Filter Scenarios](#)

[Sort](#)

[Columns](#)

Show All

Summarize Columns

Custom

[Reset Column Order](#)

[Reset Column Width](#)

[Cumulative Risk Time Units...](#)

## Zoom...

The **Zoom** command is used to enlarge or reduce the size of the nodes in the application window. To change the node size:

1. Click either the + (**Zoom In**) or - (**Zoom Out**) or (**Zoom to Fit**) magnifying glass icon on the [toolbar](#). The view of the tree changes immediately.
2. Choose **View > Zoom...** from the application menu. You will get the *Zoom* dialog box where the node size can be specified. You can either select one of the preset zoom percentages by clicking on a radio button, or you can enter a percentage in the box on the bottom of the dialog for a custom setting. In both cases, the new node size is shown in the preview window. Once the desired zoom setting is arrived at, click *OK* to apply it to the view of the tree.

## Depth Display Level...

The **Depth Display Level...** command is used for viewing the tree to the desired depth of detail making it easy to summarize the tree you are working on.

- To hide or display nodes in the application window choose **View > Depth Display Level...** from the application menu. Select the number of levels you would like to see from the pull-down list, then click *OK*.
- If you would like to display all nodes on the tree, select *All* from the pull-down list.
- The status line (at the bottom of the screen) will be updated to inform you of the number of levels in the tree that are displayed.

## Show Legend on Tree

The **View > Show Legend on Tree** command allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

This information can be set by selecting **Tools > Preferences** from the application menu, then choosing the **Node Info** tab to set indicator values to be displayed, or the **Flags** tab to define flags.

## Roll Up Subtree

The **Roll Up Subtree** command is used to hide all nodes under the selected node making it easier to view the area of the tree you are working on.

1. Select the topmost node you still want to see by clicking the node. This will cause the node to be highlighted in yellow.
2. To hide all nodes beneath the selected node, choose **View > Roll Up Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Up Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-U** or **Ctrl-<up arrow key>**.
4. The node color will change and a down pointing arrow will be added to indicate there are more nodes under this one that are currently not being displayed.

## Roll Down Subtree

The **Roll Down Subtree** command is used to show all nodes under the selected node if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. To show all nodes beneath the selected node, choose **View > Roll Down Subtree** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree** on the pop-up menu. Or, click on the node then press **Ctrl-D** or **Ctrl-<down arrow key>**.
4. The node will change to its normal colour and all nodes under this one will be displayed.

## Roll Down Subtree 1 Level

The **Roll Down Subtree 1 Level** command is used to show all nodes one level under the selected node.

1. Select a node on the tree by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree 1 Levels** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree 1 Level** on the pop-up menu. Or, click on the node then press **Ctrl-Shift-D**.
4. One level of nodes below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".

## Roll Down Subtree x Levels

The **Roll Down Subtree x Levels** command is used to show all nodes under the selected node (to the desired depth) if the subtree under the node was previously "rolled up".

1. Select a node that is "rolled up" by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Subtree x Levels...** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Subtree x Levels...** on the pop-up menu.
4. You will be asked to enter the number of levels to be rolled down. That number of levels below the selected node will be displayed, with any nodes that contain a subtree lower than the desired level being set as "rolled-up".



## Roll Down Nested Subtrees

The **Roll Down Nested Subtrees** command is used to show all nodes under the selected node.

1. Select a node that is to be the start of the subtree to be rolled down by clicking the node. This will cause the node to be highlighted in yellow.
2. Choose **View > Roll Down Nested Subtrees** from the application menu.
3. Alternately, use the right mouse button to click the selected node, then click on **Roll Down Nested Subtrees** on the pop-up menu.
4. To roll down the entire tree, select the root node.

## Display Flag Columns

The **View > Display Flag Columns** command allows you to display or hide columns for the flags defined for the tree. The column will show an "X" in the row if the attack scenario contains a node with that flag set. If there are no nodes with the flag set in the attack scenario, the cell will be blank.

The columns will only be displayed if there are flags defined for the tree.

## Display Reduced Names

The **View > Display Reduced Names** command allows you to decide how the leaf node names are displayed for the attack scenario.

If **Display Reduced Names** is selected, all leaf nodes are displayed. If it is not selected, the nodes under any subtrees that have been set as *reduced* will not be displayed. Instead, the name of the reduced subtree will be used.

## Show # times node occurs in scenarios

The **View > Show # times node occurs in scenarios** command allows you to toggle the visual display of node occurrence.

If **Show # times node occurs in scenarios** is selected, the lines joining nodes are shown as a light line for nodes that do not occur frequently, whereas nodes that occur in many scenarios will have a heavy line. The variable width line basically shows the influence of sections of the tree.

The actual number of times the node occurs in all scenarios is displayed on the right side of the node.

If indicator values are set to be displayed, the values will not be shown while this checkbox is selected. If it is not selected, the tree will be drawn with normal connecting lines.

## Show Entire Tree

The **View > Show Entire Tree** command allows you to toggle if all nodes on the tree should be displayed.

If **Show Entire Tree** is selected, all nodes are displayed but nodes that are not on the path for the selected attack scenario are shown dimly. If the checkbox is not selected, only the nodes on the path for the selected attack scenario are shown.

## Wrap Cell Text

The **View > Wrap Cell Text** command allows you to toggle the wrapping of text in the Attack Scenario column in the table.

If **Color Node Names** has been selected, selecting **Wrap Cell Text** will cause **Color Node Names** to be deselected.

## Color Node Names

The **View > Color Node Names** command allows you to toggle the coloring of node names in the Attack Scenario column in the table. If a node color is changed from the default node color (in the main window), that same color will be used in the table.

If **Wrap Cell Text** has been selected, **Color Node Names** cannot be selected.

## Filter Scenarios

The **Filter Scenarios** feature can be used to remove scenarios from the table based on defined criteria.

- To start the **Filter Scenarios** function, select the **View > Filter Scenarios** command from the menu, or click on the **Filter Scenarios** icon on the [toolbar](#).
- Choose a column name from the drop-down list, then select "Add".
- Now the criteria for filtering must be defined by specifying an operator and value.
- To filter on secondary columns, choose additional columns then click "Add" again.
- Select a criteria in the list then click the "Remove" button to remove a filter criteria
- Select a criteria in the list then click the "Edit" button to make changes to a filter criteria.
- The choice can be made to match any or match all criteria that have been defined.
- Click **OK** to filter the table. Only attack scenarios matching the criteria defined will be shown in the table.



## Sort

The sort feature can be used to sort a table on multiple columns.

1. To start the **Sort** function, select the **View > Sort** command from the menu, or click on the **Sort** icon on the [toolbar](#).
2. Choose a column name from the drop-down list, then select "Add". The column can be sorted in Ascending or Descending order.
3. To sort on secondary columns, choose additional columns then click "Add' again.
4. Click the "X" button to remove a sort criterion.
5. Click **OK** to sort the table.
6. Clicking on a column header on the table will cause the table to be sorted by that column and will override the choices in the Sort dialog.

## Columns

The **View > Columns** command allows you to display all columns or only show selected columns. The choices are: Show all, Summarize Columns, Custom.

### Show All

When *Show All* is selected, all columns in the report are displayed.

### Summarize Columns

The columns that are shown when *Summarize Columns* is selected are:

Row

Scenario

Attack Scenario

Feasibility

Desirability

Capabilistic Propensity

Stochastic Probability

Scenario Frequency

Pain Factor

Relative Risk

Cumulative Risk

Number of x until Risk Reaches Unity

Time until Risk Reaches Unity

### Custom

Selecting Custom will allow you to choose which columns should be displayed as well as customizing the number of decimal places to be shown for the values in each column.

## Reset Column Order

The **View > Reset Column Order** command will reorder the table so the columns are in a logical order. The order that the columns are put in is:

Row

Scenario # column

Scenario Type

Attack Scenarios

    each Capabilistic Behavioral indicator followed by its utility function

Feasibility

    each Attacker Benefits indicator followed by its utility function

    each Attacker Detriment indicator followed by its utility function

Desirability

Capabilistic Propensity

Stochastic Probability

Total Propensity

Attack Type

# Hostile Encounters

Scenario Frequency

    each Victim Impact indicator followed by its utility function

Loss Expectancy per Time Period for each Victim Impact

Pain Factor

Relative Risk

Cumulative Risk

Number of x until Risk Reaches Unity

Time until Risk Reaches Unity

Flag columns

## Reset Column Width

If column widths in the Advanced Analysis table are changed, the widths will be remembered until the tree is closed. The View > Reset Column Width command will set widths back to the default, which is the width of the column header.

## Cumulative Risk Time Units

The **View > Cumulative Risk Time Units** command allows you to display values in the time period that is selected. Values will be converted to this time period for these columns in the table:

- Cumulative Risk over 1 <time> period.
- Number of <time period> until Risk Reaches Unity.

This value is in effect for the current Analysis only. To save the value for the tree, set the risk time unit in the main window by selecting **Tools > Preferences > Tree Properties**.

## Analyze Menu

The following options are available under the **Analyze** menu:

Define Indicator Curves

Machine Learning

Similarities

To open the **Define Indicator Utility Functions** window, select **Analyze > Define Indicator Curves**.

See [Using SecurITree > Advanced Analysis](#) for further information on defining indicator utility functions.

To perform Machine Learning, select **Analyze > Machine Learning**.

See [Using SecurITree > Advanced Analysis > Machine Learning](#) for further information on Machine Learning.

To perform the Similarities function, select **Analyze > Similarities**.

See [Using SecurITree > Advanced Analysis > Similarities](#) for further information on using the Similarities feature.



## Tools Menu

The following options are available under the **Tools** menu:

[Display Toolbars](#)

[Show Node Information Panel](#)

[Show Charts Panel](#)

[Preferences](#)

## Display Toolbar

The **Display Toolbar** command is used to hide or display the application toolbar. Choose **Tools > Display Toolbar** from the application menu and the [toolbar](#) will toggle from being displayed or hidden.

## Show Node Information Panel

The **Tools > Show Node Information Panel** command allows you to display or hide the [Node Information](#) side panel. The panel can also be displayed or hidden by pressing **Ctrl-i**.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".

## Show Charts Panel

The **Tools > Show Charts Panel** command allows you to display or hide the right side panel which displays charts associated with the currently selected attack scenario. The panel can also be displayed or hidden by pressing **Ctrl-t**.

The panel can be detached from the window by clicking on the left margin and dragging the panel off. It can be reattached by clicking on the "X".

## Preferences

The **Preferences** option is used to define your choices and settings. Choose **Tools > Preferences** from the menu and the Preferences window will appear. The only tab available in this mode is Node Info.

Changes to Node Info settings can be made in this window.

**Display Indicator Values** is used to display the indicator values for the nodes on the tree.

Choose Values to Display:

- Select one or more of the indicators you would like displayed by clicking the check boxes.
- A legend will appear in the top left corner of the application window and the selected indicator values will then be displayed beside the nodes.
- The color the indicator value is displayed in corresponds to the color used to display the name of the indicator function in the legend.

The *Show Legend on Tree* checkbox allows you to display or hide the tree legend information. The tree legend shows on the main display area of the tree and will only be displayed if there are flags defined or if indicator values are displayed.

The legend can also be set by selecting **View > Show Legend on Tree** from the application menu.

**NOTE:** A total of five (5) Indicator Values can be displayed at one time.

The **Node Display Settings** section has controls that can be used to change the way nodes are displayed for the tree. These settings are saved with the tree and are not saved as user defined settings.

- The **Display Node ID** setting is used to display the node IDs beside the node name inside every node in the tree.
- The **Reset all node colors to default** button can be selected to change any nodes that were individually changed to different colors. If this action is selected, it cannot be cancelled or undone with the **Undo** function.
- **Auto size all nodes on tree** is used to set all node sizes so that the node name fits into the node box.
- **Reset all nodes to standard size** will reset any nodes that were individually changed to a different size and/or set to auto-size. If this action is selected, it cannot be cancelled or undone with the **Undo** function.

**NOTE:** The tree can be displayed with the default node sizes while retaining customized sizes by selecting the Interface tab then clicking on "Display Standard Node Sizes".

Click on *OK* once you have chosen the values to display. The Node Information that was selected will now be displayed on the tree.

## Help Menu

The following options are available under the **Help** menu:

[Help Index](#)

[Context Sensitive Help](#)

[Legend](#)

[About](#)

## Help Index

The **Help > Help Index** command is used to access these help files.



## Context Sensitive Help

The **Context Sensitive Help** command is used to directly access help on menu, toolbar, and side panel items by clicking on them.

1. Choose **Help > Context Sensitive Help** from the application menu. The mouse pointer will change from a *Normal Select* (just an arrow) to a *Help Select* (an arrow with a ?) pointer.
2. Move the mouse pointer to the desired menu, toolbar, and side panel item that you require help with and click on it.
3. If there is **Context Sensitive Help** the *Help Index* window will appear with the proper help topic displayed. If there is no **Context Sensitive Help** then the mouse pointer will revert back to *Normal Select*.

## Legend

The **Help > Legend** command opens a window which displays a legend describing the node types on trees. It will also show Tree Setting information including Flags and Indicator information.

## About

Displays the following information about the product:

- Current **SecurITree** Version and Build Numbers
- Contact Information
- Copyright Information

If you click on the **License** button, the *License* window will open which contains the following information:

- Type of License
- Who it is Licensed to
- License Expiration Date
- End User License Agreement (EULA)

If you click on the **JavaVM** button, the JavaVM window will open which will show:

- The Java Version that is being used for **SecurITree**
- The Total Memory available to use and the current Free Memory. To make changes to the memory available for the application, see [Memory Errors](#).

The **Properties** button will show:

- The location of the SecurITree\_console.txt file and SecurITree.cfg file.
- A listing of the Java properties.

The **Console** button will display:

- The contents of the SecurITree\_console.txt file which may contain error messages.

The **Splash** button will display the splash screen.

## Read Me

=====

SecurITree 5.5

Copyright (c) 2001-2023 Amenaza Technologies Limited

All rights reserved.

=====

Welcome to SecurITree. The following information is available in this README file:

1. SYSTEM REQUIREMENTS
2. INSTALLATION INSTRUCTIONS
3. TROUBLESHOOTING
4. RECOMMENDED READING
5. RELEASE NOTES
6. CD FILE LISTING
7. CONTACT US

1. SYSTEM REQUIREMENTS

-----

For the best results we recommend the following minimum system requirements:

- Intel i5 or AMD equivalent; i7 or i9 recommended for complex models
- 8 GB RAM minimum, more recommended for models involving large numbers of attack scenarios.

N.B., amount of RAM available to SecurITree is dependent on parameters in the SecurITree.ini file. See online Help-> Using SecurITree-> Memory Errors or call technical support for assistance.

- A monitor and graphics card that support at least 1280x768 resolution 65535+ colors. Higher resolution is recommended.

SecurITree runs on the following operating systems:

- Windows 10 and 11
- Ubuntu and Debian Linux (other Linux possible, contact Amenaza for assistance)
- Mac OS X 10.7.3+

2. INSTALLATION INSTRUCTIONS

-----

To install SecurITree on Windows systems run the SecurITree-setup.exe file.

To install SecurITree on Ubuntu/Debian systems, use the /Linux/securitree.deb file.

To install SecurITree on the Mac OS X, place the SecurITree.pkg file in any convenient location (such as your desktop).

Double-click on SecurITree.pkg to begin the installation process.

Complete installation instructions are found in InstallInstructionsV54.pdf.

3. TROUBLESHOOTING

-----

Install:

- When installing SecurITree on Windows systems, you must have administrator privileges.
- Installation on Linux may require root privilege (depending on where the software is installed).

- If your installation of SecurITree runs for 5 minutes and then exits, it is because the license activation file, license.sig, is missing or installed in the wrong location.
- When installing on a Mac, the license.sig file must be saved in the <Application Package>/Contents/Resources folder. By default, <Application Package> is set to "SecurITree/SecurITree.app". Right click (or Ctrl + click) on SecurITree.app. Select "Show Package Contents". In the finder window which pops up, select Contents, then Resources. Copy the license.sig file into the Resources folder. If copying via a terminal window, the terminal program must have "Full disk access" privilege. Open System Preferences>Security & Privacy. Select the Privacy tab. Select Full Disk Access, then click the lock icon to activate the +/- and add your Terminal.app here. su to root and perform copy operation.

#### Running SecurITree:

- If tree graphics appear fuzzy, edit SecurITree.ini. To the parameter "Virtual Machine Parameters", add "-Dsun.java2d.uiScale=1.0" (without quotes).
- When running using a 4K display, the application may appear very tiny. To resolve this, right click the SecurITree icon on the desktop and select "Properties". Go to "Compatibility" tab. Check "Override high DPI scaling behavior". Choose "System" for "Scaling performed by:".
- If your system is set to use 256 colors, you may get an error when saving trees in jpg or png format. To resolve this issue, change your display setting to 16 bit (65535 colors) or higher.

#### Error Log:

- If errors occur while running SecurITree, the error log should be checked for messages. It can be found in:  
[your home directory]\Amenaza\SecurITree\SecurITree\_console.txt  
In Windows 7, the home directory is:  
C:\Users\[username]\AppData\Roaming\  
In Windows 8, the home directory is:  
C:\Users\[username]\Application Data\  
On the Mac it is:  
/Users/[username]/Library/Application Support/  
Please send this log file to Amenaza so the error can be corrected.  
If SecurITree is restarted, the error log is over-written.

#### 4. RECOMMENDED READING

-----

The recommended reading order is as follows:

- Hostile Risk Decisions.pdf
- AttackTreeThreatRiskAnalysis.pdf

It is strongly recommended that you read the materials listed above. After the software has been installed and you are ready to begin using SecurITree, it is HIGHLY recommended that you work through the tutorial exercise described in Tutorial.pdf. Although SecurITree is very flexible and easy to use, some of the concepts are quite new and need some explanation. If you absolutely cannot go through the tutorial then you should read QuickTour.pdf.

Note that Amenaza offers training in attack tree analysis using SecurITree.

If you have questions about how to use SecurITree, do not be reticent to call the Amenaza Technical Support line. Although the support line

is not intended to provide consulting services, or to replace the two day training course, Amenaza does take a broader view of support than many software vendors. We will work with you to ensure your success with SecurITree!

#### 5. RELEASE NOTES

-----

SecurITree 5.5 - Build 013 - 2023/10/10

- Machine Learning - added similarities.
- Added Scratchpad feature. Subtrees can be saved to a scratchpad area so they can be conveniently copied or moved around the tree.
- When opening a rit file, first check the file format. Give error message if incompatible format.
- API changes: added createAdvancedAnalysisTable, importProfileExtensionsFromTemplate, saveCSVReport. Also added two new constructors for ATree to include ProfileExtensions (weighting factors) from template tree.
- Improvements to watermarks; better display positioning.
- Fixes when setting attackRecovery parameters when a previous analysis window was opened.
- When deactivating node using right-click, check which alternative sets change should be applied to.
- Other bug fixes and optimization changes.

SecurITree 5.4 - Build 014 - 2022/12/22

- Machine Learning.
- Disallow cut on nodes in an external subtree unless the subtree is converted to an internal link.
- Fixed formatting of description text for Spider Charts.
- Fixed buttons on main window so button text is properly displayed.
- Set busy cursor and progress bar for long running Find and Filter tasks.
- Optimization of Find.
- When doing Find in Attack Scenario and Advanced Analysis, if there are many scenarios, a warning is given and the option to not build the "Found in Row (Scenario)" column.
- After the Search is performed, a double-click on a row in the results table will open a window to display the contents of the "Found in Row (Scenario)" cell. If the column was not built, there is an option to build the data for this node.
- When filtering is performed, if the "Attack Scenario" column is selected, there is now an option to filter on only LEAF nodes (the data in the column) or on all nodes in the scenario path (which may take a long time on a large tree).
- Fixed bug when selecting Graphs in Advanced Analysis when Summarize or Custom columns are selected.
- In Advanced Analysis > Potential Choke Points report, changed column header from Capabilistic Propensity to Total Propensity.
- If license.sig file is not in user.dir, ask user for location of license and copy to user.dir (if allowed) or user home directory.
- When saving tree, change file name extension when a different file type is selected.
- On Scatter Graph table, label Risk column as either Relative or Cumulative.

SecurITree 5.3 - Build 012 - 2022/04/20

- Spider charts displayed on Advanced Analysis.
- When saving reports as csv files, remove line breaks in column

- headers.
  - When saving reports as csv or delimited files, give option for line separator character.
  - Added line number column in Report tables.
  - In Reports > Advanced Reports, add number of scenarios in all alternative sets to determine number of scenarios to be computed.
  - In Edit Tree in Table Format:
    - o check that probability values are in range 0-1.
    - o allow editing of External ID column.
    - o allow root node to be edited.
    - o added line number column.
    - o added link type to link column value if node is a link.
  - When performing tree calculations, check that probability values are in range 0-1.
  - If calculation error occurs in a rolled up node, allow it to be edited.
  - Change default for ST and MT attacks from 1 Year to 2 Hours and 15 Minutes respectively.
  - Fixed error in Advanced Analysis Summary report when highest Relative or Cumulative risk is 0.
  - Check for NoSuchFileException when opening file so the entry is removed from recently opened list.
  - Progress Bar:
    - o Show timer
    - o Improvements to progress display particularly when tree contains ganged links.
  - In Advanced Analysis, if Use Maximum value is selected, don't check that weight values sum to 1.
  - On display message for # scenarios, added value for non-heuristic.
  - Find: Added Link Type column to search results table.
  - When opening tree, check that all reduced nodes are rolled up.
  - When opening tree, check that children are not in alternative sets that their parents are not in. Offer to remove altsets to fix this issue.
  - Fixes to alternative sets when doing copy/paste/delete.
  - In Tree Properties, display Tree Name.
  - In Edit Profile Weight Map, display filename instead of profile ID to select entry.
  - In api:
    - o added method getAllParentNodes().
    - o fixed bug when creating a dual victim impact/attacker benefit indicator.
    - o check that probability value is in range 0-1.
    - o fixed bug when an error occurs in plugin when creating a tree, the blank tree could not be closed.
  - Fixed bug when creating tree from template and tree contains many notes.
  - Resolve problem when doing Subtree Analysis using SecurITree on Linux.
- SecurITree 5.2 - Build 011 - 2021/07/02
- New feature: m of n children of AND nodes.
  - In Graphs window, control panel is now on main graph display window.
  - Added filtering of table entries in Attack Scenarios and Advanced Analysis.
  - In Edit Tree in Table Format, allow edit of probability values.
  - Fixed bug when deleting a ganged link.
  - When Break Link is selected, if link is Ganged or Identical, allow link to be set to regular link.

- If a copied subtree contains a Sensor or Defense node, it cannot be pasted as a link.
- In Find, added "Root of links" and "SAND or Custom AND defined".
- In Node Properties, added SAND or Custom AND defined.
- In Node Edit when editing AND nodes, changed Select f(x) button to display the indicator formula in use.
- Added Potential Choke Point report.
- In API, added getExternalID and setExternalID.
- Improved saving license.sig file when file is not present.
- Changed -Xmx variable in ini file to percent of memory.

SecurITree 5.1 - Build 021 - 2021/02/16

- Ensure temporary file path/name is valid on all platforms (fix trailing / error in Linux using java.io.tmpdir).
- Fix for copy to clipboard in Linux (svg format missing).
- Change to properly accept input and display of values expressed in scientific notation.

SecurITree 5.1 - Build 018 - 2020/09/10

- Implemented Attack-Defense functionality.
- Implemented Bubble notes.
- Added Zoom to Fit.
- Moved some toolbar items to a vertical toolbar.
- Added options to Find:
  - o Reduced Nodes
  - o Benefit-based AE
  - o Encounter-based AE
- In Edit Node window, added Save & Next and Cancel & Next.
- Improvements to Help > Legend.
- Fixed Analyze Subtree.
- Improvements to graphics.
- Improvements to Drag and Drop.
- Improvements to display of nodes in deactivated subtree.
- Fix in Pruning - attack scenarios were not rebuilt if all evaluation criteria were deleted.
- When node is moved in an alternative set, it will be moved in other alternatives if all of the parent's child nodes match the active alternative set.

SecurITree 5.0 - Build 009 - 2019/10/07

- Bundled Java with SecurITree.
- Fix - when calculating tree with deactivated nodes, do not include deactivated subtree.
- Improved Look and Feel for mac.
- Improvements to Help > Legend.
- Added "Reorder" of Toolbar categories.
- Fix when loading Help files from website. Added info line to Help > Properties.
- Node Edit window relabeling.
- Changed Node Color/Font dialog to be easier to use.
- When Note Type cleanup is not selected, add empty note types to required windows.
- Fix to API to add note to tree when adding a new Note Type to a node.
- Added methods to API:
  - o ATree - constructor ATree(File, showMsg, showAltWarningMsg).
  - o ATreeNode - getInternalID, getInternalIDLong, isActive, setActive,



getAltWarningMsgAllowed, setAltWarningMsgAllowed.

- When splitting dual indicators, create both indicator types properly.
- Changes to error/info messages and labels.
- Recognise https (as well as http) in notes - underline url and open a web browser if it is double-clicked.

#### 6. CD FILE LISTING

-----

The following files are contained on the CD:

- Demos - Demo files
- Documents - Documents
- LicenseManager - Files required for the License Manager
- linux\securitree.deb - SecurITree install for Linux
- macosx\SecurITree.zip - SecurITree install for Mac OS X
- Presentations - Presentations
- autorun.inf - Autorun file
- EULA.txt - End User License Agreement
- InstallInstructionsV55.pdf - Instructions for installing SecurITree
- readme.txt - This file
- SecurITree-setup.exe - SecurITree install for Windows systems
- SecurITree-setup.exe.asc - Signature for the SecurITree-setup.exe file
- Documents folder:
  - AttackTreeThreatRiskAnalysis.pdf - Attack Tree-based Threat Risk Analysis (Methodology)
  - Hostile Risk Decisions.pdf - Hostile Risk Decisions and Capabilities-based Analysis
  - InstallInstructionsV55.pdf - Instructions for installing SecurITree
  - ScenarioReduction-v3.0.pdf - Documentation on use of scenario reduction
  - SCMagazine20-Nov2009.pdf - SecurITree named 1 of the top 20 most innovative security products of the last 20 years
  - SCMagazineReview-Feb2007.pdf - Review of SecurITree in SC Magazine
  - SecurITree.pdf - SecurITree Reference Guide
  - Tutorial.pdf - The SecurITree Tutorial

#### 7. CONTACT US

-----

Amenaza Technologies Limited  
Mailstop 125  
406 - 917 85th St. SW  
Calgary, AB  
Canada T3H 5Z9  
Tel: (403) 263-7737  
Fax: (403) 278-8437  
Toll Free: 1-888-949-9797  
International: +1 403 263 7737  
e-mail: support@amenaza.com  
Web: www.amenaza.com

## License

End User License Agreement for

Amenaza Technologies Limited SecurITree (the "Software")

18 February 2021

### LICENSE PART 1

This is to confirm that, subject to the terms and conditions below, Amenaza Technologies Limited (the "Licensor") agrees to grant to the designated recipient of this software (the "Licensee") the License to use the Software. All terms in this license agreement shall have the meaning given to them as in the Terms and Conditions below.

Please note that this License Agreement is for either: (i) a full license agreement, or (ii) an evaluation license, in which case the Licensee is agreeing to license the Software in order to evaluate whether to enter into a longer term license of the Software. In such case, the use of the Software is restricted and access to the Software will terminate after a set period as described in the Terms and Conditions below.

By agreeing with the terms and conditions below or by installing the Software, the Licensee agrees to the License of the Software for either a full license agreement or an evaluation license agreement on the Terms and Conditions below; agrees to pay such charges that the Licensor has specified apply to the license being granted to the Licensee and to any subsequent support agreements that the Licensor and Licensee enter into; acknowledges having read and understood this License Part 1 and the Terms and Conditions below; and that the person accepting this License Part 1 and the Terms and Conditions below on behalf of the Licensee is authorized to do so and has the authority to enter into this License. The License shall commence on the clicking of "YES" below (the "Effective Date") and shall continue until terminated in accordance with the Terms and Conditions below.

### TERMS AND CONDITIONS

WHEREAS the Licensor has developed the Software (as defined herein) and the Licensee desires to become a licensee of the Software, all on the terms and subject to the conditions of this Agreement; WITNESSETH that in consideration of the mutual covenants and agreements herein contained and for other good and valuable consideration, and subject to the terms and conditions hereinafter set out, the parties hereto mutually agree as follows:

#### 1. DEFINITIONS AND STANDARD INTERPRETATION

1.1 Definitions. In this Agreement:

- (a) "Business Day" means any day exclusive of Saturdays, Sundays and statutory holidays in Alberta;
- (b) "Concurrent Usage Control File" means a subfile supplied by the Licensor which specifies the number of Floating Licenses that may be concurrently assigned;
- (c) "Designated System" means (i) with respect to a Node-locked License, the computer upon whose local hard drive a License File has been installed for the purpose of or in connection with operating the Software with a Node-locked License, (ii) with respect to a Floating License, a computer within the number of computers specified in such Floating License which have been assigned access to the Floating License through network communication with the License Manager, and (iii) any computer replacing a Designated System in accordance with clause 2.2;
- (d) "Evaluation Period" means a period commencing from the Effective Date, and ending on the date specified in the evaluation license subfile embedded in the Software;
- (e) "Force Majeure" means any act of God, nature, war (declared or undeclared), act or omission of government or any regulatory body or agency or official, enactment of law, regulation, rule, riots, strikes, labour dispute, civil disturbance, acts of sabotage or terrorism, epidemics, adverse weather conditions, lightning, earthquake, natural disaster, interruption in telecommunication, power or Internet services, failure or malfunction of computer equipment or software, fire or any other similar events, acts or omissions beyond the reasonable control of the party affected thereby;
- (f) "Floating License" means a License is dynamically assigned to a particular Designated System by means of a License Manager;
- (g) "Improvements" means any and all developments or improvements of the Software (whether or not patentable) during the Evaluation Period or the Term (as the case may be);
- (h) "Indebtedness" means any obligation for the payment or repayment of money, whether as principal or surety and whether present or future, actual or contingent;
- (i) "Intellectual Property" means all of the Licensor's rights in the following items, including but not limited to all matters regarding the Software:
  - (i) all patents, patent applications, (whether or not they have been submitted to patent registration authorities), working papers, drawings, specifications, utility models, designs, design registrations, formulae, processes, inventor's certificates, inventions, shop rights, know how, trade secrets and confidential information;
  - (ii) all registered and unregistered trademarks, service marks, logos, names and other similar rights;
  - (iii) all copyrightable works and all registered and unregistered copyrights;

- (iv) all computer software and hardware, files, documentation, models, and rights relating to them;
  - (v) all modifications, improvements and development of the items described above;
  - (vi) all registrations for, and applications for registration of, any of the items described above; and
  - (vii) for the avoidance of doubt, includes this Agreement;
- (j) "Libraries" means the database of Attack Trees (being a Boolean logic and a mathematical, rooted tree diagram to show ways in which an asset might be attacked) and subtrees that may optionally be licensed for use with the SecurITree product;
- (k) "License" means the license granted by the Licensor to the Licensee in Clause 2 regarding the Software, and references to "License" shall include a Node-locked License and/or a Floating License (as the case may be);
- (l) "License Control System" means a mechanism involving either the Software and a License File (in the case of Node-locked Licenses) or the Software and a License Manager (in the case of Floating Licenses) which restricts the usage of the Software to a Designated System;
- (m) "License File" means a subfile of the Software which restricts the operation of the Software to the specific computer whose hard drive contains the subfile, and includes any Concurrent Usage Control File, License Control System and License Manager (as the case may be);
- (n) "License Manager" means a software program supplied by the Licensor and controlled by a Concurrent Usage Control File, and which communicates with the Software and dynamically assigns and revokes access to Licenses to/from a Designated System;
- (o) "Manuals" means the user documentation (including all methodologies) in any version regarding the Software prepared by the Licensor;
- (p) "Node-locked" means that a license is associated with or tied to a specific computer by means of a License File present on that computer's hard drive;
- (q) "Other Agreements" means such other agreements as may be entered into between the Licensor and the Licensee regarding fees and charges, maintenance, training, changes to the Designated System, Updates, and such other matters as the Licensor and the Licensee may agree;
- (r) "Software" means the operational object applications computer program known as SecurITree and the License File (but not in either case the source code), Libraries and Manuals owned by the Licensor and licensed to the Licensee by the Licensor and shall include any Improvements or Updates made or existing from time to time;

(s) "Taxes" includes all present and future taxes, levies, imposts, duties, fees or charges of whatever nature, including but not limited to any sales, value added or goods and services tax, together with interest thereon and penalties in respect thereof and "Taxation" shall be construed accordingly;

(t) "Term" means an indefinite period commencing from the Effective Date, or such shorter period as may be agreed to prior to the entry into this Agreement, but in every case as may be modified or terminated pursuant to the terms of this Agreement;

(u) "Updates" means any and all updates, corrections, modifications, supplements, enhancements and additions to the Software or any part thereof provided by the Licensor generally to all Licensees; and

(v) "Internal business use" means day to day activities performed by the Licensee, its employees and authorized agents, for uses internal to the Licensee's operations or to complete projects on behalf of the Licensee's clients.

1.2 Standard Interpretation. In this Agreement, unless the context otherwise requires:

(a) references to Clauses are to be construed as references to the clauses of this Agreement;

(b) references to (or to any specified provision of) this Agreement or any other document shall be construed as references to this Agreement, that provision or that document as in force for the time being and as amended in accordance with the terms thereof, or, as the case may be, with the agreement of the relevant parties and (where such consent is, by the terms of this Agreement or the relevant document, required to be obtained as a condition to such amendment being permitted) the prior written consent of that party;

(c) words importing the plural shall include the singular, and vice versa, and words importing a gender shall include the opposite or neutral gender, as the case may be;

(d) references to a person shall be construed as including references to an individual, firm, company, corporation, unincorporated body of persons or any State or agency thereof;

(e) references to statutory provisions shall include regulations made pursuant thereto, and shall be construed as references to those provisions as replaced, amended or re-enacted from time to time; and

(f) the division of this Agreement into articles and clauses is for convenience of reference only, and the use of such divisions or headings shall not modify or affect the interpretation of this Agreement.

## 2. LICENSE

2.1 License. Subject to the terms and conditions of this Agreement the Licensor hereby grants to the Licensee, and the Licensee hereby accepts from the Licensor, a personal, non-exclusive, non-transferable EXCEPT as specifically permitted in 2.3, indivisible license (the "License") from the Effective Date and either:

(a) continuing for the Term, to use the Software on the Designated System, in each case for its own internal business use only and not for use by or for any third party; or

(b) continuing for the Evaluation Period only, to use the Software on the Designated System for the purpose of its own internal evaluation of the Software so as to determine whether to enter into a longer term license of the Software, and not for use by or for any third party (the "Purpose"). The Licensee acknowledges and confirms that the Software contains subfiles which restrict the use of the Software, but in any case subject to termination in accordance with the terms of this Agreement.

2.2 Restriction to Designated System. The Licensee acknowledges and confirms that the License File will restrict the use of the Software to the Designated System. In the event that the Licensee:

(a) of a Node-locked License desires to transfer the use of the Software to a newly designated computer which shall then be the Designated System, the Licensee shall request prior written permission from the Licensor, which permission shall not be unreasonably withheld provided that such new system is in the same location as the Designated System. Upon receipt of this permission, the Licensee may transfer use of the License File to the newly designated computer. The Licensee shall destroy all copies or records of the Software in the previous Designated System or shall transfer all of these copies or records to the newly designated computer, and shall, if requested by the Licensor, promptly certify in writing that no copies or record of the Software exists outside of the newly designated computer; or

(b) of a Floating License desires to transfer the use of the Software to a newly designated computer within the Designated System, the transfer will take place automatically by exiting the Software on a computer within the Designated System and launching the Software on a newly designated computer within the Designated System which has been configured to request a Floating License from the License Manager, but provided in all cases that sufficient computers are available within such Floating License on the Designated System.

2.3 Additional Restrictions. Notwithstanding the License by the Licensor to the Licensee, the Licensee expressly acknowledges and confirms that no rights are granted pursuant to this Agreement to use the Software in any manner whatsoever except as provided for herein, and that the License shall not and does not include any right of the Licensee to directly or indirectly or permit others to:

(a) lease, sell, transfer, assign, rent, encumber, or otherwise dispose of or part with possession in any manner the License, the Software or any part thereto, including but not limited to any sublicenses of the License (with any such purported sublicense being null and void) without the prior written consent of the Licensor, which may be withheld at the discretion of the Licensor except as further provided in this clause 2.3(a). The Licensor acknowledges that, in certain cases, the Licensee has licensed the Software to complete subcontract work on behalf of the Licensee's clients, and that the terms of such subcontract may require the transfer of all project related materials to the client at the completion of the project, including the License. The Licensor agrees not to unreasonably withhold permission to transfer the License in this situation, on terms and conditions acceptable to the Licensor

in its sole discretion. These terms and conditions may include, but are not limited to that the Licensee requests approval from the Licensor at least 30 days prior to the proposed transfer; that the transferee and the Licensee execute and deliver to the Licensor such transfer and assignment documentation as the Licensor may require including, among other things, the transferee agreeing to be bound by the terms and conditions of the License; and that the Licensee complies with all other terms and conditions of this License, including but not limited to Clause 6.2 (post termination). For the avoidance of doubt, any transfer pursuant to this Clause 2.3(a) does NOT allow the Licensee to lease, rent or otherwise provide access to the Software as a service to persons that are not employees or agents of the Licensee;

- (b) deal in any manner whatsoever with any other Intellectual Property of the Licensor;
- (c) copy, duplicate or furnish to others any physical, magnetic or other version of the Software, except that if a License has been granted under clause 2.1(a) herein the Licensee may make a reasonable number of copies of the Software solely for back-up or archival purposes. Any such copy shall become the property of the Licensor, and shall be subject to the terms of this Agreement except that no further copies of this copy may be made;
- (d) use the Libraries or the Manuals except in conjunction with the Software;
- (e) remove any copyright notice contained or included in any material (including the Software) provided by the Licensor;
- (f) create or attempt to create the source computer programs or any part of them from the operational object programs or any other part of the Software licensed under this Agreement;
- (g) change, modify, prepare derivative works from, decompile, disassemble, reverse engineer, reconstruct or attempt to do any of the foregoing in any manner whatsoever to or with the Software;
- (h) maintain or repair the Software except in accordance with this Agreement;
- (i) make, allow or provide access to any party to the Software through the Internet or any network system;
- (j) merge the Software into other program material; or
- (k) do or undertake any other act not expressly allowed pursuant to this Agreement.

2.4 Licensee Acknowledgment. The Licensee acknowledges that the Licensor is the sole and rightful owner and copyright holder of the Software, that title and ownership remain fully in the Licensor notwithstanding the grant of this License, and that except for the License and rights specifically granted hereunder, all right, title, and interest, including the copyright, in the Software is retained by the Licensor. The Licensee specifically confirms and agrees that the Licensor is not restricted in any manner in dealing with the Software in its sole and absolute discretion, including but not limited to

the ability to enter any commercial arrangement with any third party regarding the Software or changing the content or format of the Software in accordance with general changes made to the Licensor's standard offerings.

2.5 Acknowledgment of Updates. For the avoidance of doubt, any and all Updates shall be deemed to be a part of the Software, and shall be governed by and subject to the terms of the License and this Agreement. The Licensee shall have no right to deal in any manner whatsoever with any Update except as specifically provided for in accordance with the terms of this Agreement.

2.6 Acknowledgment of Improvements. Except as provided in this section 2.6, Licensee shall not make any Improvements to, or modifications of, the Software. For the avoidance of doubt, any software code created by the Licensee using the application programming interface supplied with the Software, and which does not breach any other provision of this Agreement, shall not be deemed to be an Improvement.

2.7 Other Programs. Nothing contained herein shall be construed as extending to the Licensee a license to use any computer programs or software which the Licensor is using under license from any third party. The Licensee specifically acknowledges that the Software:

(a) is a Java application which executes using a Java Runtime Environment, including runtime components, classes and libraries associated with that environment. The Software has been compiled using the OpenJDK version of Java, a free and open-source implementation of the Java Platform Standard Edition. The OpenJDK Java implementation is licensed under the GNU Public License version 2 with a linking exception (sometimes known as a classpath exception). Java and OpenJDK are trademarks or registered trademarks of Oracle and its affiliates. The Java components, classes and libraries required to execute the Software are supplied by the Licensor for the convenience of the Licensee. The Licensee is responsible for complying with all copyrights and license agreements pertaining to the OpenJDK Java Runtime Environment components supplied with the Software; and

(b) uses Guild Software Copyright (c) 1998, 1999, 2000 757070 Alberta Ltd.. All rights reserved. Permission to use, copy and modify this software and to distribute this software in binary form is granted to the user Amenaza Technologies Limited.

2.8 Purchase of Updates. The Licensee shall have the right to purchase any Updates from the Licensor from time to time in accordance with the terms of this Agreement, provided that:

(a) the Licensee has paid all fees and charges due to the Licensor, and either has kept current all payments pursuant to the Other Agreements, or pays the then prevailing price of such Update as determined by the Licensor; and

(b) all Updates shall be governed by and subject to the terms of this Agreement.

### 3. RELATIONSHIP



3.1 Relationship. The relationship between the Licensor and the Licensee shall be that of licensor and licensee, and the Licensee expressly acknowledges and agrees that it has licensed the use of the Software hereunder solely for its own use and account (including the Purpose, as the case may be). The granting of the License to the Licensee under this Agreement does not constitute the Licensee, its agents or employees, as an agent, commercial agent or legal representative of the Licensor for any purpose whatsoever. The Licensee has no right or authority to assume or create, and shall not assume or create, any contract, commitment, obligation or responsibility, express or implied, on behalf of or in the name of the Licensor or to bind the Licensor in any manner or thing whatsoever. Nothing in this Agreement shall be deemed in any way or for any purpose to constitute the parties hereto partners in the conduct of any business or otherwise. The relationship created by this Agreement does not constitute the granting of a franchise to the Licensee by the Licensor and no federal, provincial or state franchise statute, law, regulation or rule is intended to or has been applied by the parties, nor shall any such franchise, statute, law, regulation or rule be deemed or construed to apply to the formation, operation, administration or termination of this Agreement.

#### 4. FEES

4.1 Fees. In consideration of the Licensor granting the License, the Licensee shall pay the Licensor such fees as may be described in the Other Agreements.

#### 5. INSTALLATION AND TECHNICAL SUPPORT

5.1 Installation. The Licensee shall be solely responsible for installing the Software on the Designated System. The Software shall be deemed to be accepted upon such installation by the Licensee (or any attempt thereof).

5.2 Technical Support. Solely in the case of a License granted under clause 2.1(a) (and not for the avoidance of doubt in the case of a License granted under clause 2.1(b)) the Licensor, following installation of the Software on the Designated System by the Licensee, shall provide the Licensee with maintenance and Updates in accordance with the terms of this Agreement and as may be separately agreed to between the parties.

5.3 Maintenance of Designated System. The Licensee shall have the sole responsibility to maintain the Designated System, and any other equipment and facilities as are necessary to allow the full and proper operation of the Software. Without limiting the generality of the foregoing, the Licensee shall have the sole responsibility at its own risk and expense to acquire, install, operate, maintain and insure against all risks the Designated System and all other computer systems, hardware and all other software, and acknowledges that the Licensor has no responsibility with respect thereto.

#### 6. TERMINATION

## 6.1 Events of Termination.

(a) Solely in the case of a License granted under clause 2.1(a) (and not for the avoidance of doubt in the case of a License granted under clause 2.1(b)) the Licensor may terminate this Agreement, and cease the provision of maintenance, in either case without notice or other act upon the occurrence of any of the following events, any of which shall be deemed to be just and reasonable cause for such termination:

(i) the Licensee taking any action, or any legal proceedings are started with respect to, or other steps are taken in respect for, the Licensee to be adjudicated or found bankrupt or insolvent, the winding-up or dissolution of the Licensee or the appointment of a liquidator, administrator, trustee, receiver or similar officer of the Licensee or the whole or any part of its undertakings, assets, rights or revenues;

(ii) the Licensee being prevented by any governmental action from carrying on business with the Licensor for any reason;

(iii) the Licensee committing any breach of or omitting to observe any of the obligations or undertakings expressed to be assumed by it under this Agreement and such breach or omission is continuing ten (10) days after written notice from the Licensor;

(iv) the Licensee assigns, sells or otherwise transfers, or purports to do so, this Agreement, the License or the Software (including for the avoidance of doubt any Update) without the prior written consent of the Licensor;

(v) the Licensee commits any breach of Clauses 2.2, 2.3 or 7; or

(vi) the Licensor is requested or required to make any payment pursuant to clause 8.5.

(b) Solely in the case of a License granted under clause 2.1(b) (and not for the avoidance of doubt in the case of a License granted under clause 2.1(a)), the Licensor may terminate the License immediately upon demand. Unless terminated earlier by the Licensor, the License and all rights granted to the Licensee pursuant to this Agreement shall terminate on the last day of the Evaluation Period, and the Licensee acknowledges and confirms that the Software contains subfiles which restrict the use of the Software after the expiry of the Evaluation Period.

6.2 Post Termination. Immediately upon termination of the License or this Agreement in any manner whatsoever:

(a) all Indebtedness of the Licensee to the Licensor shall immediately become due and payable;

(b) the Licensee shall discontinue using the Software, and delete or destroy all Software and copies of the Software, all printed material respecting the Software, all backup or tape copies of the Software,

provided that the Licensee may retain in its possession one copy of the Software for archive purposes only;

(c) the Licensee will permanently destroy or erase all copies of the Software resident in the Designated System and any other storage devices, and shall certify in writing to the Licensor upon demand that all copies of the Software and related materials have been deleted or destroyed and that no copies in any form remain in the possession or control of the Licensee except for the one copy of the Software retained for archival purposes only;

(d) all rights granted by the Licensor to the Licensee pursuant to this Agreement shall immediately be revoked, cease and shall be relinquished by the Licensee and shall revert to and revest in the Licensor without any further documentation required to be executed and delivered by either party hereto; and the provisions of this Clause, any Indebtedness due from the Licensee to the Licensor, and Clauses 7 (Intellectual Property), 8 (No Warranty) and 9 (General Matters) shall survive any termination of this Agreement. Termination of the License and this Agreement by the Licensor is in addition and without prejudice to any other remedy available to the Licensor at law or in equity.

6.3 Extensions and Waivers. Either party to this Agreement may, in writing, grant extensions of time and other indulgences or waive any breach of the covenants hereof by the other party, provided that any such grant or waiver shall not limit or affect the rights of the grantor with respect to any future time limit or breach and such grant or waiver shall be without prejudice to the liability of the recipient.

## 7. INTELLECTUAL PROPERTY

7.1 Licensee Acknowledgment. The Licensee hereby expressly acknowledges that:

(a) all Intellectual Property is the sole property of the Licensor and remains so even after delivery of any copies of the Software or any other information to the Licensee;

(b) the Software and any other data and materials supplied by the Licensor to the Licensee in machine readable form or otherwise are confidential and proprietary trade secrets of the Licensor protected by law, and are of substantial value to the Licensor, and their use and disclosure must be carefully and continuously controlled; and

(c) the Software is protected by the copyright laws of Canada and the United States of America.

7.2 Licensee Covenant. The Licensee agrees to keep all property of the Licensor (including but not limited to the Software) free and clear of all liens, claims and encumbrances. The Licensee shall have the right, during the Term or the Evaluation Period (as the case may be) and subject to due compliance with the provisions hereof, to use the Software for its own internal business use (or the Purpose, as the case may be) as described in this Agreement and, except as permitted in advance in writing by the Licensor, for no other purpose whatsoever. The Licensee will ensure that any and all

copyrights, proprietary information and trade marks of the Licensor will remain on the Software programs in machine-readable form, and on all printed material associated with the Software, and that any trade marks of the Licensor will only be used in accordance with the written directions of the Licensor. The Licensee acknowledges that the Software and the Intellectual Property contains proprietary and confidential information of the Licensor, and agrees that the Licensee shall safeguard such information by making its best efforts to prevent the unauthorized copying, use, distribution, installation or transfer of the Software and any other Intellectual Property of the Licensor that the Licensee may become aware of. The Licensee will keep the Software and any Intellectual Property confidential and will not disclose or furnish the Software or any Intellectual Property or any portion thereof to others except as expressly authorized in advance in writing by the Licensor.

7.3 Intellectual Property. The Licensee agrees with respect to the Intellectual Property of the Licensor, to:

(a) comply with all instructions issued by the Licensor relating to the form and manner in which the Intellectual Property shall be used and to discontinue immediately, upon notice from the Licensor, any practice relating to the use of the Intellectual Property which in the Licensor's opinion would or might adversely affect the rights or interests of the Licensor in the Intellectual Property;

(b) notify the Licensor immediately of any unauthorised possession, use or knowledge of any item supplied to the Licensee pursuant to this Agreement;

(c) refrain from contesting the title of the Licensor or any party through which the Licensor claims to its Intellectual Property or effecting any registrations thereof (including but not limited to the Licensor's copyrights in the Software) or taking any action to the detriment of the Licensor's interests therein; and

(d) provide assistance to the Licensor (at the Licensor's cost) to protect its Intellectual Property rights, including assisting with any registrations of the Intellectual Property that the Licensor deems necessary and keeping the Licensor informed on any infringements of the Intellectual Property that the Licensee is or becomes aware of.

7.4 Responsibility of Licensee. The Licensee shall be solely responsible for any use whatsoever of the Software, whether in accordance with this Agreement or otherwise. For the avoidance of doubt, the Licensee covenants to only use the Software in accordance with this Agreement.

## 8. NO WARRANTY

8.1 Limited Warranty. The Licensor warrants to the Licensee that with respect to the Software:

(a) it has the right to license the Software;

(b) to its actual knowledge does not infringe upon or violate any patent, copyright, trade secret or any other proprietary or intellectual property right or contractual right of any other persons.

8.2 No Other Warranties. EXCEPT AS SPECIFICALLY PROVIDED IN CLAUSE 8.1, THERE ARE NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO THIS AGREEMENT, THE SOFTWARE, ANY SERVICES PROVIDED AS MAINTENANCE, OR ANY SERVICES OR GOODS PROVIDED BY THE LICENSOR TO THE LICENSEE IN CONNECTION WITH THE SOFTWARE INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR CONFORMITY TO ANY REPRESENTATION, DESCRIPTION, MODELS OR SAMPLES OF MATERIALS. ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AND INCLUDING BUT NOT LIMITED TO ANY REPRESENTATION, WARRANTY, STATEMENT OR INFORMATION MADE OR COMMUNICATED (ORALLY OR IN WRITING) TO THE LICENSEE, WHETHER GIVEN BY THE LICENSOR OR ITS AGENTS, REPRESENTATIVES, EMPLOYEES OR OTHER PERSONS, ARE EXPRESSLY DISCLAIMED AND NEGATED. THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS. THE LICENSOR ALSO MAKES NO WARRANTY WHATSOEVER WITH RESPECT TO USE OF THE SOFTWARE IN ANY MODIFIED FORM. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, THE LICENSOR DOES NOT WARRANT THAT THE SOFTWARE WILL MEET THE LICENSEE'S REQUIREMENTS.

8.3 Intellectual Property Indemnity. The Licensor shall defend, indemnify and hold harmless the Licensee against any claim, demand, proceeding or action asserting that the SecurITree® software products in any way constitute an infringement or misappropriation of any intellectual property rights of any third party including, without limitation, any patents (except a patent issued upon an application that is now or may hereafter be withheld from issue pursuant to a Secrecy Order under 35 U.S.C. § 181), copyrights, trade secrets, trademark rights, confidentiality rights or other intellectual property rights. This indemnity shall not apply unless the Licensor shall have been informed as soon as practicable by the Licensee of the claim alleging such infringement and the Licensor shall have been given the opportunity either to assume the defence of such claim or take other steps towards dealing with such infringement or misappropriation. The Licensor is granted the sole control of the defence of any such claim, demand, proceeding or action and of all negotiations for its settlement or compromise. If the Licensor assumes the defence of such claim, the Licensee shall provide reasonable information and assistance for such defense. The Licensee must cooperate with the Licensor in all reasonable (non-financial) ways to facilitate the defence or settlement of the claim, demand, proceeding or action. Notwithstanding the foregoing, the Licensee may be represented in any such claim, demand, proceeding or action at its own expense and by its own counsel.

8.4 Licensee Representations. The Licensee represents to the Licensor, and acknowledges that the Licensor is relying on such representation to enter into this Agreement, that the Licensee accepts sole and exclusive responsibility for:

- (a) the selection of the Software to achieve the Licensee's intended results;
- (b) the use of the Software, and that the Licensor has no control over the conditions under which the Licensee uses the Software and cannot and does not warrant the results obtained by such use; and
- (c) the results (if any) obtained from the Software.

Without limiting the generality of the foregoing, the Licensee irrevocably acknowledges and confirms that (i) the use of the Software, and the results (if any) obtained, require the Licensee to weigh and apply its own individual assessment of numerous factors, including but not limited to assessment of risk; (ii) the Licensee accepts sole and complete responsibility for all such matters; and (iii) the Licensor has no responsibility or liability with respect thereto.

8.5 Licensor Liability. The Licensor's sole and exclusive liability to the Licensee shall be limited to the Licensor making repeated efforts to correct any resulting malfunction or failure in the Software. The Licensor's total liability to the Licensee for damages from any and all causes whatsoever, regardless of the form of action, whether in contract or in tort, including negligence, breach of the limited warranties and any infringement of any patent rights, copyrights or any misappropriation or unlawful use of any trade secrets, confidential information or other intellectual property rights or property of any third party shall in the aggregate be limited to an amount equal to the license fee (and not for the avoidance of doubt any support subscription or other fee) actually paid by the Licensee to the Licensor pursuant to clause 4.1. Any obligation of the Licensor to make any payment pursuant to this clause 8.5 is subject to the Licensee having a current and valid support subscription agreement in place regarding the Software at the time of any such payment request or demand. Except as otherwise provided in this Agreement, neither party shall be liable to the other for indirect, incidental, punitive, exemplary, general, special or consequential damages. Without limiting the foregoing (and not meant as a limiting or other description) neither party shall be liable to the other for any loss of revenue; loss of actual or anticipated profits; loss of anticipated savings; loss of business; loss of opportunity; loss of goodwill or reputation; or loss or corruption of data.

## 9. GENERAL MATTERS

9.1 Notice. Every notice, request, demand or other communication required to be given under this Agreement shall be given in writing by first class prepaid letter (airmail if available) or facsimile (confirmed by first class mail) and addressed to the appropriate party at the addresses designated by one party to the other from time to time. Any such notice sent by mail shall be deemed effective and received on the fifth (5th) Business Day after mailing, and if sent by facsimile, on the date and time registered in the transmitting party's transmission registry (provided that the notice is confirmed by first class mail). Any party hereto may change their address for service by sending notice to the other party as provided for herein.

9.2 Time. Time is of the essence in this Agreement.

9.3 Severability. Each of the provisions of this Agreement are severable and distinct from the others and if at any time one or more of such provisions is or becomes invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions hereof shall not in any way be affected or impaired thereby.

9.4 Entire Agreement. This Agreement and the Other Agreements constitute the entire agreement among the parties, supersedes any and all prior oral or written communications, proposals, representations and agreements, and each of the Licensor and the Licensee irrevocably confirm that there are no other written or verbal agreements or representations.

9.5 Further Assurances. Each party covenants and agrees that it will execute such further documents and do and perform or cause to be done and performed such further and other acts as may be necessary or desirable from time to time in order to give full effect to the provisions of this Agreement. In particular, but without limiting the generality of the foregoing, the Licensee shall at the Licensor's request promptly execute and assign any and all applications including, but not limited to, copyright applications, any and all assignments and any other instruments which the Licensor deems necessary to protect or maintain the Licensor's rights in its Intellectual Property, including but not limited to the Software.

9.6 Successors. This Agreement shall enure to the benefit of, and be binding upon, the parties hereto and their respective successors and permitted assigns. This Agreement and any interest therein may not be assigned by the Licensee without the express prior written consent of the Licensor, and any such purported assignment without such express prior written consent will be void.

9.7 Amendments. No amendment to this Agreement shall be valid and binding unless made in writing and signed by an authorised representative of each of the parties hereto.

9.8 Proper Law and Jurisdiction. This Agreement is governed by, interpreted and construed in accordance with, the laws of the Province of Alberta, and the Federal laws of Canada applicable therein. Each of the Licensor and the Licensee hereby agrees that any legal action or proceedings in connection with this Agreement shall be brought in the Court of Queen's Bench in the Province of Alberta, and irrevocably and unconditionally attorns and submits to and accepts the exclusive jurisdiction of such Court. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods signed in Vienna 1980, and any adoption or enactment of the same, does not apply to this Agreement and the matters described herein.

## 10. USMCA AFTER SALES SERVICE

10.1 The Licensor and the Licensee each hereby agree that the Licensee may from time to time require a business person who is employed by the Licensor to attend at the Licensee's place of business for purposes of providing after sales service (as described in Chapter 16 Temporary Entry for Business Persons, Annex 16-A of the U.S.-Mexico-Canada Agreement [USMCA]) to the Licensee

for the Software. Such business persons may be installers, repair and maintenance personnel, and supervisors, possessing specialized knowledge essential to the Licensor's contractual obligation. These personnel shall perform services or train Licensee's workers to perform services, pursuant to the Licensor's warranty or other service contract incidental to the license of the Software, and which has been licensed from the Licensor which is located outside the territory of the Licensee, during the life of the Licensor's warranty or service agreement.



# Index

## A

About (419)  
Add Indicator (33)  
Add Node (19)  
Add to Scratchpad (164)  
Adopt (28)  
Advanced Analysis (48)  
Advanced Analysis... (201)  
Advanced Analysis - Main Analysis (55)  
Advanced Analysis Menus (360)  
Advanced Analysis Overview (49)  
Advanced Analysis Toolbar (105)  
Advanced Analysis Toolbar (105)  
Advanced Analysis Windows (225)  
Agent Profile:Advanced Analysis... (201)  
Agent Profile:Edit Agent/Victim Profile (174)  
Agent Profile:Edit Agent Profile... (250)  
Agent Profile:Load Agent Profile (240)  
Agent Profile:Load Agent Profile (364)  
Agent Profile:Load Agent Profile Mode (44)  
Agent Profile:Print Agent Profile (242)  
Agent Profile:Print Agent Profile (366)  
Agent Profile:Save Agent Profile (241)  
Agent Profile:Save Agent Profile (365)  
Agent Profile Cross-Reference:Basic Reports (131)  
Agent Profile  
Cross-Reference:Reports... (281)  
Agent Profile  
Cross-Reference:Reports... (322)  
Agent Profile  
Cross-Reference:Reports... (375)  
Agent Profile  
Cross-Reference:Reports... (243)  
Agent Profiles and Pruning Criteria (45)  
AGT:Load Agent Profile (364)  
AGT:Load Agent Profile (240)  
AGT:Load Agent Profile Mode (44)  
AGT:Save Agent Profile (365)  
AGT:Save Agent Profile (241)  
Alternative Sets:Adopt to Alt Set (28)  
Alternative Sets:Alternative Sets (68)  
Alternative Sets:Define Alternative Sets (171)  
Alternative Sets:Display Alternative Sets (191)  
Amenaza (16)  
Amenaza Technologies Limited (16)  
Analysis:Close All Analysis Windows (230)  
Analysis Mode:Advanced Analysis... (201)  
Analysis Mode:Pruning Tree... (198)  
Analysis Windows:Pruning Tree... (198)

Analyze:Analyze Menu (265)  
Analyze:Analyze Menu (195)  
Analyze:Analyze Subtree (202)  
Analyze:Attacker and Victim Utility (51)  
Analyze Menu:Analyze Menu (265)  
Analyze Menu:Analyze Menu (195)  
Analyzer (13)  
AND Formula:Add Indicator (33)  
AND Formula:Edit Indicator (36)  
Associative Link (70)  
ATML:Save Tree As... (280)  
ATML:Save Tree As... (125)  
ATML:Save Tree As... (239)  
ATML:Save Tree As... (321)  
ATML:Save Tree As... (363)  
Attack:Attack Scenarios (41)  
Attack:Attack Scenarios... (266)  
Attack:What are Attack (Threat) Trees? (12)  
Attack-Defense Trees (82)  
Attacker and Victim Utility (51)  
Attacker Benefits:Add Indicator (33)  
Attacker Benefits:Attack Effectiveness (65)  
Attacker Benefits:Attacker and Victim Utility (51)  
Attacker Benefits:Edit Indicator (36)  
Attacker Benefit Utility Functions (51)  
Attacker Detriment:Add Indicator (33)  
Attacker Detriment:Edit Indicator (36)  
Attacker Resource Affinity Utility Functions (51)  
Attacker Resource Constraints (51)  
Attack Graphs (88)  
Attack Probability (49)  
Attack Scenarios:Attack Scenarios (41)  
Attack Scenarios:Attack Scenarios... (197)  
Attack Scenarios:Attack Scenarios... (266)  
Attack Scenarios:Attack Scenario Windows (228)  
Attack Scenarios Menus (318)  
Attack Scenarios Toolbar (104)  
Auto Calculate:Add Node (19)  
Auto Calculate:Auto Calculate (219)

## B

Background Color (210)  
Behavioral:Add Indicator (33)  
Behavioral:Edit Indicator (36)  
Behavioral Probability indicator (33)  
Boolean:Add Indicator (33)  
Boolean:Edit Indicator (36)  
Break Link (161)  
Bubble Notes:Add Node (19)  
Bubble Notes:Edit Node (22)  
Bubble Notes:Node Info (220)  
Bubble Notes:Notes (92)

## C

- Calculate Tree (196)
- Calculation:Change Calculation Method... (251)
- Calculation:Pruning Attack (Threat) Trees (42)
- Capability:Add Indicator (33)
- Capability:Edit Indicator (36)
- Capability-based (168)
- Cascade Windows (229)
- Chainlink (154)
- Change Calculation Method (251)
- Change Font Size (210)
- Charts (412)
- Children's Impact (22)
- Close (286)
- Close (327)
- Close (380)
- Close (130)
- Close (248)
- Close All Analysis Windows (230)
- Close Pruning Windows (248)
- Complete Node Information:Basic Reports (131)
- Complete Node Information:Reports... (322)
- Complete Node Information:Reports... (375)
- Complete Node Information:Reports... (243)
- Complete Node Information:Reports... (281)
- Contact Us:Contact Us (16)
- Contact Us:SecurITree Licensing Options (13)
- Copy (329)
- Copy (382)
- Copy (288)
- Copy (151)
- Copy (252)
- Copy:Cut (150)
- Copy:Paste (152)
- Copy:Paste as Link (154)
- Copyright (14)
- Copyright:License (426)
- Countermeasure:Add Node (19)
- Countermeasure:Alternative Sets (68)
- Countermeasure:Countermeasures (77)
- Countermeasure:Edit Node (22)
- Country (108)
- Create:New Tree... (115)
- Create:Open Tree... (117)
- Create:What are Attack (Threat) Trees? (12)
- Create Pruning Tree (198)
- Creator (13)
- Criteria:Agent Profiles and Pruning Criteria (45)

- Criteria:Explanation of Pruning Methods (46)
- Ctrl-D:Roll Down Subtree (260)
- Ctrl-D:Roll Down Subtree (337)
- Ctrl-D:Roll Down Subtree (390)
- Ctrl-D:Roll Down Subtree (187)
- Ctrl-D:Roll Down Subtree (296)
- Ctrl-I:Node Information (96)
- Ctrl-I:Show Node Information Panel (310)
- Ctrl-I:Show Node Information Panel (411)
- Ctrl-I:Show Node Information Panel (206)
- Ctrl-I:Show Node Information Panel (269)
- Ctrl-I:Show Node Information Panel (352)
- Ctrl-T:Show Tree Information Panel (207)
- Ctrl-T:Tree Information (97)
- Ctrl-U:Roll Up Subtree (186)
- Ctrl-U:Roll Up Subtree (336)
- Ctrl-U:Roll Up Subtree (389)
- Ctrl-U:Roll Up Subtree (295)
- Ctrl-U:Roll Up Subtree (259)
- Cumulative Risk Time Units (407)
- Curve Definitions:Advanced Analysis (48)
- Curve Definitions:Attacker and Victim Utility (51)
- Curves:Advanced Reports (134)
- Curves:Main Analysis (55)
- Cut:Cut (150)
- Cut:Paste (152)
- Cut:Paste as Link (154)

## D

- Data (117)
- Deactivate Node (29)
- Define Boolean Values:Advanced Analysis (48)
- Define Boolean Values:Attacker and Victim Utility (51)
- Define Curves:Advanced Analysis (48)
- Define Curves:Attacker and Victim Utility (51)
- Define Flags (222)
- Define Mapping (51)
- Delete:Delete Indicator (39)
- Delete:Delete Node (25)
- Delete:Tree Information (97)
- Delete Indicator (39)
- Delete Node (25)
- Depth Display Level (182)
- Depth Display Level (293)
- Depth Display Level (387)
- Depth Display Level (334)
- Depth Display Level (257)
- Derived:Add Indicator (33)
- Derived:Edit Indicator (36)
- Derived:Using Indicators (168)
- Desirability (55)

Deutsch (108)  
Difference Between An Agent Profile And Pruning Criteria (45)  
Disk:Save Tree (362)  
Disk:Save Tree (238)  
Disk:Save Tree (320)  
Disk:Save Tree As... (125)  
Disk:Save Tree As... (239)  
Disk:Save Tree As... (321)  
Disk:Save Tree As... (280)  
Disk:Save Tree As... (363)  
Display:Node Information (96)  
Display:Tree Information (97)  
Display Level Change:Depth Display Level... (293)  
Display Level Change:Depth Display Level... (182)  
Display Node Information (144)  
Display Pruned Nodes (264)  
Display Toolbar:Advanced Analysis (410)  
Display Toolbar:Attack Scenarios (351)  
Display Toolbar:Main Menu (204)  
Display Toolbar:Pruning (268)  
Display Toolbar:Set Operations (309)

## E

Ease of Attack (55)  
Edit:Tree Information (97)  
Edit Agent (174)  
Edit Indicator (36)  
Edit Menu (381)  
Edit Menu (287)  
Edit Menu (328)  
Edit Menu (249)  
Edit Menu (146)  
Edit Node (22)  
Edit Node:Find... (289)  
Edit Profile Weight Map (175)  
Edit Pruning Criteria (250)  
Effectiveness (65)  
e-mail (16)  
Encounter-based AE (65)  
End User License Agreement (426)  
English (108)  
Enterprise (13)  
Exit (145)  
Export Agent Profile (241)  
Extensions:Basic Reports (131)  
Extensions:Reports... (243)  
Extensions:Save Agent Profile (241)  
Extensions:Save Tree As... (125)  
Extensions:Save Tree As... (280)  
Extensions:Save Tree As... (363)  
Extensions:Save Tree As... (321)  
Extensions:Save Tree As... (239)  
External Links:Insert External... (121)

External Links:Instantiate All External Links (163)  
External Links:Instantiate External Link (162)  
External Links:Reload External (123)  
EXTTREETPATH (121)

## F

File menu (237)  
File menu (319)  
File menu (361)  
File menu (114)  
File menu (278)  
Files:Libraries vs. Trees (69)  
Files:New Tree... (115)  
Files:Open Tree... (117)  
Files:Save Subtree... (126)  
Files:Save Tree (238)  
Files:Save Tree (362)  
Files:Save Tree (279)  
Files:Save Tree (320)  
Files:Save Tree As... (125)  
Files:Save Tree As... (280)  
Files:Save Tree As... (321)  
File Types:Save Tree As... (239)  
File Types:Save Tree As... (125)  
Find:Find (178)  
Find:Find... (330)  
Find:Find... (383)  
Find:Find... (289)  
Find:Find... (253)  
Flag Columns:Display Flag Columns (300)  
Flag Columns:Display Flag Columns (394)  
Flag Columns:Display Flag Columns (341)  
Flags (222)  
Flags (94)  
Flags:Display Flag Columns (300)  
Flags:Display Flag Columns (394)  
Flags:Display Flag Columns (341)  
Font Size (210)  
Français (108)  
Full (13)

## G

Ganged Link:Links (70)  
Ganged Link:Paste as Ganged Link (156)  
Global Value:Add Indicator (33)  
Global Value:Edit Indicator (36)  
Global Value:Tree Properties (215)  
Graph (370)  
Graph eXchange Language:Save Tree As... (239)  
Graph eXchange Language:Save Tree As... (321)  
Graph eXchange Language:Save Tree As... (363)

Graph eXchange Language:Save Tree As... (280)  
GXL:Save Tree As... (125)  
GXL:Save Tree As... (239)  
GXL:Save Tree As... (321)  
GXL:Save Tree As... (363)  
GXL:Save Tree As... (280)

## H

Hacker (45)  
Help:Context Sensitive Help (274)  
Help:Context Sensitive Help (357)  
Help:Context Sensitive Help (417)  
Help:Context Sensitive Help (233)  
Help:Context Sensitive Help (315)  
Help:What Is SecurITree? (11)  
Help Index (314)  
Help Index (273)  
Help Index (416)  
Help Index (232)  
Help Index (356)  
Help Menu (272)  
Help Menu (231)  
Help Menu (415)  
Help Menu (313)  
Help Menu (355)  
Hide\_all\_enabled\_bubbles.html (194)  
High Level View (184)

## I

Identical Links:Links (70)  
Identical Links:Paste as Identical Link (155)  
Impact:Add Indicator (33)  
Impact:Add Node (19)  
Impact:Attacker and Victim Utility (51)  
Impact:Edit Indicator (36)  
Impact Indicators:Add Indicator (33)  
Impact Indicators:Add Node (19)  
Impact Indicators:Edit Indicator (36)  
Impact Indicators:Edit Node (22)  
Impact Utility Functions (51)  
Indicator:Add Indicator (33)  
Indicator:Add Node (19)  
Indicator>Delete Indicator (39)  
Indicator>Edit Indicator (36)  
Indicator:Rename Indicator (40)  
Indicator:Tree Information (97)  
Indicator:Using Indicators (168)  
Indicator Curves (51)  
Indicator Functions:Add Indicator (33)  
Indicator Functions>Edit Indicator (36)  
Indicator Functions:Tree Information (97)  
Indicator Name:Add Indicator (33)  
Indicator Name>Edit Indicator (36)  
Insert:Insert Library... (120)  
Insert:Insert New Root Node (27)

Insert:Insert Tree... (119)  
Insert External (121)  
Insert Library:Insert External... (121)  
Insert Library:Insert Library... (120)  
Insert Tree:Insert External... (121)  
Insert Tree:Insert Tree... (119)  
Instantiate (163)  
Interface (210)  
Intersect/Union Pruned Trees:Set Operations on Pruned Trees (227)  
Intersect/Union Pruned Trees:Set Operations on Pruned Trees... (200)  
Intersect/Union Pruned Trees:Set Operations on Pruned Trees Menus (277)  
Intersect/Union Pruned Trees:Set Operations on Pruned Trees Toolbar (103)  
Intersect/Union Pruned Trees Toolbar (103)  
Intersect button (200)

## J

JPEG:Save Tree As... (280)  
JPEG:Save Tree As... (363)  
JPEG:Save Tree As... (239)  
JPEG:Save Tree As... (125)  
JPEG:Save Tree As... (321)  
JPG:Save Tree As... (280)  
JPG:Save Tree As... (363)  
JPG:Save Tree As... (239)  
JPG:Save Tree As... (125)  
JPG:Save Tree As... (321)

## L

Language (108)  
Legend:Legend (418)  
Legend:Show Legend on Tree (388)  
Legend:Show Legend on Tree (183)  
Legend:Show Legend on Tree (335)  
Legend:Show Legend on Tree (294)  
Legend:Show Legend on Tree (258)  
Library:Insert Library... (120)  
Library:Libraries vs. Trees (69)  
Library:Open Library... (118)  
Library:Save Tree As... (280)  
Library:Save Tree As... (363)  
Library:Save Tree As... (239)  
Library:Save Tree As... (125)  
Library:Save Tree As... (321)  
License:Copyright (14)  
License:License (426)  
License:SecurITree Licensing Options (13)  
Link:Break Link (161)  
Link:Copy (151)  
Link:Cut (150)  
Link:Links (70)  
Link:Paste as Identical Link (155)  
Link:Paste as Link (154)

Link:Using SecurITree (17)  
Linked subtrees (70)  
Load Agent Profile:Load Agent Profile (364)  
Load Agent Profile:Load Agent Profile (240)  
Load Agent Profile:Load Agent Profile  
Mode (44)  
Look and Feel (210)

## M

Machine Learning (60)  
Main:Main Menus (113)  
Main:Main Toolbar (99)  
Main Analysis (55)  
Main Menus (113)  
Main Toolbar (99)  
Manual Mode:Calculate Tree (196)  
Manual Mode:Manual Mode (43)  
Match:Find (178)  
Match:Find... (383)  
Match:Find... (253)  
Match:Find... (330)  
Match:Find... (289)  
Memory Errors (106)  
Microsoft Excel:Basic Reports (131)  
Microsoft Excel:Reports... (375)  
Microsoft Excel:Reports... (281)  
Microsoft Excel:Reports... (243)  
Microsoft Excel:Reports... (322)  
Minimal Set (62)  
Model/tool (11)  
Mother Nature (45)

## N

Named Values (36)  
Navigate Through Tree (165)  
New Tree:New Tree... (115)  
New Tree:New Tree from Template... (116)  
Node-Based:Change Calculation  
Method... (251)  
Node-Based:Explanation of Pruning  
Methods (46)  
Node-Based:Pruning Attack (Threat)  
Trees (42)  
Node-Based:Pruning Tree... (198)  
Node ID (220)  
Node Info (220)  
Node Information:Basic Reports (131)  
Node Information:Edit Node (22)  
Node Information:Node Information (96)  
Node Information:Reports... (243)  
Node Information:Reports... (322)  
Node Information:Reports... (281)  
Node Information:Show Panel (206)  
Node Information:Show Panel (310)  
Node Information:Show Panel (411)  
Node Information:Show Panel (352)

Node Information:Show Panel (269)  
Node Information Panel:Node  
Information (96)  
Node Information Panel:Panels (205)  
Node Information Panel:Side Panels (95)  
Nodes:Edit Node (22)  
Nodes:Tree Information (97)  
Nodes:Using Nodes (165)  
Node Style (210)  
Node Value-based Pruning (46)  
Node Values:Change Node Values (167)  
Node Values:Edit Tree in Table  
Format (166)  
Notes (92)  
Notes:Note Types (173)  
Notes:Paste Notes (158)  
Number Format (108)

## O

Occurrence:Node Occurrence (396)  
Occurrence:Node Occurrence (343)  
Occurrence:Node Occurrence (302)  
Only Dangling Nodes:Basic Reports (131)  
Only Dangling Nodes:Reports... (243)  
Only Dangling Nodes:Reports... (281)  
Only Dangling Nodes:Reports... (322)  
Only Leaf Nodes:Basic Reports (131)  
Only Leaf Nodes:Reports... (375)  
Only Leaf Nodes:Reports... (243)  
Only Leaf Nodes:Reports... (281)  
Only Leaf Nodes:Reports... (322)  
Open (117)  
Open Library (118)  
Open Tree (117)  
Order Columns (404)  
OR Formula:Add Indicator (33)  
OR Formula>Edit Indicator (36)

## P

Page Layout (247)  
Page Layout (139)  
Page Layout (326)  
Page Layout (285)  
Page Layout (379)  
Page Setup:Print Tree... (246)  
Page Setup:Print Tree... (325)  
Page Setup:Print Tree... (378)  
Pain Factor:Advanced Analysis (48)  
Pain Factor:Main Analysis (55)  
Panels (205)  
Parent Node Change dialog:Add Node (19)  
Parent Node Change dialog>Edit Node (22)  
Parent Node Change dialog:Insert  
External... (121)  
Parent Node Change dialog:Insert  
Library... (120)

- Parent Node Change dialog:Insert Tree... (119)
- Pareto Charts (134)
- Paste:Paste (152)
- Paste:Paste as Link (154)
- Paste:Paste Notes (158)
- Paste:Paste Special (153)
- Paste:Paste Tree Structure (160)
- Paste:Paste Values (157)
- Paste Color (159)
- Paste Special:Paste as Link (154)
- Paste Special:Paste Color (159)
- Paste Special:Paste Notes (158)
- Paste Special:Paste Special (153)
- Paste Special:Paste Values (157)
- Pie Chart (134)
- Plugins (208)
- PNG:Save Tree As... (280)
- PNG:Save Tree As... (363)
- PNG:Save Tree As... (239)
- PNG:Save Tree As... (125)
- PNG:Save Tree As... (321)
- Preferences:Application (213)
- Preferences:Auto Calculate (219)
- Preferences:Preferences (209)
- Preferences:Preferences (413)
- Print:Reports... (281)
- Print:Reports... (322)
- Print Agent Profile (366)
- Print Agent Profile (242)
- Print Node (26)
- Print Tree... (246)
- Print Tree... (284)
- Print Tree... (325)
- Print Tree... (378)
- Print Tree... (138)
- Print Victim Profile (369)
- Probability:Add Indicator (33)
- Probability:Edit Indicator (36)
- Profile Weight Map (175)
- Propensity (55)
- Properties:Node Properties (144)
- Properties:Tree Properties (215)
- Protection (215)
- Prune Tree:Explanation of Pruning Methods (46)
- Prune Tree:Pruning Tree... (198)
- Pruning:Agent Profiles and Pruning Criteria (45)
- Pruning:Pruning Attack (Threat) Trees (42)
- Pruning:Pruning Menus (236)
- Pruning:Pruning Tree... (198)
- Pruning:Pruning Trees Toolbar (102)
- Pruning:Pruning Windows (226)
- Pruning Criteria:Agent Profiles and Pruning Criteria (45)

- Pruning Criteria:Edit Agent Profile... (250)
- Pruning Criteria:Explanation of Pruning Methods (46)
- Pruning Criteria:Load Agent Profile (240)
- Pruning Criteria:Load Agent Profile Mode (44)
- Pruning Criteria:Save Agent Profile (241)
- Pruning Methods (46)
- Pruning Mode (198)
- Pruning Sensitivity:Basic Reports (131)
- Pruning Sensitivity:Reports... (375)
- Pruning Sensitivity:Reports... (281)
- Pruning Sensitivity:Reports... (243)
- Pruning Sensitivity:Reports... (322)
- Pruning Trees Toolbar (102)
- Pruning Window:Load Agent Profile (240)
- Pruning Window:Pruning Menus (236)
- Pruning Window:Pruning Tree... (198)
- Pruning Window:Pruning Windows (226)

## R

- Read Me (420)
- Redo (148)
- Reduce:Attack Scenario Reduction (62)
- Reduce:Display Reduced Names (342)
- Reduce:Reduce Subtree (176)
- Reduced Names:Display Reduced Names (301)
- Reduced Names:Display Reduced Names (395)
- Reduction (62)
- Reg ex:Find (178)
- Reg ex:Flags (222)
- Reg ex:Regular Expressions (109)
- Regular expression:Find (178)
- Regular expression:Flags (222)
- Regular expression:Regular Expressions (109)
- Reload External (123)
- Rename (40)
- Replace (178)
- Reports:Basic Reports (131)
- Reports:Reports... (375)
- Reports:Reports... (243)
- Reports:Reports... (281)
- Reports:Reports... (322)
- Reports window (281)
- Representations (41)
- Restore (177)
- RIL File:Libraries vs. Trees (69)
- RIL File:Open Library... (118)
- RIL File:Save Tree As... (280)
- RIL File:Save Tree As... (363)
- RIL File:Save Tree As... (125)
- RIL File:Save Tree As... (239)
- RIL File:Save Tree As... (321)

Risk Metric:Advanced Analysis (48)  
 Risk Metric:Main Analysis (55)  
 Risk Reaches Unity (407)  
 Risks:Attacker and Victim Utility (51)  
 Risks:Overview (49)  
 Risks:What Is SecurITree? (11)  
 Risk Summary Reports (134)  
 RIT File:Libraries vs. Trees (69)  
 RIT File:Open Tree... (117)  
 RIT File:Save Tree As... (280)  
 RIT File:Save Tree As... (363)  
 RIT File:Save Tree As... (125)  
 RIT File:Save Tree As... (239)  
 RIT File:Save Tree As... (321)  
 Roll Down Nested Subtrees (340)  
 Roll Down Nested Subtrees (393)  
 Roll Down Nested Subtrees (190)  
 Roll Down Nested Subtrees (299)  
 Roll Down Nested Subtrees (263)  
 Roll Down Subtree (337)  
 Roll Down Subtree (390)  
 Roll Down Subtree (296)  
 Roll Down Subtree (260)  
 Roll Down Subtree (187)  
 Roll Down Subtree 1 Level (338)  
 Roll Down Subtree 1 Level (297)  
 Roll Down Subtree 1 Level (188)  
 Roll Down Subtree 1 Level (261)  
 Roll Down Subtree 1 Level (391)  
 Roll Down Subtree x Levels (392)  
 Roll Down Subtree x Levels (262)  
 Roll Down Subtree x Levels (339)  
 Roll Down Subtree x Levels (189)  
 Roll Down Subtree x Levels (298)  
 Roll Up Subtree (336)  
 Roll Up Subtree (389)  
 Roll Up Subtree (186)  
 Roll Up Subtree (295)  
 Roll Up Subtree (259)  
 Root (27)  
 Root Cause (12)  
 RPT:Basic Reports (131)  
 RPT:Reports... (375)  
 RPT:Reports... (243)  
 RPT:Reports... (281)  
 RPT:Reports... (322)

**S**

Sanitize Tree:Sanitize Subtree (128)  
 Sanitize Tree:Save Sanitized Tree (127)  
 Save:Basic Reports (131)  
 Save:Close (130)  
 Save:Open Library... (118)  
 Save:Save Agent Profile (365)  
 Save:Save Subtree... (126)  
 Save:Save Victim Profile (368)

Save Agent Profiles (241)  
 Save Subtree (126)  
 Save Tree (279)  
 Save Tree (362)  
 Save Tree (238)  
 Save Tree (124)  
 Save Tree (320)  
 Save Tree As... (280)  
 Save Tree As... (363)  
 Save Tree As... (321)  
 Save Tree As... (239)  
 Save Tree As... (125)  
 Scalable Vector Graphics:Save Tree As... (239)  
 Scalable Vector Graphics:Save Tree As... (321)  
 Scalable Vector Graphics:Save Tree As... (280)  
 Scalable Vector Graphics:Save Tree As... (125)  
 Scalable Vector Graphics:Save Tree As... (363)  
 Scatter Charts (134)  
 Scenario:Attack Scenarios (41)  
 Scenario:Attack Scenarios... (197)  
 Scenario:Attack Scenarios... (266)  
 Scenario Based (251)  
 Scenario-based:Explanation of Pruning Methods (46)  
 Scenario-based:Pruning Attack (Threat) Trees (42)  
 Scenario-based:Pruning Tree... (198)  
 Scenario Sensitivity:Basic Reports (131)  
 Scenario Sensitivity:Reports... (281)  
 Scenario Sensitivity:Reports... (243)  
 Scenario Sensitivity:Reports... (322)  
 Scenarios Toolbar (104)  
 Scenario Window (318)  
 Scratchpad (185)  
 Scroll (210)  
 Search:Find (178)  
 Search:Find... (383)  
 Search:Find... (289)  
 Search:Find... (253)  
 Search:Find... (330)  
 SecurITree:Using SecurITree (17)  
 SecurITree:What Is SecurITree? (11)  
 SecurITree Licensing Options (13)  
 SecurITree models (11)  
 Select Font Size (22)  
 Sensitivity (243)  
 Set Operations on Pruned Trees (227)  
 Set Operations on Pruned Trees... (200)  
 Set Operations on Pruned Trees Menus (277)

- Set Operations on Pruned Trees
- Toolbar (103)
- Show (97)
- Show\_m\_of\_n (192)
- Show/Hide Node Information (96)
- Show/Hide Tree Information (97)
- Show all enabled bubbles (193)
- Show Entire Tree (303)
- Show Entire Tree (344)
- Show Entire Tree (397)
- Side Panels:Node Information (96)
- Side Panels:Panels (205)
- Side Panels:Show Node Information Panel (206)
- Side Panels:Show Node Information Panel (310)
- Side Panels:Show Node Information Panel (352)
- Side Panels:Show Node Information Panel (411)
- Side Panels:Show Node Information Panel (269)
- Side Panels:Show Tree Information Panel (207)
- Side Panels:Side Panels (95)
- Side Panels:Tree Information (97)
- Sign Tree (129)
- Similarities (61)
- Sort (401)
- Sort (306)
- Sort (348)
- Spelling (210)
- Subtree:Cut (150)
- Subtree:Roll Down Subtree (187)
- Subtree:Sanitize Subtree (128)
- Subtree:Save Subtree... (126)
- Summarize Columns (402)
- SVG:Save Tree As... (321)
- SVG:Save Tree As... (280)
- SVG:Save Tree As... (125)
- SVG:Save Tree As... (363)
- SVG:Save Tree As... (239)

## T

- Table: Color Node Names (346)
- Table: Color Node Names (305)
- Table: Color Node Names (399)
- Table: Wrap Cell Text (345)
- Table: Wrap Cell Text (398)
- Table: Wrap Cell Text (304)
- Table Column Width:Reset Column Width (406)
- Table Column Width:Reset Column Width (349)
- Table Column Width:Reset Column Width (307)

- Table Format (166)
- Template (116)
- TERMS AND CONDITIONS (426)
- Threat Agent:Agent Profiles and Pruning Criteria (45)
- Threat Agent:Attacker and Victim Utility (51)
- Threat Agent>Edit Agent Profile... (250)
- Threat Agent:Pruning Tree... (198)
- Threat Tree:Using Indicators (168)
- Threat Tree:What are Attack (Threat) Trees? (12)
- Threat Tree:What Is SecurITree? (11)
- Time Parameters (67)
- Toolbars (98)
- Tools Menu (267)
- Tools Menu (350)
- Tools Menu (308)
- Tools Menu (409)
- Tools Menu (203)
- Tree:Libraries vs. Trees (69)
- Tree:Open Tree... (117)
- Tree:Pruning Trees Toolbar (102)
- Tree:Roll Down Nested Subtrees (340)
- Tree:Roll Down Nested Subtrees (393)
- Tree:Roll Down Nested Subtrees (190)
- Tree:Roll Down Nested Subtrees (299)
- Tree:Tree Information (97)
- Tree:What are Attack (Threat) Trees? (12)
- Tree:What Is SecurITree? (11)
- Tree Information:Reports... (322)
- Tree Information:Reports... (281)
- Tree Information:Show Tree Information Panel (207)
- Tree Information:Tree Information (97)
- Tree Information Panel:Panels (205)
- Tree Information Panel:Show Tree Information Panel (207)
- Tree Information Panel:Side Panels (95)
- Tree Information Panel:Tree Information (97)
- Tree Properties (215)
- Tree Pruning:Explanation of Pruning Methods (46)
- Tree Pruning:Pruning Attack (Threat) Trees (42)
- Tree Pruning:Pruning Tree... (198)
- Tree Structure From Clipboard (160)
- TXT:Basic Reports (131)
- TXT:Reports... (322)
- TXT:Reports... (375)
- TXT:Reports... (281)
- TXT:Reports... (243)
- Type (97)

## U

- Undo:Redo (148)



Undo:Undo (147)  
Undo:Undo Levels... (149)  
Undo Levels (149)  
Union (200)  
Using Indicators (168)  
Using Nodes (165)  
Using SecurITree (17)  
Utility Function:Main Analysis (55)  
Utility Function:Order Columns (404)  
Utility Function Columns (48)  
Utility Mapping (201)

## V

Value Range:Add Indicator (33)  
Value Range:Edit Indicator (36)  
Victim Impacts:Add Indicator (33)  
Victim Impacts:Attacker and Victim Utility (51)  
Victim Impacts:Edit Indicator (36)  
Victim Impacts:Overview (49)  
Victim Profile:Advanced Analysis... (201)  
Victim Profile:Attacker and Victim Utility (51)  
Victim Profile:Edit Agent/Victim Profile (174)  
Victim Profile:Load Victim Profile (367)  
Victim Profile:Print Victim Profile (369)  
Victim Profile:Save Victim Profile (368)  
Victim Utility Functions (51)  
View:Node Information (96)  
View:Roll Down Nested Subtrees (340)  
View:Roll Down Nested Subtrees (393)  
View:Roll Down Nested Subtrees (190)  
View:Roll Down Nested Subtrees (299)  
View:Roll Down Subtree (296)  
View:Roll Down Subtree (390)  
View:Roll Up Subtree (186)  
View:Tree Information (97)  
View:Zoom... (256)  
Viewer (13)  
View Menu (180)  
View Menu (332)  
View Menu (385)  
View Menu (291)  
View Menu (255)  
Viewport (210)  
VIP:Load Victim Profile (367)  
VIP:Save Victim Profile (368)

## W

Watermarks (215)  
Window Menu (224)  
Windows (229)  
WYSIWYG:Basic Reports (131)  
WYSIWYG:Reports... (243)  
WYSIWYG:Reports... (322)  
WYSIWYG:Reports... (281)

## X

XML:Save Tree As... (280)  
XML:Save Tree As... (125)  
XML:Save Tree As... (239)  
XML:Save Tree As... (321)  
XML:Save Tree As... (363)  
Xms (106)  
Xmx (106)

## Z

Zoom... (256)  
Zoom... (386)  
Zoom... (333)  
Zoom... (292)  
Zoom... (181)