



Security Threat Response Manager

Category Offense Investigation Guide

Release_2008.1

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Category Offense Investigation Guide
Release 2008.1

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

31 January 2008—Revision 1

The information in this document is current as of the date listed in the revision history.

CONTENTS

1 ACCESS OFFENSES

- What is an Access Offense? 5
- How do I Investigate an Access Offense? 6
- How do I Tune an Access Offense? 9

2 SIM AUDIT OFFENSES

- What is SIM Audit? 11
- How do I Investigate a SIM Audit Offense? 11
- How do I Tune a SIM Audit Offense? 14
 - Tuning Using False Positive Function 14
 - Tuning Using Custom Rules Wizard 16

3 AUTHENTICATION OFFENSES

- What is an Authentication Offense? 19
- How do I Investigate an Authentication Offense? 19
- How do I Tune an Authentication Offense? 23

4 CRE OFFENSES

- What is a CRE Offense? 25
- How do I Investigate a CRE Offense? 25
- How do I Tune a CRE Offense? 28

5 DENIAL OF SERVICE (DOS) OFFENSES

- What is a DoS Offense? 29
 - What is a DoS Flood Attack? 29
 - What is a DoS Service Exploit? 30
- How do I Investigate a DoS Offense? 30
- How do I Tune a DoS Offense? 34
 - Tuning Using False Positive Function 34
 - Tuning Using Sentries 35
 - Tuning Using Custom Rules Wizard 35
- How Can I Verify If STRM is Receiving Valid DoS Offenses? 36

6 EXPLOIT OFFENSES

- What is an Exploit Attack? 37

How do I Investigate an Exploit Offense	37
How do I Tune an Exploit Offenses?	41
How Can I Verify That STRM is Receiving Valid Exploit Offenses?	42

7 MALWARE OFFENSES

What is Malware?	43
What is Malware?	43
What is a Malware Offense?	43
How do I Investigate a Malware Offense?	44
How do I Tune a Malware Offense?	47

8 NETWORK ANOMALIES OFFENSES

What is an Network Anomaly Offense?	49
Policy	49
Threshold	49
Anomaly	50
Behavior	50
How do I Investigate a Network Anomaly Offense	50
How do I Tune a Network Anomaly Offense?	52

9 POLICY OFFENSES

What is a Policy Offense?	53
How do I Investigate a Policy Offense?	53
How do I Tune a Policy Offense?	56
Tuning Using False Positive Function	56
Tuning Using Custom Rules Wizard	57
How Can I Verify That STRM is Receiving Valid Offenses?	57

10 POTENTIAL EXPLOIT OFFENSES

What is a Potential Exploit Offense?	59
How do I Investigate a Potential Exploit Offense?	59
How do I Tune a Potential Exploit Offense?	61

11 RECONNAISSANCE OFFENSES

What is Reconnaissance?	63
What is Network Reconnaissance?	63
What is a Reconnaissances Offense?	63
How do I Investigate a Reconnaissance Offense?	64
How do I Tune a Reconnaissance Offense?	67
Tuning Using False Positive Function	67
Tuning Using Custom Rules Wizard	69

12 SUSPICIOUS ACTIVITY OFFENSES

What is a Suspicious Attack?	71
What is Suspicious Traffic?	71

What is a Suspicious Offense?	71
How do I Investigate Suspicious Offense	72
How do I Tune a Suspicious Offenses?	75

13 SYSTEM OFFENSES

What is a System Offense?	79
How do I Investigate a System Offense?	79
How do I Tune a System Offense?	82
How Can I Verify That STRM is Receiving Valid Offenses?	83

14 USER DEFINED OFFENSES

What is a User Defined Offense?	85
How do I Investigate a User Defined Offense?	85
How do I Tune a User Defined Offense?	88

ABOUT THIS GUIDE

This preface provides the following guidelines for using the *Category Offense Investigation Guide*:

- [Documentation Feedback](#)
- [Requesting Support](#)

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Support

Open a support case using the Case Management link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

1

ACCESS OFFENSES

This chapter provides information on access offenses including:

- [What is an Access Offense?](#)
- [How do I Investigate an Access Offense?](#)
- [How do I Tune an Access Offense?](#)

What is an Access Offense?

Limiting access to your network and networked resources is an essential component of any network security strategy. In most cases, this is accomplished using firewalls. Monitoring the activity of the firewalls in your network is a massive undertaking for most organizations since the amount of logs generated can be overwhelming. STRM intelligently collects and analyzes firewall logs and then automatically reports any abnormal and/or suspicious behavior.

STRM generates offenses based on access related behavior when a user is attempting to gain illegal access to your network. By analyzing the firewall and other intrusion prevention device logs, STRM determines when a particular IP address has been denied access in a manner that requires investigation. STRM can also detect suspicious failed access to the same destination as well as multiple attempts across many distributed destinations.

How do I Investigate an Access Offense?

To investigate an access offense:

Step 1 Click the **Offense Manager** tab.

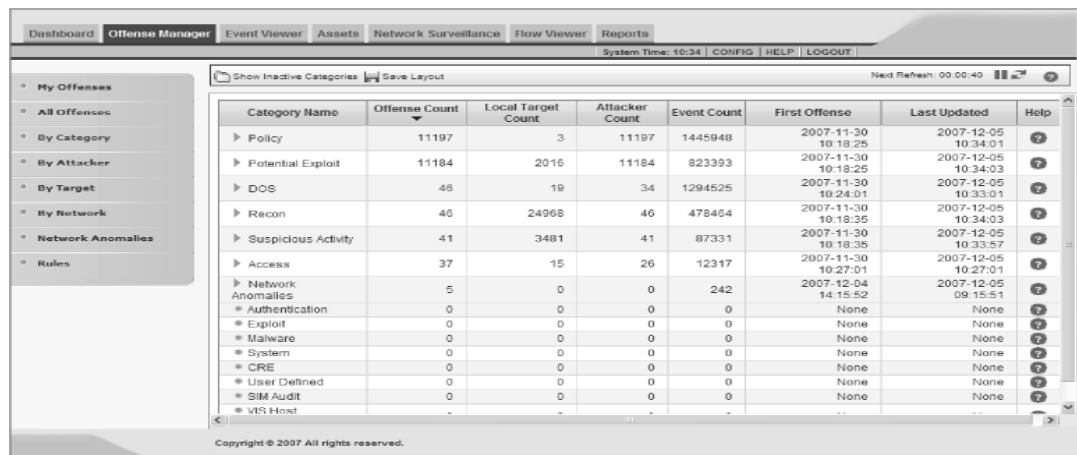
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Access category, click the arrow icon next to Access.

Category Name	Offense Count	Local Target Count	Attacker Count	Event Count	First Offense	Last Updated	Help
▼ Access	22	85	22	5027	2007-02-01 09:52:50	2007-02-01 11:50:15	?
Firewall Deny	4	0	4	941	2007-02-01 11:29:15	2007-02-01 11:50:15	
Firewall Permit	1	0	1	437	2007-02-01 10:05:24	2007-02-01 11:49:30	
Flow Context Response	17	84	17	2157	2007-02-01 11:22:30	2007-02-01 11:50:15	
Misc Authorization	1	1	1	496	2007-02-01 09:52:50	2007-02-01 11:49:30	
Misc Network Communication Event	1	1	1	996	2007-02-01 09:52:50	2007-02-01 11:49:30	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
190	Local TCP Scanner Detected, Default - DoS - External - Poten...	10.101.240.222		Remote (1699)	10	all	other	28177	2007-02-01 10:01:12	2m 12s
118	Default - DoS - External - Potential Unresponsive Service or ...	10.103.251.45		Remote (1869)	2	Benefits	other	2075	2007-02-01 10:00:02	3m 7s
81	Default - Recon - External - Potential Network Scan, Default...	10.101.133.167		Remote (6728)	7	Hong_Kong	other	35981	2007-02-01 09:59:45	2m 11s

Step 5 Double-click the offense you wish to view.

The details panel appears.

Offense 190 Summary

Magnitude		Relevance	7	Severity	7	Credibility	6
Description	Local TCP Scanner Detected preceded by Default - DoS - External - Potential Unresponsive Service or Distributed DoS preceded by Possible Local Worm Detected preceded by Default - Suspicious - External - Rejected Communication Attempts		Event count	30129 events in 10 categories			
Attacker/Src	10.101.240.222	Start	2007-02-01 10:01:12				
Target(s)/Dest	Remote (1744)	Duration	1h 52m 45s				
Network(s)	other	Assigned to	Not assigned				
Notes							

Attacker Summary Details

Magnitude		User	Unknown
Description	10.101.240.222	MAC	Unknown
Vulnerabilities	0	Asset Weight	0
Location	ComputingServices.Helpdesk.all		

Top 5 Categories Categories

Name	Magnitude	Local Target Count	Events	Last Event
Potential worm activity		0	6	02-01 11:46:30
Distributed DoS		0	1213	02-01 11:54:00
Empty Packet Flows		0	1	02-01 11:46:30
Potential Botnet connection		0	0	3
Flow Context Response		0	6	02-01 11:30:00

Top 10 Events Events

Event Name	Magnitude	Device	Category	Destination	Start Time
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	132.8.56.109:33434	02-01 10:10:47
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	66.218.71.112:33434	02-01 10:24:36
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	202.0.182.1:33434	02-01 10:44:44
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	194.176.169.1:33434	02-01 10:57:29

Step 6 To investigate the attacker, view the Attacker Summary box:


- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to

STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.

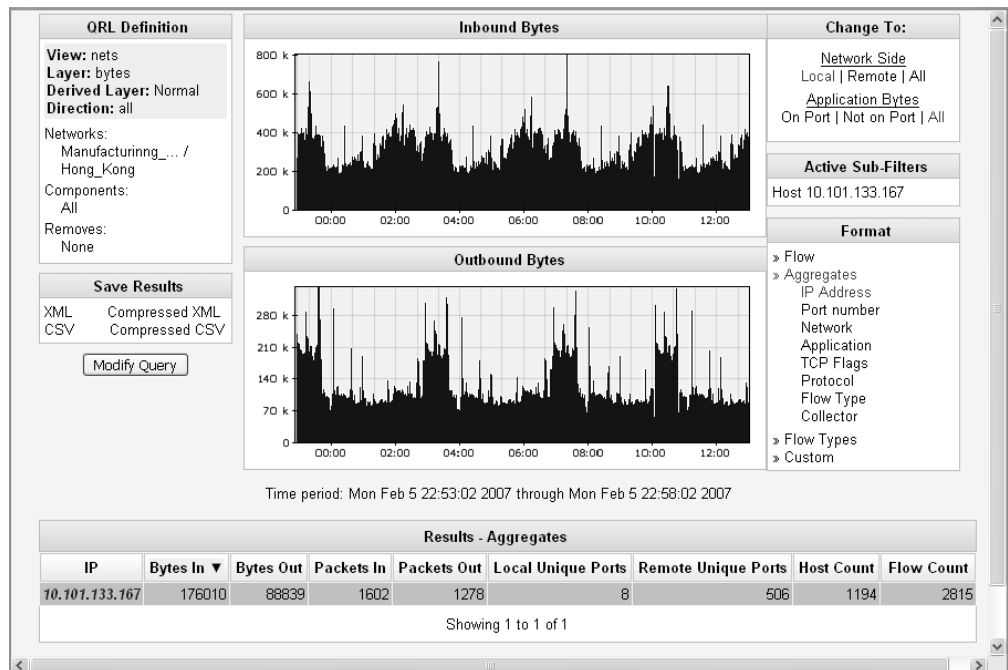
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the Select **Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user. You can also determine if the user associated to the offense is a valid user on the device they are attempting to access.

STRM generates access events when the same source IP address causes multiple failed access attempts, such as, from a firewall. If you determine that this is normal behavior, you can tune STRM to no longer create offenses for this behavior. For information, see [How do I Tune an Access Offense?](#).

Step 7 Determine if the user associated with the offense was attempting to illegally gain access to the network or a restricted area of the network. If you determine that the user had malicious intent:

- Click  **Flows** to further the user’s activity to make sure that the user did not obtain access to a restricted area of the network.

The Flow Search window appears.



- Use the Event Viewer to search for events relating to this user associated with firewall accept messages. For more information on the Event Viewer, see Using the Event Viewer in the *STRM Users Guide*.


- Step 8** Once you have determined the impact of the offense, you must perform the necessary steps to rectify the source of the activity. If you have determined this behavior is normal, you can tune STRM to no longer detect this activity. For more information, see [How do I Tune an Access Offense?](#)
- Step 9** Once you are satisfied that you have resolved the offense, you can close or hide the offense.

For more information on closing or hiding an offense, see Investigating Offenses in the *STRM Users Guide*.

How do I Tune an Access Offense?

If you determine that the access activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

To tune access activity using the false positive function:

- Step 1** In the offense details interface, click  **Events**.

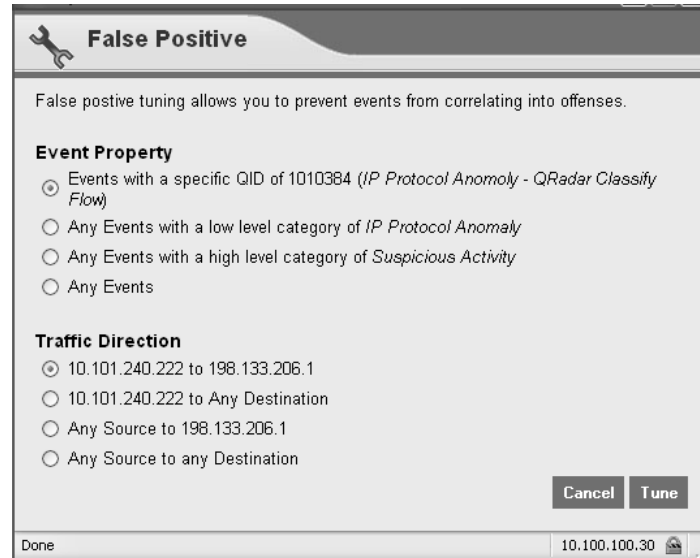
The List of Events window appears.

Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
Anomaly - Event CRE	eventprocessor0::clio	1	2007-02-01 11:58:57	Anomaly	10.101.240.222:50285	198.133.206.1:33447	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50304	198.133.206.1:33442	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50248	198.133.206.1:33445	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:49924	147.28.0.60:33442	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50151	147.28.0.60:33438	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50285	198.133.206.1:33448	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50285	198.133.206.1:33452	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50285	198.133.206.1:33447	NA	
Suspicious Packet - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	Suspicious Packet	10.101.240.222:12543	209.25.132.107:33434	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:49918	198.133.206.1:33442	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50248	198.133.206.1:33442	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50227	147.28.0.60:33448	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50046	192.83.230.1:33451	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50325	147.28.0.60:33444	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50046	192.83.230.1:33439	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50285	198.133.206.1:33451	NA	
IP Protocol Anomaly - QRadar Classif...	classif0::clio	1	2007-02-01 11:58:57	IP Protocol Anomaly	10.101.240.222:50285	198.133.206.1:33451	NA	

- Step 2** Select the event that includes the known source IP address that is reported to produce suspicious activity.

- Step 3** Click  **False Positive**.

The False Positive window appears with information derived from the selected event.



Step 4 Select the necessary event properties to tune as a false positive.

Step 5 Click **Tune**.

STRM will no longer create additional offense for this source IP address when this type of activity occurs.

2

SIM AUDIT OFFENSES

This chapter provides information on SIM audit offenses including:

- [What is SIM Audit?](#)
- [How do I Investigate a SIM Audit Offense?](#)
- [How do I Tune a SIM Audit Offense?](#)

What is SIM Audit?

STRM generates an records SIM audit events for system and configuration changes occurring within the STRM deployment. This information may be required for compliance regulations, troubleshooting, or internal tracking.

When STRM detects suspicious or unapproved SIM audit events, a SIM audit offense is created. STRM is able to monitor SIM audit activity for many different aspects of the STRM product. In certain situations, this data may also be combined with other events and flows associated to the attacker, and correlated into one offense. If an attacker does gain access to the STRM system, they may try and de-activate certain features or turn monitoring off on certain areas of the network. These suspicious changes would generate an offense in STRM.

How do I Investigate a SIM Audit Offense?

This section provides information on further investigating SIM audit offenses.

To investigate SIM audit offenses:

Step 1 Click the **Offense Manager** tab.

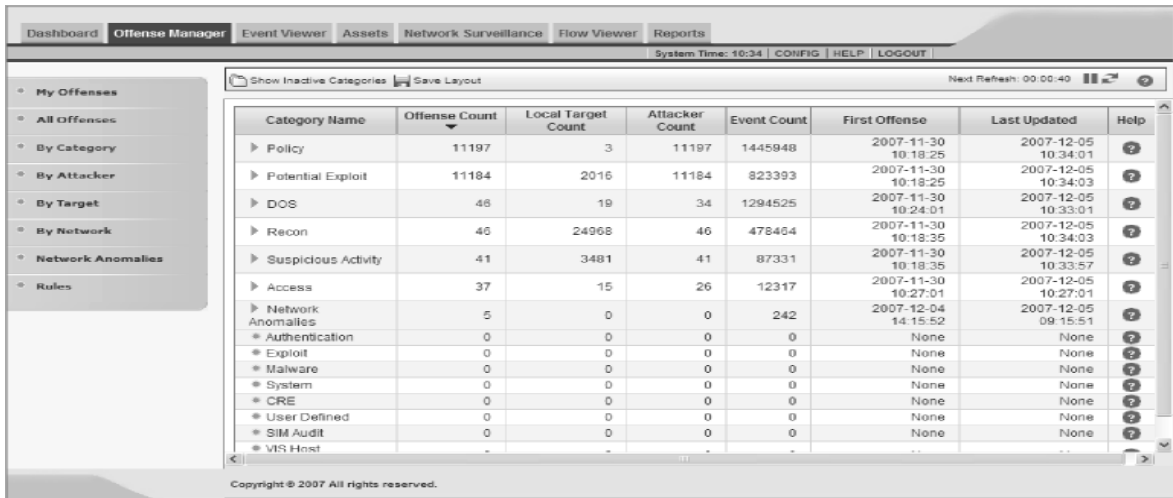
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.




Step 3 To view additional low-level category information for the SIM Audit category, click the arrow icon next to SIM Audit.

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Attacker Net	Target Net	Events	Start Date	Last Event
13767	User Login , User Logout	10.100.100.106	■	Remote (1)	other	other	4	2007-09-20 14:21:21	27m 31s
13780	User Login	10.100.50.71	■	Remote (1)	other	other	1	2007-09-20 14:24:02	25m 7s
13804	User Login	10.100.100.104	■	Remote (1)	other	other	1	2007-09-20 14:36:41	12m 28s

Step 5 Double-click the offense you wish to view. The details panel appears.

Step 6 View the Attacker Summary box to understand the attacker:

Attacker Summary  Details			
Magnitude		User	Unknown
Description	10.100.100.106	MAC	Unknown
Vulnerabilities	0	Asset Weight	0
Location	other		

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.

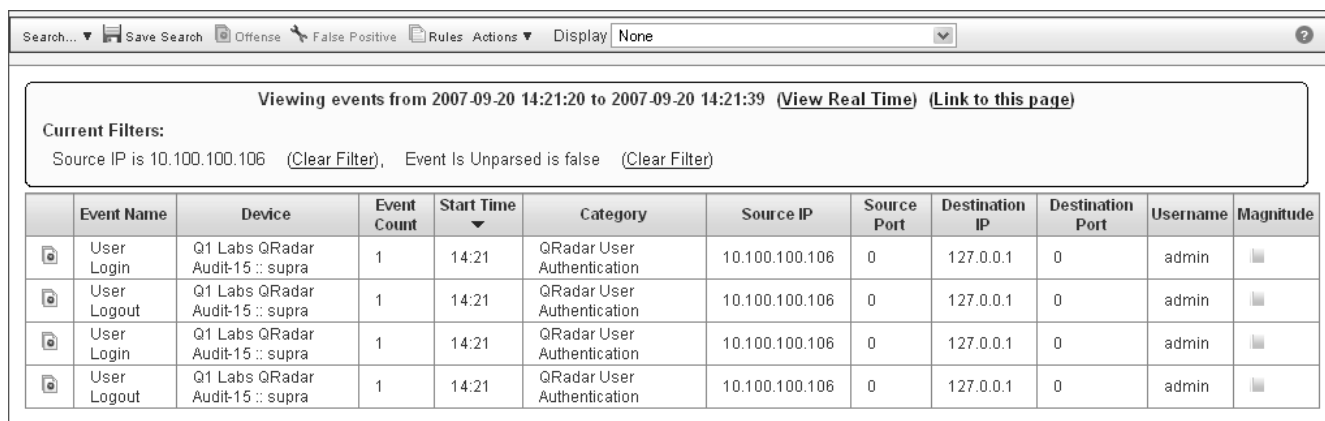
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the suspicious traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the **Select Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.

If the activity is normal (for example, a valid user is making approved configuration changes to the STRM deployment), then you can use the Rules function in the Offense Manager to tune out this activity. For more information, see [How do I Tune a SIM Audit Offense?](#)

Step 7 In the Attacker Summary box, place your mouse over the Description text. If the number of offenses is greater than 1, we recommend that you investigate the attacker to determine if the attacker is attempting to disguise his activities from other offenses. Unauthorized changes to your STRM deployment can lead to serious threats and attacks to the network being undetected.









Step 8 Click  Events.

The List of Events appears for the selected offense.



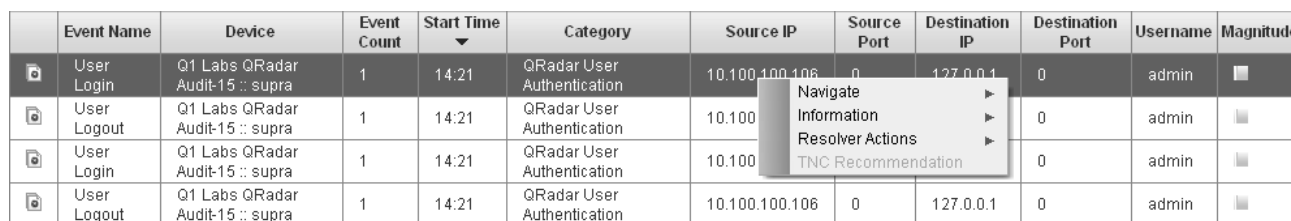
Viewing events from 2007-09-20 14:21:20 to 2007-09-20 14:21:39 (View Real Time) (Link to this page)









Current Filters:
Source IP is 10.100.100.106 (Clear Filter), Event Is Unparsed is false (Clear Filter)

	Event Name	Device	Event Count	Start Time	Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
	User Login	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	
	User Logout	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	
	User Login	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	
	User Logout	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	

The Device column provides the device that detected the event. If multiple devices are reporting similar events, the credibility value for this offense increases.

Step 9 To further investigate the target, right-click on an IP address in the Source column. The right-click menu appears.



	Event Name	Device	Event Count	Start Time	Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
	User Login	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	
	User Logout	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100			0	admin	
	User Login	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100			0	admin	
	User Logout	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	

Step 10 Select **Information > Asset Profile**.

The Asset Profile appears.

Asset Profile
Ports History

Name			
Description			
IP Address	10.101.167.102	VA Risk Level	1
Operating System		How Threatening	8
Host Name (DNS Name)	10.101.167.102	How Threatened	0
Asset Weight	0 - Not Important		
MAC		Host Name	
Machine Name			
User		User Group	
Extra Data			

Save Changes Cancel Close Window

Port	OSVDB ID	Name	Description	Risk / Severity	Last Seen	First Seen
3531				1	2007-01-24 22:00:00 (Passive)	2007-01-24 22:00:00 (Passive)

Step 11 Once you have determined the impact of the offense, you must either block the source of the unauthorized configuration activity, then take the desired action against the offense.

Step 12 Once you have resolved the offense, close or hide the offense.

For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a SIM Audit Offense?

If you determine that the SIM audit activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

You can tune STRM using one of the following methods:

- [Tuning Using False Positive Function](#)
- [Tuning Using Custom Rules Wizard](#)

Tuning Using False Positive Function

To tune SIM audit activity using the false positive function:

- Step 1** In the SIM audit offense details interface, click Events. The List of Events appears for the selected offense.

Event Name	Device	Event Count	Start Time	Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
User Login	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	■
User Logout	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	■
User Login	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	■
User Logout	Q1 Labs QRadar Audit-15 :: supra	1	14:21	QRadar User Authentication	10.100.100.106	0	127.0.0.1	0	admin	■

Step 2 Select the event with the source IP address known to be producing the SIM audit activity.

Step 3 Click **False Positive**.

The False Positive window appears with information derived from the selected event.

🔧
False Positive

False positive tuning allows you to prevent events from correlating into offenses.

Event Property

- Events with a specific QID of 1202486 (*User Login*)
- Any Events with a low level category of *QRadar User Authentication*
- Any Events with a high level category of *QRadar Audit*
- Any Events

Traffic Direction

- 10.100.100.106 to 127.0.0.1
- 10.100.100.106 to Any Destination
- Any Source to 127.0.0.1
- Any Source to any Destination

Cancel
Tune

Step 4 Select the necessary event properties to tune as a false positive.

For example, in the window above, the Events with specific QID option is selected to tune the specific IP address and the event high-level category that is creating the false positive SIM audit event.

For additional information on using the False Positive tuning function, see the *STRM Users Guide*.

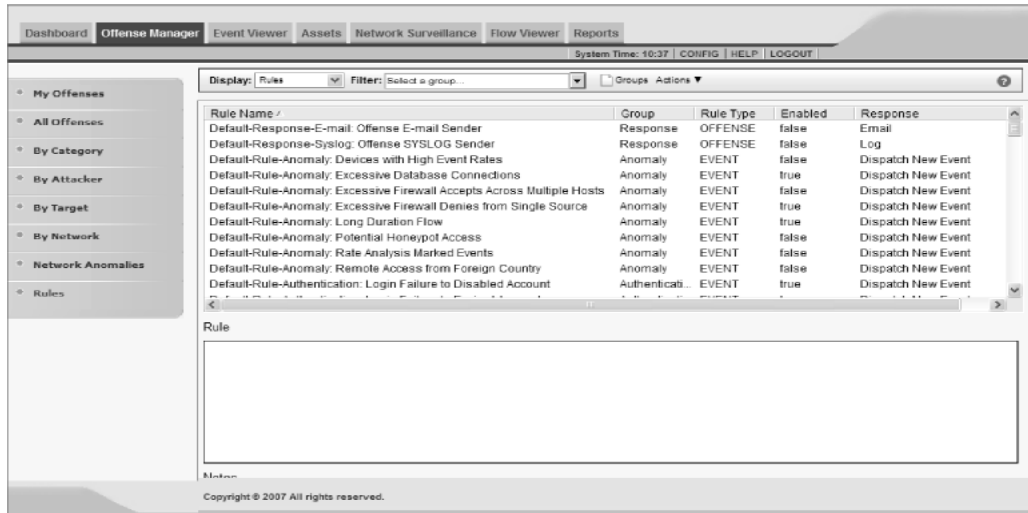
Step 5 Click **Tune**.

STRM will no longer create additional offenses for this source IP address when performing normal VA or network management tasks.

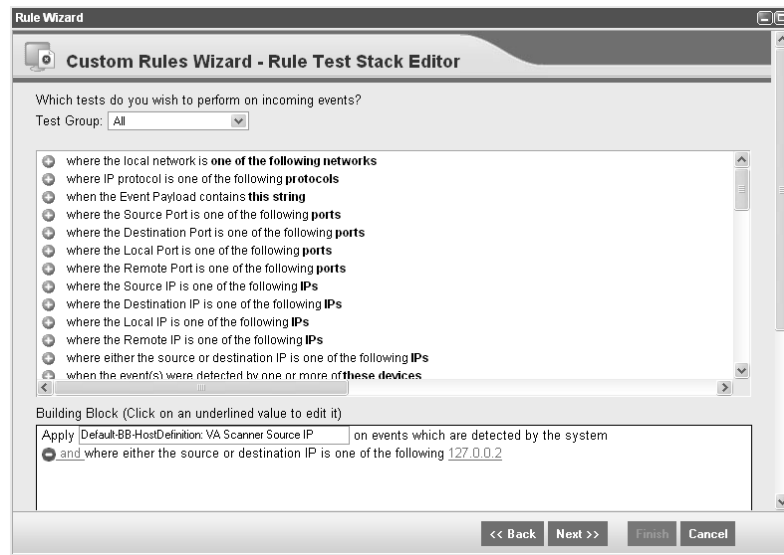
Tuning Using Custom Rules Wizard

To tune SIM audit activity using the custom rules wizard:

- Step 1** In the navigation bar of the Offense Manager, click **Rules**.
The Rules interface appears.



- Step 2** Using the Display drop-down list box, select Building Blocks.
- Step 3** In the Block Name list, locate the **Default-BB-HostDefinition: VA Scanner Source IP** building block.
- Step 4** From the Actions drop-down list box, select **Edit**.
The Rules Wizard appears.



- Step 5** In the Building Block section, click the IP address that appears.
A configuration window appears.

The screenshot shows a web form with the following elements:

- A text input field with the placeholder text "Enter an IP address or CIDR and click 'Add'".
- An "Add" button to the right of the input field.
- A section titled "Selected Values" containing a list box with the value "127.0.0.2".
- A "Remove" button to the right of the list box.
- "Submit" and "Cancel" buttons at the bottom right of the form.

- Step 6** In the **Enter an IP address or CIDR and click 'Add'** field, enter the IP address of the VA scanner or IP address that is producing false positives.
- Step 7** Click **Add**.
- Step 8** Repeat for all VA scanners or IP address(es).
- Step 9** Click **Submit**.
- Step 10** Complete the rules wizard.

For more information on using the Custom Rules Wizard, see the *STRM Administration Guide*.

3

AUTHENTICATION OFFENSES

This chapter provides information on authentication offenses including:

- [What is an Authentication Offense?](#)
- [How do I Investigate an Authentication Offense?](#)
- [How do I Tune an Authentication Offense?](#)

What is an Authentication Offense?

Typically, the first level of network security starts with authentication. When a user navigates a protected network, the network generally requires authentication at various level of the network infrastructure. STRM supports the monitoring of many authentication points throughout a network, including host machines, firewalls, databases, application servers, and authentication servers.

While analyzing authentication events from devices, STRM detects any abnormal or potentially threatening activity, for example, when there are multiple log in failures followed by a successful login. Since authentication activity is based on access to the network, STRM creates offenses when invalid users are attempting to, or more importantly, have already gained access to the network. STRM features intelligent security event logic capable of filtering authentication-based activity and creating offenses on truly suspicious behavior.

How do I Investigate an Authentication Offense?

To investigate an authentication offense:

Step 1 Click the **Offense Manager** tab.

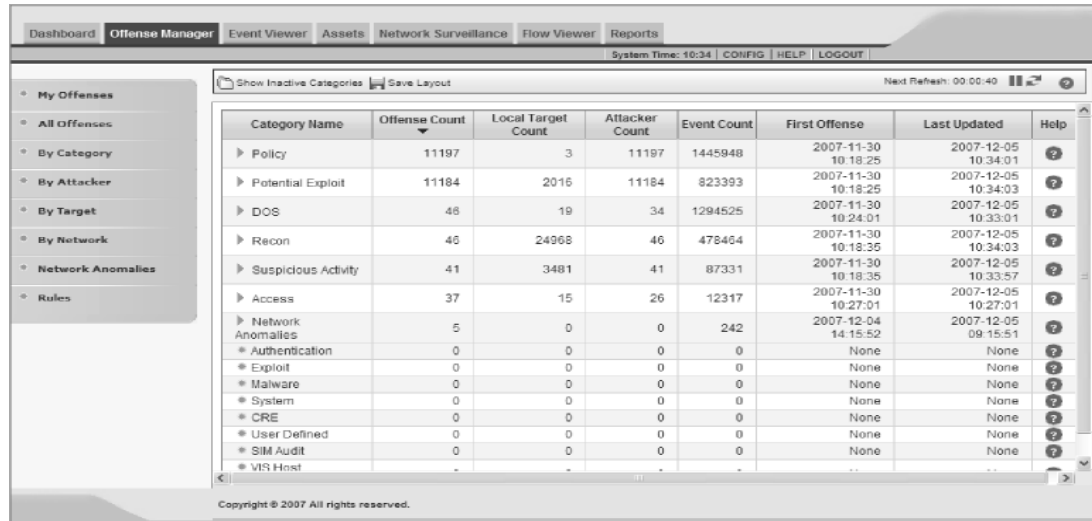
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Authentication category, click the arrow icon next to Authentication.

Authentication	16	16	16	16518	2007-01-31 13:28:43	2007-01-31 14:32:58	?
Remote Access Login Failed	16	16	16	1640	2007-01-31 13:28:43	2007-01-31 14:32:58	
Auth Server Login Failed	10	10	10	5513	2007-01-31 13:28:43	2007-01-31 14:32:58	
Auth Server Session Opened	4	4	4	2276	2007-01-31 13:28:43	2007-01-31 14:32:13	
Host Login Failed	2	2	2	959	2007-01-31 13:29:28	2007-01-31 14:32:13	
Misc Login Failed	2	2	2	636	2007-01-31 13:29:28	2007-01-31 14:32:58	
FTP Login Failed	2	2	2	628	2007-01-31 13:30:58	2007-01-31 14:32:58	
Host Login Succeeded	1	1	1	323	2007-01-31 13:29:28	2007-01-31 14:32:13	
Misc Login Succeeded	1	1	1	312	2007-01-31 13:32:28	2007-01-31 14:32:58	
Auth Server Login Succeeded	1	1	1	326	2007-01-31 13:28:43	2007-01-31 14:32:13	
Web Service Login Succeeded	1	1	1	326	2007-01-31 13:28:43	2007-01-31 14:32:13	
Web Service Login Failed	1	1	1	1968	2007-01-31 13:28:43	2007-01-31 14:32:13	
General Authentication Failed	1	1	1	325	2007-01-31 13:28:43	2007-01-31 14:32:13	
Telnet Login Failed	1	1	1	324	2007-01-31 13:29:28	2007-01-31 14:32:13	
Misc Logout	1	1	1	650	2007-01-31 13:29:28	2007-01-31 14:32:13	
Admin Logout	1	1	1	312	2007-01-31 13:32:28	2007-01-31 14:32:58	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
7	Authentication: Repeated Login Failures Single Host	10.100.100.19	■■■■	Multiple (5)	16	other	Multiple (2)	18519	2007-01-31 13:29:03	1m 58s
5	Authentication: Repeated Login Failures Single Host	10.100.100.90	■■■	Multiple (2)	3	other	Multiple (2)	1240	2007-01-31 13:28:51	2m 4s
6	Authentication: Repeated Login Failures Single Host	12.45.241.120	■■■	Multiple (2)	2	other	Multiple (2)	818	2007-01-31 13:29:03	2m 2s
10	Authentication: Repeated Login Failures Single Host	205.174.174.143	■■■	Multiple (2)	2	other	Multiple (2)	411	2007-01-31 13:29:47	1m 18s
11	Authentication: Repeated Login Failures Single Host	205.174.174.75	■■■	Multiple (2)	2	other	Multiple (2)	411	2007-01-31 13:29:47	1m 18s

Step 5 Double-click the offense you wish to view.

The details panel appears.

All Offenses 2 Offense 7 (Summary)

Offense 7 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude		Relevance	3	Severity	5	Credibility	5
Description	Authentication: Repeated Login Failures Single Host		Event count	21338 events in 16 categories			
Attacker/Src	10.100.100.19		Start	2007-01-31 13:29:03			
Target(s)/Dest	10.100.100.19 Remote (4)		Duration	1h 21m 9s			
Network(s)	Multiple (2)		Assigned to	Not assigned			
Notes							

Attacker Summary Details			Top 5 Categories Categories			
Magnitude		User	Unknown			
Description	10.100.100.19		MAC	Unknown		
Vulnerabilities	0		Asset Weight	0		
Location	other					

Name	Magnitude	Local Target Count	Events	Last Event
TCP DoS	■■■	1	1248	01-31 14:50:13
ICMP DoS	■■■	1	416	01-31 14:50:13
UDP DoS	■■■	1	416	01-31 14:50:13
Remote Access Login Failed	■■■	1	240	01-31 14:50:13
Misc Network Communication Event	■■■	1	836	01-31 14:50:13

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
10.100.100.19		Unknown	Yes			other	0

Event Name	Magnitude	Device	Category	Destination	Start Time
ICMP Packet Volume Too High	■■■	Auto-discovered IntruShield at intrushield_host	ICMP DoS	10.100.100.19:0	01-31 13:29:21
TCP Data Segment Volume Too High	■■■	Auto-discovered IntruShield at intrushield_host	TCP DoS	10.100.100.19:0	01-31 13:29:43
ICMP Packet Volume Too High	■■■	Auto-discovered IntruShield at intrushield_host	ICMP DoS	10.100.100.19:0	01-31 13:29:33
TCP RST Volume Too High	■■■	Auto-discovered IntruShield at intrushield_host	TCP DoS	10.100.100.19:0	01-31 13:29:33

Step 6 To investigate the attacker, view the Attacker Summary box:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to

STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.

- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the Select **Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.

Authentication offenses occur when the same source IP address causes multiple log in failures. This may be caused by many users using the same network path to reach a particular server. Your network may also include an entire development team accessing a Windows server from the same Linux or Solaris server. In this case, false positive offenses may be generated when multiple users attempt to log in to different servers from the same server incorrectly. If this is the case, you can tune STRM to no longer create offenses for this behavior. For more information, see [How do I Tune an Authentication Offense?](#).


- Step 7** Determine if the user associated with the offense was attempting to illegally gain access to the network with malicious intent or a user who has forgotten their password. If you determine that the user had malicious intent, we recommend that you restrict this user's access to the network. We also recommend that you use the Event Viewer to search for events relating to this user to determine if your network was successfully breached. For more information on the Event Viewer, see the *STRM Users Guide*.
- Step 8** Once you have determined the impact of the offense, you must perform the necessary steps to rectify the source of the activity. If you have determined this behavior is normal, you can tune STRM to no longer detect this activity. For more information, see [How do I Tune an Authentication Offense?](#).
- Step 9** Once you are satisfied that you have resolved the offense, you can close or hide the offense.

For more information on closing or hiding an offense, see Investigating Offenses in the *STRM Users Guide*.

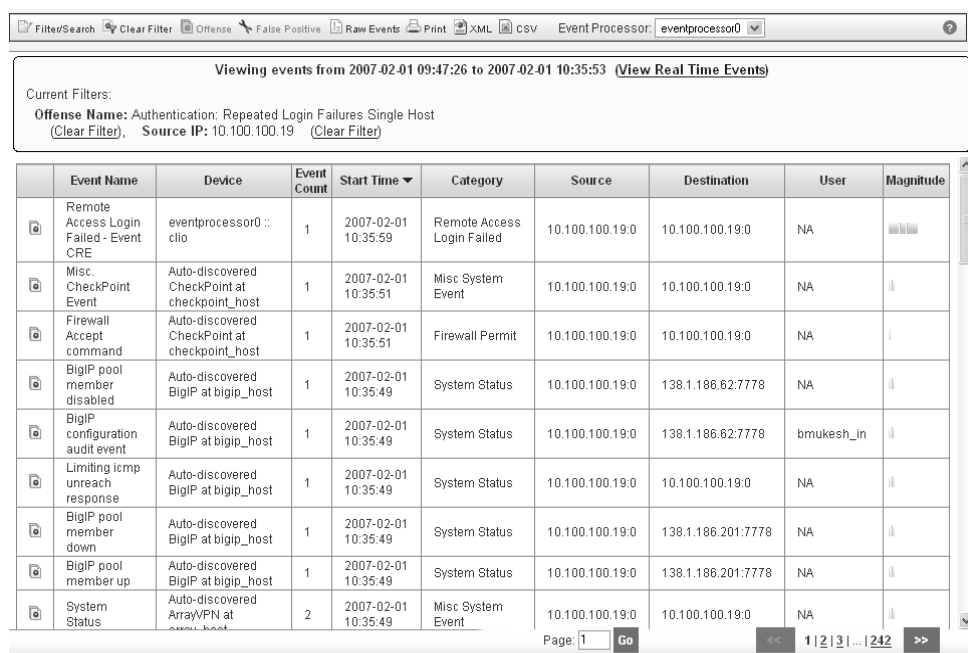
How do I Tune an Authentication Offense?

If you determine that the authentication activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

To tune authentication activity using the false positive function:









Step 1 In the offense details interface, click  **Events**.

The List of Events window appears.



Viewing events from 2007-02-01 09:47:26 to 2007-02-01 10:35:53 [View Real Time Events](#)

Current Filters:
Offense Name: Authentication: Repeated Login Failures Single Host
 (Clear Filter) **Source IP:** 10.100.100.19 (Clear Filter)

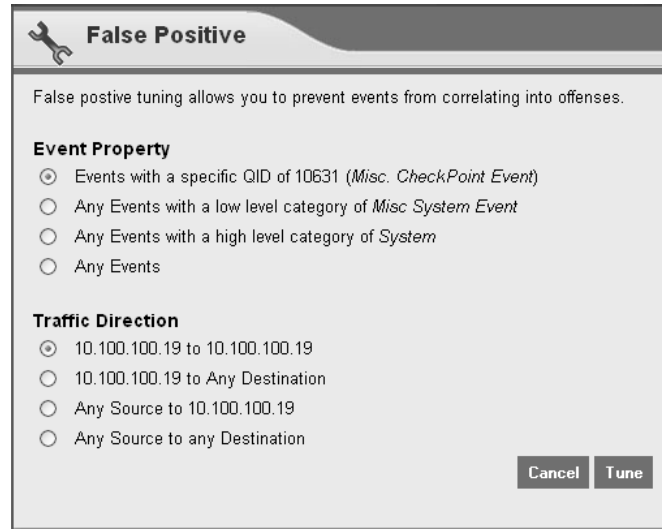
	Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
	Remote Access Login Failed - Event CRE	eventprocessor0 :: clio	1	2007-02-01 10:35:59	Remote Access Login Failed	10.100.100.19:0	10.100.100.19:0	NA	
	Misc. CheckPoint Event	Auto-discovered CheckPoint at checkpoint_host	1	2007-02-01 10:35:51	Misc System Event	10.100.100.19:0	10.100.100.19:0	NA	
	Firewall Accept command	Auto-discovered CheckPoint at checkpoint_host	1	2007-02-01 10:35:51	Firewall Permit	10.100.100.19:0	10.100.100.19:0	NA	
	BigIP pool member disabled	Auto-discovered BigIP at bigip_host	1	2007-02-01 10:35:49	System Status	10.100.100.19:0	138.1.186.62:7778	NA	
	BigIP configuration audit event	Auto-discovered BigIP at bigip_host	1	2007-02-01 10:35:49	System Status	10.100.100.19:0	138.1.186.62:7778	bmukesh_in	
	Limiting icmp unreachable response	Auto-discovered BigIP at bigip_host	1	2007-02-01 10:35:49	System Status	10.100.100.19:0	10.100.100.19:0	NA	
	BigIP pool member down	Auto-discovered BigIP at bigip_host	1	2007-02-01 10:35:49	System Status	10.100.100.19:0	138.1.186.201:7778	NA	
	BigIP pool member up	Auto-discovered BigIP at bigip_host	1	2007-02-01 10:35:49	System Status	10.100.100.19:0	138.1.186.201:7778	NA	
	System Status	Auto-discovered ArrayVPN at arrayvpn_host	2	2007-02-01 10:35:49	Misc System Event	10.100.100.19:0	10.100.100.19:0	NA	

Page: 1 Go << 1 | 2 | 3 | ... | 242 >>

Step 2 Select the event that includes the known source IP address that is reported to produce suspicious activity.

Step 3 Click  **False Positive**.

The False Positive window appears with information derived from the selected event.



Step 4 Select the necessary event properties to tune as a false positive.

Step 5 Click **Tune**.

STRM will no longer create additional offense for this source IP address when this type of activity occurs.

4

CRE OFFENSES

This chapter provides information on CRE offenses including:

- [What is a CRE Offense?](#)
- [How do I Investigate a CRE Offense?](#)

What is a CRE Offense?

Custom Rule Engine (CRE) offenses are generated through user defined custom rules or sentries. A CRE offense appears in the Offense Manager by a custom rule when a user attempts to map an event to a category not supported by STRM. You should not receive CRE events in offenses or reports using the standard templates with STRM.

For more information on rules, sentries, or templates, see the *STRM Administration Guide*.

How do I Investigate a CRE Offense?

To investigate a CRE offense:

Step 1 Click the **Offense Manager** tab.

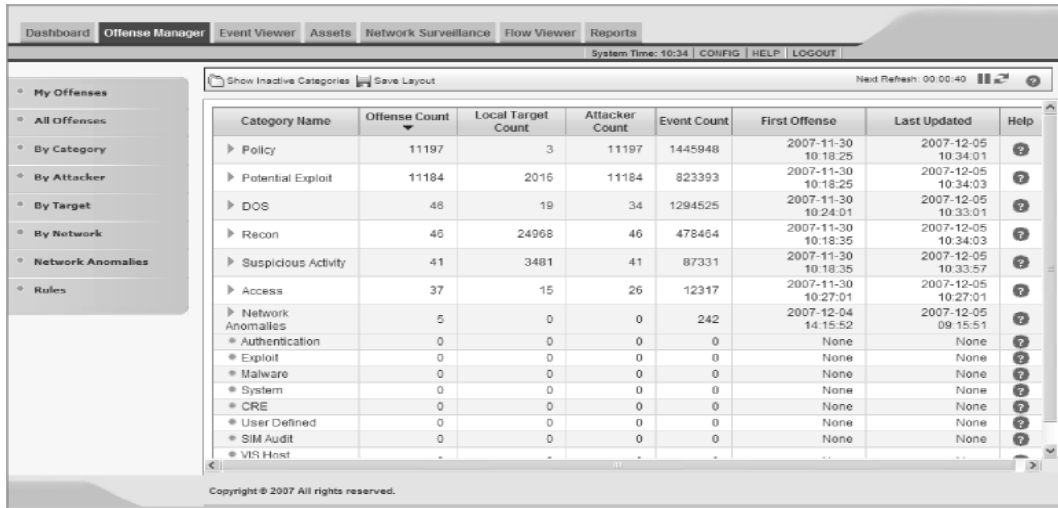
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the CRE category, click the arrow icon next to CRE

Category Name	Offense Count	Local Target Count	Attacker Count	Event Count	First Offense	Last Updated	Help
Policy	11197	3	11197	1445948	2007-11-30 10:18:25	2007-12-05 10:34:01	?
Potential Exploit	11184	2016	11184	823393	2007-11-30 10:18:25	2007-12-05 10:34:03	?
DOS	48	19	34	1294525	2007-11-30 10:24:01	2007-12-05 10:33:01	?
Recon	46	24968	46	478464	2007-11-30 10:18:35	2007-12-05 10:34:03	?
Suspicious Activity	41	3481	41	87331	2007-11-30 10:18:35	2007-12-05 10:33:57	?
Access	37	15	26	12317	2007-11-30 10:27:01	2007-12-05 10:27:01	?
Network Anomalies	5	0	0	242	2007-12-04 14:15:52	2007-12-05 09:15:51	?
• Authentication	0	0	0	0	None	None	?
• Exploit	0	0	0	0	None	None	?
• Malware	0	0	0	0	None	None	?
• System	0	0	0	0	None	None	?
• CRE	0	0	0	0	None	None	?
• User Defined	0	0	0	0	None	None	?
• SIM Audit	0	0	0	0	None	None	?
• VIR Host	0	0	0	0	None	None	?

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

?	Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
	11	Exploit/Malware Events Across Multiple Targets	172.16.50.10		Multiple (17)	9	Ian50	Multiple (3)	52	2007-02-19 12:46:14	6m 57s

Step 5 Double-click the offense you wish to view. The details panel appears.

All Offenses Offense 11 (Summary)

Offense 11 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude			Relevance	4	Severity	5	Credibility	3
Description	Exploit/Malware Events Across Multiple Targets		Event count	52 events in 9 categories				
Attacker/Src	172.16.50.10		Start	2007-02-19 12:46:14				
Target(s)/Dest	Local (8) Remote (9)		Duration	22h 57m 29s				
Network(s)	Multiple (3)		Assigned to	lan150				
Notes	How much i sthat doggy in the window? WoofWoof..							

Attacker Summary Details				Top 5 Categories				
Magnitude		User	Unknown	Name	Magnitude	Local Target Count	Events	Last Event
Description	172.16.50.10	MAC	Unknown	FTP Exploit		1	3	02-20 11:44:42
Vulnerabilities	0	Asset Weight	0	SNMP Exploit		1	3	02-20 11:44:42
Location	Net_172.1an50			Mail Exploit		1	3	02-20 11:44:42
				RPC Exploit		1	3	02-20 11:44:42
				Buffer Overflow		4	6	02-20 11:44:42

Top 5 Local Targets							
IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
172.16.60.20		Unknown	No	Unknown	Unknown	lan60	0
172.16.50.35		Unknown	No	Unknown	Unknown	lan50	0
172.16.50.36		Unknown	No	Unknown	Unknown	lan50	0
172.16.50.37		Unknown	No	Unknown	Unknown	lan50	0
172.16.50.38		Unknown	No	Unknown	Unknown	lan50	0

Top 10 Events						
Event Name	Magnitude	Device	Category	Destination	Start Time	
RPC EXPLOIT statdx		Auto-discovered Snort at snort	RPC Exploit	172.16.50.37.47276	02-19 12:50:36	
SMTP sendmail 8.6.9 exploit		Auto-discovered Snort at snort	Mail Exploit	172.16.50.36.47276	02-19 12:50:36	
FTP EXPLOIT OpenBSD x86 ftpd		Auto-discovered Snort at snort	FTP Exploit	172.16.50.35.47276	02-19 12:50:36	

Step 6 View the Attacker Summary box to understand the attacker:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the suspicious traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the **Select Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.

Step 7 Once you have determined the impact of the offense, you must either block the source of the scan, patch, or shut down services on the appropriate systems, then take the desired action against the offense.

Step 8 Once you have resolved the offense, close or hide the offense.

For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a CRE Offense?

If you determine that the CRE activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity. You can use the Custom Rules wizard in the Offense Manager to create a building block to allow this behavior. For more information on using the Custom Rules Wizard, see the *STRM Administration Guide*.

5

DENIAL OF SERVICE (DoS) OFFENSES

This chapter provides information on DoS offenses including:

- [What is a DoS Offense?](#)
- [How do I Investigate a DoS Offense?](#)
- [How do I Tune a DoS Offense?](#)
- [How Can I Verify If STRM is Receiving Valid DoS Offenses?](#)

What is a DoS Offense?

A DoS attack is an attempt to prevent an application or host from behaving in accordance with its intended purpose. When STRM detects a correlated series of events, a DoS offense is created. DoS attacks may include:

- [What is a DoS Flood Attack?](#)
- [What is a DoS Service Exploit?](#)

What is a DoS Flood Attack?

A DoS flood attack includes one or more source attempts to flood the target hosts or application with transaction requests until the host is unable to process transactions for users in a timely manner. There are three types of DoS flood offenses including:

- **Network DoS** - Includes a packet flood targeted at an IP address intended to overwhelm a host in a flood of data until the host becomes unable to process transaction for the users.
- **DDoS** - Includes a DoS attack from many sources and may target a host or a listening port.
- **Service DoS** - Includes an attack targeted at a specific port used by an application. A flood of empty or invalid transaction requests are directed at an application port, with the intention of overwhelming the application.

What is a DoS Service Exploit?

The intention of a DoS service exploit is to cause a disruption in service for a host or service. A DoS exploit attempts to disrupt a service by sending an exploit, which may be a single packet containing a DoS exploit, to a port where a vulnerable service is listening. Such an exploit may cause memory corruption that results in a failure of service or the operating system to cease functioning. These events are created by STRM sentries using Network Behavioral Anomaly Detection (NBAD). DoS events are also created by intrusion detection and prevention sensors.

STRM correlates DoS events with other relevant data, such as the presence or absence of the target host and vulnerabilities on the target port, when vulnerability assessment data is available. DoS exploits are ineffective when the target host vulnerability has been patched or when the exploit packs are blocked by firewalls or in-line devices, such as proxy servers or IPSs.

How do I Investigate a DoS Offense?

To investigate a DoS offenses:

Step 1 Click the **Offense Manager** tab.

The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.

Category Name	Offense Count	Local Target Count	Attacker Count	Event Count	First Offense	Last Updated	Help
▶ Policy	11197	3	11197	1445948	2007-11-30 10:18:25	2007-12-05 10:34:01	?
▶ Potential Exploit	11184	2016	11184	823393	2007-11-30 10:18:25	2007-12-05 10:34:03	?
▶ DOS	48	19	34	1294525	2007-11-30 10:24:01	2007-12-05 10:33:01	?
▶ Recon	46	24968	46	478464	2007-11-30 10:18:35	2007-12-05 10:34:03	?
▶ Suspicious Activity	41	3481	41	87331	2007-11-30 10:18:35	2007-12-05 10:33:57	?
▶ Access	37	15	26	12317	2007-11-30 10:27:01	2007-12-05 10:27:01	?
▶ Network Anomalies	5	0	0	242	2007-12-04 14:15:52	2007-12-05 09:15:51	?
▶ Authentication	0	0	0	0	None	None	?
▶ Exploit	0	0	0	0	None	None	?
▶ Malware	0	0	0	0	None	None	?
▶ System	0	0	0	0	None	None	?
▶ CRE	0	0	0	0	None	None	?
▶ User Defined	0	0	0	0	None	None	?
▶ SIM Audit	0	0	0	0	None	None	?
▶ VIS Host	-	-	-	-	-	-	?

Step 3 To view additional low-level category information for the DoS category, click the arrow icon next to DOS.

DOS	41	2646	41	300471	2007-01-30 10:10:38	2007-01-30 14:50:20	?
Distributed DoS	40	2645	40	293231	2007-01-30 11:10:30	2007-01-30 14:50:20	
ICMP DoS	1	1	1	1448	2007-01-30 10:10:38	2007-01-30 14:49:35	
TCP DoS	1	1	1	4344	2007-01-30 10:10:38	2007-01-30 14:49:35	
UDP DoS	1	1	1	1448	2007-01-30 10:10:38	2007-01-30 14:49:35	

Step 4 Double-click any low-level category to view the list of associated offenses.
The list of offenses appear.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
10661	Default - DoS - External - Potential Unresponsive Service or ...	192.168.91.48		Local (457)	2	other	Multiple (3)	467	2007-01-30 14:39:02	8m 6s
10000	Default - DoS - External - Potential Unresponsive Service or ...	192.168.91.8		Local (167)	2	other	Multiple (2)	172	2007-01-30 14:25:02	22m 5s
62	Default - Recon - External - Potential Network Scan , Default...	10.101.133.167		Remote (10832)	7	Hong_Kong	other	93193	2007-01-30 11:10:02	1m 5s
74	Default - DoS - External - Potential Unresponsive Service or ...	192.168.91.20		Local (546)	2	other	Multiple (3)	43183	2007-01-30 11:10:02	2m 5s

Step 5 Double-click the offense you wish to view.
The details panel appears.

Offense 10661 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude		Relevance	5	Severity	8	Credibility	2
Description	Default - DoS - External - Potential Unresponsive Service or Distributed DoS containing Distributed DoS - QRadar Classify Flow		Event count	467 events in 2 categories			
Attacker/Src	192.168.91.48	Start	2007-01-30 14:39:02				
Target(s)/Dest	Local (457)	Duration	4m 59s				
Network(s)	Multiple (3)	Assigned to	Not assigned				
Notes							

Attacker Summary Details				Top 5 Categories Categories				
Magnitude		User	Unknown	Name	Magnitude	Local Target Count	Events	Last Event
Description	192.168.91.48	MAC	Unknown	Distributed DoS		457	457	01-30 14:39:04
Vulnerabilities	0	Asset Weight	0	Flow Context Response		2	10	01-30 14:44:20
Location	other							

Top 5 Local Targets Targets							
IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
10.101.130.169		Unknown	No	Unknown	Unknown	Hong_Kong	0
10.101.130.170		Unknown	No	Unknown	Unknown	Hong_kong	0
10.101.130.172		Unknown	No	Unknown	Unknown	Hong_Kong	0
10.101.131.207		Unknown	No	Unknown	Unknown	Hong_Kong	0
10.101.131.219		Unknown	No	Unknown	Unknown	Hong_Kong	0

Top 10 Events Events						
Event Name	Magnitude	Device	Category	Destination	Start Time	
Distributed DoS - QRadar Classify Flow		classify0 :: clio	Distributed DoS	10.101.137.52:123	01-30 14:39:02	
Distributed DoS - QRadar Classify Flow		classify0 :: clio	Distributed DoS	10.101.137.233:123	01-30 14:39:02	
Distributed DoS - QRadar Classify Flow		classify0 :: clio	Distributed DoS	10.101.137.29:123	01-30 14:39:02	
Distributed DoS - QRadar Classify Flow		classify0 :: clio	Distributed DoS	10.101.136.249:123	01-30 14:39:02	

Step 6 View the Description field and determine the activity associated with this offense. This may indicate multiple types of activity. If the offense is a DDoS attack, the following terms appear:

- Distributed DoS Attack (Low, Medium, or High Number of Hosts)
- Potential Unresponsive Service or Distributed DoS

In a DDoS attack, the IP address listed in the Attacker Summary box is the address of the target since DDoS offenses are correlated by the target address. Also, in the Top 5 Local Targets box, the IP addresses listed are the sources of the DDoS attack.

Step 7 View the Attacker Summary box to understand the attacker:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located. If the attack is local, contact the user associated with the IP address to determine the source of the attack. If this is deemed normal behavior, you can tune STRM to no longer create offenses for this activity. See [How do I Tune a DoS Offense?](#). If this is not normal behavior, go to [Step 9](#).
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. If the attacker is remote, go to [Step 8](#).
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the **Select Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.

Step 8 If the attack is remote:

- a Investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic.
- b Determine if STRM is correlating firewall events. If you are correlating firewall events, the Offense Manager includes firewall or ACL deny events that indicate the attack is being blocked.
- c Determine if the target is an Internet facing server, which means that the traffic may be permitted through the firewall. For assistance, contact your network administrator.

If the target is an Internet facing server and you are investigating a DoS attack, right-click on the IP address located in the Description field of the Attacker Summary box to determine the ownership of the IP address sending the DoS attack. From the right-click menu, select **Information > WHOIS Lookup** or **DNS Lookup**. For more information on using the right-click menu, see the *STRM Users Guide*.

If the target is an Internet facing server and you are investigating a DDoS attack, right-click on an IP address located in the Destination field of the Top 5 Local Targets box to determine the ownership of the IP address sending the

DoS attack. From the right-click menu, select **Information > WHOIS Lookup** or **DNS Lookup**. For more information on using the right-click menu, see the *STRM Users Guide*.

Once you have determined ownership, contact your network administrator to determine if the source IP address(es) of the DoS attack may be blocked using your firewall or intrusion prevention device.

Step 9 Determine if the IP address of the attacker is being spoofed (using an IP address that is invalid), trace the path of the traffic back to the switch port in the original form. To determine if the IP address is being spoofed, contact your network administrator. If you determine that the IP address is being spoofed, use one of the following methods to determine the originator of the traffic:

- STRM Collector View. For more information on views, see the *STRM Administration Guide*.
- Switch and router port statistics.
- Egress filtering, which is useful for stopping outbound spoofed traffic.

Step 10 Determine if the attacker is a desktop computer, which may be running a network application or infected with malware. For assistance, contact your network administrator. If the desktop is running a network application, you can tune STRM to no longer generate offenses for this behavior. See [How do I Tune a DoS Offense?](#)

Step 11 Once you have determined the impact of the offense, you must perform the necessary steps to rectify the source of the activity. If you have determined this behavior is normal, you can tune STRM to no longer detect this activity. For more information, see [How do I Tune a DoS Offense?](#).

Step 12 Once you are satisfied that you have resolved the offense, you can close or hide the offense.

For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a DoS Offense?


If you determine that the DoS activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

You can tune STRM using one of the following methods:

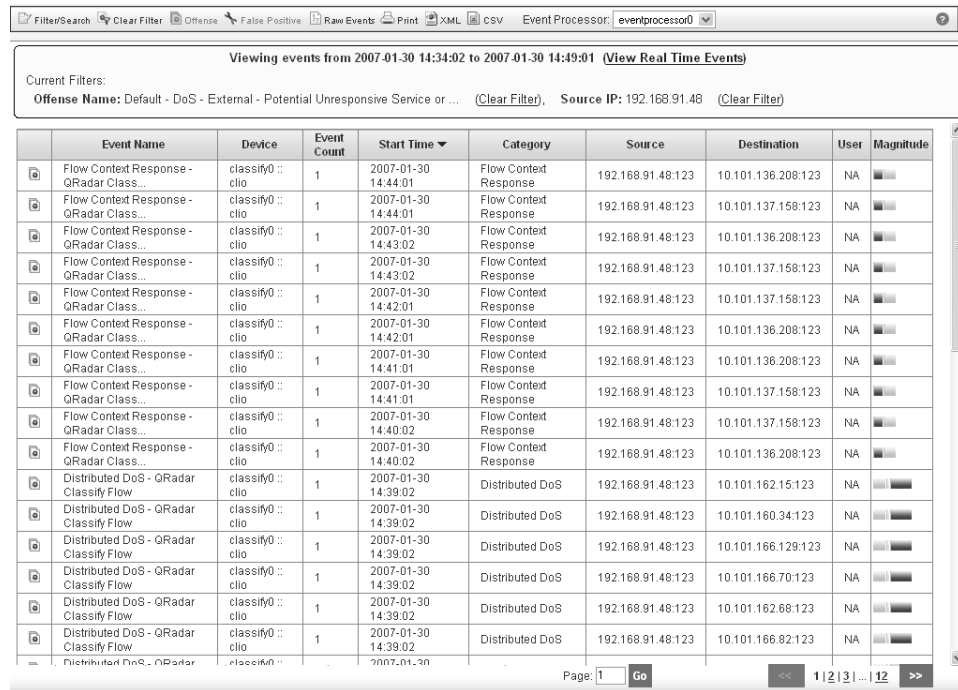
- [Tuning Using False Positive Function](#)
- [Tuning Using Sentries](#)
- [Tuning Using Custom Rules Wizard](#)

Tuning Using False Positive Function

To tune DoS activity using the false positive function:

Step 1 In the offense details interface, click  **Events**.

The List of Events appears.

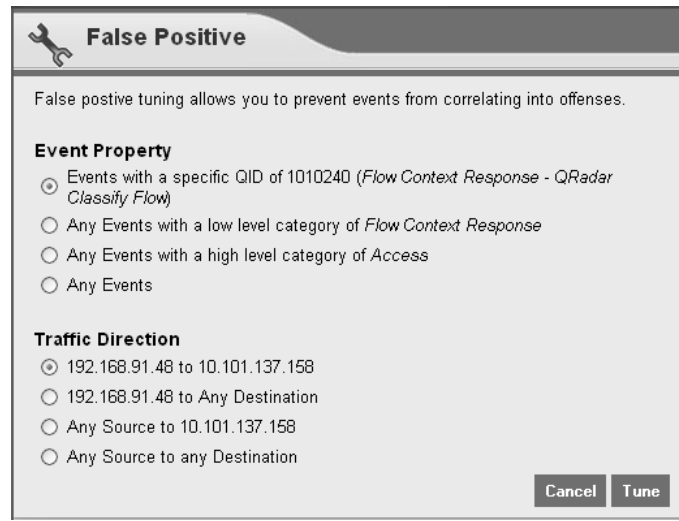


Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:44:01	Flow Context Response	192.168.91.48:123	10.101.136.208:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:44:01	Flow Context Response	192.168.91.48:123	10.101.137.158:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:43:02	Flow Context Response	192.168.91.48:123	10.101.136.208:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:43:02	Flow Context Response	192.168.91.48:123	10.101.137.158:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:42:01	Flow Context Response	192.168.91.48:123	10.101.136.208:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:42:01	Flow Context Response	192.168.91.48:123	10.101.136.208:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:41:01	Flow Context Response	192.168.91.48:123	10.101.136.208:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:41:01	Flow Context Response	192.168.91.48:123	10.101.137.158:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:40:02	Flow Context Response	192.168.91.48:123	10.101.137.158:123	NA	■■■
Flow Context Response - QRadar Class...	classify0 :: clio	1	2007-01-30 14:40:02	Flow Context Response	192.168.91.48:123	10.101.136.208:123	NA	■■■
Distributed DoS - QRadar Classify Flow	classify0 :: clio	1	2007-01-30 14:39:02	Distributed DoS	192.168.91.48:123	10.101.162.15:123	NA	■■■■
Distributed DoS - QRadar Classify Flow	classify0 :: clio	1	2007-01-30 14:39:02	Distributed DoS	192.168.91.48:123	10.101.160.34:123	NA	■■■■
Distributed DoS - QRadar Classify Flow	classify0 :: clio	1	2007-01-30 14:39:02	Distributed DoS	192.168.91.48:123	10.101.166.129:123	NA	■■■■
Distributed DoS - QRadar Classify Flow	classify0 :: clio	1	2007-01-30 14:39:02	Distributed DoS	192.168.91.48:123	10.101.166.70:123	NA	■■■■
Distributed DoS - QRadar Classify Flow	classify0 :: clio	1	2007-01-30 14:39:02	Distributed DoS	192.168.91.48:123	10.101.162.68:123	NA	■■■■
Distributed DoS - QRadar Classify Flow	classify0 :: clio	1	2007-01-30 14:39:02	Distributed DoS	192.168.91.48:123	10.101.166.82:123	NA	■■■■

Step 2 Select the event that includes the known source IP address that is reported to produce suspicious activity.

Step 3 Click  **False Positive**.

The False Positive window appears with information derived from the selected event.



Step 4 In the Event Properties option, select the first option.

Step 5 In the Traffic Direction option, choose one of the following options:

- a For a DoS attack, select the <IP address> to Any Destination option.
- b For a DDos attack, select the <IP address> to DoS target option, which is listed as the Attacker source and Any Destination option.

For example, in the window above, the source IP address and the event high-level category that is creating the false positive suspicious offense. For additional information on using the False Positive tuning function, see the *STRM Users Guide*.

Step 6 Click **Tune**.

STRM will no longer create additional offense for this source IP address when this type of activity occurs.

Tuning Using Sentries

If the attacker is local and events are being received from the Classification Engine, you can assume that the events are being created as a result of a STRM sentry. You can enable or disable DoS sentries for internal and external networks. For more information on sentries, see the *STRM Administration Guide*.

Tuning Using Custom Rules Wizard

You can use the Custom Rules wizard to edit a building block that contains the IP address(es) of the attackers and the DoS category. For more information on creating or editing a building block, see the *STRM Administration Guide*.

How Can I Verify If STRM is Receiving Valid DoS Offenses?

If you believe STRM should be receiving DoS offenses but none have appeared in the Offense Manager, verify that the events were received and processed using the Event Viewer interface. If no events are being received, verify that the appropriate DoS sentries within STRM and other security devices are enabled, as appropriate. For more information, see Configuring Rules in the *STRM Administration Guide*.

6

EXPLOIT OFFENSES

This chapter provides information on an exploit attack including:

- [What is an Exploit Attack?](#)
- [How do I Investigate an Exploit Offense](#)
- [How do I Tune an Exploit Offenses?](#)

What is an Exploit Attack?

STRM generates exploit offenses when the events associated to an offense are part of the exploit category. Typically, exploit events are generated by Intrusion Detection Systems (IDSs) or Intrusion Prevention System (IPSs). These systems may include stand-alone network sensors such as Sourcefire or Enterasys Dragon, part of an IPS within a firewall (such as Juniper Networks ISG), or host-based IDS systems (such as the Cisco Security Agent). By default, STRM attempts to detect high exploits that are likely to be successful or show a pattern of the attacker attempting to exploit multiple host or using multiple types of attacks. Unfortunately, these devices may cause the creation of false positive offenses so you can tune STRM to no longer create offenses for these events while maintaining an audit of all events generated from the device for compliance and forensics purposes.

How do I Investigate an Exploit Offense

To investigate an exploit offense:

Step 1 Click the **Offense Manager** tab.

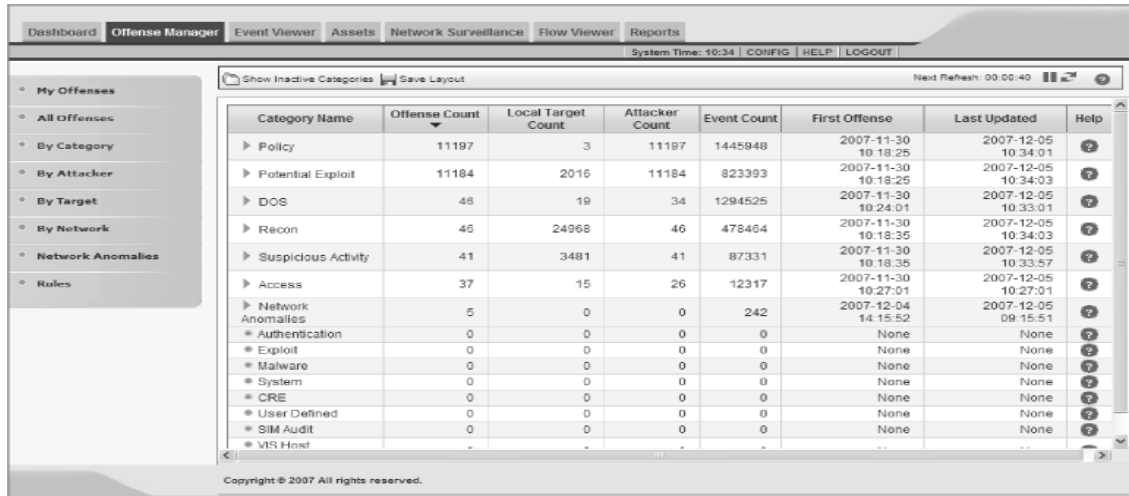
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Exploit category, click the arrow icon next to Exploit.

Exploit	1	2	1	13	2007-02-01 09:52:50	2007-02-01 09:54:20	?
Worm Active	1	2	1	13	2007-02-01 09:52:50	2007-02-01 09:54:20	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
9	Worm Events Detected	172.16.2.1		Multiple (2)	1	other	Multiple (2)	13	2007-02-01 09:52:46	3h 53m 40s

Step 5 Double-click the offense you wish to view. The details panel appears.

All Offenses Offense 9 (Summary)

Offense 9 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude			Relevance	5	Severity	9	Credibility	2
Description	Worm Events Detected containing Slapper Worm		Event count	13 events in 1 categories				
Attacker/Src	172.16.2.1		Start	2007-02-01 09:52:46				
Target(s)/Dest	172.16.60.23 Remote (1)		Duration	1m 30s				
Network(s)	Multiple (2)		Assigned to	Not assigned				
Notes								

Attacker Summary Details

Magnitude		User	Unknown
Description	172.16.2.1	MAC	Unknown
Vulnerabilities	0	Asset Weight	0
Location	other		

Top 5 Categories

Name	Magnitude	Local Target Count	Events	Last Event
Worm Active		2	13	02-01 09:54:20

Top 5 Local Targets

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
172.16.60.23		Unknown	No	Unknown	Unknown	other	0

Top 10 Events

Event Name	Magnitude	Device	Category	Destination	Start Time
Worm Active - Event CRE		eventprocessor0 :: clio	Worm Active	172.16.60.23:1756	02-01 09:52:46
Worm Active - Event CRE		eventprocessor0 :: clio	Worm Active	172.16.60.23:1756	02-01 09:52:58
Worm Active - Event CRE		eventprocessor0 :: clio	Worm Active	172.16.60.23:1756	02-01 09:53:42
Worm Active - Event CRE		eventprocessor0 :: clio	Worm Active	172.16.60.23:1756	02-01 09:53:30
Worm Active - Event CRE		eventprocessor0 :: clio	Worm Active	172.16.60.23:1756	02-01 09:53:10
Slapper Worm		Auto-discovered NetScreenIDP at netscreenidp_host	Worm Active	172.16.60.23:1756	02-01 09:52:46
Slapper Worm		Auto-discovered NetScreenIDP at netscreenidp_host	Worm Active	172.16.60.23:1756	02-01 09:52:58

Step 6 Determine if the offense is a result of a remote host attempting to exploit one or more local hosts.

Typically the target of the attacker is located inside the Demilitarized Zone (DMZ) or in the public facing Network Address Translation (NAT) range. However, if you have assigned public addresses to internal hosts, this behavior could be occurring on any host in the network. To determine if the offense is a result of a remote host attempting to exploit one or more local hosts:

- View the Attacker/Src field to determine if the attacker is associated with this offense is local or remote. If local, go to step [Step 7](#).
- View the Target(s)/Dest field to determine if the target for this offense is local or remote. If remote, go to [Step 8](#).
- View the Description field to determine the behavior associated with this offense. If the exploit was followed by suspicious behavior, you can determine the validity of the event if a Flow Context Response events appears. If the offense does not include any Flow Context Response events, this indicates that no flow context was detected, which is desired.



Note: For you to view Flow Context Response events, your network must include a flow source monitoring the same location as the IDS product.

- View the Annotations box to view the details of the offense. If the annotation indicates that this offense includes chaining, this indicates that the target of the attack is now attacking other hosts. If the chained offense started after the exploit, this may indicate that the host was successfully exploited.

Step 7 Determine if the offense is the result of a local host attempting to exploit another local host on your network.

If this is the case, this is one of the most serious types of offenses, but also the most likely to be a false positive offense. To determine if the offense is a result of a local host attempting to exploit another local host:

- a View the Attacker/Src field to determine if the attacker is associated with this offense is local or remote.
- b View the Target(s)/Dest field to determine if the target for this offense is local or remote.
- c View the Description field to determine the behavior associated with this offense. To determine the intention of this offense, determine if the attacker attempted some form of reconnaissance or suspicious activity before the exploit. You can also determine if the attacker attempted different types of attacks on the same host or tried multiple targets.

Step 8 Determine if the offense is the result of a remote host attempting to exploit another remote host:

- a Verify your network hierarchy configuration. For more information on your network hierarchy, see *Managing STRM* in the *STRM Administration Guide*.
- b Verify if one of the hosts involved in the offense belongs to the local network. If you do not recognize the hosts involved in the offense, right-click on the IP address in either the Target(s)/Dest or Attacker/Src fields and select **Information > WHOIS** to obtain further information.
- c If you recognize either host involved in the offense, add that information to your network hierarchy.
- d View the Description field to determine the behavior associated with this offense. To determine the intention of this offense, determine if the attacker attempted some form of reconnaissance or suspicious activity before the exploit. You can also determine if the attacker attempted different types of attacks on the same host or tried multiple targets.

Step 9 Once you have determined the impact of the offense, you must perform the necessary steps to rectify the source of the activity. If you have determined this behavior is normal, you can tune STRM to no longer detect this activity. For more information, see [How do I Tune an Exploit Offenses?](#).


Step 10 Once you are satisfied that you have resolved the offense, you can close or hide the offense.

For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune an Exploit Offenses?

If you determine that the exploit activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

To tune exploit offenses using the false positive function:

Step 1 In the offense details interface, click  **Categories**.

The category details appear.

Step 2 In the List of Event Categories, double-click the related category to display associated events. These categories should be low-level exploit categories, such as, buffer overflow, FTP exploit, or worm active.

Step 3 Select the event that includes the known source IP address that is reported to produce suspicious activity.

Step 4 Click  **False Positive**.

The False Positive window appears with information derived from the selected event.



Step 5 If only a single offense of this type exists and the offense contains only a single target, select the first option in the Event Property options.

Step 6 If this offense includes multiple attackers generating similar offenses but all to the same destination (typically a multiple host communicating with a single server), use the SRC to any option.



Note: If all the hosts associated to this offense are related, you can also create a building block using the Rules Wizard to include all the hosts and QIDs (events) that are creating the false positives. Then, add this new building block to the Default-Rule-FalsePositives: All false positive building blocks rule.

Step 7 If this event includes a single offense of this type but the same event (QID) has been used against many targets, select the second option in the Traffic Properties options.

Step 8 Click **Tune**.

STRM will no longer create additional offense for this source IP address when this type of activity occurs.

How Can I Verify That STRM is Receiving Valid Exploit Offenses?

To verify that STRM is receiving valid offenses:

- Step 1** By default, STRM automatically removes noise and false positives commonly associated with IDS devices. However, there are certain circumstances where STRM may not create an offense for an attack. For example, when no vulnerability information exists in the asset profile and an attempt is made to exploit that asset (using a common tool, such as Metasploit), STRM may not create an offense for this attack if no other corresponding suspicious activity is detected or could be correlated to indicates a successful attack. If you wish all exploit attempts to become offenses, see [Step 3](#).
- STRM may also not generate an offense for an exploit as a result of the data source. We recommend that you verify that the IDS is monitoring a location where it is able to detect the attack. You can also use the Event Viewer to search for the attacker's IP address. If an exploit event is not detected, verify your IDS configuration.
- Step 2** If you are not able to use vulnerability information, STRM provides additional options. For example, STRM searches for an attacker attempting multiple methods of exploits against a target so if you run multiple exploits, STRM creates an offense. You can also exploit multiple targets with the same attack, which generates an offense. You can adjust these thresholds by editing the Custom Rules with exploits.
- Step 3** In the Rules function within the Offense Manager, you can enable or disable rules, as necessary. You can enable any rules that allow STRM to make all exploit attempts become offenses. We do not recommend that you do not deploy this within a live environment but is useful for testing purposes.

7

MALWARE OFFENSES

This chapter provides information on malware offenses including:

- [What is Malware?](#)
- [How do I Investigate a Malware Offense?](#)
- [How do I Tune a Malware Offense?](#)

What is Malware?

This section provides information regarding malware including:

- [What is Malware?](#)
- [What is a Malware Offense?](#)

What is Malware?

Malware is a broad term associated with many types of threats, such as, trojans, viruses, adware, spyware, and worms. The term malware describes any software that is intended to gain access to a host or damage a host without the consent of the owner.

What is a Malware Offense?

STRM detects malware by correlating events and flows from security devices. The default STRM rules report on spyware, viruses, hostile mail attachments, backdoor detection, and other relevant events and logs from security devices. STRM also adds additional information to the malware offenses to provide additional network context to the offense. For example, if your network does not include IDSs monitoring host port scanning, STRM detects this type of behavior leading up to an attack, such as, a backdoor exploit by monitoring the network flows and correlating this behavior to the malware offense.

How do I Investigate a Malware Offense?

To investigate a malware offenses:

Step 1 Click the **Offense Manager** tab.

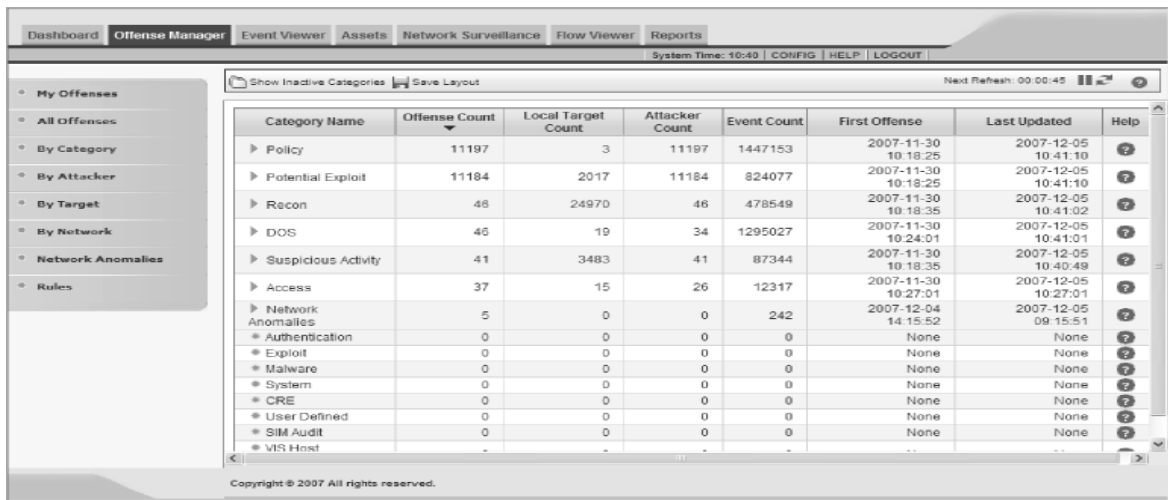
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Malware category, click the arrow icon next to Malware.

Malware	2	1	2	1127	2007-02-02 02:09:13	2007-02-05 10:22:50	?
Backdoor Detected	1	1	1	1041	2007-02-05 10:19:50	2007-02-05 10:22:50	
Spyware Detected	1	0	1	86	2007-02-02 02:09:13	2007-02-05 08:40:48	

Step 4 Double-click any low-level category to view the list of associated offenses.

The list of offenses appear.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
1136	BACKDOOR black curse 4.0 runtime detection - normal init conn...	141.112.2.24	█	172.16.60.1	1	other	Net_172_16_0_0	1041	2007-02-05 10:19:22	16m 4s

Step 5 Double-click the offense you wish to view.

The details panel appears.

All Offenses **Offense 1136 (Summary)**

Offense 1136 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude				Relevance	4	Severity	9	Credibility	1
Description	BACKDOOR black curse 4.0 runtime detection - normal init connection			Event count	1041 events in 1 categories				
Attacker/Src	141.112.2.24			Start	2007-02-05 10:19:22				
Target(s)/Dest	172.16.60.1			Duration	2m 1s				
Network(s)	Net-10-172-192.Net_172_16_0_0			Assigned to	Not assigned				
Notes									

Attacker Summary Details				Top 5 Categories Categories				
Magnitude		User	Unknown	Name	Magnitude	Local Target Count	Events	Last Event
Description	141.112.2.24	MAC	Unknown	Backdoor Detected		1	1041	02-05 10:22:50
Vulnerabilities	0	Asset Weight	0					
Location	NorthAmericaContinent							

Top 5 Local Targets Targets								
IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight	
172.16.60.1		Unknown	Yes	Unknown	Unknown	Net_172_16_0_0	0	

Top 10 Events Events						
Event Name	Magnitude	Device	Category	Destination	Start Time	
BACKDOOR black curse 4.0 runtime det...		Auto-discovered Snort at snort	Backdoor Detected	172.16.60.1:80	02-05 10:19:22	
BACKDOOR black curse 4.0 runtime det...		Auto-discovered Snort at snort	Backdoor Detected	172.16.60.1:80	02-05 10:19:22	
BACKDOOR black curse 4.0 runtime det...		Auto-discovered Snort at snort	Backdoor Detected	172.16.60.1:80	02-05 10:19:22	

Step 6 View the Attacker Summary box to understand the attacker:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the **Select Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.



Normal activity may be detected by security devices as malware. For example, if a user telecommutes and uses a wireless network at home, when they return to the office, their computer may attempt to connect to their own ISPs name server. This activity may generate a botnet detection.

Step 7 View the Top 5 Local Targets box, which displays the targets that are most vulnerable or have the highest business value. This box also indicates if the target

has become chained to another offense. Chaining means that the target has become an attacker of another offense. This indicates a self-propagating malware.




Note: Any remote targets associated to a malware offense may be foreign or unknown servers that the source IP address is communicating with to receive instructions to upload data.

- Step 8** View the Top 5 Categories box, which displays the various types of activities associated to the attacker during the time of the offense.
- Step 9** View the Top 10 Events box, which displays the top events for this offense, organized by severity.
- Step 10** View the Top 5 Annotations box, which displays the most significant correlation tests that contributed to the overall magnitude of the offense. Annotations provide important information, such as, which devices have contributed events to the offense.
- Step 11** Double-click any event that you wish to investigate in further details and view the Source Port field. Port 6667 is commonly used by bots as an IRC-based control channel. Spyware commonly use ports 80 and 443.
- Step 12** In the offense details window, click  **Flows** to view network flows from the attacker IP address. When investigating flows, select the port or application in question. If the traffic volume and the number of conversation pairs seem to be too high for the user, this may indicate potential malware.
- Step 13** In the offense details window, click  **Targets**, which are organized by vulnerability risk and business value.
- Step 14** Right-click on a targets IP address and select **Information > Asset Profile**, which displays which services the targets are responding to.
- Step 15** Once you have determined the impact of the offense, you must either block the source of the scan, patch or shut down services on the appropriate systems, then take the desired action against the offense.
- Step 16** Once you have resolved the offense, close or hide the offense.
For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a Malware Offense?

If you determine that the malware activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

To tune reconnaissance activity using the false positive function:
















Step 1 In the reconnaissance offense details interface, click  Events.

The List of Events appears for the selected offense.

Filter/Search Clear Filter Offense False Positive Raw Events Print XML CSV Event Processor: eventprocessor0

Viewing events from 2007-02-05 10:14:22 to 2007-02-05 10:26:24 [\(View Real Time Events\)](#)

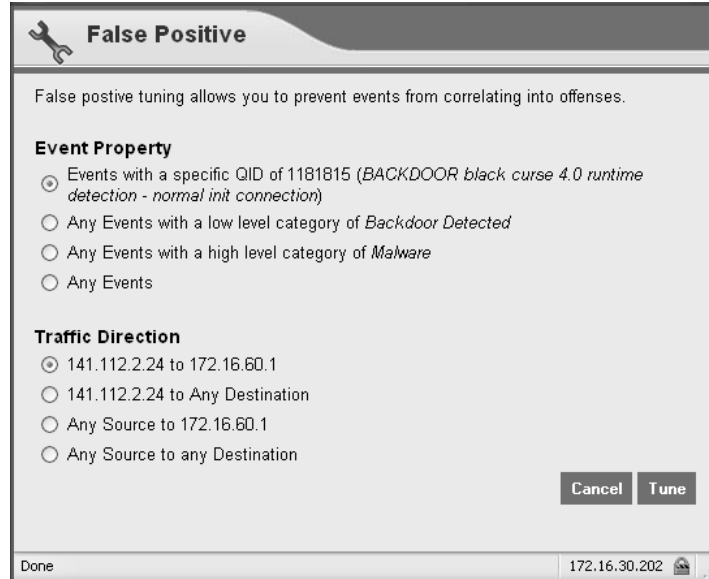
Current Filters:
Offense Name: BACKDOOR black curse 4.0 runtime detection - normal init conn... [\(Clear Filter\)](#), **Source IP:** 141.112.2.24 [\(Clear Filter\)](#)

	Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	62	2007-02-05 10:21:14	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	92	2007-02-05 10:21:04	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	86	2007-02-05 10:20:54	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	85	2007-02-05 10:20:43	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	85	2007-02-05 10:20:33	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	91	2007-02-05 10:20:23	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	92	2007-02-05 10:20:13	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	92	2007-02-05 10:20:03	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	91	2007-02-05 10:19:53	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	92	2007-02-05 10:19:43	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	86	2007-02-05 10:19:33	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	84	2007-02-05 10:19:22	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	1	2007-02-05 10:19:22	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	1	2007-02-05 10:19:22	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
	BACKDOOR black curse 4.0 runtime det...	Auto-discovered Snort at snort	1	2007-02-05 10:19:22	Backdoor Detected	141.112.2.24:47276	172.16.60.1:80	NA	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>

Step 2 Select the event with the source IP address known to be producing reconnaissance activity.

Step 3 Click  False Positive.

The False Positive window appears with information derived from the selected event.



- Step 4** Select the necessary event properties to tune as a false positive. In the case of a malware offense, select the type of event and the event high-level category, which is creating the false positive malware offense.

For additional information on using the False Positive tuning function, see the *STRM Users Guide*.

- Step 5** Click **Tune**.

STRM will no longer create additional offenses for this source IP address when performing normal VA or network management tasks.

8

NETWORK ANOMALIES OFFENSES

This chapter provides information on network anomaly offenses including:

- [What is a Network Anomaly Offense?](#)
- [How do I Investigate a Network Anomaly Offense](#)
- [How do I Tune a Network Anomaly Offense?](#)

What is a Network Anomaly Offense?

Network anomaly offenses are generated using Network Behavior Anomaly Detection (NBAD) and occur if STRM is receiving flow data (for example, NetFlow, sFlow, or J-Flow) or monitoring the network using a SPAN or TAP. There are four types of network anomaly offenses:

- [Policy](#)
- [Threshold](#)
- [Anomaly](#)
- [Behavior](#)



Note: For more information on sentries, see *Managing Sentries in the STRM Users Guide*.

Policy

Using the Network Surveillance interface, you can configure policy sentries with the auto-learn policy option enabled. This type of sentry learns what services are present in an area of the network and sends an alert when a new sentry is detected. Once the services have been learned, any new services continue to alert until the sentry generates another alert. If you wish to apply a policy sentry that adjusts to changes in traffic over time, see [Anomaly](#).

By default, STRM does not include any auto-learn policy sentries, so you must create a policy sentry with the auto-learn policy enabled if you wish to monitor this type of traffic.

Threshold

A threshold offense includes time series flow data being above, below, or outside the range (threshold) being monitored. You can create a threshold sentry to monitor activity, such as, high bandwidth on a particular link or monitoring above noise of a certain type of suspicious traffic. By default, STRM includes several

threshold sentries, however, we recommend that you edit the value of the threshold sentries to values that meet the needs of your network.

- Anomaly** An anomaly based offense includes changes in the amount of time particular services or networks are active. This includes three states:
- Detection of services, such as a mail server being installed in the Demilitarized Zone (DMZ) or FTP being installed on a server that has not previously included FTP.
 - Detecting failed services, for example, a web server that is active 100% of the time stops responding to communications.
 - Monitoring for change in the activity level of commonly used services. For example, if your network includes a corporate mail server that has SSH installed but is only used a few times a week. Then, if a user attempts to exploit the mail server and starts using the SSH service, an alert generates and an offense is created.
- Behavior** Behavior offenses includes changes in rate or volume levels at a particular time of day on a certain day of the week. For example, the level of an alert that activates at 2 am when traffic is low is very different than an alert for traffic at 3 pm when traffic volume is much higher. This makes it much harder for a malicious user to trick or train the learning system.

These offenses detects issues, such as, mail viruses that leverages the corporate SMTP in the middle of the night or a slow increase in Syn traffic. Behavior offenses also alert to abnormal decreases in traffic as well, which may represent failed backups or if a web server stops responding.

How do I Investigate a Network Anomaly Offense

To investigate a network anomaly offense:

Step 1 Click the **Offense Manager** tab.

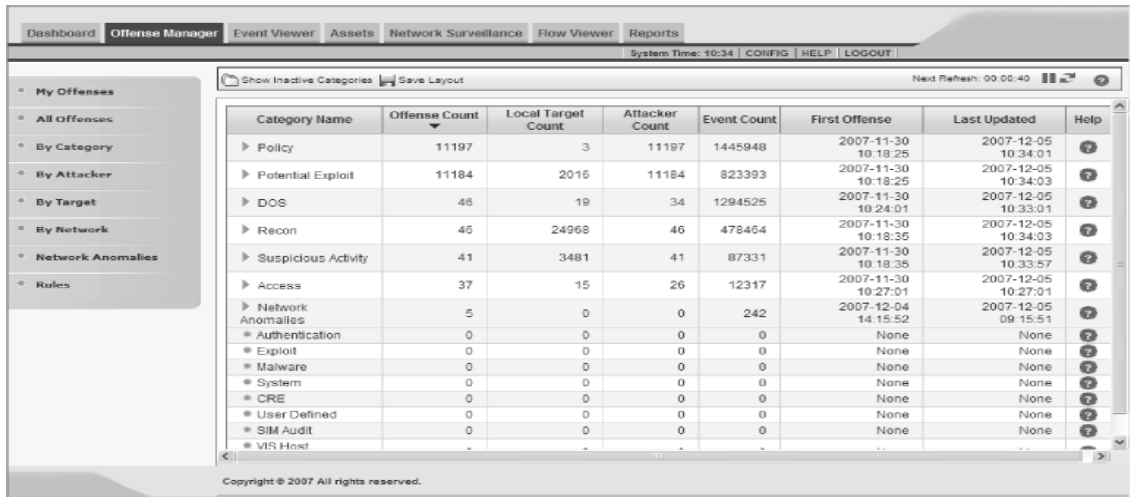
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Network Anomalies category, click the arrow icon next to Network Anomalies.

Network Anomalies	2	0	0	2	2007-02-05 10:12:24	2007-02-05 10:23:24	?
Behavior	2	0	0	2	2007-02-05 10:12:24	2007-02-05 10:23:24	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

Last Alert	Sentry Name	Network	Object	Events	Category	Weight
Mon Feb 05 10:24:24 AST 2007	Behavior	all	I2I	1	Behavior	39
Mon Feb 05 10:12:24 AST 2007	Behavior	all	Net-10-172-192	1	Behavior	26

Step 5 Double-click the offense you wish to view. The details panel appears.

Back [Event from I2I](#)

Incident: Started At: Mon Feb 5 10:25:24 2007 Show All

Event: Inbound Bytes - Mon Feb 5 10:25:24 2007 Show All

View: nets - Flows are classified by the defined n...

Object(s): all

Network Location: all

Layer: Inbound Bytes

Event Number: 1

Response Number: 1133 of Unlimited

Response: Behavioral Change

At Time Of Alert:

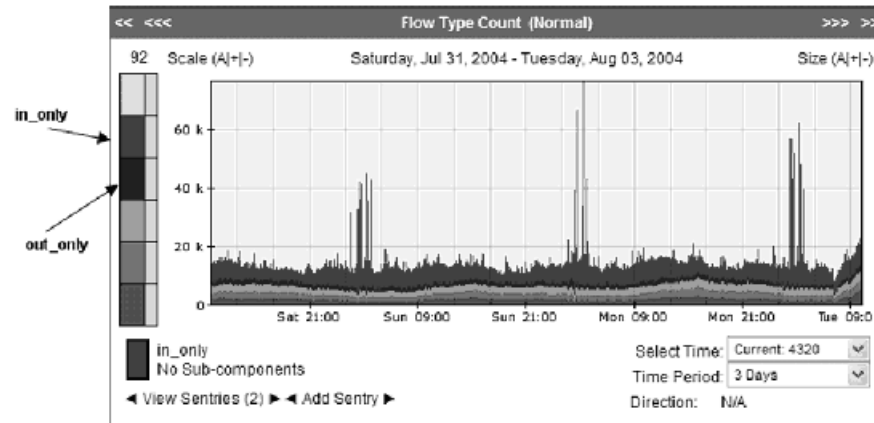
Now:

Show Flows Save Report Email

Step 6 Click the At Time of Alert graph to investigate the flows creating this offense.

Step 7 Click the graph to zoom in on the information.

Step 8 Click the legend with the corresponding color to isolate the problem.



Step 9 Click on the lower half of the graph.

Step 10 In the Pivot To Box, click **By Networks** to further investigate the network location of the issue.

Step 11 In the View Flows Box, click **Full**.

Step 12 Click the portion of the graph you wish to investigate.

Step 13 In the table, click an IP address to further investigate the traffic for the host.

How do I Tune a Network Anomaly Offense?

If you determine that the suspicious activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

If you are monitoring an area of the network and need to remove a host from the profile, you must add the host to a different network object and then remove that object before applying the sentry. This action removes that host from the profile. If the exception is complete, you may need to create an object in a view and remove that as object as well.

Also, when creating a behavioral sentry, we recommend that you select the Test Objects as Group check box.

For more information on STRM sentries, see the *STRM Administration Guide*.

9

POLICY OFFENSES

This chapter provides information on policy offenses including:

- [What is a Policy Offense?](#)
- [How do I Investigate a Policy Offense?](#)
- [How do I Tune a Policy Offense?](#)
- [How Can I Verify That STRM is Receiving Valid Offenses?](#)

What is a Policy Offense?

Policy offenses include correlated events that may constitute violations of security policy, misuse, or wasted resources. This may include Peer-to-Peer (P2P) traffic, instant messaging traffic, gaming, potential information leaks, or suspicious web browsing activity. You can configure STRM to adhere to your company policy and create offenses on traffic that you consider outside your policy.

How do I Investigate a Policy Offense?

To investigate a policy offense:

Step 1 Click the **Offense Manager** tab.

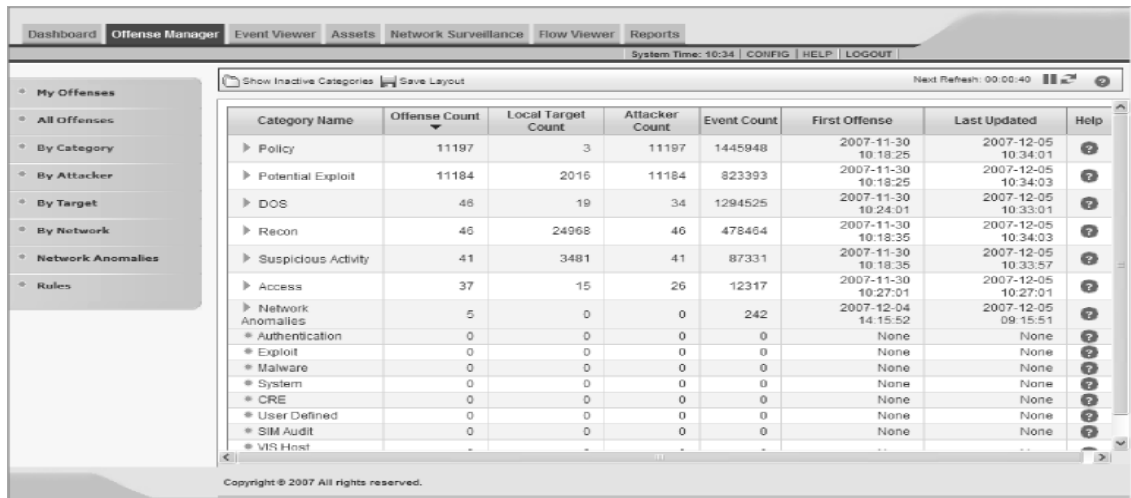
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Policy category, click the arrow icon next to Policy

▼ Policy	2202	2	2202	37035	2007-01-31 08:14:24	2007-01-31 09:00:55	?
IRC Policy Violation	2174	0	2174	3137	2007-01-31 08:14:24	2007-01-31 09:00:55	
P2P Policy Violation	27	0	27	30483	2007-01-31 08:14:24	2007-01-31 09:00:55	
Mail Policy Violation	7	0	7	3413	2007-01-31 08:14:24	2007-01-31 09:00:55	
Application Policy Violation	2	2	2	2	2007-01-31 08:18:54	2007-01-31 08:48:55	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

?	Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
	15	Potential Botnet Activity (IRC Detected) , Local TCP Scanner ...	10.105.37.125	■■■■	Remote (2575)	8	Sales	other	10869	2007-01-31 08:14:21	17m 55s
	14	Potential Botnet Activity (IRC Detected) , Default - Policy - ...	10.101.145.178	■■■■	Remote (144)	4	Detroit	other	1817	2007-01-31 08:14:19	1m 55s
	226	Local TCP Scanner Detected , Default - Policy - External - IR...	10.105.97.135	■■■■	Remote (93)	5	Sales	other	101	2007-01-31 08:17:11	34m 54s

Step 5 Double-click the offense you wish to view. The details panel appears.

All Offenses **Offense 15** (Summary)

Offense 15 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude				Relevance	6	Severity	6	Credibility	6
Description	Potential Botnet Activity (IRC Detected) preceded by Local TCP Scanner Detected preceded by Host Port Scan Detected by Local Host preceded by Possible Local Worm Detected preceded by Default - Suspicious - External - Unidirectional TCP Flows			Event count	10869 events in 8 categories				
Attacker Src	10.105.37.125			Start	2007-01-31 08:14:21				
Target(s) Dest	Remote (2575)			Duration	30m 33s				
Network(s)	other			Assigned to	Not assigned				
Notes									

Attacker Summary Details				Top 5 Categories Categories				
Magnitude			User	Unknown				
Description	10.105.37.125		MAC	Unknown				
Vulnerabilities	0		Asset Weight	0				
Location	Corporate_HQ_Sales							


Name	Magnitude	Local Target Count	Events	Last Event
Potential worm activity		0	31	01-31 08:44:25
Potential Botnet connection		0	6	01-31 08:39:55
Host Port Scan		0	200	01-31 08:44:25
Anomaly		0	378	01-31 08:44:25
TCP Reconnaissance		0	168	01-31 08:44:25

Event Name	Magnitude	Device	Category	Destination	Start Time
Potential worm activity - Event CRE		eventprocessor0 :: acadian	Potential worm activity	82.126.214.17:27759	01-31 08:15:00
Potential worm activity - Event CRE		eventprocessor0 :: acadian	Potential worm activity	24.25.167.170:32101	01-31 08:15:51
Potential worm activity - Event CRE		eventprocessor0 :: acadian	Potential worm activity	68.67.250.61:26252	01-31 08:16:47
Potential worm activity - Event CRE		eventprocessor0 :: acadian	Potential worm activity	168.243.73.4:4155	01-31 08:17:45

Step 6 View the Attacker Summary box to understand the attacker:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the **Select Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user. You can also select **Information > DNS Lookup** or **WHOIS Lookup** to further investigate the user associated with the attacker IP address.

Step 7 Once you have identified the user associated with an IP address, contact your system administrator to determine the appropriate action. You can use several methods to determine the user associated with an IP address. For example, you can use Windows active directory event logs, VPN authentication logs, or the Windows nbstat command.

Step 8 View the Top 10 Events box. This box contains the top 10 events that contributed to this offense. To view all events, click  **Events**.

- Step 9** Once you have determined the impact of the offense, you must perform the necessary steps to rectify the source of the activity. If you have determined this behavior is normal, you can tune STRM to no longer detect this activity. For more information, see [How do I Tune a Policy Offense?](#)
- Step 10** Once you are satisfied that you have resolved the offense, you can close or hide the offense.
For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a Policy Offense?



If you determine that the policy activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

You can tune STRM using one of the following methods:

- [Tuning Using False Positive Function](#)
- [Tuning Using Custom Rules Wizard](#)

Tuning Using False Positive Function

To tune policy activity using the false positive function:

- Step 1** In the offense details interface, click  **Events**.
The List of Events appears.
- Step 2** Select the event that includes the known source IP address that is reported to produce suspicious activity.
- Step 3** Click  **False Positive**.
The False Positive window appears with information derived from the selected event.



Step 4 Select the necessary event properties to tune as a false positive.

Step 5 Click **Tune**.

STRM will no longer create additional offense for this source IP address when this type of activity occurs.

Tuning Using Custom Rules Wizard

You can use the Custom Rules wizard in the Offense Manager to create a building block that includes the IP address(es) or CIDRs that you wish to exclude from creating policy offenses. This allows you to suppress policy offenses for groups of IP addresses. For more information on using the Custom Rules Wizard, see the *STRM Administration Guide*.

How Can I Verify That STRM is Receiving Valid Offenses?

By default, only P2P events cause the creation of a policy offense. You can enable other types of policy offenses to create offenses if those behaviors constitute policy violations on your network. To verify valid offense creation:

- Step 1** If an expected policy violation did not occur, verify that the appropriate rules and sentries are enabled. For more information on enabling rules and sentries, see the *STRM Administration Guide*.
- Step 2** Verify that the appropriate rules are enabled with other security devices, as appropriate.
- Step 3** Using the Event Viewer, verify that the low-level policy events were received and processed by STRM or from other security devices.

10

POTENTIAL EXPLOIT OFFENSES

This chapter provides information on potential exploit offenses including:

- [What is a Potential Exploit Offense?](#)
- [How do I Investigate a Potential Exploit Offense?](#)
- [How do I Tune a Potential Exploit Offense?](#)

What is a Potential Exploit Offense?

Potential exploit offenses may be generated from many different sources, such as, a custom rule created in STRM or from an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) product with a high false positive prone signature. If offenses are categorized as potential exploits, we recommend that you investigate the users associated with the offense to validate the authenticity of the offense.

How do I Investigate a Potential Exploit Offense?

This section provides information on further investigating a potential exploit offense.

To investigate a potential exploit offenses:

Step 1 Click the **Offense Manager** tab.

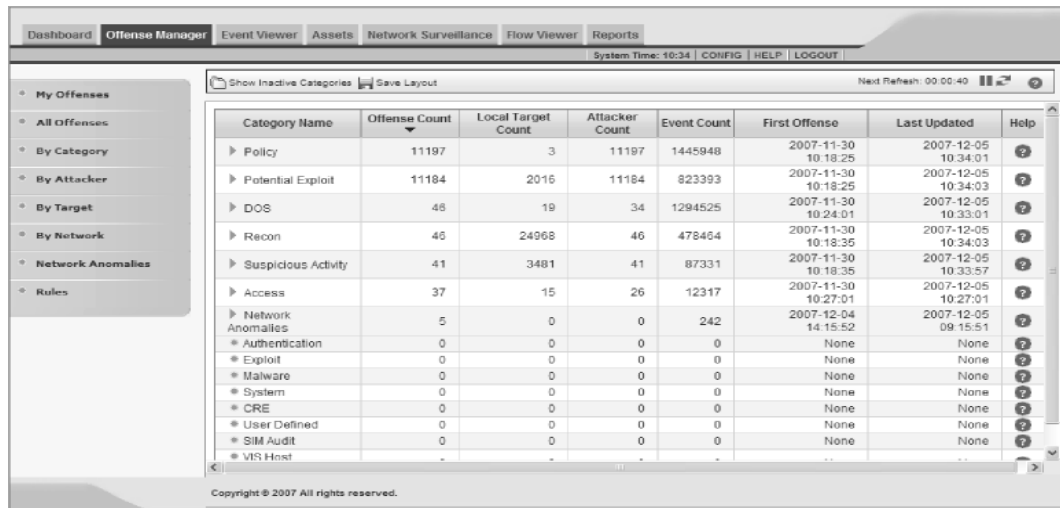
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Potential Exploit category, click the arrow icon next to Potential Exploit.

Potential Exploit	2404	29	2404	4341	2007-02-20 08:54:17	2007-02-20 09:44:33	?
Potential Botnet connection	2393	4	2393	4257	2007-02-20 08:54:17	2007-02-20 09:44:33	
Potential worm activity	13	25	13	84	2007-02-20 08:58:02	2007-02-20 09:44:33	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

?	Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
	878	Local TCP Scanner Detected , Potential Botnet Activity (IRC D...	10.105.37.125	■■■	Remote (2055)	8	Sales	other	13262	2007-02-20 09:09:04	52s
	156	Suspicious - External - Rejected Communication Attempts , Loc...	10.101.240.222	■■■	Remote (1286)	9	all	other	14535	2007-02-20 08:55:39	52s
	430	Potential Botnet Activity (IRC Detected) , Local P2P Server D...	10.105.97.135	■■■	Remote (419)	6	Sales	other	979	2007-02-20 09:00:35	1m 39s
	70	Potential Botnet Activity (IRC Detected) , Local P2P Server D...	10.101.145.178	■■■	Remote (176)	6	Detroit	other	1835	2007-02-20 08:54:43	1m 38s

Step 5 Double-click the offense you wish to view. The details panel appears.

Step 6 View the Attacker Summary box to understand the attacker:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the

remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.

- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the suspicious traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the Select **Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.

Step 7 View the Annotations box and locate any CRE Event annotation, which means that this offense is the result of a custom rule created for STRM. The annotations for an offense describes the offense details and the reasons for investigating this offense.

For example, an annotation may indicate that a system, which is not known to be a DNS server, communicates to a DNS server outside the customer networks. The annotations for this offense explains that many bots that get installed on client hosts have a built in DNS client to avoid DNS-based remediation techniques and that you should investigate this communication.

Step 8 View the Annotations box and locate any real-time flow analysis annotation, which describes the behavior of the host or other exploit attempts from the same attacker. This type of annotation occurs when the offense is generated by IDS or IPS products.

Step 9 Once you have determined the impact of the offense, you must either block the source of the scan, patch or shut down services on the appropriate systems, then take the desired action against the offense.


Step 10 Once you have resolved the offense, close or hide the offense.

For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a Potential Exploit Offense?

If you determine that the potential exploit activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

To tune potential exploit activity using the false positive function:

Step 1 In the offense details interface, click  Events.

The List of Events appears for the selected offense.

Filter/Search Clear Filter Offense False Positive Raw Events Print XML CSV Event Processor: eventprocessor0

Viewing events from 2007-02-20 09:04:04 to 2007-02-20 10:03:48 (View Real Time Events)

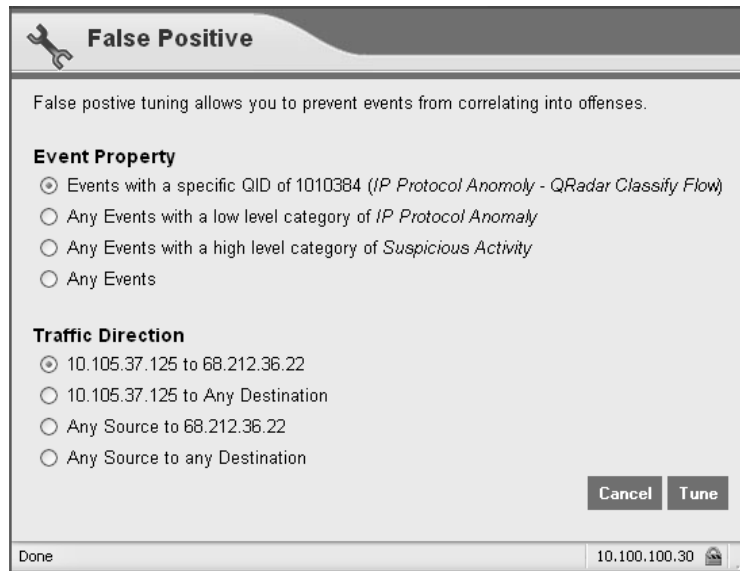
Current Filters:
Offense Name: Local TCP Scanner Detected , Potential Botnet Activity (IRC D... (Clear Filter), **Source IP:** 10.105.37.125 (Clear Filter)

	Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
	Anomaly - Event CRE	eventprocessor0 :: clio	1	2007-02-20 10:03:59	Anomaly	10.105.37.125:1305	67.162.145.74:29487	NA	
	IP Protocol Anomaly - QRadar Classif...	classify0 :: clio	1	2007-02-20 10:03:59	IP Protocol Anomaly	10.105.37.125:1305	67.162.145.74:29487	NA	
	IP Protocol Anomaly - QRadar Classif...	classify0 :: clio	1	2007-02-20 10:03:59	IP Protocol Anomaly	10.105.37.125:1348	68.212.36.22:7438	NA	
	IP Protocol Anomaly - QRadar Classif...	classify0 :: clio	1	2007-02-20 10:03:59	IP Protocol Anomaly	10.105.37.125:1339	68.237.182.36:39303	NA	
	IP Protocol Anomaly - QRadar Classif...	classify0 :: clio	1	2007-02-20 10:03:59	IP Protocol Anomaly	10.105.37.125:1324	66.136.99.39:13905	NA	
	IP Protocol Anomaly - QRadar Classif...	classify0 :: clio	1	2007-02-20 10:03:59	IP Protocol Anomaly	10.105.37.125:1360	65.43.163.8:33184	NA	
	IP Protocol Anomaly - QRadar Classif...	classify0 :: clio	1	2007-02-20 10:03:59	IP Protocol Anomaly	10.105.37.125:1347	80.127.3.237:21075	NA	
	IP Protocol Anomaly - QRadar Classif...	classify0 :: clio	1	2007-02-20 10:03:59	IP Protocol Anomaly	10.105.37.125:1374	128.252.250.9:22280	NA	

Step 2 Select the event with the source IP address known to be producing this activity.

Step 3 Click False Positive.

The False Positive window appears with information derived from the selected event.



Step 4 Select the necessary event properties to tune as a false positive.

For additional information on using the False Positive tuning function, see the *STRM Users Guide*.

Step 5 Click **Tune**.

STRM will no longer create additional offenses for this source IP address when performing normal VA or network management tasks.

11

RECONNAISSANCE OFFENSES

This chapter provides information on reconnaissance offenses including:

- [What is Reconnaissance?](#)
- [How do I Investigate a Reconnaissance Offense?](#)
- [How do I Tune a Reconnaissance Offense?](#)

What is Reconnaissance?

STRM detects reconnaissance activity, which is the first step in thwarting and blocking serious network attacks. This section provides additional information regarding reconnaissance including:

- [What is Network Reconnaissance?](#)
- [What is a Reconnaissances Offense?](#)

What is Network Reconnaissance?

Malicious users (attackers) use network reconnaissance to obtain information about your network's vulnerabilities with malicious and exploitive intentions. Network reconnaissance can provide malicious users with a significant amount of detail regarding your network including:

- Potential targets within your network.
- Target information, such as, vulnerabilities (open ports and services) and operating systems.
- Potential vulnerabilities (holes) in your security. For example, if your firewalls are configured improperly.
- Network topology.

What is a Reconnaissances Offense?

When STRM detects reconnaissance activity, a reconnaissance offense is created. STRM is able to detect many different methods that attackers use to scan and probe a network. STRM also combines network flow and event correlation for a comprehensive view of the network. By examining network traffic, STRM may detect scanning and probing activity by analyzing flow behavior. Typically, attackers attempt to remain undetected by using a lower frequency and scan intensity, perhaps only scanning a small number of hosts over a long period of time. STRM detects low, medium, and high intensity scans by monitoring a single source IP address attempting to connect to an abnormal amount of target hosts over a long period of time.

If reconnaissance activity from a specific attacker is followed by an exploit attack, STRM correlates this information to the offense to provide full details of the attacks.

How do I Investigate a Reconnaissance Offense?

This section provides information on further investigating a reconnaissance offense.

To investigate a reconnaissance offenses:

Step 1 Click the **Offense Manager** tab.

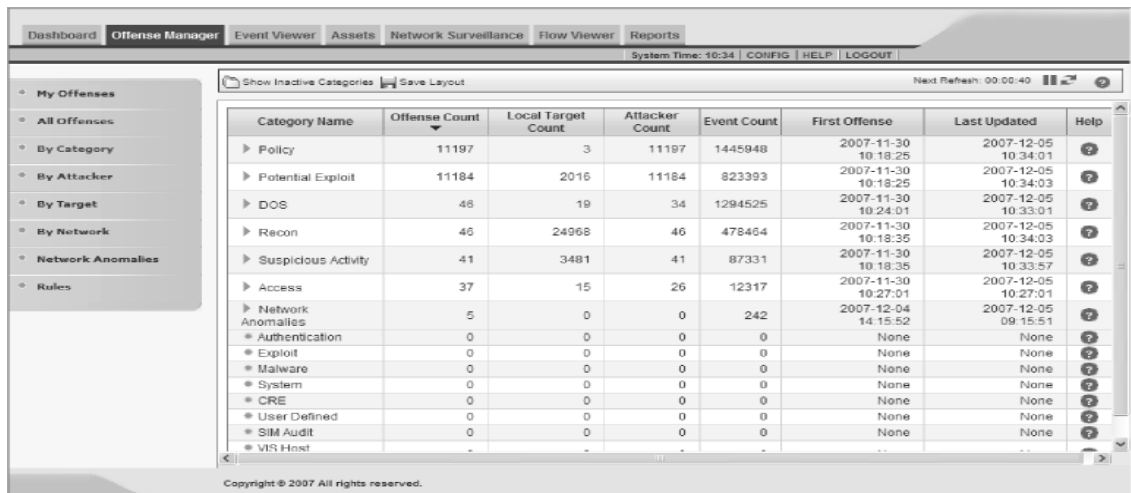
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Recon category, click the arrow icon next to Recon.

Recon	194	68930	194	99092	2007-01-24 15:54:40	2007-01-24 16:20:56	?
Network Sweep	160	68644	160	95498	2007-01-24 15:55:25	2007-01-24 16:20:56	
TCP Reconnaissance	158	893	158	1074	2007-01-24 15:54:40	2007-01-24 16:20:56	
Windows Reconnaissance	14	105	14	105	2007-01-24 15:56:10	2007-01-24 16:20:56	
Database Reconnaissance	9	1545	9	1549	2007-01-24 15:54:40	2007-01-24 16:20:56	
Host Port Scan	8	29	8	242	2007-01-24 15:54:40	2007-01-24 16:20:56	
UDP Reconnaissance	7	12	7	100	2007-01-24 15:56:10	2007-01-24 16:20:11	
Misc Recon Event	4	0	4	72	2007-01-24 15:55:25	2007-01-24 16:20:56	
ICMP Reconnaissance	3	0	3	431	2007-01-24 15:57:41	2007-01-24 16:20:56	
FTP Reconnaissance	2	17	2	17	2007-01-24 15:54:40	2007-01-24 16:10:26	
Mail Reconnaissance	1	0	1	4	2007-01-24 15:54:41	2007-01-24 15:56:11	

Step 4 Double-click any low-level category to view the list of associated offenses.

The list of offenses appear.

?	Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
	94	Local P2P Scanner , Default - Recon - External - Potential Ne...	10.101.171.92		Remote (1067)	9	Liverpool	other	3428	2007-01-24 15:55:02	1m 53s
	12	Default - Recon - External - Potential Network Scan , Default...	10.101.133.167		Remote (2917)	7	Hong_Kong	other	10950	2007-01-24 15:54:07	1m 8s
	161	Aggressive Remote Scanner Detected , Default - Recon - Extern...	206.53.239.113		Local (680)	4	other	Training	838	2007-01-24 15:56:01	25m 46s

Step 5 Double-click the offense you wish to view.

The details panel appears.

Step 6 View the Attacker Summary box to understand the attacker:

Attacker Summary	
Magnitude	User Unknown
Description	10.106.1.229
Vulnerabilities	0 Asset Weight 0
Location	Corporate_HQ.Accounting.Audit

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the suspicious traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the Select **Information** > **Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.

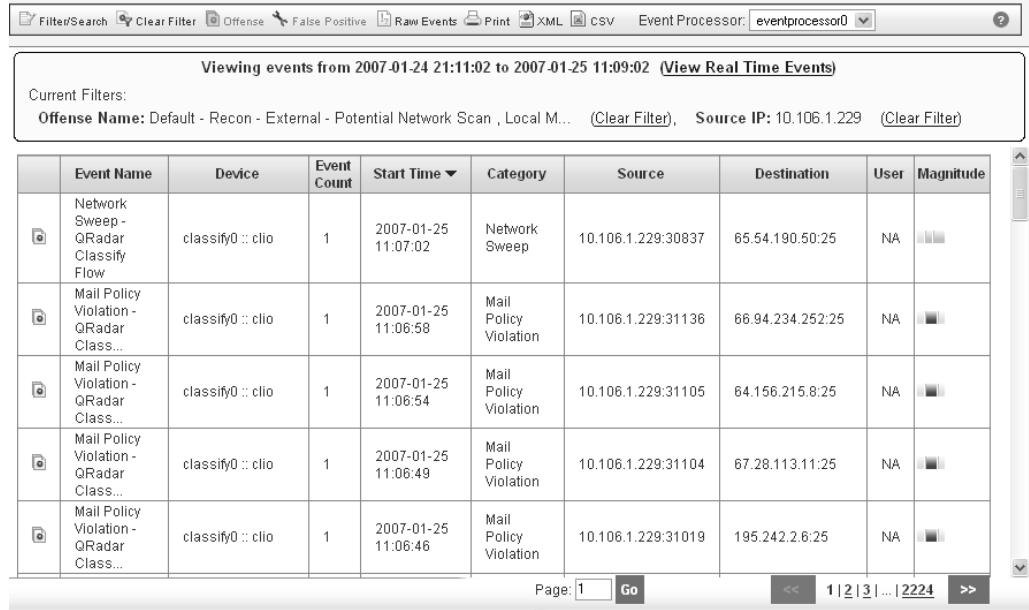
If the activity is normal (for example, scanning originating from a known vulnerability scanner or network management system that may be probing the network with SNMP traffic) then you can use the Rules function in the Offense Manager to tune out this activity. For more information, see [How do I Tune a Reconnaissance Offense?](#)











Step 7 In the Attacker Summary box, place your mouse over the Magnitude bar. If the VA Risk value is greater than 0, we recommend that you investigate the target to

determine if the target responded to the scan. A scan is worth investigating if it receives a reply. This may indicate the initial behavior of a worm or an employee operating an unauthorized VA scanner.

Step 8 Click  Events.

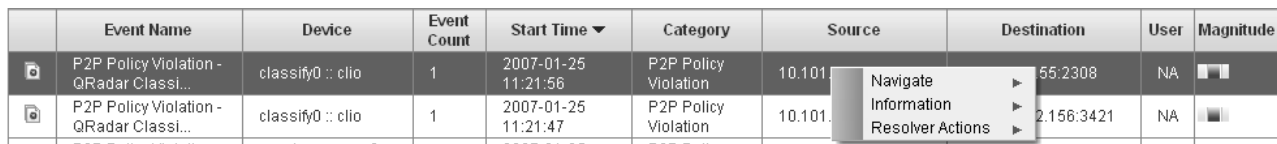
The List of Events appears for the selected offense.







	Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
	Network Sweep - QRadar Classify Flow	classify0 :: clio	1	2007-01-25 11:07:02	Network Sweep	10.106.1.229:30837	65.54.190.50:25	NA	
	Mail Policy Violation - QRadar Class...	classify0 :: clio	1	2007-01-25 11:06:58	Mail Policy Violation	10.106.1.229:31136	66.94.234.252:25	NA	
	Mail Policy Violation - QRadar Class...	classify0 :: clio	1	2007-01-25 11:06:54	Mail Policy Violation	10.106.1.229:31105	64.156.215.8:25	NA	
	Mail Policy Violation - QRadar Class...	classify0 :: clio	1	2007-01-25 11:06:49	Mail Policy Violation	10.106.1.229:31104	67.28.113.11:25	NA	
	Mail Policy Violation - QRadar Class...	classify0 :: clio	1	2007-01-25 11:06:46	Mail Policy Violation	10.106.1.229:31019	195.242.2.6:25	NA	

The Device column provides the device that detected the event. If multiple devices are reporting similar events, the credibility value for this offense increases.

Step 9 To further investigate the target, right-click on an IP address in the Source column. The right-click menu appears.



	Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
	P2P Policy Violation - QRadar Classi...	classify0 :: clio	1	2007-01-25 11:21:56	P2P Policy Violation	10.101.1.1	65.2308	NA	
	P2P Policy Violation - QRadar Classi...	classify0 :: clio	1	2007-01-25 11:21:47	P2P Policy Violation	10.101.1.1	2.156:3421	NA	

Step 10 Select Information > Asset Profile.

The Asset Profile appears.

Asset Profile Ports History

Name	<input type="text"/>		
Description	<input style="height: 30px;" type="text"/>		
IP Address	10.101.167.102	VA Risk Level	1
Operating System		How Threatening	8
Host Name (DNS Name)	10.101.167.102	How Threatened	0
Asset Weight	0 - Not Important <input type="button" value="v"/>		
MAC	<input type="text"/>	Host Name	<input type="text"/>
Machine Name	<input type="text"/>		
User	<input type="text"/>	User Group	<input type="text"/>
Extra Data	<input type="text"/>		

Port	OSVDB ID	Name	Description	Risk / Severity	Last Seen	First Seen
3531				1	2007-01-24 22:00:00 (Passive)	2007-01-24 22:00:00 (Passive)

Step 11 Once you have determined the impact of the offense, you must either block the source of the scan, patch or shut down services on the appropriate systems, then take the desired action against the offense.

Step 12 Once you have resolved the offense, close or hide the offense.
 For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a Reconnaissance Offense?


If you determine that the reconnaissance activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

You can tune STRM using one of the following methods:

- [Tuning Using False Positive Function](#)
- [Tuning Using Custom Rules Wizard](#)

Tuning Using False Positive Function

To tune reconnaissance activity using the false positive function:

Step 1 In the reconnaissance offense details interface, click  Events.
 The List of Events appears for the selected offense.

Filter/Search Clear Filter Offense False Positive Raw Events Print XML CSV Event Processor: eventprocessor0

Viewing events from 2007-01-24 21:11:02 to 2007-01-25 11:09:02 (View Real Time Events)

Current Filters:
Offense Name: Default - Recon - External - Potential Network Scan , Local M... (Clear Filter) **Source IP:** 10.106.1.229 (Clear Filter)

	Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
	Network Sweep - QRadar Classify Flow	classify0 :: clio	1	2007-01-25 11:07:02	Network Sweep	10.106.1.229:30837	65.54.190.50:25	NA	■■■
	Mail Policy Violation - QRadar Class...	classify0 :: clio	1	2007-01-25 11:06:58	Mail Policy Violation	10.106.1.229:31136	66.94.234.252:25	NA	■■■
	Mail Policy Violation - QRadar Class...	classify0 :: clio	1	2007-01-25 11:06:54	Mail Policy Violation	10.106.1.229:31105	64.156.215.8:25	NA	■■■
	Mail Policy Violation - QRadar Class...	classify0 :: clio	1	2007-01-25 11:06:49	Mail Policy Violation	10.106.1.229:31104	67.28.113.11:25	NA	■■■
	Mail Policy Violation - QRadar Class...	classify0 :: clio	1	2007-01-25 11:06:46	Mail Policy Violation	10.106.1.229:31019	195.242.2.6:25	NA	■■■

Page: 1 Go << 1 | 2 | 3 | ... | 2224 >>

Step 2 Select the event with the source IP address known to be producing reconnaissance activity.

Step 3 Click False Positive.

The False Positive window appears with information derived from the selected event.

False Positive

False positive tuning allows you to prevent events from correlating into offenses.

Event Property

- Events with a specific QID of 1202486 (User Login)
- Any Events with a low level category of QRadar User Authentication
- Any Events with a high level category of QRadar Audit
- Any Events

Traffic Direction

- 10.100.100.106 to 127.0.0.1
- 10.100.100.106 to Any Destination
- Any Source to 127.0.0.1
- Any Source to any Destination

Step 4 Select the necessary event properties to tune as a false positive.

For example, in the window above, the Events with specific QID option is selected to tune the specific IP address and the event high-level category that is creating the false positive reconnaissance event.

For additional information on using the False Positive tuning function, see the *STRM Users Guide*.

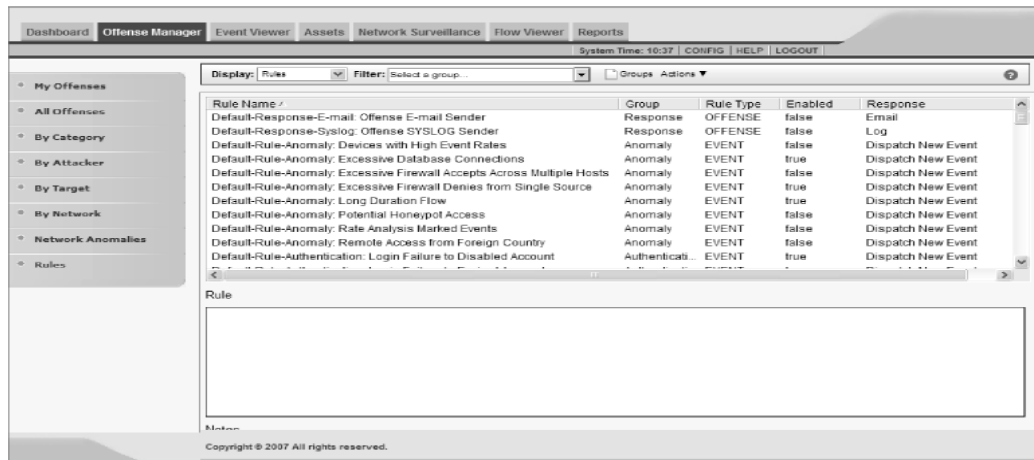
Step 5 Click Tune.

STRM will no longer create additional offenses for this source IP address when performing normal VA or network management tasks.

Tuning Using Custom Rules Wizard

To tune reconnaissance activity using the custom rules wizard:

- Step 1** In the navigation bar of the Offense Manager, click **Rules**.
The Rules interface appears.

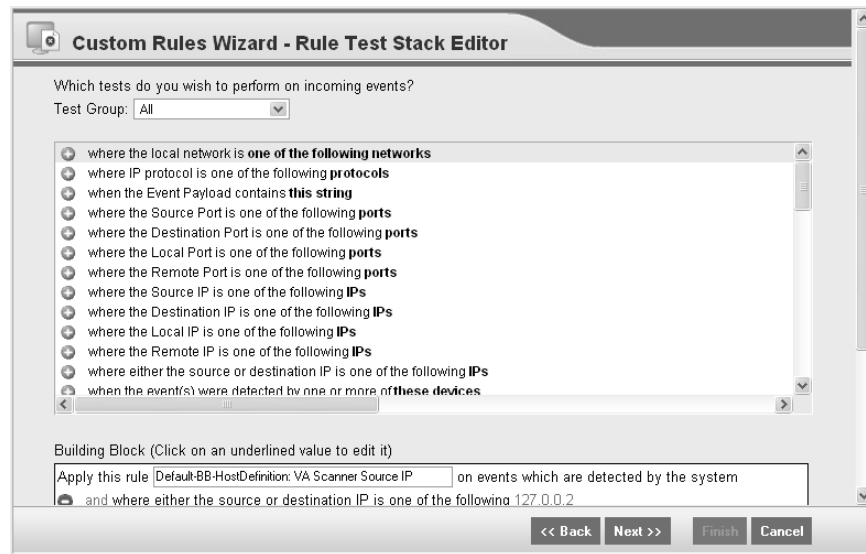


- Step 2** Using the Display drop-down list box, select Building Blocks.

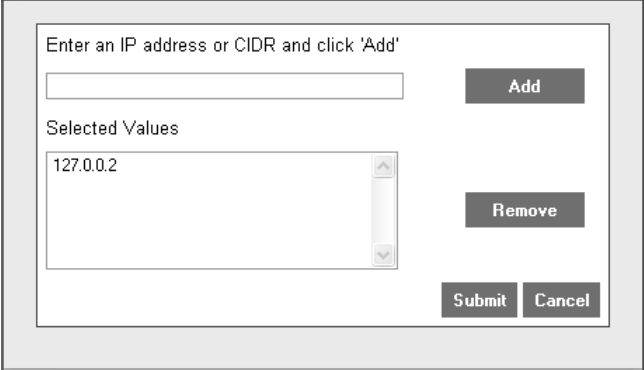
- Step 3** In the Block Name list, locate the **Default-BB-HostDefinition: VA Scanner Source IP** building block.

- Step 4** Click **Edit**.

The Rules Wizard appears.



Step 5 In the Building Block section, click the IP address that appears. A configuration window appears.



The screenshot shows a configuration window with a light gray border. At the top, it says "Enter an IP address or CIDR and click 'Add'". Below this is a text input field. To the right of the input field is a dark gray button labeled "Add". Below the input field is a section titled "Selected Values" containing a list box with the IP address "127.0.0.2" and a vertical scrollbar. To the right of the list box is a dark gray button labeled "Remove". At the bottom right of the window are two dark gray buttons labeled "Submit" and "Cancel".

Step 6 In the **Enter an IP address or CIDR and click 'Add'** field, enter the IP address of the VA scanner or IP address that is producing false positives.

Step 7 Click **Add**.

Step 8 Repeat for all VA scanners or IP address(es).

Step 9 Click **Submit**.

Step 10 Complete the rules wizard.

For more information on using the Custom Rules Wizard, see the *STRM Administration Guide*.

12

SUSPICIOUS ACTIVITY OFFENSES

This chapter provides information on a suspicious attack including:

- [What is a Suspicious Attack?](#)
- [How do I Investigate Suspicious Offense](#)
- [How do I Tune a Suspicious Offenses?](#)

What is a Suspicious Attack?

This section provides information on a suspicious attack including:

- [What is Suspicious Traffic?](#)
- [What is a Suspicious Offense?](#)

What is Suspicious Traffic?

STRM detects suspicious activity, which is security events, patterns of security events, or network flows that have been classified as suspicious and may represent a potential threat to the network. A potential threat is traffic that may include a virus, potential vulnerability, or potential unauthorized access. Many devices, such as IDSs, report events when suspicious packets are detected. For example, STRM should not detect data on a SYN packet. STRM also monitors for patterns of events that may be considered suspicious, such as multiple log in failures by the same source IP address followed by a successful log in. When STRM detects these types of events, a suspicious offense is created.

What is a Suspicious Offense?

STRM performs several tests on suspicious events and network flows prior to creating a suspicious offense to rule out false positives. Suspicious events and flows are correlated into an offense based on the results of the STRM correlation rules.

For example, STRM considers the following questions when analyzing suspicious traffic and events:

- [What is the event rate?](#)
- [Who is the attacker \(source IP address\)?](#)
- [Who are the targets \(destination IP addresses\)?](#)
- [Are the targets vulnerable?](#)
- [Are there any patterns in the events or flows that can be suspicious?](#)

What is the event rate?

STRM profiles the event rate for a device to determine the normal and abnormal rate for a device. If STRM detects a sudden increase in event rate from a device, or related to a specific source IP address, an offense is created.

Who is the attacker (source IP address)?

STRM profiles attackers and maintains a historical record of all detected attackers. For each attacker, the following information is recorded:

- Types of offenses in which these attackers were involved
- Targets attacked
- Potential of threat for this source IP address.

If the source IP address of the suspicious activity is known as a threat, STRM creates an offense.

Who are the targets (destination IP addresses)?

You can associate weights (value) to hosts, such as mission critical business servers. This weight allows you to tune STRM to create an offense when any type of threatening or suspicious traffic is directed at a critical business asset with high asset weighting.

Are the targets vulnerable?

If STRM receives suspicious events, the asset profile database correlates vulnerability assessment data and passive host profile data to correlate if the target has a vulnerability to the suspicious activity.

Are there any patterns in the events or flows that can be suspicious?

STRM's correlation rules searches for patterns of behavior that may be a potential threat, such as multiple log in failures followed by a successful log in.

How do I Investigate Suspicious Offense

To investigate a suspicious offense:

Step 1 Click the **Offense Manager** tab.

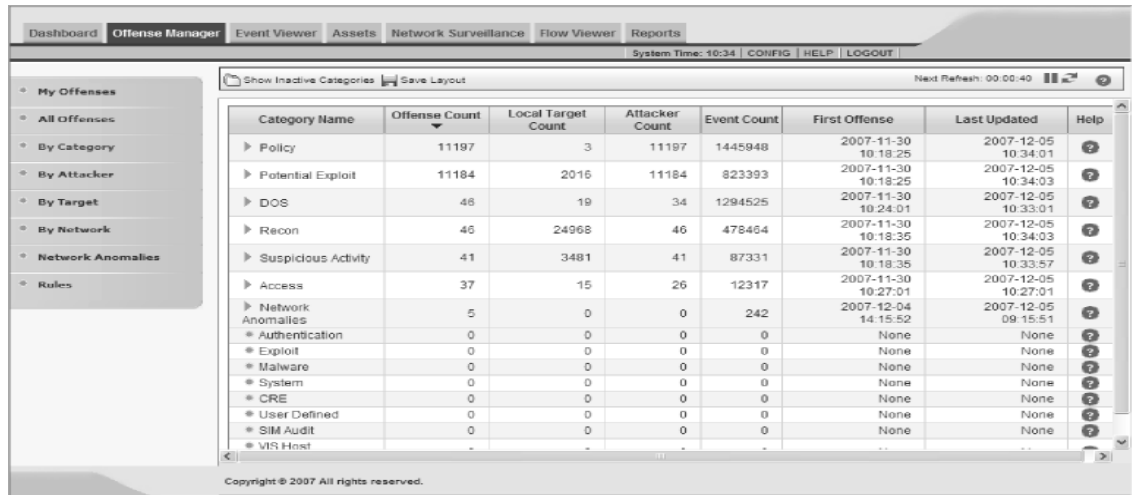
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the Suspicious Activity category, click the arrow icon next to Suspicious Activity.

Suspicious Activity	352	35300	352	90149	2007-01-30 10:09:53	2007-01-30 12:27:47	?
IP Protocol Anomaly	343	35258	343	79822	2007-01-30 11:09:45	2007-01-30 12:27:47	
Suspicious Packet	23	45	23	10325	2007-01-30 11:09:45	2007-01-30 12:27:47	
Suspicious Pattern Detected	2	1	2	2	2007-01-30 10:09:53	2007-01-30 11:09:00	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
25	Default - Policy - External - IRC Connections , Potential Bot...	10.105.37.125		Remote (3250)	8	Sales	other	18361	2007-01-30 11:09:41	1m 41s
871	Host Port Scan Detected by Local Host , Local Game Server Sca...	10.101.171.145		Remote (835)	6	Liverpool	other	1085	2007-01-30 11:23:10	1h 5m 16s
86	Host Port Scan Detected by Local Host , Default - DoS - Exter...	10.101.145.124		Remote (546)	5	Detroit	other	4281	2007-01-30 11:10:02	2m 11s

Step 5 Double-click the offense you wish to view. The details panel appears.

All Offenses **Offense 25 (Summary)**

Offense 25 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude		Relevance	6	Severity	6	Credibility	2
Description	Default - Policy - External - IRC Connections preceded by Potential Botnet Activity (IRC Detected) preceded by Local TCP Scanner Detected preceded by Host Port Scan Detected by Local Host preceded by Possible Local Worm Detected preceded by Default - Suspicious - External - Rejected Communication Attempts		Event count	19385 events in 8 categories			
Attacker Src	10.105.37.125	Start	2007-01-30 11:09:41				
Target(s) Dest	Remote (3281)	Duration	1h 21m 50s				
Network(s)	other	Assigned to	Not assigned				
Notes							

Attacker Summary Details				Top 5 Categories Categories				
Magnitude		User	Unknown					
Description	10.105.37.125		MAC	Unknown				
Vulnerabilities	0	Asset Weight	0					
Location	Corporate_HQ_Sales							

Name	Magnitude	Local Target Count	Events	Last Event
Potential worm activity		0	53	01-30 12:31:32
Potential Botnet connection		0	15	01-30 12:27:02
Host Port Scan		0	355	01-30 12:31:32
Anomaly		0	689	01-30 12:31:32
TCP Reconnaissance		0	298	01-30 12:31:32

Event Name	Magnitude	Device	Category	Destination	Start Time
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	68.191.6.2:35061	01-30 11:10:34
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	65.31.193.239:10765	01-30 11:11:28
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	68.162.130.21:26066	01-30 11:12:27
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	192.168.0.81:31420	01-30 11:13:26
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	172.189.218.128:10441	01-30 11:14:20
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	200.77.160.243:7713	01-30 11:15:15
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	69.14.172.28:39653	01-30 11:15:56
Potential worm activity - Event CRE		eventprocessor0 :: clio	Potential worm activity	168.243.73.4:4155	01-30 11:16:46


Step 6 View the Description field and determine the suspicious activity associated with this offense. This may include multiple types of activity.

Step 7 View the Attacker Summary box to understand the attacker:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network object (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the suspicious traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the **Select Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.

Step 8 View the Top 10 Events box to view the most severe events correlated to this offense. This box provides a view of the type of events that are being correlated to the offense, the devices from which event are being received, and the detailed event names.


Step 9 If this offense includes local targets, the Top 5 Local Targets box appears. This box displays the top 5 destination IP addresses associated with this offense. Targets are rated based on their overall magnitude, which takes into consideration the severity of the overall offense, if the target is vulnerable, or if the asset has been assigned a high weight value (indicating that this is a critical business asset). This box allows you to determine the overall impact of this offense on your network since you are able to determine if the host is being targeted.

Step 10 If you determine that the observed activity is not normal, click  **Flows** to further investigate the events and network flows correlated to the offense to further understand all suspicious activity.

The Flow Search window appears to view the network flows for this offense. This provides you with a detailed view of the communications for the attacker on your network and allow you to visually identify unacceptable behavior.

Step 11 From the Format box, select **Flow > Unioned flows**.

A comprehensive view of the flow data appears. If the Flow Collector is deployed, you can use the actual content from the flows for forensic investigation.

Step 12 In the Offense Summary details panel, view the Top 10 Events box. This box provides detailed information on the most severe events correlated to this offense such as the reporting device, destination IP address, severity, and when STRM first received the event. If you wish to view additional events, click  **Events** to view all events.

Step 13 Once you have determined the impact of the offense, you must perform the necessary steps to rectify the source of the suspicious traffic. If you have determined this behavior is normal, you can tune STRM to no longer detect this activity. For more information, see [How do I Tune a Suspicious Offenses?](#)


Step 14 Once you are satisfied that you have resolved the offense, you can close or hide the offense.

For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a Suspicious Offenses?

If you determine that the suspicious activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

To tune suspicious offenses using the false positive function:

Step 1 In the offense details interface, click  **Categories**.

The category details appear.

All Offenses Offense 871 (All Categories)

Offense 871 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude			Relevance	6	Severity	6	Credibility	2
Description	Host Port Scan Detected by Local Host preceded by Local Game Server Scanner Detected preceded by Default - Suspicious - External - Unidirectional UDP or Misc Flows preceded by Possible Local Worm Detected preceded by Local UDP Scanner Detected containing IP Protocol Anomaly - QRadar Classify Flow	Event count	3248 events in 6 categories					
Attacker Src	10.101.171.145	Start	2007-01-30 11:23:10					
Target(s) Dest	Remote (1428)	Duration	1h 44m 46s					
Network(s)	other	Assigned to	Not assigned					
Notes								

List of Event Categories Events

Name	Magnitude	Local Target Count	Events	Last Event
Misc Recon Event		0	34	01-30 13:09:03
UDP Reconnaissance		0	18	01-30 13:09:03
Host Port Scan		0	21	01-30 13:09:03
Potential worm activity		0	9	01-30 13:09:03
Anomaly		0	89	01-30 13:09:03
IP Protocol Anomaly		0	3077	01-30 13:09:03

Step 2 In the List of Event Categories, double-click the related category to display associated events.

Step 3 Select the event that includes the known source IP address that is reported to produce suspicious activity.

Step 4 Click  **False Positive**.

The False Positive window appears with information derived from the selected event.

 **False Positive**

False positive tuning allows you to prevent events from correlating into offenses.

Event Property

- Events with a specific QID of 1010089 (*Misc Recon Event - Event CRE*)
- Any Events with a low level category of *Misc Recon Event*
- Any Events with a high level category of *Recon*
- Any Events

Traffic Direction

- 10.101.171.145 to 81.223.12.174
- 10.101.171.145 to Any Destination
- Any Source to 81.223.12.174
- Any Source to any Destination

Done 10.100.100.30 

Step 5 Select the necessary event properties to tune as a false positive.

For example, in the window above, the source IP address and the event high-level category that is creating the false positive suspicious offense. For additional information on using the False Positive tuning function, see the *STRM Users Guide*.

Step 6 Click **Tune**.

STRM will no longer create additional offense for this source IP address when this type of activity occurs.

13

SYSTEM OFFENSES

This chapter provides information on system offenses including:

- [What is a System Offense?](#)
- [How do I Investigate a System Offense?](#)
- [How do I Tune a System Offense?](#)

What is a System Offense?

An important component of a network security solution is monitoring the health status of the hosts and connected devices. The possibility of a critical network device or vital component of your network malfunctioning is a serious threat to your network's security. STRM monitors system logs from security devices, network devices, and host computers.

STRM generates a system offense when a host or device on your network reaches a critical system state. By analyzing system logs from all supported devices, STRM can accurately determine when a system has reached a critical state, potentially leaving the network vulnerable or inoperable.

How do I Investigate a System Offense?

To investigate a system offense:

Step 1 Click the **Offense Manager** tab.

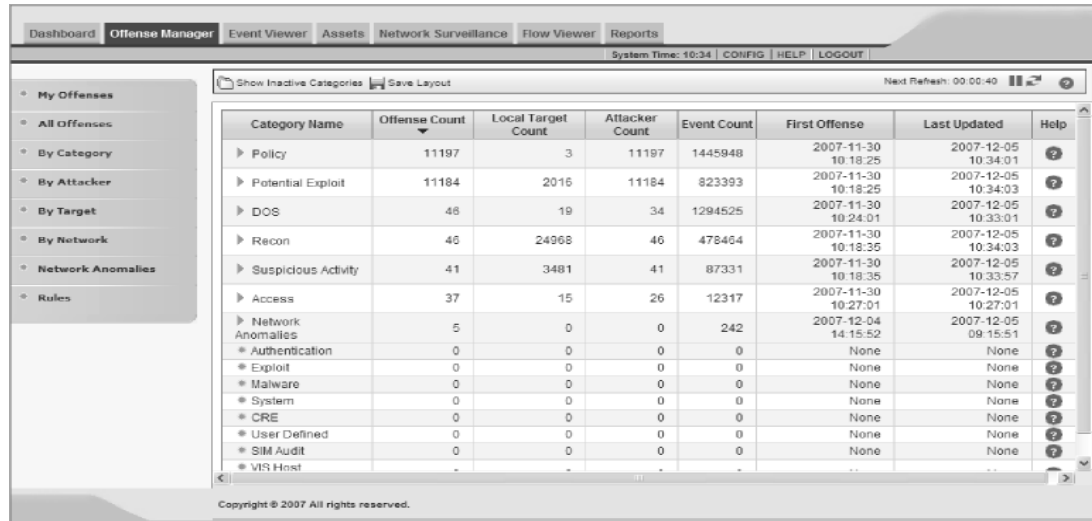
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the System category, click the arrow icon next to System.

System	5	9	5	17	2007-02-01 16:40:08	2007-02-05 10:54:20	?
Misc System Event	4	6	4	11	2007-02-01 16:40:08	2007-02-05 10:54:20	
System Status	1	3	1	6	2007-02-02 14:46:13	2007-02-02 14:46:13	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	S
6	SHELLCODE x86 setgid 0 , ICMP Destination Unreachable Communi...	172.16.150.151		Local (4)	2	Net_172_16_0_0	Multiple (2)	251414	2 1
54	SHELLCODE x86 setgid 0 , Web Protocol Anomaly , BLEEDING-EDG...	10.100.100.123		Local (3)	4	Net_10_0_0_0	Net_172_16_0_0	12	2 0
59	SHELLCODE x86 setuid 0 , SHELLCODE x86 setgid 0 , BLEEDING-ED...	172.16.50.100		Local (5)	2	Net_172_16_0_0	Net_172_16_0_0	7	2 0
24	SHELLCODE x86 NOOP , Web Exploit , Misc Policy Violation , SH...	172.16.20.100		172.16.50.100	4	Net_172_16_0_0	Net_172_16_0_0	50	2 1

Step 5 Double-click the offense you wish to view. The details panel appears.

All Offenses 2 Offense 6 (Summary)

Offense 6 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude				Relevance	5	Severity	3	Credibility	2
Description	SHELLCODE x86 setgid 0 preceded by ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited preceded by ICMP Destination Unreachable Port Unreachable			Event count	251603 events in 2 categories				
Attacker/Src	172.16.150.151			Start	2007-02-01 16:07:06				
Target(s)/Dest	Local (4)			Duration	3d 18h 55m 24s				
Network(s)	Multiple (2)			Assigned to	Not assigned				
Notes									

Attacker Summary Details				Top 5 Categories Categories			
Magnitude			User	Unknown			
Description	172.16.150.151		MAC	Unknown			
Vulnerabilities	0		Asset Weight	0			
Location	Net-10-172-192.Net_172_16_0_0						

Name	Magnitude	Local Target Count	Events	Last Event
ICMP Reconnaissance		3507	251601	02-05 11:02:36
Misc System Event		1	2	02-05 10:34:05

IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
172.16.60.96		Unknown	Yes	Unknown	Unknown	Net_172_16_0_0	0
172.16.10.98		Unknown	Yes	Unknown	Unknown	Net_172_16_0_0	0
172.16.10.19		Unknown	No	Unknown	Unknown	Net_172_16_0_0	0

Step 6 View the Attacker Summary box to understand the attacker:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the **Select Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user.

When a system event occurs, the source and destination IP addresses may indicate the same host. This host may have suffered a system error. For example, a memory issue, configuration errors, or hardware issues.


Step 7 Once you determine the nature of the error, you must determine the root cause, for example, user error, hardware failure, or an unexpected spike in traffic.

- Step 8** Once you determine the root cause of the error, notify the proper administrators to rectify the situation. If you have determined this behavior is normal, you can tune STRM to no longer detect this activity. For more information, see [How do I Tune a System Offense?](#)
- Step 9** Once you are satisfied that you have resolved the offense, you can close or hide the offense.
- For more information on closing or hiding an offense, see the *STRM Users Guide*.

How do I Tune a System Offense?

If you determine that the system activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

To tune system activity using the false positive function:

- Step 1** In the offense details interface, click  **Events**.
The List of Events window appears.




The maximum time range allowed for an event search is 24h. Only returning the first 24h of your query.

Viewing events from 2007-02-01 16:02:06 to 2007-02-02 16:02:06 ([View Real Time Events](#))

Current Filters:
Offense Name: SHELLCODE x86 setgid 0 , ICMP Destination Unreachable Communi... (Clear Filter), Source IP: 172.16.150.151 (Clear Filter)

	Event Name	Device	Event Count	Start Time	Category	Source	Destination	User	Magnitude
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	8	2007-02-02 16:02:49	ICMP Reconnaissance	172.16.150.151:0	172.16.10.98:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	7	2007-02-02 16:02:39	ICMP Reconnaissance	172.16.150.151:0	172.16.10.98:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	9	2007-02-02 16:02:35	ICMP Reconnaissance	172.16.150.151:0	172.16.10.19:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	7	2007-02-02 16:02:29	ICMP Reconnaissance	172.16.150.151:0	172.16.10.98:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	13	2007-02-02 16:02:19	ICMP Reconnaissance	172.16.150.151:0	172.16.10.19:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	7	2007-02-02 16:02:18	ICMP Reconnaissance	172.16.150.151:0	172.16.10.98:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	8	2007-02-02 16:02:08	ICMP Reconnaissance	172.16.150.151:0	172.16.10.19:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	8	2007-02-02 16:02:07	ICMP Reconnaissance	172.16.150.151:0	172.16.10.98:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	8	2007-02-02 16:01:56	ICMP Reconnaissance	172.16.150.151:0	172.16.10.98:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	8	2007-02-02 16:01:55	ICMP Reconnaissance	172.16.150.151:0	172.16.10.98:0	NA	
	ICMP Destination Unreachable Port Un...	Auto-discovered Snort at 172.16.80.96	8	2007-02-02 16:01:54	ICMP Reconnaissance	172.16.150.151:0	172.16.10.98:0	NA	

Page: 1 | Go | 1 | 2 | 3 | ... | 282 | >>

- Step 2** Select the event that includes the known source IP address that is reported to produce system activity.
- Step 3** Click  **False Positive**.
The False Positive window appears with information derived from the selected event.
- Step 4** Select the necessary event properties to tune as a false positive.
- Step 5** Click **Tune**.

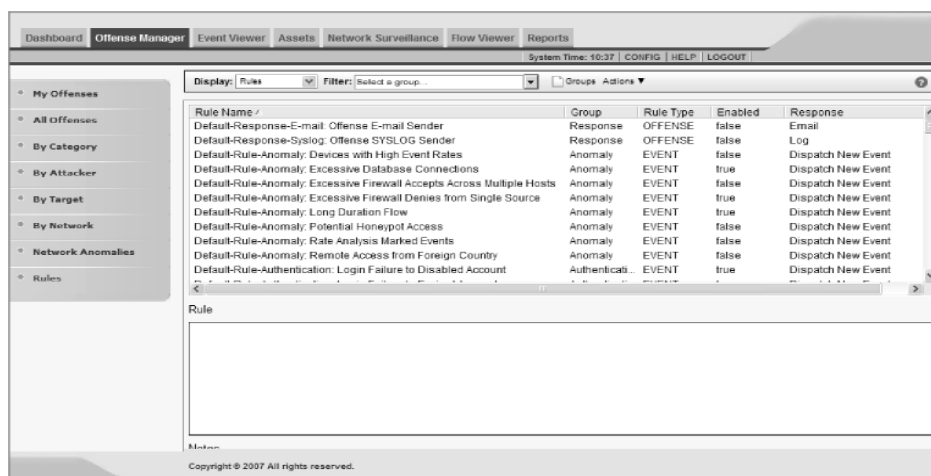
STRM will no longer create additional offense for this source IP address when this type of activity occurs.

How Can I Verify That STRM is Receiving Valid Offenses?

By default, STRM generates system offenses as a result of multiple system errors occurring within a specified time frame on the same host. If STRM detects system errors occurring on your network that are not creating offenses, this is likely related to the number of errors that have occurred or the time frame in which the errors have occurred. To tune these values using the Custom Rules Wizard:

Step 1 In the navigation bar of the Offense Manager, click **Rules**.

The Rules interface appears.



Step 2 Using the Display drop-down list box, select **All Deployed Rules**.

Step 3 Locate the **Default-Rule-System: Multiple System Errors** rule.

Step 4 Click **Edit**.

The Rules Wizard appears.

Which tests do you wish to perform on incoming events?
 Test Group: All Export as Building Block

- where the local network is **one of the following networks**
- where IP protocol is one of the following **protocols**
- when the Event Payload contains **this string**
- where the Source Port is one of the following **ports**
- where the Destination Port is one of the following **ports**
- where the Local Port is one of the following **ports**
- where the Remote Port is one of the following **ports**
- where the Source IP is one of the following **IPs**
- where the Destination IP is one of the following **IPs**
- where the Local IP is one of the following **IPs**
- where the Remote IP is one of the following **IPs**
- where either the source or destination IP is one of the following **IPs**
- when the event(s) were detected by one or more of **these devices**

Rule (Click on an underlined value to edit it)

Apply this rule Default-Rule-System: Multiple System Errors on events which are detected by the system
 and when we see any of these Default-BB-CategoryDefinition: System Errors and Failures with the same source IP more than 10 times, across more than 0 destination IP(s) within 3 minutes

Notes (Enter your notes about this rule)

Reports when as source has 10 system errors within 3 minutes.

- Step 5** In the Rule box, click the number that appears in the **more than 10 times** statement.
- Step 6** In the Enter a rule count field, enter the number that meets the needs of your network.
- Step 7** In the Rule box, click the number that appears in the **within 3 minutes** statement.
- Step 8** Edit the time frame, as necessary
- Step 9** Complete the rules wizard.

14

USER DEFINED OFFENSES

This chapter provides information on user defined offenses including:

- [What is a User Defined Offense?](#)
- [How do I Investigate a User Defined Offense?](#)
- [How do I Tune a User Defined Offense?](#)

What is a User Defined Offense?

You can use many different tools, techniques, and strategies to protect your network. The variety of techniques implemented by the numerous security devices available makes defining network attacks and offenses an increasingly complex task. STRM allows you to map events that do not belong to traditional event categories as user defined offenses.

STRM generates a user defined offense when many user defined events are detected by the system. You can define your own custom algorithm's into the system and map the resulting offenses to the user defined category. This allows you to identify extraordinary or non-traditional network offenses.

How do I Investigate a User Defined Offense?

To investigate a user defined offense:

Step 1 Click the **Offense Manager** tab.

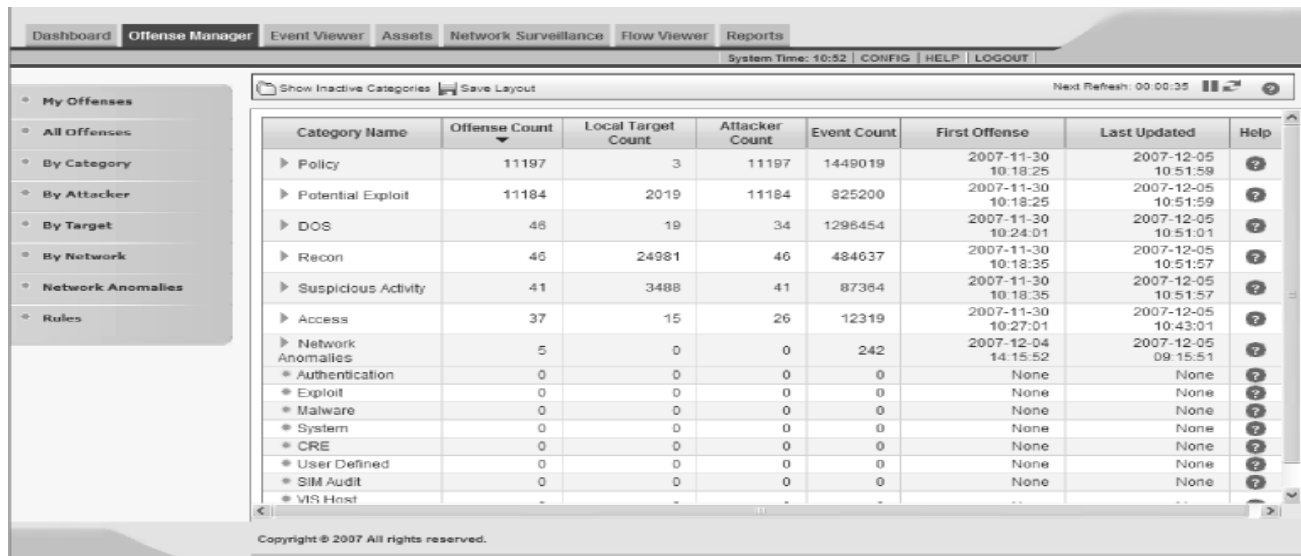
The Offense Manager window appears.

Step 2 Click **By Category** from the navigation menu.

The By Category view appears displaying high-level categories. The counts for each category are accumulated from the values in the low-level categories.



Hint: Only low-level categories with associated offenses appear with an arrow. You can click the arrow to view the associated low-level categories. If you wish to view all categories, click **Show Inactive Categories**.



Step 3 To view additional low-level category information for the User Defined category, click the arrow icon next to User Defined.

▼ User Defined	23	42	23	1448	2007-02-19 09:18:52	2007-02-19 10:12:08	?
Custom Policy 1	9	0	9	691	2007-02-19 09:18:52	2007-02-19 10:12:08	
Custom Policy 3	19	42	19	773	2007-02-19 09:34:38	2007-02-19 10:12:08	

Step 4 Double-click any low-level category to view the list of associated offenses. The list of offenses appear.

?	Id	Description	Attacker/Src	Magnitude	Target(s)/Dest	Cat.	Attacker Net	Target Net	Events	Start Date	Last Event
	56	Potential Botnet Activity (IRC Detected) , Custom Local to Lo...	172.16.60.230	■■■■	Multiple (39)	10	HighSpeed_Servers	Multiple (3)	742	2007-02-19 10:04:39	1m 18s
	9	Custom Local to Local Event , Potential Botnet Activity (IRC ...	172.16.60.161	■■■■	Multiple (190)	8	HighSpeed_Servers	Multiple (2)	1212	2007-02-15 18:32:33	9m 20s
	58	Custom Local to Local Event , Custom Local to Remote Event	172.16.150.40	■■■■	Multiple (3)	2	Performance_Servers	Multiple (2)	295	2007-02-19 10:04:39	1m 24s

Step 5 Double-click the offense you wish to view. The details panel appears.

All Offenses 2 Offense 56 (Summary)

Offense 56 Summary Targets Categories Annotations Networks Events Flows Actions

Magnitude				Relevance	6	Severity	4	Credibility	6
Description	Potential Botnet Activity (IRC Detected) preceded by Custom Local to Local Event preceded by Host Port Scan Detected by Local Host preceded by Custom Local to Remote Event preceded by Default - Suspicious - Internal - Unidirectional TCP Flows			Event count	941 events in 10 categories				
Attacker Src	172.16.60.230			Start	2007-02-19 10:04:39				
Target(s)/Dest	Local (19) Remote (20)			Duration	11m 13s				
Network(s)	Multiple (3)			Assigned to	Not assigned				
Notes									

Attacker Summary Details			
Magnitude		User	Unknown
Description	172.16.60.230	MAC	Unknown
Vulnerabilities	0	Asset Weight	0
Location	Q1-Internal QA.HighSpeed_Servers		

Top 5 Categories Categories				
Name	Magnitude	Local Target Count	Events	Last Event
Potential Botnet connection		0	2	02-19 10:09:53
Custom Policy 1		0	76	02-19 10:15:53
Host Port Scan		2	3	02-19 10:15:53
Executable Code Detected		2	28	02-19 10:11:23
IP Protocol Anomaly		22	290	02-19 10:15:53

Top 5 Local Targets Targets							
IP/DNS Name	Magnitude	Vulnerable	Chained	User	MAC	Location	Weight
172.16.107.201		Unknown	No	Unknown	Unknown	QA_107_subnet	0
172.16.107.205		Unknown	No	Unknown	Unknown	QA_107_subnet	0
172.16.107.206		Unknown	No	Unknown	Unknown	QA_107_subnet	0
172.16.107.195		Unknown	No	Unknown	Unknown	QA_107_subnet	0
172.16.107.199		Unknown	No	Unknown	Unknown	QA_107_subnet	0

Top 10 Events Events					
Event Name	Magnitude	Device	Category	Destination	Start Time

Step 6 To investigate the attacker, view the Attacker Summary box:

- **Location** - Allows you to determine if the attacker is local or remote:
 - **Local** - This field specifies the network (group) in which it is located.
 - **Remote** - This field specifies the geographic location of the attacker, for example, Asia. We recommend that you investigate the traffic from the remote source IP address to make sure that your firewalls are probably configured to block any threatening traffic. If firewall logs are being sent to STRM, use the Event Viewer to investigate firewall logs to make sure it is probably configured. For more information on the Event Viewer, see the *STRM Users Guide*.
- **User** - If the attacker is local or a VPN user and STRM is receiving user identity logs, this field indicates user identity information. This allows you identify the user who is the source of the traffic. To obtain further information about the user, right-click on the IP address in the Description field to access additional menu options. From the menu, select use the **Select Information > Asset Profile**. The Asset Profile window allows you to determine additional information regarding the identify of the source user. You can also determine if the user associated to the offense is a valid user on the device they are attempting to access.

Step 7 Since user defined offenses are based on configurable user defined data, there are a variety of methods for investigating these offenses. You must understand the logic used to create the offense and inspect the network events associated with this offense.

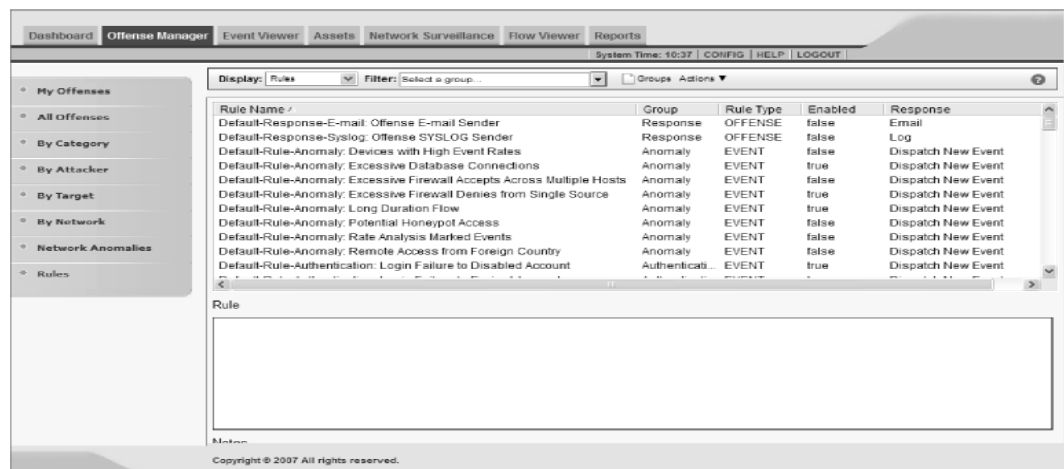
- Step 8** Once you have determined the impact of the offense, you must perform the necessary steps to rectify the source of the activity. If you have determined this behavior is normal, you can tune STRM to no longer detect this activity. For more information, see [How do I Tune a User Defined Offense?](#).
- Step 9** Once you are satisfied that you have resolved the offense, you can close or hide the offense.
- For more information on closing or hiding an offense, see Investigating Offenses in the *STRM Users Guide*.

How do I Tune a User Defined Offense?

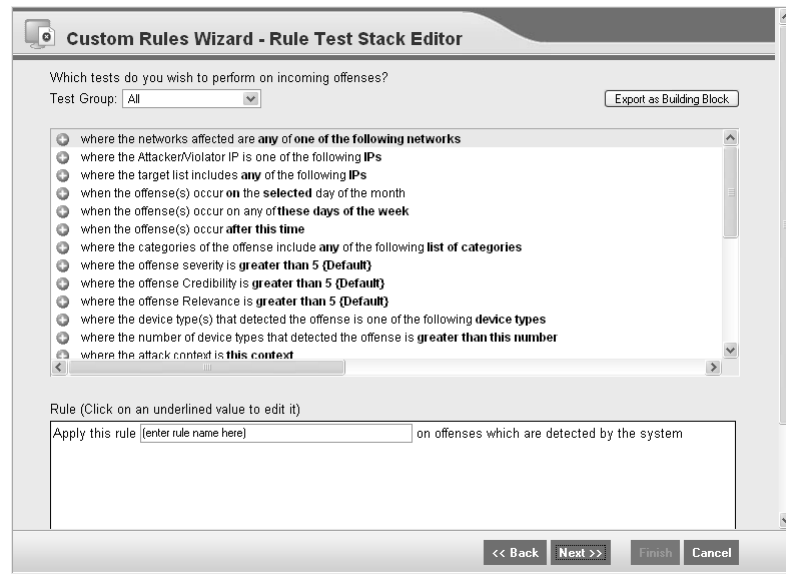
If you determine that the activity is normal and STRM is creating false positive offenses, you can tune STRM to make sure no more offenses are created due to this activity.

To tune reconnaissance activity using the custom rules wizard:

- Step 1** In the navigation bar of the Offense Manager, click **Rules**.
- The Rules interface appears.



- Step 2** Click **New Event Rule**.



Step 3 Use the available rules and building blocks to create the required logic necessary to generate the offense.

Step 4 Click **Next**.

Step 5 The Rules Response Window appears.

Step 6 Select the **Dispatch New Events** check box.

Additional optional appears.



Step 7 From the High-Level Category drop-down list box, select User Defined.

Step 8 Select the **Ensure the dispatched event is part of an offense** check box.

Step 9 Complete the rules wizard.

For more information on using the Custom Rules Wizard, see the *STRM Administration Guide*.