



Security Threat Response Manager

**Event Category Correlation
Reference Guide**

Release_2008.1

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-023498-01, Revision 1

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.

Event Category Correlation Reference 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

EVENT CATEGORY CORRELATION

About Event Category Correlation	1
High-Level Event Categories	3
Event Correlation Processing	4
Additional Event Processing	14
Recon	14
DoS	16
Authentication	18
Access	22
Exploit	24
Malware	25
Suspicious Activity	25
System	28
Policy	30
CRE	31
Potential Exploit	32
SIM Audit	33
VIS Host Discovery	33

ABOUT THIS GUIDE

This preface provides the following guidelines for using the *Security Threat Response Manager Event Category Correlation Reference 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).

EVENT CATEGORY CORRELATION

This document provides information on the types of event categories and the processing of events. For example, the event category determines if events will have an offense automatically created, real-time flow analysis, rate analysis, and the default correlation tests performed. This document provides information on event correlation including:

- [About Event Category Correlation](#)
- [Recon](#)
- [DoS](#)
- [Authentication](#)
- [Access](#)
- [Exploit](#)
- [Malware](#)
- [Suspicious Activity](#)
- [System](#)
- [Policy](#)
- [CRE](#)
- [Potential Exploit](#)
- [SIM Audit](#)
- [VIS Host Discovery](#)

About Event Category Correlation

An Event Processor processes events collected from one or more Event Collector(s). Once received, the Event Processor correlates the information from STRM and distributes to the appropriate Correlation Group for processing.

The Correlation Groups perform tests on the events to determine factors such as vulnerability data, relevance of the targets, importance, or credibility of the events. The results of the Correlation Group tests appear as annotations in the Offense Manager and Event Viewer. Also, custom rules are applied to additional events for specific incident recognition. Once complete, the Event Processor stores the event in the Ariel database and, in some circumstances, performs real-time flow analysis to determine the appropriate routing of the event.

For example, [Figure 2-1](#) provides a representation of the process within the Event Processor for processing events. Once the Event Processor receives an event, the Category Router determines the appropriate Correlation Group to apply tests to the event. Once complete, the event is passed through the Custom Rules Engine to determine the custom rules that apply to the event. The event is then passed through the Ariel database for storage and the Flow Context and Routing components to determine if real-time flow analysis should be performed and if the event should automatically generate a new offense or become part of an existing offense. If this is the case, the event is sent to the Magistrate. If real-time flow analysis is requested of the event, a request is sent to the Classification Engine to determine routing.

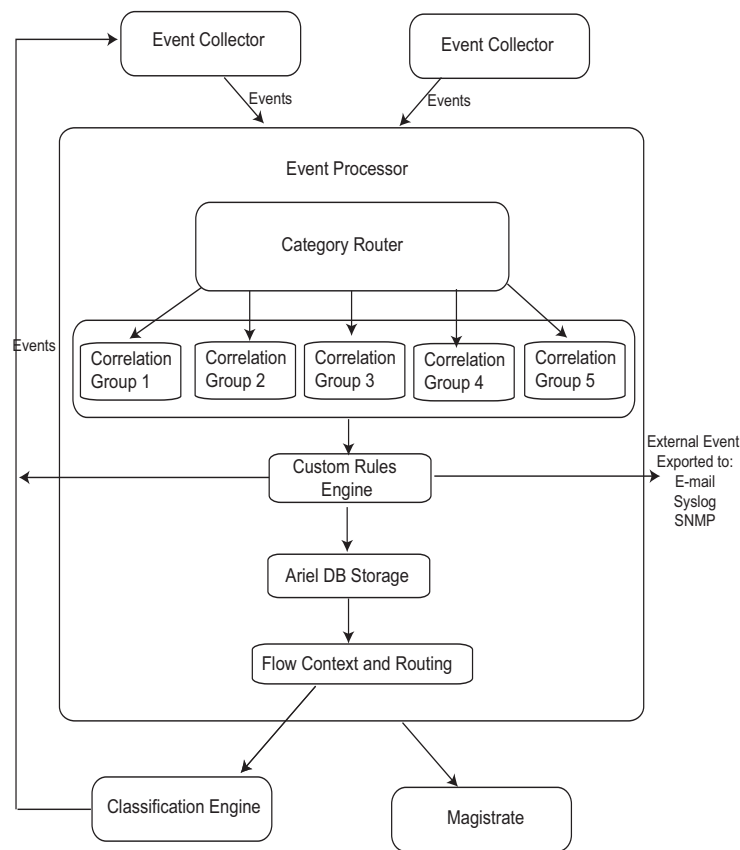


Figure 2-1 Event Category Correlation Process

This section includes:

- [High-Level Event Categories](#)
- [Event Correlation Processing](#)
- [Additional Event Processing](#)

High-Level Event Categories

The high-level event categories include:

Table 2-1 High-Level Event Categories

Category	Description
Recon	Events relating to scanning and other techniques used to identify network resources, for example, network or host port scans.
DoS	Events relating to Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks against services or hosts, for example, brute force network DoS attacks.
Authentication	Events relating to authentication controls, group, or privilege change, for example, log in or log out.
Access	Events resulting from an attempt to access network resources, for example, firewall accept or deny.
Exploit	Events relating to application exploits and buffer overflow attempts, for example, buffer overflow or web application exploits.
Malware	Events relating to viruses, trojans, back door attacks, or other forms of hostile software. This may include a virus, trojan, malicious software, or spyware.
Suspicious Activity	The nature of the threat is unknown but behavior is suspicious including protocol anomalies that potentially indicate evasive techniques, for example, packet fragmentation or known IDS evasion techniques.
System	Events related to system changes, software installation, or status messages.
Policy	Events regarding corporate policy violations or misuse.
CRE	Events generated from an offense or event rule. For more information on creating custom rules, see the <i>STRM Administration Guide</i> .
Potential Exploit	Events relating to potential application exploits and buffer overflow attempts.
SIM Audit	Events relating to user interaction with the Console and STRM Administration Console.
VIS Host Discovery	Events relating to the host, ports, or vulnerabilities that the VIS component discovers.

Event Correlation Processing

For each event category, the Correlation Group determines the correlation rules (tests) that are performed on each event. Each test is performed and assigned a value between 0 and 10. Once all tests are complete, all test results are weighted and the data for the event is provided in the event viewer. [Table 2-2](#) provides a list of possible correlation rules (tests).

Table 2-2 Correlation Rules (Tests)

Rule	Description
Relevance of the day of the week	Determines the relevance of the day of the week for this event. For example, if the event occurs on the weekend, an attack may have a higher relevance.
Device credibility	Credibility rating can be applied on a per device basis that allows users to associate a credibility to a device based on the level of trust for the device and the validity of the produced event. For example, a highly tuned IDS in front of a key server may have a credibility of 7 while an IDS outside the corporate network may have a credibility of 3.
Event rate	Determines if the event rate of this event type is greater than normal. This is determined on a category by category basis.
Attacker	Determines if the attacker is one of the configured assets.
Target	Determines if the target is one of the configured assets.
Source port	Determines if the source port is less than 1024. If the port is less than 1024, the attacker may be attempting to fool a stateless firewall.
Attacker age	Determines the relative importance of how long the attacker has been known to the system. If the attacker is new, the relevance of this attacker increases.
Target age	Determines the relative importance of how long the target has been known to the system.
Remote attacker	Determines the relative importance of the attacker network.
Remote target	Determines the relative importance of the target network.
Target port	Determines if the target port is included in the list of most attacked ports provided by the incidents.org data.
Attacker risk	Determine the overall risk assessment value for the attacker based on the asset profile data.
Target risk	Determine the overall risk assessment value for the target.
Time of the attack	Determines the time of attack. For example, if the attack occurs in the middle of the night, which is deemed to be a low traffic time, this indicates a higher relevance of the attack.
Vulnerable targeted port	If the port is open, determine if the targeted port is vulnerable to the current exploit.
Vulnerable port	Determines if the port is vulnerable to any type of attack or exploit.
Open target port	Determines if the target port is open.

Table 2-2 Correlation Rules (Tests) (continued)

Rule	Description
Remote Target	Determines if the target network is defined as a remote network in STRM views.
Geographic Location	Determines the relative importance of the geographic location of the target.
Remote attacker	Determines if the attacker network is defined as a remote network in STRM views.
Attacker IP address	Determines if the attacker IP address is included in the list of IP addresses that are highlighted as suspicious in the Remote Services View.
Attacker port	Determines if the attacker port is included in the list of ports from which attacks originate as provided by the incidents.org data.

Each low-level event category is processed by one of five event Correlation Groups. This section provides information on the Correlation Groups including:

- [Correlation Group 1](#)
- [Correlation Group 2](#)
- [Correlation Group 3](#)
- [Correlation Group 4](#)
- [Correlation Group 5](#)

Correlation Group 1

The Correlation Group 1 correlation model provides tests for the following traffic types:

Table 2-3 Correlation Group 1 Tests

Traffic Type	Correlation Rules (Tests)
Local-to-Local	<p>Correlation Group 1 performs the following tests for Local-to-Local traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker • Target • Source port • Target port • Cross host • Attacker age • Target age • Attacker network • Target network • Vulnerable targeted port • Attacker risk • Target risk • Time of the attack • Open target port • Vulnerable port

Note: For test details, see [Table 2-2](#).

Table 2-3 Correlation Group 1 Tests (continued)

Traffic Type	Correlation Rules (Tests)
Local-to-Remote	<p data-bbox="704 352 1308 411">Correlation Group 1 performs the following tests for Local-to-Remote traffic:</p> <ul data-bbox="704 426 1133 919" style="list-style-type: none"> <li data-bbox="704 426 1133 453">• Relevance of the day of the week <li data-bbox="704 468 938 495">• Device credibility <li data-bbox="704 510 862 537">• Event rate <li data-bbox="704 552 837 579">• Attacker <li data-bbox="704 594 878 621">• Source port <li data-bbox="704 636 870 663">• Target port <li data-bbox="704 678 889 705">• Attacker age <li data-bbox="704 720 938 747">• Attacker network <li data-bbox="704 762 886 789">• Attacker risk <li data-bbox="704 804 919 831">• Remote Target <li data-bbox="704 846 984 873">• Geographic Location <li data-bbox="704 888 951 915">• Time of the attack <p data-bbox="704 930 1138 957">Note: For test details, see Table 2-2.</p>
Remote-to-Local	<p data-bbox="704 976 1308 1035">Correlation Group 1 performs the following tests for Remote-to-Local traffic:</p> <ul data-bbox="704 1050 1133 1717" style="list-style-type: none"> <li data-bbox="704 1050 1133 1077">• Relevance of the day of the week <li data-bbox="704 1092 938 1119">• Device credibility <li data-bbox="704 1134 862 1161">• Event rate <li data-bbox="704 1176 821 1203">• Target <li data-bbox="704 1218 878 1245">• Source port <li data-bbox="704 1260 870 1287">• Target age <li data-bbox="704 1302 894 1329">• Attacker port <li data-bbox="704 1344 935 1371">• Remote attacker <li data-bbox="704 1386 971 1413">• Attacker IP address <li data-bbox="704 1428 976 1455">• Geographic location <li data-bbox="704 1470 951 1497">• Time of the attack <li data-bbox="704 1512 919 1539">• Target network <li data-bbox="704 1554 870 1581">• Target risk <li data-bbox="704 1596 935 1623">• Open target port <li data-bbox="704 1638 1024 1665">• Vulnerable targeted port <li data-bbox="704 1680 919 1707">• Vulnerable port <p data-bbox="704 1722 1138 1749">Note: For test details, see Table 2-2.</p>

Correlation Group 2

The Correlation Group 2 correlation model provides tests for the following traffic types:

Table 2-4 Correlation Group 2 Tests

Traffic Type	Correlation Rules (Tests)
Local-to-Local	<p>Correlation Group 2 performs the following tests for Local-to-Local traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker • Target • Source port • Attacker age • Target age • Attacker network • Target port • Attacker risk • Target risk • Time of the attack • Open target port <p>Note: For test details, see Table 2-2.</p>
Local-to-Remote	<p>Correlation Group 2 performs the following tests for Local-to-Remote traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker • Source port • Target port • Attacker age • Attacker network • Attacker risk • Remote target • Target • Geographic location • Time of the attack <p>Note: For test details, see Table 2-2.</p>

Table 2-4 Correlation Group 2 Tests (continued)

Traffic Type	Correlation Rules (Tests)
Remote-to-Local	<p data-bbox="704 352 1308 411">Correlation Group 2 performs the following tests for Remote-to-Local traffic:</p> <ul data-bbox="704 426 1133 1050" style="list-style-type: none"><li data-bbox="704 426 1133 453">• Relevance of the day of the week<li data-bbox="704 468 938 495">• Device credibility<li data-bbox="704 510 862 537">• Event rate<li data-bbox="704 552 818 579">• Target<li data-bbox="704 594 878 621">• Source port<li data-bbox="704 636 867 663">• Target age<li data-bbox="704 678 889 705">• Attacker port<li data-bbox="704 720 867 747">• Target port<li data-bbox="704 762 938 789">• Remote Attacker<li data-bbox="704 804 971 831">• Attacker IP address<li data-bbox="704 846 976 873">• Geographic location<li data-bbox="704 888 951 915">• Time of the attack<li data-bbox="704 930 915 957">• Target network<li data-bbox="704 972 867 999">• Target risk<li data-bbox="704 1014 932 1041">• Open target port

Note: For test details, see [Table 2-2](#).

Correlation Group 3

The Correlation Group 3 correlation model provides tests for the following traffic types:

Table 2-5 Correlation Group 3 Tests

Traffic Type	Correlation Rules (Tests)
Local-to-Local	<p>Correlation Group 3 performs the following tests for Local-to-Local traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker • Target • Source port • Attacker age • Target age • Attacker network • Target network • Target port • Attacker risk • Target risk • Time of the attack <p>Note: For test details, see Table 2-2.</p>
Local-to-Remote	<p>Correlation Group 3 performs the following tests for Local-to-Remote traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker • Source port • Target port • Attacker age • Attacker network • Attacker risk • Geographic location • Time of the attack <p>Note: For test details, see Table 2-2.</p>

Table 2-5 Correlation Group 3 Tests (continued)

Traffic Type	Correlation Rules (Tests)
Remote-to-Local	<p data-bbox="704 352 1308 411">Correlation Group 3 performs the following tests for Remote-to-Local traffic:</p> <ul data-bbox="704 426 1133 1003" style="list-style-type: none"><li data-bbox="704 426 1133 453">• Relevance of the day of the week<li data-bbox="704 468 938 495">• Device credibility<li data-bbox="704 510 862 537">• Event rate<li data-bbox="704 552 818 579">• Target<li data-bbox="704 594 878 621">• Source port<li data-bbox="704 636 867 663">• Target age<li data-bbox="704 678 894 705">• Attacker port<li data-bbox="704 720 867 747">• Target port<li data-bbox="704 762 971 789">• Attacker IP address<li data-bbox="704 804 976 831">• Geographic location<li data-bbox="704 846 951 873">• Time of the attack<li data-bbox="704 888 915 915">• Target network<li data-bbox="704 930 867 957">• Target risk<li data-bbox="704 972 935 999">• Remote attacker

Note: For test details, see [Table 2-2](#).

Correlation Group 4

The Correlation Group 4 correlation model provides tests for the following traffic types:

Table 2-6 Correlation Group 4 Tests

Traffic Type	Correlation Rules (Tests)
Local-to-Local	<p>Correlation Group 4 performs the following tests for Local-to-Local traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker • Target • Attacker age • Target age • Attacker network • Target network • Time of the attack <p>Note: For test details, see Table 2-2.</p>
Local-to-Remote	<p>Correlation Group 4 performs the following tests for Local-to-Remote traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker • Attacker age • Attacker network • Remote Target • Geographic location • Time of the attack <p>Note: For test details, see Table 2-2.</p>

Table 2-6 Correlation Group 4 Tests (continued)

Traffic Type	Correlation Rules (Tests)
Remote-to-Local	<p>Correlation Group 4 performs the following tests for Remote-to-Local traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Target • Target age • Attacker port • Remote attacker • Geographic location • Time of the attack • Target network • Vulnerable port <p>Note: For test details, see Table 2-2.</p>

Correlation Group 5

The Correlation Group 5 correlation model provides tests for the following traffic types:

Table 2-7 Correlation Group 5 Tests

Traffic Type	Correlation Rules (Tests)
Local-to-Local	<p>Correlation Group 5 performs the following tests for Local-to-Local traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker • Target • Attacker network • Target network • Time of the attack <p>Note: For test details, see Table 2-2.</p>

Table 2-7 Correlation Group 5 Tests (continued)

Traffic Type	Correlation Rules (Tests)
Local-to-Remote	<p>Correlation Group 5 performs the following tests for Local-to-Remote traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Attacker network • Time of the attack <p>Note: For test details, see Table 2-2.</p>
Remote-to-Local	<p>Correlation Group 5 performs the following tests for Remote-to-Local traffic:</p> <ul style="list-style-type: none"> • Relevance of the day of the week • Device credibility • Event rate • Target • Target network • Time of the attack <p>Note: For test details, see Table 2-2.</p>

Additional Event Processing

Each event is processed using one of the following scenarios:

- **Scenario 1** - Event information is forwarded to the Magistrate component by automatically creating offenses. Even though offenses are created automatically, no real-time flow analysis is performed. Events are stored in the Event Processor.
- **Scenario 2** - Events are stored in the Event Processor. Offenses are not automatically created and no flow analysis is performed.

Recon

The Recon category indicates events relating to scanning and other techniques used to identify network resources. The associated low-level event categories include:

Table 2-8 Recon Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown Form of Recon	Indicates an unknown form of reconnaissance.	2	Correlation Group 2	Scenario 2
Application Query	Indicates reconnaissance to applications on your system.	3	Correlation Group 2	Scenario 2

Table 2-8 Recon Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Host Query	Indicates reconnaissance to a host in your network.	3	Correlation Group 2	Scenario 2
Network Sweep	Indicates reconnaissance on your network.	4	Correlation Group 2	Scenario 2
Mail Reconnaissance	Indicates reconnaissance on your mail system.	3	Correlation Group 2	Scenario 2
Windows Reconnaissance	Indicates reconnaissance for windows.	3	Correlation Group 2	Scenario 2
Portmap / RPC Request	Indicates reconnaissance on your portmap or RPC request.	3	Correlation Group 2	Scenario 2
Host Port Scan	Indicates a scan occurred on the host's ports.	4	Correlation Group 2	Scenario 2
RPC Dump	Indicates Remote Procedure Call (RPC) information is removed.	3	Correlation Group 2	Scenario 2
DNS Reconnaissance	Indicates reconnaissance on the DNS server.	3	Correlation Group 2	Scenario 2
Misc Reconnaissance Event	Indicates a miscellaneous reconnaissance event.	2	Correlation Group 2	Scenario 2
Web Reconnaissance	Indicates web reconnaissance on your network.	3	Correlation Group 2	Scenario 2
Database Reconnaissance	Indicates database reconnaissance on your network.	3	Correlation Group 2	Scenario 2
ICMP Reconnaissance	Indicates reconnaissance on ICMP traffic.	3	Correlation Group 2	Scenario 2
UDP Reconnaissance	Indicates reconnaissance on UDP traffic.	3	Correlation Group 2	Scenario 2
SNMP Reconnaissance	Indicates reconnaissance on SNMP traffic.	3	Correlation Group 2	Scenario 2
ICMP Host Query	Indicates an ICMP host query.	3	Correlation Group 2	Scenario 2
UDP Host Query	Indicates a UDP host query.	3	Correlation Group 2	Scenario 2
NMAP Reconnaissance	Indicates NMAP reconnaissance.	3	Correlation Group 2	Scenario 2
TCP Reconnaissance	Indicates TCP reconnaissance on your network.	3	Correlation Group 2	Scenario 2
Unix Reconnaissance	Indicates reconnaissance on your UNIX network.	3	Correlation Group 2	Scenario 2
FTP Reconnaissance	Indicates FTP reconnaissance.	3	Correlation Group 2	Scenario 2

DoS The DoS category indicates events relating to Denial Of Service (DoS) attacks against services or hosts. The associated low-level event categories include:

Table 2-9 DoS Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown DoS Attack	Indicates an unknown DoS attack.	8	Correlation Group 2	Scenario 2
ICMP DoS	Indicates an ICMP DoS attack.	9	Correlation Group 2	Scenario 2
TCP DoS	Indicates a TCP DoS attack.	9	Correlation Group 2	Scenario 2
UDP DoS	Indicates a UDP DoS attack.	9	Correlation Group 2	Scenario 2
DNS Service DoS	Indicates a DNS service DoS attack.	8	Correlation Group 2	Scenario 2
Web Service DoS	Indicates a web service DoS attack.	8	Correlation Group 2	Scenario 2
Mail Service DoS	Indicates a mail server DoS attack.	8	Correlation Group 2	Scenario 2
Distributed DoS	Indicates a distributed DoS attack.	9	Correlation Group 2	Scenario 2
Misc DoS	Indicates a miscellaneous DoS attack.	8	Correlation Group 2	Scenario 2
Unix DoS	Indicates a Unix DoS attack.	8	Correlation Group 2	Scenario 2
Windows DoS	Indicates a Windows DoS attack.	8	Correlation Group 2	Scenario 2
Database DoS	Indicates a database DoS attack.	8	Correlation Group 2	Scenario 2
FTP DoS	Indicates an FTP DoS attack.	8	Correlation Group 2	Scenario 2
Infrastructure DoS	Indicates a DoS attack on the infrastructure.	8	Correlation Group 2	Scenario 2
Telnet DoS	Indicates a Telnet DoS attack.	8	Correlation Group 2	Scenario 2
Brute Force Login	Indicates access to your system through unauthorized methods.	8	Correlation Group 2	Scenario 2
High Rate TCP DoS	Indicates a high rate TCP DoS attack.	8	Correlation Group 2	Scenario 2
High Rate UDP DoS	Indicates a high rate UDP DoS attack.	8	Correlation Group 2	Scenario 2
High Rate ICMP DoS	Indicates a high rate ICMP DoS attack.	8	Correlation Group 2	Scenario 2
High Rate DoS	Indicates a high rate DoS attack.	8	Correlation Group 2	Scenario 2
Medium Rate TCP DoS	Indicates a medium rate TCP attack.	8	Correlation Group 2	Scenario 2
Medium Rate UDP DoS	Indicates a medium rate UDP attack.	8	Correlation Group 2	Scenario 2
Medium Rate ICMP DoS	Indicates a medium rate ICMP attack.	8	Correlation Group 2	Scenario 2
DoS	Indicates a DoS attack.	8	Correlation Group 2	Scenario 2

Table 2-9 DoS Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Medium Rate DoS	Indicates a medium rate DoS attack.	8	Correlation Group 2	Scenario 2
Low Rate TCP DoS	Indicates a low rate TCP DoS attack.	8	Correlation Group 2	Scenario 2
Low Rate UDP DoS	Indicates a low rate UDP DoS attack.	8	Correlation Group 2	Scenario 2
Low Rate ICMP DoS	Indicates a low rate ICMP DoS attack.	8	Correlation Group 2	Scenario 2
Low Rate DoS	Indicates a low rate DoS attack.	8	Correlation Group 2	Scenario 2
Distributed High Rate TCP DoS	Indicates a distributed high rate TCP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed High Rate UDP DoS	Indicates a distributed high rate UDP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed High Rate ICMP DoS	Indicates a distributed high rate ICMP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed High Rate DoS	Indicates a distributed high rate DoS attack.	8	Correlation Group 2	Scenario 2
Distributed Medium Rate TCP DoS	Indicates a distributed medium rate TCP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed Medium Rate UDP DoS	Indicates a distributed medium rate UDP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed Medium Rate ICMP DoS	Indicates a distributed medium rate ICMP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed Medium Rate DoS	Indicates a distributed medium rate DoS attack.	8	Correlation Group 2	Scenario 2
Distributed Low Rate TCP DoS	Indicates a distributed low rate TCP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed Low Rate UDP DoS	Indicates a distributed low rate UDP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed Low Rate ICMP DoS	Indicates a distributed low rate ICMP DoS attack.	8	Correlation Group 2	Scenario 2
Distributed Low Rate DoS	Indicates a distributed low rate DoS attack.	8	Correlation Group 2	Scenario 2
High Rate TCP Scan	Indicates a high rate TCP scan.	8	Correlation Group 2	Scenario 2
High Rate UDP Scan	Indicates a high rate UDP scan.	8	Correlation Group 2	Scenario 2
High Rate ICMP Scan	Indicates a high rate ICMP scan.	8	Correlation Group 2	Scenario 2
High Rate Scan	Indicates a high rate scan.	8	Correlation Group 2	Scenario 2

Table 2-9 DoS Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Medium Rate TCP Scan	Indicates a medium rate TCP scan.	8	Correlation Group 2	Scenario 2
Medium Rate UDP Scan	Indicates a medium rate UDP scan.	8	Correlation Group 2	Scenario 2
Medium Rate ICMP Scan	Indicates a medium rate ICMP scan.	8	Correlation Group 2	Scenario 2
Medium Rate Scan	Indicates a medium rate scan.	8	Correlation Group 2	Scenario 2
Low Rate TCP Scan	Indicates a low rate TCP scan.	8	Correlation Group 2	Scenario 2
Low Rate UDP Scan	Indicates a low rate UDP scan.	8	Correlation Group 2	Scenario 2
Low Rate ICMP Scan	Indicates a low rate ICMP scan.	8	Correlation Group 2	Scenario 2
Low Rate Scan	Indicates a low rate scan.	8	Correlation Group 2	Scenario 2
VoIP DoS	Indicates a VoIP DoS attack	8	Correlation Group 2	Scenario 2

Authentication

The authentication category indicates events relating to authentication and access controls. The associated low-level event categories include:

Table 2-10 Authentication Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown Authentication	Indicates unknown authentication	1	Correlation Group 3	Scenario 2
Host Login Succeeded	Indicates the host login was successful.	1	Correlation Group 3	Scenario 2
Host Login Failed	Indicates the host login failed.	3	Correlation Group 3	Scenario 2
Misc Login Succeeded	Indicates that the login sequence succeeded.	1	Correlation Group 3	Scenario 2
Misc Login Failed	Indicates that login sequence failed.	3	Correlation Group 3	Scenario 2
Privilege Escalation Failed	Indicates that the privileged escalation failed.	3	Correlation Group 3	Scenario 2
Privilege Escalation Succeeded	Indicates that the privilege escalation succeeded.	1	Correlation Group 3	Scenario 2
Mail Service Login Succeeded	Indicates that the mail service login succeeded.	1	Correlation Group 3	Scenario 2
Mail Service Login Failed	Indicates that the mail service login failed.	3	Correlation Group 3	Scenario 2

Table 2-10 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Auth Server Login Failed	Indicates that the authentication server login failed.	3	Correlation Group 3	Scenario 2
Auth Server Login Succeeded	Indicates that the authentication server login succeeded.	1	Correlation Group 3	Scenario 2
Web Service Login Succeeded	Indicates that the web service login succeeded.	1	Correlation Group 3	Scenario 2
Web Service Login Failed	Indicates that the web service login failed.	3	Correlation Group 3	Scenario 2
Admin Login Successful	Indicates the administrative login was successful.	1	Correlation Group 3	Scenario 2
Admin Login Failure	Indicates the administrative login failed.	3	Correlation Group 3	Scenario 2
Suspicious Username	Indicates that a user attempted to access the network using an incorrect username.	4	Correlation Group 3	Scenario 2
Login with username/ password defaults successful	Indicates that a user accessed the network using the default username and password.	4	Correlation Group 3	Scenario 2
Login with username/ password defaults failed	Indicates that a user was unsuccessful accessing the network using the default username and password.	4	Correlation Group 3	Scenario 2
FTP Login Succeeded	Indicates that the FTP login was successful.	1	Correlation Group 3	Scenario 2
FTP Login Failed	Indicates that the FTP login failed.	3	Correlation Group 3	Scenario 2
SSH Login Succeeded	Indicates that the SSH login was successful.	1	Correlation Group 3	Scenario 2
SSH Login Failed	Indicates that the SSH login failed.	2	Correlation Group 3	Scenario 2
User Right Assigned	Indicates that user access to network resources was successfully granted.	1	Correlation Group 3	Scenario 2
User Right Removed	Indicates that user access to network resources was successfully removed.	1	Correlation Group 3	Scenario 2
Trusted Domain Added	Indicates that a trusted domain was successfully added to your deployment.	1	Correlation Group 3	Scenario 2
Trusted Domain Removed	Indicates that a trusted domain was removed from your deployment.	1	Correlation Group 3	Scenario 2
System Security Access Granted	Indicates that system security access was successfully granted.	1	Correlation Group 3	Scenario 2

Table 2-10 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
System Security Access Removed	Indicates that system security access was successfully removed.	1	Correlation Group 3	Scenario 2
Policy Added	Indicates that a policy was successfully added.	1	Correlation Group 3	Scenario 2
Policy Change	Indicates that a policy was successfully changed.	1	Correlation Group 3	Scenario 2
User Account Added	Indicates that a user account was successfully added.	1	Correlation Group 3	Scenario 2
User Account Changed	Indicates a change to an existing user account.	1	Correlation Group 3	Scenario 2
Password Change Failed	Indicates that an attempt to change an existing password failed.	3	Correlation Group 3	Scenario 2
Password Change Succeeded	Indicates that a password change was successful.	1	Correlation Group 3	Scenario 2
User Account Removed	Indicates that a user account was successfully removed.	1	Correlation Group 3	Scenario 2
Group Member Added	Indicates that a group member was successfully added.	1	Correlation Group 3	Scenario 2
Group Member Removed	Indicates that a group member was removed.	1	Correlation Group 3	Scenario 2
Group Added	Indicates that a group was successfully added.	1	Correlation Group 3	Scenario 2
Group Changed	Indicates a change to an existing group.	1	Correlation Group 3	Scenario 2
Group Removed	Indicates a group was removed.	1	Correlation Group 3	Scenario 2
Computer Account Added	Indicates a computer account has been successfully added.	1	Correlation Group 3	Scenario 2
Computer Account Changed	Indicates a change to an existing computer account.	1	Correlation Group 3	Scenario 2
Computer Account Removed	Indicates a computer account has been successfully removed.	1	Correlation Group 3	Scenario 2
Remote Access Login Succeeded	Indicates that access to the network using a remote login was successful.	1	Correlation Group 3	Scenario 2
Remote Access Login Failed	Indicates that an attempt to access the network using a remote login failed.	3	Correlation Group 3	Scenario 2
General Authentication Successful	Indicates that the authentication processes was successful	1	Correlation Group 3	Scenario 2

Table 2-10 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
General Authentication Failed	Indicates that the authenticating process failed.	3	Correlation Group 3	Scenario 2
Telnet Login Succeeded	Indicates that the telnet login was successful.	1	Correlation Group 3	Scenario 2
Telnet Login Failed	Indicates that the telnet login failed.	3	Correlation Group 3	Scenario 2
Suspicious Password	Indicates that a user attempted to login using a suspicious password.	4	Correlation Group 3	Scenario 2
Samba Login Successful	Indicates a user successfully logged in using Samba.	1	Correlation Group 3	Scenario 2
Samba Login Failed	Indicates user login failed using Samba.	3	Correlation Group 3	Scenario 2
Auth Server Session Opened	Indicates that a communication session with the authentication server was started.	1	Correlation Group 3	Scenario 2
Auth Server Session Closed	Indicates that a communication session with the authentication server was closed.	1	Correlation Group 3	Scenario 2
Firewall Session Closed	Indicates that a firewall session was closed.	1	Correlation Group 3	Scenario 2
Host Logout	Indicates that a host successfully logged out.	1	Correlation Group 3	Scenario 2
Misc Logout	Indicates that a user successfully logged out.	1	Correlation Group 3	Scenario 2
Auth Server Logout	Indicates that the process to log out of the authentication server was successful.	1	Correlation Group 3	Scenario 2
Web Service Logout	Indicates that the process to log out of the web service was successful.	1	Correlation Group 3	Scenario 2
Admin Logout	Indicates that the administrative user successfully logged out.	1	Correlation Group 3	Scenario 2
FTP Logout	Indicates that the process to log out of the FTP service was successful.	1	Correlation Group 3	Scenario 2
SSH Logout	Indicates that the process to log out of the SSH session was successful.	1	Correlation Group 3	Scenario 2
Remote Access Logout	Indicates that the process to log out using remote access was successful.	1	Correlation Group 3	Scenario 2

Table 2-10 Authentication Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Telnet Logout	Indicates that the process to log out of the Telnet session was successful.	1	Correlation Group 3	Scenario 2
Samba Logout	Indicates that the process to log out of Samba was successful.	1	Correlation Group 3	Scenario 2
SSH Session Started	Indicates that the SSH login session has been initiated on a host.	1	Correlation Group 5	Scenario 2
SSH Session Finished	Indicates the termination of an SSH login session on a host.	1	Correlation Group 5	Scenario 2
Admin Session Started	Indicates that a login session has been initiated on a host by an administrative or privileged user.	1	Correlation Group 5	Scenario 2
Admin Session Finished	Indicates the termination of an administrator or privileged users login session on a host.	1	Correlation Group 5	Scenario 2
VoIP Login Succeeded	Indicates a successful VoIP service login	1	Correlation Group 3	Scenario 2
VoIP Login Failed	Indicates an unsuccessful attempt to access VoIP service.	1	Correlation Group 3	Scenario 2
VoIP Logout	Indicates a user logout,	1	Correlation Group 3	Scenario 2
VoIP Session Initiated	Indicates the beginning of a VoIP session.	1	Correlation Group 3	Scenario 2
VoIP Session Terminated	Indicates the end of a VoIP session.	1	Correlation Group 3	Scenario 2

Access The access category indicates events relating to authentication and access controls. The associated low-level event categories include:

Table 2-11 Access Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown Network Communication Event	Indicates an unknown network communication event.	3	Correlation Group 3	Scenario 2
Firewall Permit	Indicates access to the firewall was permitted.	0	Correlation Group 3	Scenario 2
Firewall Deny	Indicates access to the firewall was denied.	4	Correlation Group 3	Scenario 2

Table 2-11 Access Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Flow Context Response	Indicates events from the Classification Engine in response to a SIM request.	5	No event pass-through	Scenario 2
Misc Network Communication Event	Indicates a miscellaneous communications event.	3	Correlation Group 3	Scenario 2
IPS Deny	Indicates Intrusion Prevention Systems (IPS) denied traffic.	4	Correlation Group 3	Scenario 2
Firewall Session Opened	Indicates the firewall session has been opened.	0	Correlation Group 3	Scenario 2
Firewall Session Closed	Indicates the firewall session has been closed.	0	Correlation Group 3	Scenario 2
Dynamic Address Translation Successful	Indicates that dynamic address translation was successful.	0	Correlation Group 3	Scenario 2
No Translation Group Found	Indicates that no translation group has been found.	2	Correlation Group 3	Scenario 2
Misc Authorization	Indicates that access was granted to a miscellaneous authentication server.	2	Correlation Group 3	Scenario 2
ACL Permit	Indicates that an ACL was permitted access.	0	Correlation Group 3	Scenario 2
ACL Deny	Indicates that an ACL was denied access.	4	Correlation Group 3	Scenario 2

Exploit

The exploit category indicates events where a communication or access has occurred. The associated low-level event categories include:

Table 2-12 Exploit Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown Exploit Attack	Indicates an unknown exploit attack.	9	Correlation Group 1	Scenario 2
Buffer Overflow	Indicates a buffer overflow.	9	Correlation Group 1	Scenario 2
DNS Exploit	Indicates a DNS exploit.	9	Correlation Group 1	Scenario 2
Telnet Exploit	Indicates a Telnet exploit.	9	Correlation Group 1	Scenario 2
Linux Exploit	Indicates a Linux exploit.	9	Correlation Group 1	Scenario 2
Unix Exploit	Indicates a Unix exploit.	9	Correlation Group 1	Scenario 2
Windows Exploit	Indicates a Windows exploit.	9	Correlation Group 1	Scenario 2
Mail Exploit	Indicates a mail server exploit.	9	Correlation Group 1	Scenario 2
Infrastructure Exploit	Indicates an infrastructure exploit.	9	Correlation Group 1	Scenario 2
Misc Exploit	Indicates a miscellaneous exploit.	9	Correlation Group 1	Scenario 2
Web Exploit	Indicates a web exploit.	9	Correlation Group 1	Scenario 2
Session Hijack	Indicates a session in your network has been interceded.	9	Correlation Group 2	Scenario 2
Worm Active	Indicates an active worm.	10	Correlation Group 1	Scenario 2
Password Guess/Retrieve	Indicates that a user has requested access to their password information from the database.	9	Correlation Group 2	Scenario 2
FTP Exploit	Indicates an FTP exploit.	9	Correlation Group 1	Scenario 2
RPC Exploit	Indicates an RPC exploit.	9	Correlation Group 1	Scenario 2
SNMP Exploit	Indicates an SNMP exploit.	9	Correlation Group 1	Scenario 2
NOOP Exploit	Indicates an NOOP exploit.	9	Correlation Group 1	Scenario 2
Samba Exploit	Indicates an Samba exploit.	9	Correlation Group 1	Scenario 2
Database Exploit	Indicates a database exploit.	9	Correlation Group 1	Scenario 2
SSH Exploit	Indicates an SSH exploit.	9	Correlation Group 1	Scenario 2
ICMP Exploit	Indicates an ICMP exploit.	9	Correlation Group 1	Scenario 2
UDP Exploit	Indicates a UDP exploit.	9	Correlation Group 1	Scenario 2
Browser Exploit	Indicates an exploit on your browser.	9	Correlation Group 1	Scenario 2
DHCP Exploit	Indicates a DHCP exploit	9	Correlation Group 1	Scenario 2
Remote Access Exploit	Indicates a remote access exploit	9	Correlation Group 1	Scenario 2

Malware The malicious software (malware) category indicates events relating to application exploits and buffer overflow attempts. The associated low-level event categories include:

Table 2-13 Malware Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown Malware	Indicates an unknown virus.	4	Correlation Group 2	Scenario 2
Backdoor Detected	Indicates that a backdoor to the system has been detected.	9	Correlation Group 2	Scenario 2
Hostile Mail Attachment	Indicates a hostile mail attachment.	6	Correlation Group 2	Scenario 2
Malicious Software	Indicates a virus.	6	Correlation Group 2	Scenario 2
Hostile Software Download	Indicates a hostile software download to your network.	6	Correlation Group 2	Scenario 2
Virus Detected	Indicates a virus has been detected.	8	Correlation Group 2	Scenario 2
Misc Malware	Indicates miscellaneous malicious software	4	Correlation Group 2	Scenario 2
Trojan Detected	Indicates a trojan has been detected.	7	Correlation Group 2	Scenario 2
Spyware Detected	Indicates spyware has been detected on your system.	6	Correlation Group 2	Scenario 2

Suspicious Activity The suspicious activity category indicates events relating to viruses, trojans, back door attacks, and other forms of hostile software. The associated low-level event categories include:

Table 2-14 Suspicious Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown Suspicious Event	Indicates an unknown suspicious event.	3	Correlation Group 2	Scenario 2
Suspicious Pattern Detected	Indicates a suspicious pattern has been detected.	3	Correlation Group 2	Scenario 2
Content Modified By Firewall	Indicates that content has been modified by the firewall.	3	Correlation Group 2	Scenario 2
Invalid Command or Data	Indicates an invalid command or data.	3	Correlation Group 2	Scenario 2
Suspicious Packet	Indicates a suspicious packet.	3	Correlation Group 2	Scenario 2
Suspicious Activity	Indicates suspicious activity.	3	Correlation Group 2	Scenario 2
Suspicious File Name	Indicates a suspicious file name.	3	Correlation Group 2	Scenario 2

Table 2-14 Suspicious Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Suspicious Port Activity	Indicates suspicious port activity.	3	Correlation Group 2	Scenario 2
Suspicious Routing	Indicates suspicious routing.	3	Correlation Group 2	Scenario 2
Potential Web Vulnerability	Indicates potential web vulnerability.	3	Correlation Group 2	Scenario 2
Unknown Evasion Event	Indicates an unknown evasion event.	5	Correlation Group 2	Scenario 2
IP Spoof	Indicates an IP spoof.	5	Correlation Group 2	Scenario 2
IP Fragmentation	Indicates IP fragmentation.	3	Correlation Group 2	Scenario 2
Overlapping IP Fragments	Indicates overlapping IP fragments.	5	Correlation Group 2	Scenario 2
IDS Evasion	Indicates an IDS evasion.	5	Correlation Group 2	Scenario 2
DNS Protocol Anomaly	Indicates a DNS protocol anomaly.	3	Correlation Group 2	Scenario 2
FTP Protocol Anomaly	Indicates an FTP protocol anomaly.	3	Correlation Group 2	Scenario 2
Mail Protocol Anomaly	Indicates a mail protocol anomaly.	3	Correlation Group 2	Scenario 2
Routing Protocol Anomaly	Indicates a routing protocol anomaly.	3	Correlation Group 2	Scenario 2
Web Protocol Anomaly	Indicates a web protocol anomaly.	3	Correlation Group 2	Scenario 2
SQL Protocol Anomaly	Indicates an SQL protocol anomaly.	3	Correlation Group 2	Scenario 2
Executable Code Detected	Indicates that an executable code has been detected.	5	Correlation Group 2	Scenario 2
Misc Suspicious Event	Indicates a miscellaneous suspicious event.	3	Correlation Group 2	Scenario 2
Information Leak	Indicates an information leak.	1	Correlation Group 2	Scenario 2
Potential Mail Vulnerability	Indicates a potential vulnerability in the mail server.	4	Correlation Group 2	Scenario 2
Potential Version Vulnerability	Indicates a potential vulnerability in the STRM version.	4	Correlation Group 2	Scenario 2
Potential FTP Vulnerability	Indicates a potential FTP vulnerability.	4	Correlation Group 2	Scenario 2
Potential SSH Vulnerability	Indicates a potential SSH vulnerability.	4	Correlation Group 2	Scenario 2
Potential DNS Vulnerability	Indicates a potential vulnerability in the DNS server.	4	Correlation Group 2	Scenario 2
Potential SMB Vulnerability	Indicates a potential SMB (Samba) vulnerability.	4	Correlation Group 2	Scenario 2

Table 2-14 Suspicious Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Potential Database Vulnerability	Indicates a potential vulnerability in the database.	4	Correlation Group 2	Scenario 2
IP Protocol Anomaly	Indicates a potential IP protocol anomaly	3	Correlation Group 2	Scenario 2
Suspicious IP Address	Indicates a suspicious IP address has been detected.	2	Correlation Group 2	Scenario 2
Invalid IP Protocol Usage	Indicates an invalid IP protocol misuse.	2	Correlation Group 2	Scenario 2
Invalid Protocol	Indicates an invalid protocol.	4	Correlation Group 2	Scenario 2
Suspicious Window Events	Indicates a suspicious event with a screen on your desktop.	2	Correlation Group 2	Scenario 2
Suspicious ICMP Activity	Indicates suspicious ICMP activity.	2	Correlation Group 2	Scenario 2
Potential NFS Vulnerability	Indicates a potential Network File System (NFS) vulnerability.	4	Correlation Group 2	Scenario 2
Potential NNTP Vulnerability	Indicates a potential Network News Transfer Protocol (NNTP) vulnerability.	4	Correlation Group 2	Scenario 2
Potential RPC Vulnerability	Indicates a potential RPC vulnerability.	4	Correlation Group 2	Scenario 2
Potential Telnet Vulnerability	Indicates a potential Telnet vulnerability on your system.	4	Correlation Group 2	Scenario 2
Potential SNMP Vulnerability	Indicates a potential SNMP vulnerability.	4	Correlation Group 2	Scenario 2
Illegal TCP Flag Combination	Indicates an invalid TCP flag combination has been detected.	5	Correlation Group 2	Scenario 2
Suspicious TCP Flag Combination	Indicates a potentially invalid TCP flag combination has been detected.	4	Correlation Group 2	Scenario 2
Illegal ICMP Protocol Usage	Indicates an invalid use of the ICMP protocol has been detected.	5	Correlation Group 2	Scenario 2
Suspicious ICMP Protocol Usage	Indicates a potentially invalid use of the ICMP protocol has been detected.	4	Correlation Group 2	Scenario 2
Illegal ICMP Type	Indicates an invalid ICMP type has been detected.	5	Correlation Group 2	Scenario 2
Illegal ICMP Code	Indicates an invalid ICMP code has been detected.	5	Correlation Group 2	Scenario 2
Suspicious ICMP Type	Indicates a potentially invalid ICMP type has been detected.	4	Correlation Group 2	Scenario 2

Table 2-14 Suspicious Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Suspicious ICMP Code	Indicates a potentially invalid ICMP code has been detected.	4	Correlation Group 2	Scenario 2
TCP port	Indicates a TCP packet using a reserved port for source or destination.	4	Correlation Group 2	Scenario 2
UDP port	Indicates a UDP packets using a reserved port for source or destination.	4	Correlation Group 2	Scenario 2
Hostile IP	Indicates the use of a known hostile IP address.	4	Correlation Group 2	Scenario 2
Watch list IP	Indicates the use of an IP address from a watch list of IP addresses.	4	Correlation Group 2	Scenario 2
Known offender IP	Indicates the use of an IP address of a known offender.	4	Correlation Group 2	Scenario 2
RFC 1918 (private) IP	Indicates the use of an IP address from a private IP address range.	4	Correlation Group 2	Scenario 2
Potential VoIP Vulnerability	Indicates a potential VoIP vulnerability.	4	Correlation Group 2	Scenario 2

System

The system category indicates that the nature of threat is unknown but the behavior is suspicious including protocol anomalies potentially indicating evasive techniques. The associated low-level event categories include:

Table 2-15 System Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown System Event	Indicates an unknown system event.	1	Correlation Group 5	Scenario 2
System Boot	Indicates a system boot.	1	Correlation Group 5	Scenario 2
System Configuration	Indicates a change in the system configuration.	1	Correlation Group 5	Scenario 2
System Halt	Indicates the system has been halted.	1	Correlation Group 5	Scenario 2
System Failure	Indicates a system failure.	6	Correlation Group 5	Scenario 2
System Status	Indicates any information event.	1	Correlation Group 5	Scenario 2
System Error	Indicates a system error.	3	Correlation Group 5	Scenario 2
Misc System Event	Indicates a miscellaneous system event.	1	Correlation Group 5	Scenario 2

Table 2-15 System Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Service Started	Indicates system services have started.	1	Correlation Group 5	Scenario 2
Service Stopped	Indicates system services have stopped.	1	Correlation Group 5	Scenario 2
Service Failure	Indicates a system failure.	6	Correlation Group 5	Scenario 2
Successful Registry Modification	Indicates that a modification to the registry has been successful.	1	Correlation Group 5	Scenario 2
Successful Host-Policy Modification	Indicates that a modification to the host policy has been successful.	1	Correlation Group 5	Scenario 2
Successful File Modification	Indicates that a modification to a file has been successful.	1	Correlation Group 5	Scenario 2
Successful Stack Modification	Indicates that a modification to the stack has been successful.	1	Correlation Group 5	Scenario 2
Successful Application Modification	Indicates that a modification to the application has been successful.	1	Correlation Group 5	Scenario 2
Successful Configuration Modification	Indicates that a modification to the configuration has been successful.	1	Correlation Group 5	Scenario 2
Successful Service Modification	Indicates that a modification to a service has been successful.	1	Correlation Group 5	Scenario 2
Failed Registry Modification	Indicates that a modification to the registry has failed.	1	Correlation Group 5	Scenario 2
Failed Host-Policy Modification	Indicates that a modification to the host policy has failed.	1	Correlation Group 5	Scenario 2
Failed File Modification	Indicates that a modification to a file has failed.	1	Correlation Group 5	Scenario 2
Failed Stack Modification	Indicates that a modification to the stack has failed.	1	Correlation Group 5	Scenario 2
Failed Application Modification	Indicates that a modification to an application has failed.	1	Correlation Group 5	Scenario 2
Failed Configuration Modification	Indicates that a modification to the configuration has failed.	1	Correlation Group 5	Scenario 2
Failed Service Modification	Indicates that a modification to the service has failed.	1	Correlation Group 5	Scenario 2
Registry Addition	Indicates that an new item has been added to the registry.	1	Correlation Group 5	Scenario 2
Host-Policy Created	Indicates that a new entry has been added to the registry.	1	Correlation Group 5	Scenario 2

Table 2-15 System Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
File Created	Indicates that a new has been created in the system.	1	Correlation Group 5	Scenario 2
Application Installed	Indicates that a new application has been installed on the system.	1	Correlation Group 5	Scenario 2
Service Installed	Indicates that a new service has been installed on the system.	1	Correlation Group 5	Scenario 2
Registry Deletion	Indicates that a registry entry has been deleted.	1	Correlation Group 5	Scenario 2
Host-Policy Deleted	Indicates that a host policy entry has been deleted.	1	Correlation Group 5	Scenario 2
File Deleted	Indicates that a file has been deleted.	1	Correlation Group 5	Scenario 2
Application Uninstalled	Indicates that an application has been uninstalled.	1	Correlation Group 5	Scenario 2
Service Uninstalled	Indicates that a service has been uninstalled.	1	Correlation Group 5	Scenario 2
System Informational	Indicates system information.	3	Correlation Group 5	Scenario 2
System Action Allow	Indicates that an attempted action on the system has been authorized.	3	Correlation Group 5	Scenario 2
System Action Deny	Indicates that an attempted action on the system has been denied.	4	Correlation Group 5	Scenario 2

Policy The policy category indicates events relating to system changes, software installation, or status messages. The associated low-level event categories include:

Table 2-16 Policy Categories

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown Policy Violation	Indicates an unknown policy violation.	2	Correlation Group 4	Scenario 2
Web Policy Violation	Indicates a web policy violation.	2	Correlation Group 4	Scenario 2
Remote Access Policy Violation	Indicates a remote access policy violation.	2	Correlation Group 4	Scenario 2
IRC/IM Policy Violation	Indicates an instant messenger policy violation.	2	Correlation Group 4	Scenario 2

Table 2-16 Policy Categories (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
P2P Policy Violation	Indicates a Peer-to-Peer (P2P) policy violation.	2	Correlation Group 4	Scenario 2
IP Access Policy Violation	Indicates an IP access policy violation.	2	Correlation Group 4	Scenario 2
Application Policy Violation	Indicates an application policy violation.	2	Correlation Group 4	Scenario 2
Database Policy Violation	Indicates a database policy violation.	2	Correlation Group 4	Scenario 2
Network Threshold Policy Violation	Indicates a network threshold policy violation.	2	Correlation Group 4	Scenario 2
Porn Policy Violation	Indicates a porn policy violation.	2	Correlation Group 4	Scenario 2
Games Policy Violation	Indicates a games policy violation.	2	Correlation Group 4	Scenario 2
Misc Policy Violation	Indicates a miscellaneous policy violation.	2	Correlation Group 4	Scenario 2
Compliance Policy Violation	Indicates a compliance policy violation.	2	Correlation Group 4	Scenario 2
Mail Policy Violation	Indicates a mail policy violation.	2	Correlation Group 4	Scenario 2
IRC Policy Violation	Indicates an IRC policy violation	2	Correlation Group 4	Scenario 2
IM Policy Violation	Indicates a policy violation related to instant messaging (IM) activities.	2	Correlation Group 4	Scenario 2
VoIP Policy Violation	Indicates a VoIP policy violation	2	Correlation Group 4	Scenario 2

CRE The CRE category indicates events generated from a custom offense or event rule. The associated low-level event categories include:

Table 2-17 CRE Category

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown CRE Event	Indicates an unknown custom rules engine event.	5	No event pass-through	Scenario 1
Single Event Rule Match	Indicates a single event rule match.	5	No event pass-through	Scenario 1
Event Sequence Rule Match	Indicates an event sequence rule match.	5	No event pass-through	Scenario 1

Table 2-17 CRE Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Cross-Offense Event Sequence Rule Match	Indicates a cross-offense event sequence rule match.	5	No event pass-through	Scenario 1
Offense Rule Match	Indicates an offense rule match.	5	No event pass-through	Scenario 1

Potential Exploit The Potential Exploit category indicates events relating to potential application exploits and buffer overflow attempts. The associated low-level event categories include:

Table 2-18 Potential Exploit Category

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Unknown Potential Exploit Attack	Indicates a potential exploitative attack has been detected.	7	Correlation Group 1	Scenario 2
Potential Buffer Overflow	Indicates a potential buffer overflow has been detected.	7	Correlation Group 1	Scenario 2
Potential DNS Exploit	Indicates a potentially exploitative attack through the DNS server has been detected.	7	Correlation Group 1	Scenario 2
Potential Telnet Exploit	Indicates a potentially exploitative attack through Telnet has been detected.	7	Correlation Group 1	Scenario 2
Potential Linux Exploit	Indicates a potentially exploitative attack through Linux has been detected.	7	Correlation Group 1	Scenario 2
Potential Unix Exploit	Indicates a potentially exploitative attack through Unix has been detected.	7	Correlation Group 1	Scenario 2
Potential Windows Exploit	Indicates a potentially exploitative attack through Windows has been detected.	7	Correlation Group 1	Scenario 2
Potential Mail Exploit	Indicates a potentially exploitative attack through mail has been detected.	7	Correlation Group 1	Scenario 2
Potential Infrastructure Exploit	Indicates a potential exploitative attack on the system infrastructure has been detected.	7	Correlation Group 1	Scenario 2
Potential Misc Exploit	Indicates a potentially exploitative attack has been detected.	7	Correlation Group 1	Scenario 2

Table 2-18 Potential Exploit Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
Potential Web Exploit	Indicates a potentially exploitative attack through the web has been detected.	7	Correlation Group 1	Scenario 2
Potential Botnet connection	Indicates a potentially exploitative attack using Botnet has been detected.	6	Correlation Group 1	Scenario 2
Potential worm activity	Indicates a potentially exploitative attack using worm activity has been detected.	6	Correlation Group 1	Scenario 2

SIM Audit

The SIM Audit events category indicates events related to user interaction with the Console and the Administration Console. User logins and configuration changes will generate events that are sent to the Event Collector, which correlates with other security events from the network. The associated low-level event categories include:

Table 2-19 SEM Audit Event Category

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
SIM User Authentication	Indicates a user login or logout on the Console.	5	Correlation Group 5	Scenario 2
SIM Configuration Change	Indicates that a user has made a change to the SIM configuration or deployment.	3	Correlation Group 5	Scenario 2
SIM User Action	Indicates that a user has initiated a process in the SIM module. This may include starting a backup process or generated a report.	3	Correlation Group 5	Scenario 2

VIS Host Discovery

When the VIS component discovers and stores new hosts, ports, or vulnerabilities detected on the network, the VIS component generates events. These events are sent to the Event Collector to be correlated with other security events.

The associated low-level event categories include:

Table 2-20 VIS Host Discovery Category

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
New Host Discovered	Indicates that the VIS component has detected a new host.	3	Correlation Group 5	Scenario 2

Table 2-20 VIS Host Discovery Category (continued)

Low Level Event Category	Description	Severity Level (0 to 10)	Event Correlation/ Processing	Additional Event Processing
New Port Discovered	Indicates that the VIS component has detected a new open port.	3	Correlation Group 5	Scenario 2
New Vuln Discovered	Indicates that the VIS component has detected a new vulnerability.	3	Correlation Group 5	Scenario 2
New OS Discovered	Indicates that the VIS component has detected a new operating system on a host.	3	Correlation Group 5	Scenario 2
Bulk Host Discovered	Indicates that the VIS component has detected many new hosts in a short period of time.	3	Correlation Group 5	Scenario 2