



Temasek Polytechnic School of Informatics & IT

Introduction to Security Incident Response & Management

Security Incident Investigation in a SOC Environment with IBM QRadar SIEM
(Part B - 1.5 HRS)

(Important Note: Notes are given mainly for reference. Emphasis will be on the hands-on demo / lab exercises)

References

References for Cyber Security Incident Response & Management Concepts:

Relevant NIST/CMU SEI Guides:

- NIST SP 800-61 - Computer Security Incident Handling Guide (both Revisions 1 & 2)
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-83 - Guide to Malware Incident Prevention and Handling
- RFC 3227 - Guidelines for Evidence Collection and Archiving
- CMU/SEI - Organizational Models for Computer Security Incident Response Teams (CSIRTs)
- CMU/SEI - Handbook for Computer Security Incident Response Teams (CSIRTs)
- CMU/SEI - First Responders to Computer Forensics

References

References for Network Traffic Forensics & IBM Security QRadar SIEM:

- Bejtlich, R. (2013).
The practice of network security monitoring: Understanding incident detection and response.
San Francisco, CA: No Starch Press, Inc.
- Davidoff, S., & Ham, J. (2012).
Network Analysis: Tracking Hackers Through Cyberspace.
Upper Saddle River, NJ: Prentice Hall.
- Lillard, T.V., Garrison, C. P., Schiller, C. A., & Steele, J. (2010).
Digital forensics for network, internet, and cloud computing: A forensic evidence guide for moving targets and data.
Burlington, MA.: Syngress.
- Sanders, C. (2011).
Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems (2nd Ed.).
San Francisco, CA.: No Starch Press.
- Relevant IBM SIEM training modules:
 - *IBM Security Intelligence Fundamentals (BQ600)*
 - *IBM Security QRadar SIEM Foundations (BQ102)*
 - *IBM Security QRadar SIEM 7.2 Administration and Configuration (XIS08)*



Disclaimer for Copyright

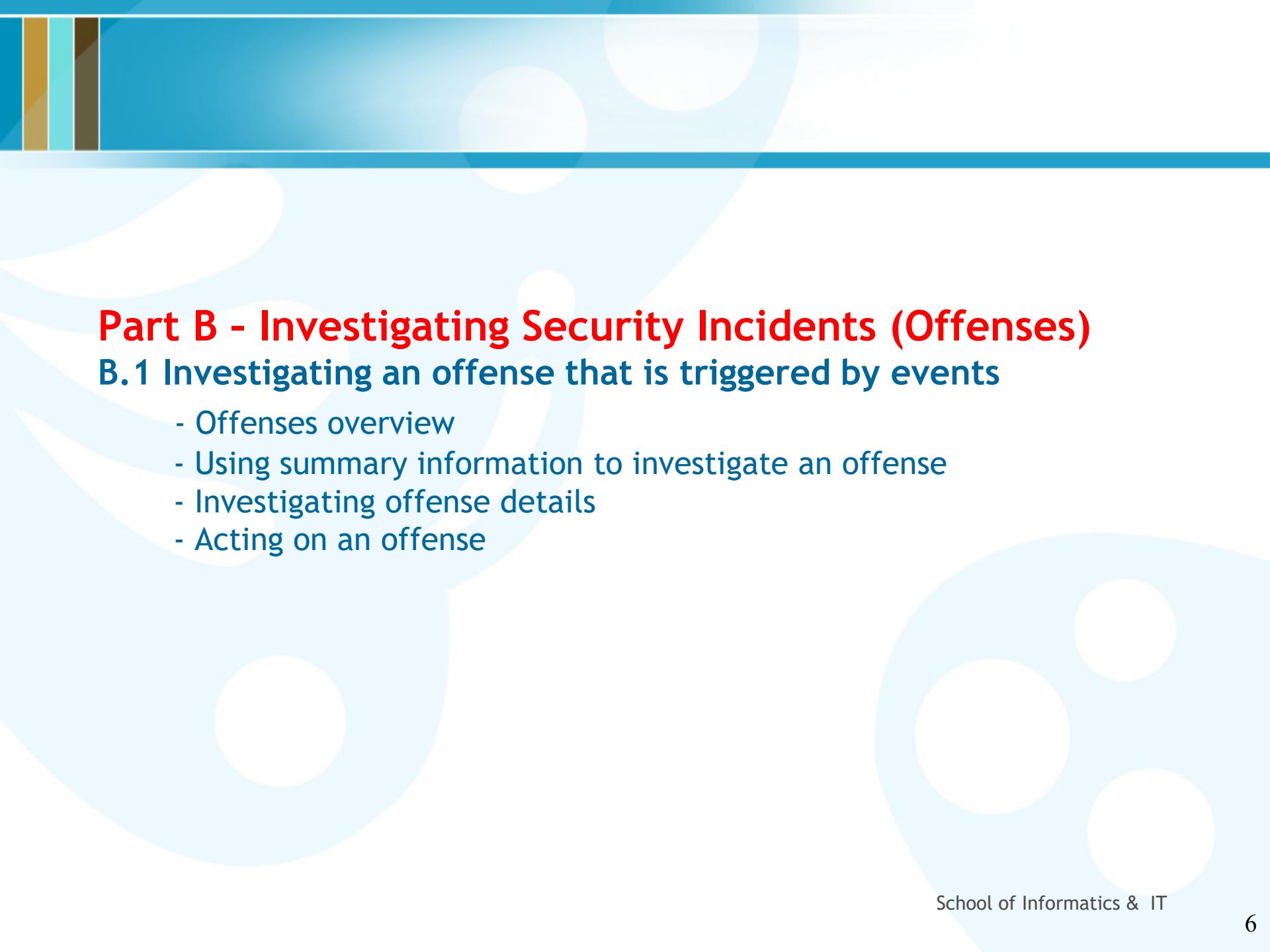
- All copyrights and other intellectual property rights in the course materials (course notes, lab exercises, etc.) are reserved and shall remain with the original owner(s).



Use of IBM Security QRadar SIEM in a SOC Environment

(Part B) - Investigating Security Incidents (Offenses)

- B.1 Investigating an offense that is triggered by events
- B.2 Investigating the events of an offense
- B.3 Investigating an offense that is triggered by flows



Part B - Investigating Security Incidents (Offenses)

B.1 Investigating an offense that is triggered by events

- Offenses overview
- Using summary information to investigate an offense
- Investigating offense details
- Acting on an offense



Objectives

- Explain the concept of offenses
- Investigate an offense, which includes this information
 - Summary information
 - The details of an offense
- Respond to an offense



Offenses overview

Introduction to offenses

- The prime benefit of QRadar SIEM for security analysts is that it detects suspicious activities and ties them together into *offenses*
- An offense represents a suspected attack or policy breach; some common offenses include these examples
 - Multiple login failures
 - Worm infection
 - P2P traffic
 - Scanner reconnaissance
- Treat offenses as security incidents and have a security analyst investigate them

© Copyright IBM Corporation 2015

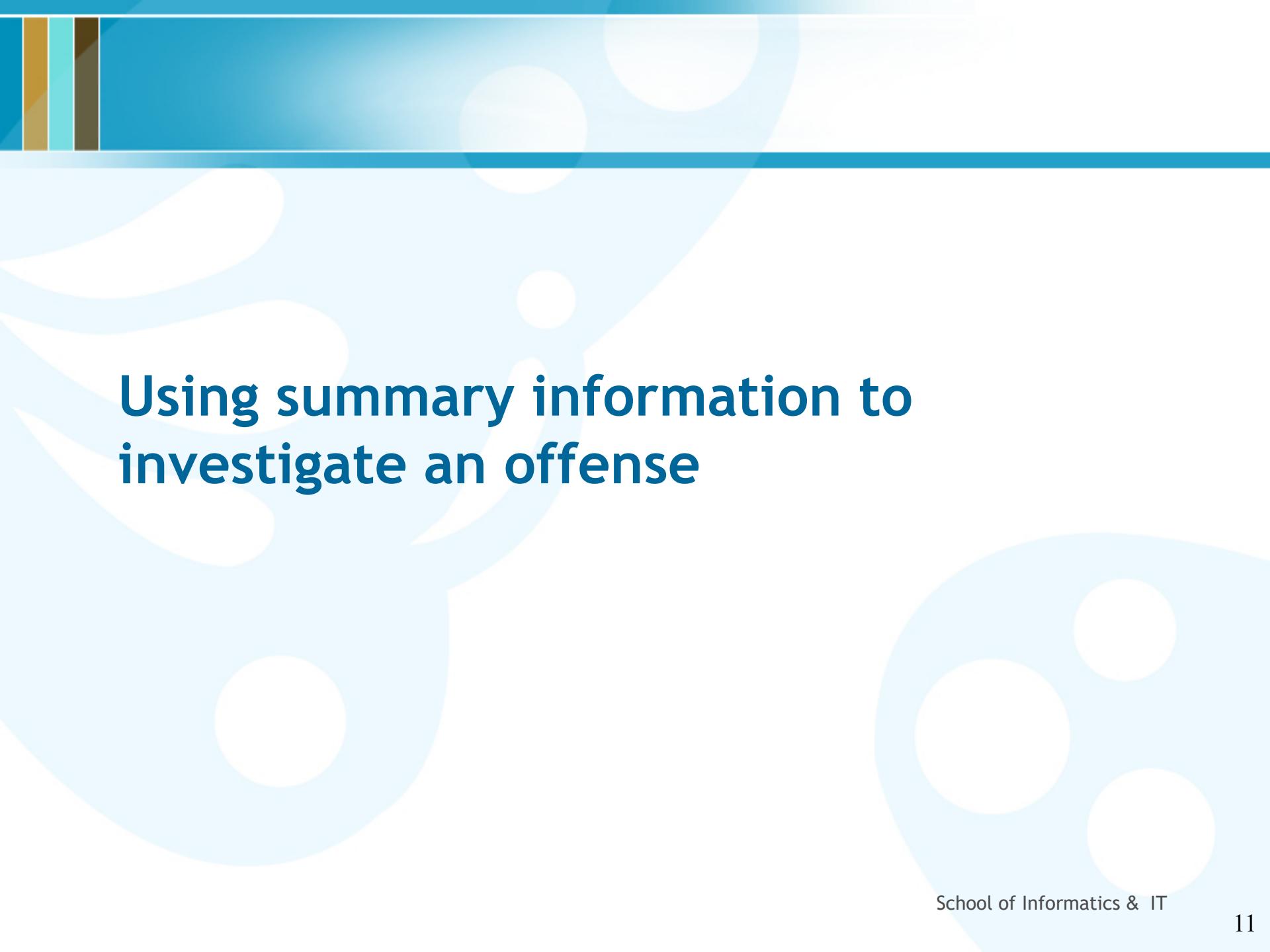
Introduction to offenses

Creating and rating offenses

Creating and rating offenses

- QRadar SIEM creates an offense when events, flows, or both meet the test criteria specified in changeable **rules** that analyze the following information
 - Incoming events and flows
 - Asset information
 - Known vulnerabilities
- The **magistrate** in QRadar SIEM rates each offense by its **magnitude**, which has these characteristics
 - Ranges from 1 to 10, with 1 being low and 10 being high
 - Specifies the relative importance of the offense

© Copyright IBM Corporation 2015



Using summary information to investigate an offense

Selecting an offense to investigate

Offenses are listed in these locations

- In Dashboard items
- In the Offense Manager on the **Offenses** tab

The screenshot shows the IBM QRadar Security Intelligence web interface. At the top, there's a navigation bar with tabs: Dashboard, Offenses (which is selected and highlighted in blue), Log Activity, Network Activity, Assets, Reports, and Admin. Below the navigation bar, on the left, is a sidebar with a tree menu under the 'Offenses' heading. The tree includes 'My Offenses', 'All Offenses', 'By Category', 'By Source IP', 'By Destination IP', 'By Network', and 'Rules'. On the right, the main content area has a search bar at the top with fields for 'Search...', 'Save Criteria', 'Actions', and 'Print'. Below the search bar, there are buttons for 'All Offenses' and 'View Offenses' followed by a dropdown menu labeled 'Select An Option'. A section titled 'Current Search Parameters:' contains two buttons: 'Exclude Hidden Offenses (Clear Filter)' and 'Exclude Closed Offenses (Clear Filter)'. The main part of the screen is a table listing offenses. The table has columns for Id, Description, Offense Type, Offense Source, and Magnitude. There are 7 rows of data:

#	Description	Offense Type	Offense Source	Magnitude
3	Large ping	Event Name	Large ping	High
7	Local UDP Scanner Detected containing HTTPWeb	Source IP	10.20.0.80	Medium
2	Login Failures Followed By Success from the same Source IP preceded by Large ping	Source IP	10.0.120.10	Medium
1	Multiple Login Failures to the Same Destination preceded by Large ping	Destination IP	10.0.120.10	Medium
6	Multiple Login Failures to the Same Destination preceded by Login Failures Followed By Success from the same Source IP preceded by Large ping	Destination IP	10.0.120.11	Medium
4	Multiple Login Failures for the Same User containing Logon Failures Followed By Success from the same Source IP preceded by Large ping	Username	nina	Medium
5	Multiple Login Failures for the Same User containing MSSQL Logon Failures Followed By Success from the same Source IP preceded by Large ping	Username	sqladmin	Medium

Selecting an offense to investigate

Selecting an offense to investigate (cont.)

This slide presents the **Offenses** tab:

- The default view of the **Offenses** tab is called **Offense Manager**.
- Double-click an offense to view the detailed **Offense Summary** of that offense.
- Use the left navigation to view the offenses from different perspectives. For example, select **Offenses by Source IP** or **Offenses by Destination IP** to view this information:
 - Repeat offenders
 - IP addresses that generate a multitude of events
 - Systems that are continually under attack
- Use the **Search** menu to find offenses according to search criteria.

Offense Summary window

Offense Summary window

The offense summary displays information about the ICMP scanning offense

The remainder of the unit examines the window sections in the same way as the security analyst does to investigate an offense.

The screenshot shows the Offense Summary window with the following sections:

- Offense ID:** Shows details for Offense ID 10000000000000000000000000000000, including Description, Status, Offense Type, and Offense IP.
- Offense Source Summary:** Lists source IP (10.127.10.31), location (Web-30-302-100-248.10.31.21.2), and interface (eth0).
- Last 10 Events:** A table showing recent events with columns: Date, Offense ID, and Offense Type.
- Top 4 Resource IPs:** A table showing top resource IPs with columns: Source IP, Magnitude, Location, Value, User, MAC, Weight, Offense ID, Last Event Time, and Event ID.
- Top 4 Destination IPs:** A table showing top destination IPs with columns: Destination IP, Magnitude, Location, Value, User, MAC, Weight, Offense ID, Out, Last Event Time, and Event ID.
- Top 5 Log Services:** A table showing top log services with columns: Name, Description, Group, CreationTime, Offense ID, and LastEventTime.
- Top 5 Users:** A table showing top users with columns: Name, CreationDate, Offense ID, and LastEventDate.
- Last 10 Offenses:** A table showing recent offenses with columns: Offense ID, Description, Offense Type, CreationTime, LastEventTime, and Offense ID.
- Last 10 Events:** A table showing recent events with columns: Event ID, Offense ID, Log Service, Category, Offense ID, and Time.
- Last 10 Flows:** A table showing recent flows with columns: Application, Source IP, Source Port, Destination IP, Destination Port, Total Bytes, and Last Packet Time.
- Last 5 Annotations:** A table showing recent annotations with columns: Annotation, Time, and Weight.

© Copyright IBM Corporation 2015

Offense Summary window

Offense Summary window (cont.)

The Offense Summary window includes these sections:

- Offense Parameters
- Offense Source Summary
- Last 5 Notes
- Top 5 Source IPs
- Top 5 Destination IPs
- Top 5 Log Sources
- Top 5 Users
- Top 5 Categories
- Top 10 Events
- Top 10 Flows
- Top 5 Annotations

We review these sections in the remainder of the unit.

Offense parameters (1 of 4)

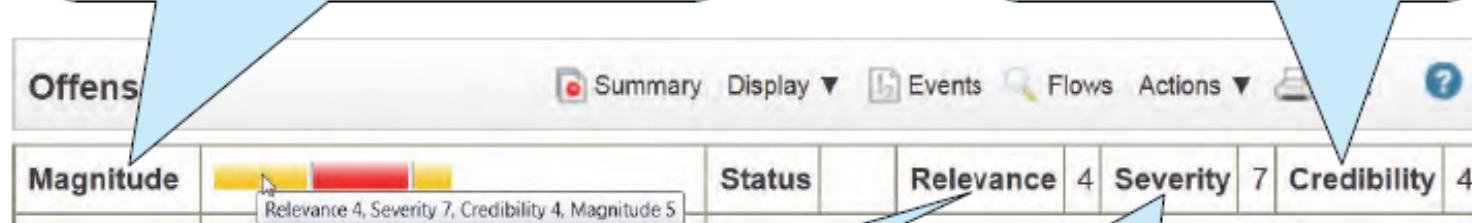
Investigating an offense begins with the parameters at the top of the offense summary window

Magnitude:

Relative importance of the offense, as calculated from relevance, severity, and credibility

Credibility:

How valid is information from that source?
20% of magnitude



Relevance:

How important is the destination?
50% of magnitude

Severity:

How high is the potential damage to the destination?
30% of magnitude

© Copyright IBM Corporation 2015

Offense parameters

Offense parameters (2 of 4)

Offense Type:

General root cause of the offense; the offense type determines which information is displayed in the next section of the Offense Summary

Magnitude	  	Status	Relevance 4	Severity 7	Credibility 4
Description	Local ICMP Scanner preceded by Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewall Deny	Offense Type	Source IP		
		Event/Flow count	410 events and 0 flows in 3 categories		

Description:

Reflects the causes for the offense; the description can change when new events or flows are associated with the offense

Event count:
Number of events associated with this offense

Flow count:
Number of flows associated with this offense

© Copyright IBM Corporation 2015

Offense Types

Offense Type: The rule that created the offense determines the one of the following Offense Types:

- Event Name
- Destination MAC Address
- Source Port
- Destination IPv6
- Rule
- Source IP Identity
- Source IP
- Username
- Log Source
- Destination Port
- Source ASN
- App ID
- Destination IP
- Source MAC Address
- Host Name
- Source IPv6
- Destination ASN

Offense parameters (3 of 4)

Magnitude	Severity	Start	Relevance	Severity	Credibility
Description	Local ICMP Scanner preceded by Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewall Deny	Offense Type	Source IP		
Source IP(s)	<u>10.127.15.37</u>	Event count	<u>410 events</u> and <u>0 flows</u> in 3 categories		
Destination IP(s)	<u>Local (2) Remote (360)</u>	Start	Jul 31, 2013 9:42:44 AM		
		Duration	41m 27s		

Destination IP(s):
Targets of the ICMP scanning

Duration:
Amount of time elapsed since the first event or flow associated with the offense was created

© Copyright IBM Corporation 2015

Offense parameters (3 of 4)

Offense parameters (4 of 4)

Magnitude	 	Status	Relevance 4	Severity 7	Credibility 4
Description	Local ICMP Scanner preceded by Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewall Deny	Offense Type	Source IP		
		Event/Flow count	410 events and 0 flows in 3 categories		
Source IP(s)	10.127.15.37	Start	Jul 31, 2013 9:42:44 AM		
Destination IP(s)	Local (2) Remote (360)	Duration	41m 27s		
Network(s)	Multiple (2)	Assigned to	Unassigned		

Network(s):
Local networks of the local Destination IPs that have been scanned

Assigned to:
QRadar SIEM user assigned to investigate this offense

© Copyright IBM Corporation 2015

Offense parameters (4 of 4)

Investigating offense details

Notes

QRadar SIEM users can add notes to offenses

- You cannot edit or delete notes
- The maximum length is 2000 characters

The screenshot shows a user interface for managing notes in QRadar SIEM. At the top, there are two blue speech bubble buttons: 'Notes: View all notes of the offense' and 'Add Note: Create new note'. Below them is a table titled 'Last 5 Notes' with three columns: 'Notes', 'Username', and 'Creation Date'. A single row of data is shown: 'compromised host disconnected from network' (Notes), 'lynette' (Username), and 'Jul 31, 2013 6:06 PM' (Creation Date). At the bottom right of the table area are two small buttons: 'Notes' and 'Add Note', each with a yellow exclamation mark icon.

Notes	Username	Creation Date
compromised host disconnected from network	lynette	Jul 31, 2013 6:06 PM

© Copyright IBM Corporation 2015

Notes

Top 5 Source IPs

QRadar SIEM lists the five IP addresses with the highest magnitude, which is where the suspected attack or policy breach originates

Location:

Hover the mouse over a shortened field value to display the full value

Sources:

View all source IP addresses of the offense

Top 5 Source IPs											Sources
Source IP	Magn...	Location	Vuln...	User	MAC	Weight	Off...	Dest...	Last Event/Flow	Events/Flows	
10.127.15.37	██████	Net-10-... Net-10-172-192.Net_10_0_0_0	No	Unknown	Unknown NIC	0	1	2	4h 39m 37s	410	

Note: The table contains only one row because the example offense has only one source IP address

© Copyright IBM Corporation 2015

Top 5 Source IPs

Top 5 Source IPs (cont.)

Right-click anywhere on the row to view more information about the source IP address

The screenshot shows a table titled "Top 5 Source IPs". The first row contains the following data:

Source IP	Magn...	Location	Vuln...	User	MAC	Weight	Off...	Dest...	Last Event/Flow	Events/Flows
10.127.15.37	Yellow	Net-10...	No	Unknown	Unknown NIC	0	1	2	4h 39m 37s	410

A context menu is open over the first row, with the "View" option highlighted. The menu includes "Destinations" and "Offenses".

Destinations:
List all destination IP addresses targeted by the source IP address

Offenses:
List all offenses for which the source IP address is source or destination IP address

© Copyright IBM Corporation 2015

Top 5 Source IPs (continued)

Top 5 Destination IPs

QRadar SIEM lists the five local IP addresses with the highest magnitude, which were targets of the ICMP scan

Chained:

Indicates whether the destination IP address is the source IP address in another offense

Destinations:

View all destinations IP addresses of the offense

Top 5 Destination IPs											
Destination IP	Magn...	Location	Vuln...	Chained	User	MAC	Weight	Off...	Sou...	Last Event/Flow	Events/Flows
MORIA	██████	Net-10...	YES	No	maqda	00:30:18:AF:0B:83	0	1	1	4h 52m 46s	3
10.26.1	Network: 10.26.1	Net-10-172-192.Net_10_0_0_0	Destination Magnitude: ██████████ (0/10)	Offenses: 1	Asset Name: MORIA	Detected IP(s): [10.26.10.5]	Detected MAC(s): [00:30:18:AF:0B:83]	Operating System: UNIX	User Name: N/A		

Right click for more information on MORIA

Destination IP:

Hover the mouse over the asset name or IP address to display further information

Note: The table contains only two rows because only two local IP addresses were scanned

© Copyright IBM Corporation 2015

Top 5 Destination IPs

Top 5 Log Sources

A firewall provided the log messages about firewall denies; this firewall is the major log source of the ICMP scanner offense

Events:

Number of events sent by the log source contributing to the offense

Log Sources:

View all log sources contributing to the offense

Top 5 Log Sources						Log Sources
Name	Description	Group	Events/Flows	Offenses	Total Events/Flows	
CheckPoint @ FW-1Machine	CheckPoint device		393	24	9181	
Custom Rule Engine-8 :: COE	Custom Rule Engine		17	23	51	

Custom Rule Engine:
The QRadar SIEM CRE creates events and adds them to offenses

Offenses:
Number of offenses related to the log source

Total Events:
Sum of all events received from this log source while the offense is active

© Copyright IBM Corporation 2015

Top 5 Log Sources

Top 5 Users

QRadar SIEM lists the five users with the most events contributing to the offense

Users:

View all users associated to the offense

Top 5 Users			
Name	Events/Flows	Offenses	Total Events/Flows
No results were returned.			

Note: In this example, QRadar SIEM did not receive an event with user information and therefore does not list a user

© Copyright IBM Corporation 2015

Top 5 Users

Top 5 Categories

QRadar SIEM categorized most events into the Firewall Deny category; from this categorization and the nature of the events, rules deduced the ICMP scanning

Categories:
View all low-level categories of the events contributing to the offense

Top 5 Categories							 Categories
Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow		
Network Sweep		0	11	Jul 31, 2013 9:47:17 AM	Jul 31, 2013 10:22:56 AM		
Firewall Deny		2	393	Jul 31, 2013 9:47:16 AM	Jul 31, 2013 10:22:52 AM		
ICMP Reconnaissance		0		Jul 31, 2013 9:48:57 AM	Jul 31, 2013 10:20:41 AM		

Name:
Low-level category of the event

Local Destination Count:
Number of local destination IP addresses affected by offenses with events in this category

© Copyright IBM Corporation 2015

Top 5 Categories

Top 5 Categories (cont.)

Right-click anywhere on the row to view events and flows

Top 5 Categories							 Categories
Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow		
Network Sweep		0	11	Jul 31, 2013 9:47:17 AM	Jul 31, 2013 10:22:56 AM		
Firewall Deny		2	393	2013 9:47:16 AM	Jul 31, 2013 10:22:52 AM		
ICMP Reconnaissance		0	6	2013 9:48:57 AM	Jul 31, 2013 10:20:41 AM		

Events:

List all events that contribute to the viewed offense in the category under the mouse pointer

Flows:

List all flows that contribute to the viewed offense in the category under the mouse pointer

© Copyright IBM Corporation 2015

Top 5 Categories (continued)

Last 10 Events

Double-click anywhere on a row to open a window with details about the event

Dst Port:
The destination port is 0 for layer 3 protocol traffic such as ICMP

Events:
View all events that contribute to the offense

Last 10 Events						
Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.251	0	Jul 31, 2013 10:23:50 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.252	0	Jul 31, 2013 10:23:48 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.253	0	Jul 31, 2013 10:23:41 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.254	0	Jul 31, 2013 10:23:36 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.144.1	0	Jul 31, 2013 10:23:29 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.144.2	0	Jul 31, 2013 10:23:19 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.144.3	0	Jul 31, 2013 10:23:08 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.144.4	0	Jul 31, 2013 10:23:03 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.242	0	Jul 31, 2013 10:24:11 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.244	0	Jul 31, 2013 10:24:07 AM

© Copyright IBM Corporation 2015

Last 10 Events

Last 10 Flows

No flows contributed to the ICMP scanner offense; therefore, QRadar SIEM does not list any flows

Total Bytes:
Sum of bytes transferred in both directions

Flows:
View all flows that contribute to the offense

Last 10 Flows						
Application	Source IP	Source Port	Destination IP	Destination Port	Total Bytes	Last Packet Time
No results were returned.						

© Copyright IBM Corporation 2015

Last 10 Flows

Annotations

- Annotations provide insight into why QRadar SIEM considers the event or observed traffic threatening
- QRadar SIEM can add annotations when it adds events and flows to an offense
- Read the oldest annotation because it was added when the offense was created

Annotation:

Hold the mouse over a shortened annotation to show the full annotation

Annotations:

View all annotations of the offense

Top 5 Annotations		
Annotation	Time	Weight
"CRE Event". CRE Rule description: [Local ICMP Scanner] Detected a source IP address attempting reconnaissance or suspicious connections on common ICMP ports to more than 60 hosts in 10 minutes.	Jul 31, 2013 10:08:59 AM	6
"[2] "Destination/Event Analysis". The number of events this source generated during this attack, ...	Jul 31, 2013 10:25:03 AM	6
"CRE Event". CRE Rule description: [Excessive Firewall Denies Across Multiple Hosts From A L...	Jul 31, 2013 9:47:49 AM	6

© Copyright IBM Corporation 2015

Annotations

Offense Summary toolbar

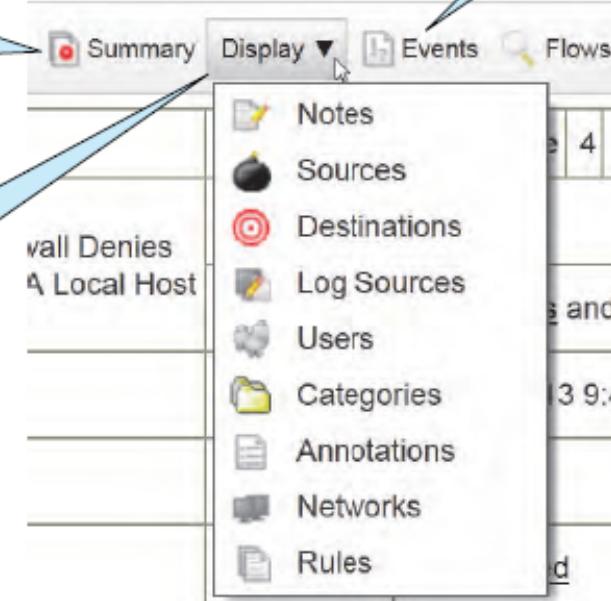
The Offense Summary toolbar provides direct links to the information that you just investigated

Events:
View all events contributing to the offense

Summary:
View the Offense Summary

Flows:
View all flows contributing to the offense

Display:
View offense information introduced on previous slides



© Copyright IBM Corporation 2015

Offense Summary toolbar



Acting on an offense

Offense actions

After investigating an offense, click **Actions** at the top of the Offense Summary page to set flags and status

The screenshot shows the QRadar SIEM Offense Summary page. At the top, there are tabs for Display, Events, Flows, and Actions. The Actions tab is currently selected, showing a dropdown menu with the following options: Follow up, Hide, Protect Offense, Close, Email, Add Note, and Assign. Below the menu, there is a table with offense details:

Status	Relevance	4	\$
Offense Type	Source IP		
Event/Flow count	411 events and		
Start	Jul 31, 2013 9:4		
Duration	46m 37s		
Assigned to	Unassigned		

Four callout boxes provide descriptions for each action:

- Follow up:** Choose if you want to revisit the offense
- Hide:** Use with caution because QRadar SIEM still updates the offense; alarming updates can stay hidden
- Protect Offense:** Prevent QRadar SIEM from deleting the offenses
- Close:** When you have resolved the offense, close it

© Copyright IBM Corporation 2015

Offense actions

Offense actions (cont.)



Note: All actions on the Offense Summary page are available on the **Offense** list except for **Email** and **Add Note**.

The **Actions** menu includes the following options:

- **Display:** Click to view offense information that was introduced on previous slides.
- **Hide:** An offense that is *hidden* by a QRadar SIEM user is also *hidden* for all other users.
 - The Offense Manager on the **Offenses** tab does not list *hidden* offenses by default.
 - To display *hidden* offenses, clear the **Exclude Hidden Offenses** filter.
 - An *inactive* offense can be hidden, but a *closed* offense cannot be *hidden*.
 - If a user closes a *hidden active* or *inactive* offense, QRadar SIEM displays it.

Offense actions (cont.)

- **Protect Offense** and status *inactive*: QRadar SIEM deletes unprotected offenses with an *inactive* status after the retention period elapses. Administrators can change the default retention period of three days.
 - QRadar SIEM changes an offense status from *active* to *inactive* under the following occurrences:
 - ◆ After the offense has been closed
 - ◆ After the offense does not receive an event or flow for five days
 - ◆ When the QRadar SIEM installation is upgraded
 - A protected *active* offense can become *inactive* but QRadar SIEM does not delete it. QRadar SIEM stores a protected *inactive* offense indefinitely until a QRadar SIEM user unprotects it.
 - An *inactive* offense cannot become *active* again. If an event or flow arrives that matches an *inactive* offense, QRadar SIEM creates a new offense.
 - Only QRadar SIEM can turn an offense *inactive*.
 - Only users can automatically protect, unprotect, hide, or close an offense.
- **Close**: When a QRadar SIEM user closes an offense, the offense moves from the status of *active* to *inactive and closed*.
- **Email and Add Note**: The **Email** and **Add Note** actions are available only on the Offense Summary page.
- **Assign**: Delegate the offense to another QRadar SIEM user.

Offense status and flags

Status: Icon indicates

- Protected
- Inactive
- Closed
- Follow up
- Notes
- Assigned

The actions available depend on the status of the offense

The screenshot shows a QRadar SIEM interface. At the top, there are tabs: Primary, Display ▾, Events, Flows, Actions ▾, Print, and a help icon. Below the tabs is a table with offense details:

Status	Relevance
Offense Type	Source IP
Event/Flow count	411 events and flows
Start	Jul 31, 2013 9:46 AM
Duration	46m 37s
Assigned to	lynnette

A blue callout points from the 'Status' column to a list of actions in the 'Actions' dropdown menu. The menu items are:

- Follow up
- Hide
- Unprotect Offense
- Close
- Email
- Add Note
- Assign

Unprotect Offense:
Allow QRadar SIEM
to delete this
protected offense

© Copyright IBM Corporation 2015

Offense status and flags

Investigating Security Incidents (Offenses)

B.1 Investigating an offense that is triggered by events

- Offense overview
- Using summary information to investigate an offense
- Investigating offense details
- Acting on an offense



Part B - Investigating Security Incidents (Offenses)

B.2 Investigating the events of an offense

- Investigating event details
- Using filters to investigate events
- Using grouping to investigate events
- Saving a search
- Modifying saved searches
- Adding a search to the dashboard



Objectives

- Use the list of events to navigate event details
- Filter events included in an offense
- Group events to gain different perspectives
- Save a search that monitors a suspicious host
- Modify a saved search
- Add a search to the dashboard

Investigating event details

Navigating to the events

In the Offense Summary, click **Events** to open the list of events

Events:
View all events
that contribute
to the offense

Last 10 Events						
Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.251	0	Jul 31, 2013 10:23:50 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.252	0	Jul 31, 2013 10:23:48 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.253	0	Jul 31, 2013 10:23:41 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.254	0	Jul 31, 2013 10:23:36 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.144.1	0	Jul 31, 2013 10:23:29 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.144.2	0	Jul 31, 2013 10:23:19 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.144.3	0	Jul 31, 2013 10:23:08 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.144.4	0	Jul 31, 2013 10:23:03 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.242	0	Jul 31, 2013 10:24:11 AM
Firewall Deny	██████	CheckPoint @ FW-1Machine	Firewall Deny	200.142.143.244	0	Jul 31, 2013 10:24:07 AM

© Copyright IBM Corporation 2015

Navigating to the events

List of events

Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel Help Monitor Rules Actions

Quick Filter Search

Viewing events from Oct 15, 2014, 4:31:00 AM to Oct 15, 2014, 4:35:00 AM View: Select An Option ▾ Display Default (Normalized) ▾ Results Limit ▾

Current Filters: Offense is Excessive Firewall Denies Across Multiple Hosts From A Local... (Clear Filter)

Completed Current Statistics

Records Matched Over Time 10/15/14 4:31 AM - 10/15/14 4:35 AM

Hide graphical charts

Update Details Hide Chart

Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source IP	Source Port	Destination IP	Dest Port	Username	Magnitude
Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:0...	Firewall Deny	10.28.72.209	N/A	10.108.10.2	N/A	N/A	■■■■■
Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:4...	Firewall Deny	10.28.72.209	N/A	172.22.6.6	N/A	N/A	■■■■■
Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:4...	Firewall Deny	10.28.72.209	58008	■■■■■ 197.0.0.10	0	N/A	■■■■■
Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:4...	Firewall Deny	10.28.72.209	58008	■■■■■ 197.0.0.11	0	N/A	■■■■■
Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:3...	Firewall Deny	10.28.72.209	N/A	10.108.10.2	N/A	N/A	■■■■■
Excessive Firewall Denies Across...	Custom Rule Engine-8 : COE	1	Oct 15, 2014, 4:32:3...	Network Sweep	10.28.72.209	N/A	N/A	N/A	N/A	■■■■■
Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:3...	Firewall Deny	10.28.72.209	N/A	10.108.10.2	N/A	N/A	■■■■■

View event details by double-clicking a row

© Copyright IBM Corporation 2015

List of events

Event details: Base information

Event Information:
Similar offense parameters

Event Information							
Event Name:	Firewall Deny						
Low Level Category:	Firewall Deny						
Event Description:	Firewall Deny						
Magnitude:	██████ (5)	Relevance:	6	Severity:	4	Credibility:	5
Username:	N/A						
Start Time:	Jul 31, 2013 10:08:22 AM	Storage Time:	Jul 31, 2013 10:08:22 AM	Log Source Time:	Jul 31, 2013 10:08:22 AM		
Policy:	N/A						

Source and Destination Information:
Most fields do not matter for this particular event because NAT and IPv6 were not used

Source and Destination Information			
Source IP:	10.127.15.37	Destination IP:	200.142.143.251
Source Asset Name:	N/A	Destination Asset Name:	N/A
Source Port:	N/A	Destination Port:	N/A
Pre NAT Source IP:		Pre NAT Destination IP:	
Pre NAT Source Port:	0	Pre NAT Destination Port:	0
Post NAT Source IP:		Post NAT Destination IP:	
Post NAT Source Port:	0	Post NAT Destination Port:	0
IPv6 Source:	0.0.0.0.0.0.0.0	IPv6 Destination:	0.0.0.0.0.0.0.0
Source MAC:	00:00:00:00:00:00	Destination MAC:	00:00:00:00:00:00

© Copyright IBM Corporation 2015

Event details: Base information

Event details: Base information

Event details: Base information

Typically, only a few fields in the event information and source and destination information areas include data.

- **Start Time:** The time when QRadar SIEM received the raw event from the log source
- **Storage Time:** The time when QRadar SIEM stored the normalized event in its database
- **Log Source Time:** The time that is recorded in the raw event

Event details: Reviewing the raw event

Each normalized event carries its raw event as the payload

Payload Information

utf hex base64

Wrap Text

```
<182>Nov 04 02:56:58 FW-1Machine
<158>logger: 22:11:39 drop
checkpoint.firewall-1.test.com >eth0 rule
205; rule_uid: {9EA7BC8D-
7FE5-4D60-9C89-4F949392E866};
profile: Default_Atlantis;
dst: 208.111.161.105; proto: tcp; product:
VPN-1 & FireWall-1; service: http;
s_port: 4696;
```

Review the raw event for information that QRadar SIEM has not normalized into fields, which therefore does not display in the UI

An example is the firewall profile name Default_Atlantis

© Copyright IBM Corporation 2015

Event details: Reviewing the raw event

Event details: Additional details

Protocol:
Network protocol

QID:
The QID determines the name, low-level category, and high-level category of an event

Additional Information

Protocol:	icmp_ip	QID:	2750010
Log Source:	CheckPoint @ FW-1Machine	Event Count:	1

Log Source:
This log source provided the raw event that QRadar SIEM normalized into this event

Event Count:
Number of raw events bundled into this normalized event

© Copyright IBM Corporation 2015

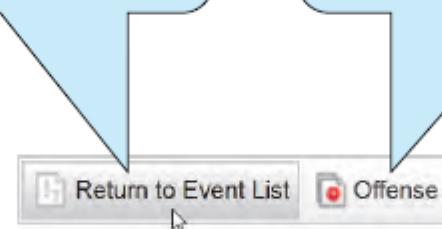
Event details: Additional details

Returning to the list of events

After investigating the event details, click **Return to Event List**, in the upper-left corner of the event details window, to return to the event list

Return to Event List:
Navigate to the list of events for the offense

Offense:
Navigate to the offense the event contributes to



Event Information

Event Name:	Firewall Deny
-------------	---------------

© Copyright IBM Corporation 2015

Returning to the list of events



Using filters to investigate events

Filtering events (1 of 3)

- In the list of events, you can use filters to explore the offense further
 - Most events in this offense are *Firewall Deny*
 - Because other events provide more insight, right-click the event name to filter for events that are not Firewall Deny

	Event Name	Log Source	Event Count
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	Filter on Event Name is Firewall Deny	1
	Firewall Deny	Filter on Event Name is not Firewall Deny	1
	Firewall Deny	False Positive	1
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	CheckPoint @ FW-1Machine	1

© Copyright IBM Corporation 2015

Filtering events

Filtering events (2 of 3)

By filtering **Firewall Deny** events, you can focus on events that do not originate from the firewall

	Event Name	Log Source
①	Local ICMP Scanner	Custom Rule Engine-8 :: COE
②	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
③	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
④	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
⑤	Local ICMP Scanner	Custom Rule Engine-8 :: COE
⑥	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
⑦	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
⑧	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
⑨	Local ICMP Scanner	Custom Rule Engine-8 :: COE

The Custom Rule Engine (CRE) in QRadar SIEM created the events in this list to alert you to suspicious activity

© Copyright IBM Corporation 2015

Filtering events (3 of 3)

Viewing events from Jul 31, 2013 9:25:00 AM to Jul 31, 2013 10:10:00 AM View:

Select An Option: ▾

Display: ▾

Default (Normalized) ▾

Original Filters:

Offense is Local ICMP Scanner , Excessive Firewall Denies Across Multipl... ([Clear Filter](#))

Current Filters:

Event Name is not Firewall Deny ([Clear Filter](#))

▶ Current Statistics

Clear Filter:

Click to view the Firewall Deny events again

	Event Name	Log Source
<input checked="" type="checkbox"/>	Local ICMP Scanner	Custom Rule Engine-8 :: COE
<input checked="" type="checkbox"/>	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
<input checked="" type="checkbox"/>	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE

Unlike searches, filters do not query each event processor

© Copyright IBM Corporation 2015

Applying a Quick Filter to the payload

- The payload of an event contains the raw event that mentions the firewall profile that denied the connection
- To verify that the company's main profile, Atlantis, was always active, filter events without **profile: Default_Atlantis** in the payload

Quick Filter:

Filter for events that do not contain
profile: Default_Atlantis in the
payload

Quick Filter

NOT "profile: Default_Atlantis"

Viewing events from Oct 23, 2014, 8:01:00 AM to Oct 23, 2014, 8:45:00 AM

View: Select An Option

Display: Default (Normal)

Current Filters:

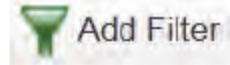
Offense is Local ICMP Scanner preceded by Excessive Firewall Denies A... [\(Clear Filter\)](#) Quick Filter is NOT "profile: Default_Atlantis" [\(Clear Filter\)](#)

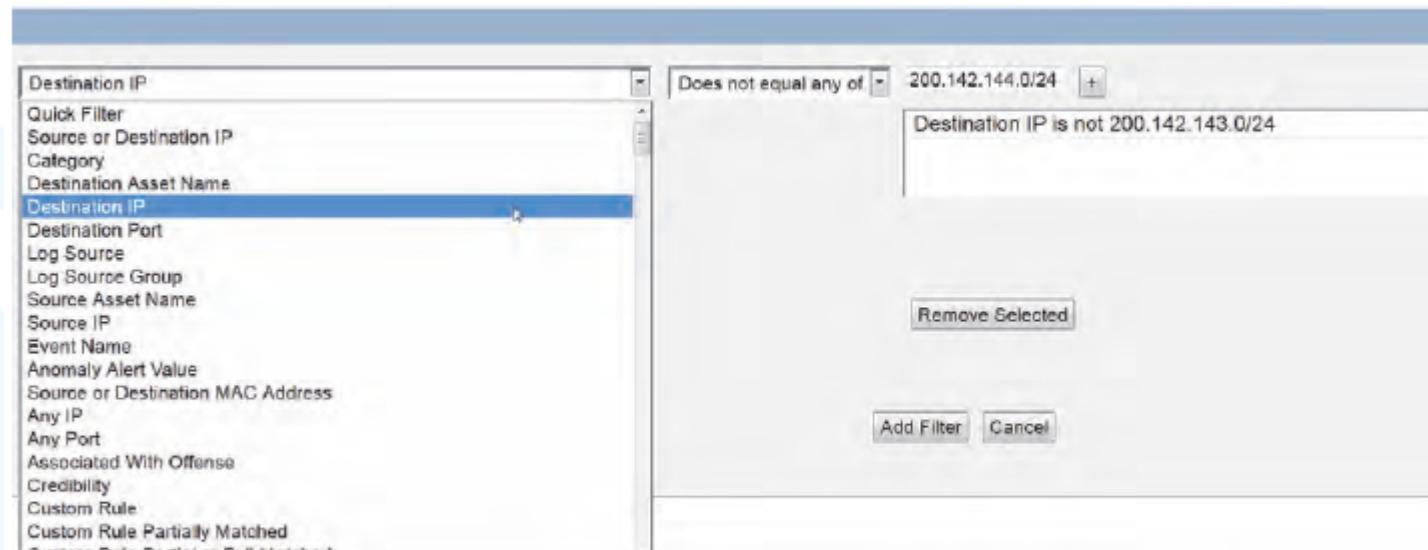
Clear Filter:

Click to view all events
of the offense again

Applying a Quick Filter to the payload

Using another filter option

- You can use each event field as a filter
- To create a filter, in the top menu bar, click the icon 



© Copyright IBM Corporation 2015

Using another filter option



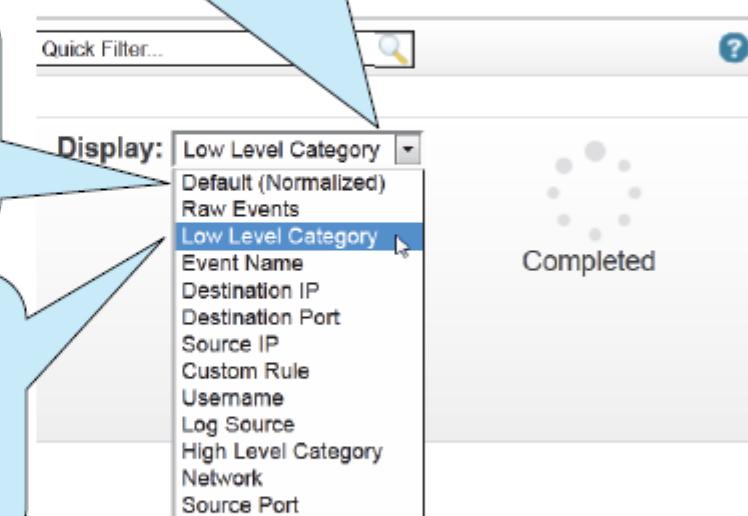
Using grouping to investigate events

Grouping events

Default (Normalized):
By default, QRadar SIEM shows normalized events without grouping

Raw Events:
Instead of grouping, QRadar SIEM shows the raw events stored in the payload of each normalized event

Display:
Explore the events further by grouping them; for example, group them by their **Low Level Category**



© Copyright IBM Corporation 2015

Grouping events

Grouping events by low-level category

Grouping By:

QRadar SIEM shows the currently selected grouping above the filters

The screenshot shows the QRadar SIEM interface. At the top, there is a search bar with the date range "Jul 31, 2013 9:25:00 AM to Jul 31, 2013 10:10:00 AM". Below it, a "View" dropdown says "Select An Option" and a "Display" dropdown is open, showing a list of categories. The "Low Level Category" option is selected. Other options in the list include Default (Normalized), Raw Events, Event Name, Destination IP, Destination Port, Source IP, Custom Rule, Username, Log Source, High Level Category, Network, and Source Port. On the left, a sidebar shows "Grouping" and "Low Level Category". In the main pane, under "Original Filters", it says "Offense is Local ICMP Scanner , Excessive Firewall Denies Across Multipl..." with a "(Clear Filter)" link. Below that is a "Current Statistics" section with a "(Show Charts)" link. The main table has columns: Low Level Category, Source IP (Unique Count), Destination IP (Unique Count), Destination Port (Unique Count), Event Name (Unique Count), Log Source (Unique Count), Protocol (Unique Count), Username (Unique Count), and Magnitude (Maximum). The data in the table is as follows:

Low Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destinat Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)
Firewall Deny	10.127.15.37	Multiple (380)	0	Firewall Deny	CheckPoint @ FW-1Machine	Multiple (2)	N/A	5
Network Sweep	10.127.15.37	Multiple (13)	0	Excessive Firewall...	Custom Rule Engine-8 :: COE	tcp_ip	N/A	8
ICMP Reconn...	10.127.15.37	Multiple (7)	0	Local ICMP Scanner	Custom Rule Engine-8	tcp_ip	N/A	4

All events are aggregated by their low-level category

In this example, exploring by grouping indicates a second protocol

Protocol:
Some events recorded an additional protocol; click Multiple (2)

© Copyright IBM Corporation 2015

Grouping events by low-level category

Grouping events by protocol

In the Protocol column, click **Multiple (2)** to open a window with events grouped by protocol; you learn that the firewall denied **udp_ip** in addition to **icmp_ip**

Grouping By:
QRadar SIEM can group by Protocol

Current Filters:
The previous grouping, Low Level Category, became a filter

Viewing events from Jul 31, 2013 9:25:00 AM to Jul 31, 2013 10:00 AM View: Select An Option: Display: Custom

Grouping By:
Protocol

Current Filters:
Offense is Local ICMP Scanner , Excessive Firewall Denies Across Multiple ... ([Clear Filter](#)).
Low Level Category is Firewall Deny ([Clear Filter](#))

▶ Current Statistics

(Show Charts)

Protocol	Event Name	Log Source	Event Count	Start Time	Low Level Category	Source IP	Source Port	Destination IP	Destin Port	Usern	Magni
icmp_ip	Firewall Deny	CheckPoint ...	405	7/31/13...	Firewall Deny	10.127.15.37	0	Multiple (378)	0	N/A	5
udp_ip	Firewall Deny	CheckPoint ...	7	7/31/13...	Firewall Deny	10.127.15.37	1055	Multiple (2)	0	N/A	5

© Copyright IBM Corporation 2015

Removing grouping criteria

Display:
Group by Default (Normalized)
to remove the grouping by Low Level Category

Viewing events from Jul 31, 2013 9:25:00 AM to Jul 31, 2013 10:10:00 AM View: Display: Raw Events Low Level Category Event Name Destination IP Destination Port Source IP Custom Rule Username Log Source High Level Category Network Source Port

Grouping By:
Low Level Category

Original Filters:
Offense Is Local ICMP Scanner , Excessive Firewall Denies Across Multipl... ([Clear Filter](#))

▶ Current Statistics

(Show Charts)

Low Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destinat Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)
Firewall Deny	10.127.15.37	Multiple (380)	0	Firewall Deny	CheckPoint @ FW-1Machine	Multiple (2)	N/A	5
Network Sweep	10.127.15.37	Multiple (13)	0	Excessive Firewall...	Custom Rule Engine-8 :: COE	icmp_ip	N/A	8
ICMP Reconn...	10.127.15.37	Multiple (7)	0	Local ICMP Scanner	Custom Rule Engine-8 :: COE	icmp_ip	N/A	4

© Copyright IBM Corporation 2015

Removing grouping criteria

Viewing a range of events

If events are still added to the investigated offenses, view them

- **Real Time (streaming)**: Shows events as they arrive at the Event Processor (EP); grouping and sorting are not available
- **Last Interval (auto refresh)**: Shows the last minute of events; refreshes automatically after 1 minute

Find Results Cancel False Positive Rules Actions

Select An Option: Display: Default (Normalized) Result

Real Time (streaming)
Last Interval (auto refresh)
Last 5 Minutes
Last 15 Minutes
Last 30 Minutes
Last 45 Minutes
Last Hour
Last 3 Hours
Last 6 Hours
Last 12 Hours
Last 24 Hours
Last 3 Days
Last 7 Days

Duration: 108ms
More Details

Time ▾ Low Level Category Source IP Source Port Destination IP Destination Port

results were returned.

© Copyright IBM Corporation 2015

Viewing a range of events

Saving a search

Monitoring the scanning host (1 of 3)

The event list always displays search results; to view traffic to and from the scanning host, edit this search, save it, and add it to the dashboard

Clear Filter:

To monitor all traffic, remove the offense filter

Current Filters:

Offense is Local ICMP Scanner , Excessive Firewall Denies Across Multipl... [\(Clear Filter\)](#)

Filter:

Right-click the Source IP to filter

[\(Show Charts\)](#)

Event Name	Log	Ev Co	Time ▾	Low Level Category	Source IP
Firewall Deny	CheckPoint @ FW- Machine	1	7/31/13 10:08:43 AM	Firewall Deny	10.127.15.37
Firewall Deny	CheckPoint @ FW-		Filter on Source IP is 10.127.15.37		127.15.37
Firewall Deny	CheckPoint @ FW-		Filter on Source IP is not 10.127.15.37		127.15.37
Local ICM...	Custom Rule Engin		Filter on Source or Destination IP is 10.127.15.37		127.15.37
Firewall Deny	CheckPoint @ FW-		False Positive		127.15.37
Firewall Deny	CheckPoint @ FW-		More options...		127.15.37

© Copyright IBM Corporation 2015

Monitoring the scanning host

Monitoring the scanning host (2 of 3)

The screenshot shows two dropdown menus side-by-side. The left menu is labeled 'View:' and has a list of time intervals. The right menu is labeled 'Display:' and has a list of categories. Both menus have a blue selection bar at the bottom.

View:	Display:
Select An Option:	High Level Category
Real Time (streaming)	Default (Normalized)
Last Interval (auto refresh)	Raw Events
Last 5 Minutes	Low Level Category
Last 15 Minutes	Event Name
Last 30 Minutes	Destination IP
Last 45 Minutes	Destination Port
Last Hour	Source IP
Last 3 Hours	Custom Rule
Last 6 Hours	Username
Last 12 Hours	Log Source
Last 24 Hours	High Level Category
Last 3 Days	Network
Last 7 Days	Source P

View:
List events of the last 24 hours

Display:
Group by High Level Category

© Copyright IBM Corporation 2015

Monitoring the scanning host (2 of 3)

Monitoring the scanning host (3 of 3)

Save Criteria:
Save the criteria of
the current search

Now the screen shows the selected time range, grouping, and filtering

The screenshot shows a search interface with the following elements:

- Search bar: Search... ▾ Quick Searches ▾ Add Filter
- Buttons: Save Criteria, Save Results, Cancel, False Positive, Rules ▾ Actions ▾
- Text: Viewing events from Jul 30, 2013 12:12:00 PM to Jul 31, 2013 12:12:00 PM. View: Select An Option.
- Grouping By: High Level Category (Grouping)
- Current Filters: Source or Destination IP is 10.127.15.37 (Clear Filter) (Filtering)
- Statistics: ▶ Current Statistics (Show Charts)

Annotations with callouts:

- Save Criteria:** Save the criteria of the current search (points to the Save Criteria button)
- Time range:** Now the screen shows the selected time range, grouping, and filtering (points to the time range text)
- Grouping:** Grouping By: High Level Category (points to the High Level Category grouping option)
- Filtering:** Current Filters: Source or Destination IP is 10.127.15.37 (points to the IP filter)
- Save Results:** Save the results of the current search (points to the Save Results button)

High Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)
Access	10.127.15.37	Multiple (380)	0	Firewall Deny	CheckPoint ...	Firewall Deny	Multiple (2)
Recon	10.127.15.37	Multiple (20)	0	Multiple (2)	Custom Rule...	Multiple (2)	icmp_ip

© Copyright IBM Corporation 2015

Monitoring the scanning host (3 of 3)

Saving search criteria

Save the search with the criteria specified

Please enter the name of this search below.

Search Name: Dept - 10.127.15.37

Prepend name with department name or initials for easy identification

Timespan options:

Last Interval (auto refresh) Recent

Last 24 Hours

Include in my Quick Searches Set as Default

Share With Everyone Include in my Dashboard

Assign Search to Group(s) Manage Groups

Assign to group

Set as default search for the Log Activity tab

OK Cancel

© Copyright IBM Corporation 2015



Saving search criteria

Event list using the saved search

Search... ▼ Quick Searches ▼ Add Filter Save Criteria Save Results

Using Search:
The event list shows the result of the saved search

Viewing events from Jul 30, 2013 12:12:00 PM to Jul 31, 2013 12:12:00 PM View: Select An Option:

Using Search: Dept - 10.127.15.37

Grouping By:
High Level Category

Current Filters:
Source or Destination IP is 10.127.15.37 ([Clear Filter](#))

▶ Current Statistics

(Show Charts)

High Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)
Access	10.127.15.37	Multiple (380)	0	Firewall Deny	CheckPoint ...	Firewall Deny	Multiple (2)
Recon	10.127.15.37	Multiple (20)	0	Multiple (2)	Custom Rule...	Multiple (2)	icmp_ip

© Copyright IBM Corporation 2015

Event list using the saved search

Modifying saved searches

About Quick Searches

When you select **Include in my Quick Searches** when saving a search, QRadar SIEM lists the saved search in the predefined **Quick Searches** list

The screenshot shows the QRadar SIEM interface with the 'Quick Searches' list open. The list contains various predefined searches, and one specific search, 'Dept - 10.127.15.37 - Last 24 Hours', is highlighted with a blue background. On the left side of the interface, there is a sidebar with sections for 'Grouping' (High Level, Current F...), 'Source c...', and 'Curren...'. Below these sections is a 'High Level Category' section with three options: 'Access' and 'Recon'. At the bottom of the interface, there is a copyright notice: '© Copyright IBM Corporation 2015'.

Search Name
Compliance: Source IPs Involved in Compliance Rules - Last 6 Hours
Compliance: Username Involved in Compliance Rules - Last 6 Hours
Default-IDS / IPS-All: Top Alarm Signatures - Last 6 Hours
Dept - 10.127.15.37 - Last 24 Hours
Event Category Distribution - Last 6 Hours
Event Processor Distribution - Last 6 Hours
Event Rate (EPS) - Last 6 Hours
Exploit By Source - Last 6 Hours
Exploits By Destination - Last 6 Hours
Exploits by Type - Last 6 Hours
Firewall Deny by DST IP - Last 6 Hours
Firewall Deny by DST Port - Last 6 Hours
Firewall Deny by SRC IP - Last 6 Hours
Firewall Permit By Log Source - Last 6 Hours
Firewall Permit by Source IP - Last 24 Hours
Flow Rate (FPS) - Last 6 Hours
Inbound Events by Country/Region - Last 6 Hours
Login Failures by Log Source - Last 6 Hours
Offenses by Destination IP - Last 6 Hours

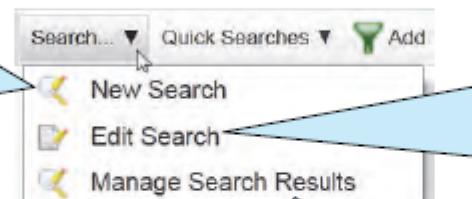
© Copyright IBM Corporation 2015

About Quick Searches

Using alternative methods to create and edit searches

- Most predefined saved searches are not listed under **Quick Searches**
- To find, use, and edit saved searches, select **Search** in the top menu bar

New Search:
Load a saved search; edit the loaded search or create a new search



Manage Search Results:
QRadar SIEM stores the result from each search for 24 hours; you can revisit, save, or delete results

Edit Search:
The Event List is the result of a search; edit this current search or edit another saved search

© Copyright IBM Corporation 2015

Using alternative methods to create and edit searches

Finding and loading a saved search

If you select **New Search** or **Edit Search**, the Event Search window opens

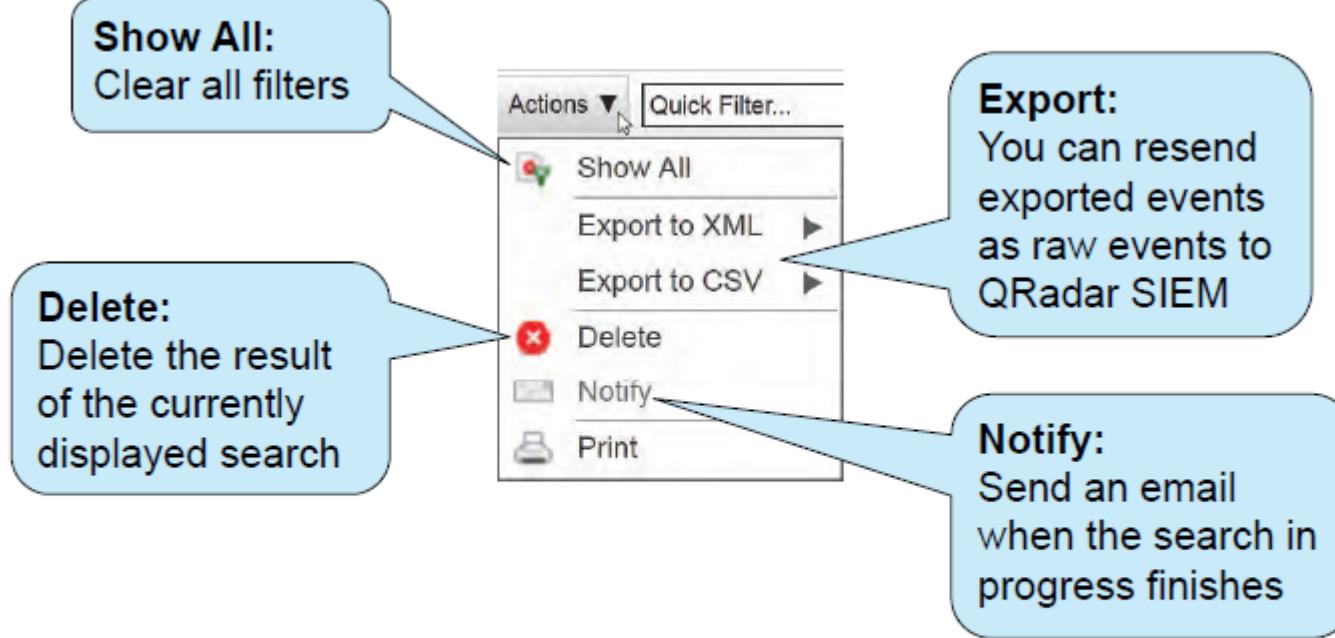
Type Saved Search:
To find saved searches easily, type your department name, if you prepended your saved searches with it

The screenshot shows the 'Saved Searches' window. At the top, there is a dropdown menu labeled 'Group: Select a group...'. Below it is a search bar with the placeholder 'Type Saved Search or Select from List' containing the letters 'de'. A list of 'Available Saved Searches' is displayed below, including:
Default-VPN-VPNGateway: Top Time Connected by IP
Default-VPN-VPNGateway: Top Time Connected by User
Default-VPN-VPNGateway: Top Users by #s of Connections
Default-VPN-VPNGateway: Warnings
Dept - 10.127.15.37
DOS Attacks by Destination IP
The item 'Dept - 10.127.15.37' is highlighted with a blue selection bar. At the bottom of the window are two buttons: 'Load' and 'Delete'.

© Copyright IBM Corporation 2015

Finding and loading a saved search

Search actions



© Copyright IBM Corporation 2015

Search actions

Adding a search to the dashboard

Adding a saved search as a dashboard item

To watch the scanning IP address from the dashboard, add the saved search as a dashboard item

The screenshot shows a user interface for adding a dashboard item. On the left, there's a sidebar with options like Network Activity, Offenses, Log Activity, Reports, System Summary, System Notifications, and Internet Threat Information Center. A dropdown menu is open under 'Event Searches' with items such as Top Authentications by User, Top Services Denied through Firewalls, Top Services/Ports Through Firewalls, Top Systems Attacked (IDS/IDP/IPS), Top Systems Sourcing Attacks (IDS/IDP/IPS), Top VPN Users, Compliance: Source IPs Involved in Compliance Rules, Compliance: Username Involved in Compliance Rules, Firewall Deny by SRC IP, Firewall Permit By Log Source, Firewall Permit by Source IP, Top IDS/IPS Alert by Country/Region, and Dept - 10.127.15.37. The 'Dept - 10.127.15.37' item is highlighted with a blue bar at the bottom of the list.

Note: This screen capture shows the **Dashboard** tab

Adding a saved search as a dashboard item

Saving a search as a dashboard item

The screenshot shows a dashboard interface with three tabs at the top: Dashboard, Offenses, and Log Activity. The Log Activity tab is selected. Below the tabs, there is a search bar labeled "Show Dashboard: Threat and Security Monitor". A specific dashboard item is highlighted, showing a bar chart titled "Dept - 10.127.15.37 (Count)" for the "Last Minute". The chart has two bars: a green bar for "Access" reaching approximately 8, and a blue bar for "Recon" reaching approximately 1. Below the chart is a legend with "Access" and "Recon" entries. At the bottom of the item is a link "View in Log Activity". A blue callout bubble points to the "Settings button" (a small icon with a gear and a minus sign) with the text: "Settings button: Modify the settings of an item". Another callout bubble points to the "Last Minute" label with the text: "Last Minute: Unless time-series data is captured, the dashboard item shows only the result of the last 1-minute interval". A third callout bubble points to the "View in Log Activity" link with the text: "View in Log Activity: Show the saved search with a 24-hour time range on Log Activity tab".

Dashboard Offenses Log Activity

Show Dashboard: Threat and Security Monitor

Dept - 10.127.15.37 (Count)

Last Minute

10
5
0

Legend: Access (Green Bar, approx 8), Recon (Blue Bar, approx 1)

[View in Log Activity](#)

Settings button:
Modify the settings of an item

Last Minute:
Unless time-series data is captured,
the dashboard item shows only the
result of the last 1-minute interval

View in Log Activity:
Show the saved search with a 24-hour
time range on Log Activity tab

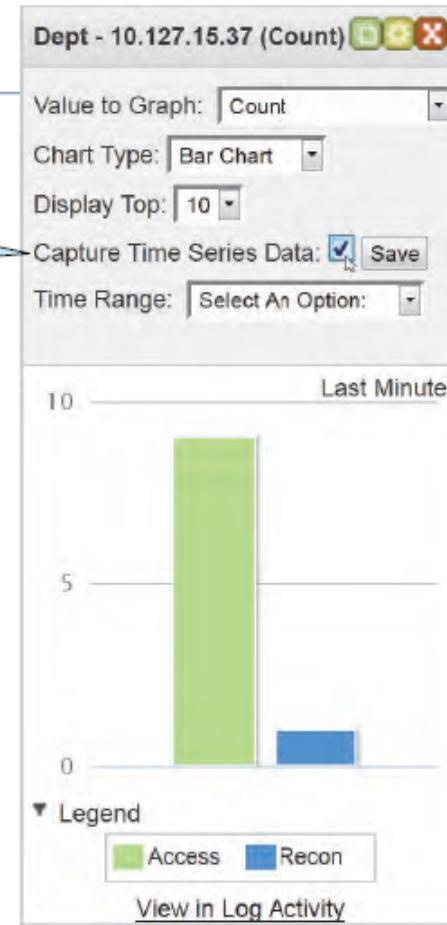
Saving a search as a dashboard item

Enabling time-series data

Enabling time-series data

Capture Time Series Data:
Select to accumulate time-series data to count events and click **Save**

- Capturing time-series data means that QRadar SIEM counts incoming events according your search criteria, grouping, and chosen value to graph
- Most of the predefined searches capture time-series data
- Capturing time-series data can negatively affect the performance of QRadar SIEM



© Copyright IBM Corporation 2015

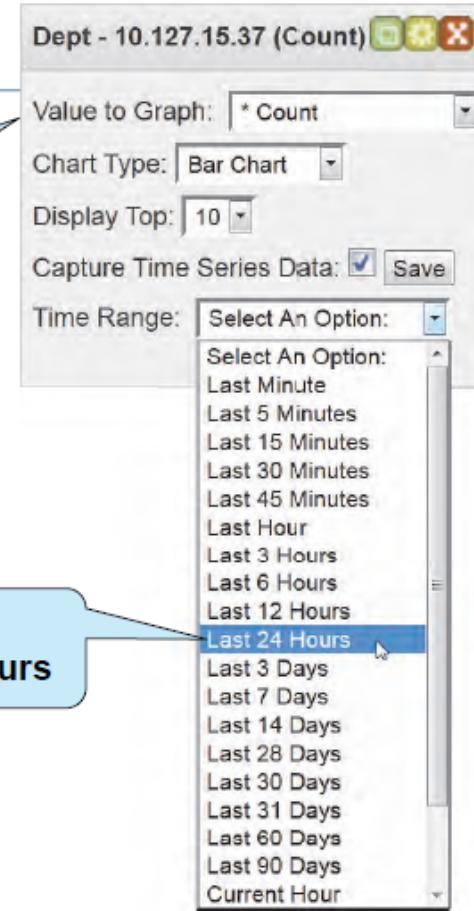
Enabling time-series data

Saving the time range

Selecting the time range

Value to Graph:
The asterisk (*) indicates
that QRadar SIEM
accumulates time-series
data for this value

Time Range:
Select Last 24 Hours



© Copyright IBM Corporation 2015

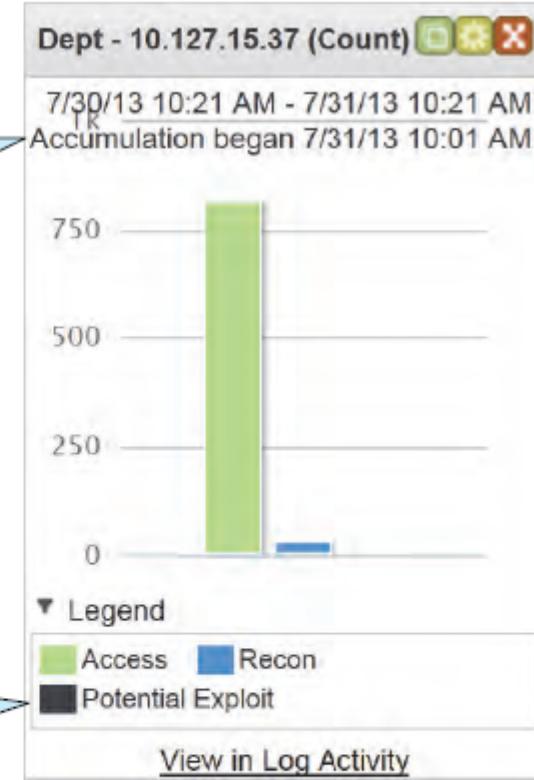
Selecting the time range

Displaying 24 hours in a dashboard item

Accumulation began:
QRadar SIEM started
accumulating time-series
data on this date at this time

A third high-level category shows now

Potential Exploit:
This third high-level category
does not have enough events
to display in a bar chart



© Copyright IBM Corporation 2015

Displaying 24 hours in a dashboard item

Modifying items in the chart type table

Chart Type: Table

To view all high-level categories, select the chart type **Table**

Chart Type: Time Series

To view trending of data, select the chart type **Time Series**

Potential Exploit:

Two events of high-level category Potential Exploit

Dept - 10.127.15.37 (Count) (Minimize) (Maximize) (Close)

Value to Graph: * Count

Chart Type: **Table** Bar Chart
Pie Chart
Table Table Time Series Save

Display Top: Select An Option: ▼

Capture Time: 7/30/13 10:21 AM - 7/31/13 10:21 AM
Accumulation began 7/31/13 10:01 AM

High Level Category	Count
Access	814
Recon	31
Potential Exploit	2

[View in Log Activity](#)

© Copyright IBM Corporation 2015

Modifying items in the chart type table

Investigating Security Incidents (Offenses)

B.2 Investigating the events of an offense

- Investigating event details
- Using filters to investigate events
- Using grouping to investigate events
- Saving a search
- Modifying saved searches
- Adding a search to the dashboard

Part B - Investigating Security Incidents (Offenses)

B.3 Investigating an offense that is triggered by flows

- Viewing and grouping flows
- Using summary information to investigate an offense
- Navigating flow details
- False positives overview
- Investigating superflows



Objectives

- Find and group flows on the **Network Activity** tab
- Investigate the summary of an offense that is triggered by flows
- Investigate flow details
- Tune false positives
- Investigate superflows

Viewing and grouping flows

About flows

- A flow provides information about network communication between two systems
- A flow can include information about the conversation, such as these examples
 - Source and destination IP address
 - Protocol transport
 - Source and destination port
 - Application information
 - Traffic statistics
 - Quality of service
 - Packet payload from unencrypted traffic

© Copyright IBM Corporation 2015

About flows

Network Activity tab

- Click the **Network Activity** tab to perform these tasks
 - Investigate flows sent to QRadar SIEM
 - Perform detailed searches
 - View network activity
- Flows on the **Network Activity** tab are shown in a similar way as events are on the **Log Activity** tab

The screenshot shows the Network Activity tab interface. At the top, there is a navigation bar with tabs: Dashboard, Offenses, Log Activity, Network Activity (which is selected and highlighted in blue), Assets, Reports, and Admin. Below the navigation bar is a toolbar with various buttons: Search..., Quick Searches, Add Filter, Save Criteria, Save Results, Cancel, False Positive, Rules, and Actions.

The main area displays a table of network flows. The table has the following columns: Flow Type, First Packet Time, Source IP, Source Port, Destination IP, Destination Port, Protocol, Application, Source Bytes, Destination Bytes, Source Packets, and Destination Packets. There are four rows of data in the table:

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets
█	Oct 15, ...	Multiple (6)	N/A	10.20.0.80	N/A	icmp_ip	ICMP.Destination-Unre...	408 (C)	N/A	6	N/A
█	Oct 15, ...	10.10.0.80	8029	174.108.50.173	33705	udp_ip	VoIP.Skype	134 (C)	67 (C)	2	1
█	Oct 15, ...	10.10.0.80	8029	113.253.144.84	34868	udp_ip	VoIP.Skype	160 (C)	0	2	0
█	Oct 15, ...	192.168.1...	64120	192.168.10.10	443	tcp_ip	Web.SecureWeb	78,330	141,129	151	108

At the bottom of the interface, there is a copyright notice: © Copyright IBM Corporation 2015.

Network Activity tab

Grouping flows

Some flow grouping options differ from event grouping options.

Viewing flows from Aug 8, 2013 8:44:00 AM to Aug 8, 2013 11:44:00 AM

Grouping By: Application

Display: Application

Default (Normalized)
Unioned Flows
Source or Destination IP
Source IP
Destination IP
Source Port
Destination Port
Source Network
Destination Network
Application
Geographic
Protocol
Flow Bias
ICMP Type
Custom

Application	Source IP (Unique Count)	Source IP (Unique Count)	Destination IP (Unique Count)
other	Multiple (18)	Multiple (18)	Multiple (16)
Multimedia.Intellex	10.20.0.80	Net_10_0_0_0	Multiple (16)
FileTransfer.NETBIOS	192.168.10.1	Net_192_168_10_1	192.168.10.255
Web.SecureWeb	Multiple (2)	Net_10_0_0_0	Multiple (10)
P2P.BitTorrent	10.20.0.80	Net_10_0_0_0	Multiple (16)
InnerSystem.Flowgen	10.20.0.80	Net_10_0_0_0	Multiple (24)
Web.Misc	Multiple (3)	Net_10_0_0_0	Multiple (15)
Misc.domain	Multiple (23)	Multiple (2)	Multiple (3)
DataTransfer.WindowsFileSharing	Multiple (3)	Multiple (3)	Multiple (3)
VoIP.Skype	10.10.0.80	Net_10_0_0_0	Multiple (17)
RemoteAccess.MSTerminalServ...	10.10.0.80	Net_10_0_0_0	10.10.0.50

Display:
Group by Application for an overview of the application data transported in the flows

© Copyright IBM Corporation 2015

Grouping flows

Finding an offense

A red icon indicates that a flow contributes to an offense

To navigate to the offense a flow contributes to, click the icon

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destin Port	Protocol
	8/8/13 10:38:41 AM	10.20.0.80	58467	93.158.65.201	80	tcp_ip
	8/8/13 10:38:34 AM	59.95.169.29	N/A	10.20.0.80	N/A	icmp_ip
	8/8/13 10:38:40 AM	10.20.0.80	51898	190.58.212.103	28454	tcp_ip
	8/8/13 10:38:24 AM	10.20.0.80	51907	59.95.169.29	21668	tcp_ip
	8/8/13 10:38:40 AM	10.20.0.80	56196	208.67.222.222	53	udp_ip
	8/8/13 10:38:40 AM	10.20.0.80	64199	208.67.222.222	53	udp_ip

© Copyright IBM Corporation 2015

Finding an offense



Using summary information to investigate an offense

Offense parameters

The parameter at the top of the offense summary provides the first clues to investigate the offense

Description:

From suspicious DNS traffic, QRadar SIEM concluded botnet activity; rules compile the description

Flows contributed to this offense

Offense 1		Summary Display ▾ Events Flows Actions ▾ Print ?					
Magnitude			Status		Relevance	3	Severity 4 Credibility 2
Description	Potential Botnet Activity containing Misc.domain	Offense Type	Source IP				
		Event/Flow count	1 events and 204 flows in 6 categories				
Source IP(s)	<u>10.20.0.80</u> (10.20.0.80)	Start	Aug 8, 2013 11:22:02 AM				
Destination IP(s)	<u>192.168.1.2</u> Remote (81)	Duration	3m				
Network(s)	<u>Multiple</u> (2)	Assigned to	Unassigned				

© Copyright IBM Corporation 2015

Offense parameters

Top 5 Source and Destination IPs

- Source and destination IP addresses provide information about the origin of the offense and its local targets
- Remote source IP addresses are displayed, but remote destination IP addresses are not

Top 5 Source IPs											Sources
Source IP	Magnitude	Location	Vuln...	User	MAC	Weight	Offenses	Desti...	Last Event/Flow	Events/Flows	
10.20.0.80	Yellow	Net-10-1...	No	Unknown	Unknown	0	1	1	1h 16m 56s	205	

Top 5 Destination IPs												Destinations
Destination IP	Magnitude	Location	Vuln...	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/Flows	
192.168.1.2	Yellow	Net-10-1...	No	No	Unkno	Unkno	0	1	1	1h 17m 42s	2	

© Copyright IBM Corporation 2015

Top 5 Source and Destination IPs

Top 5 Log Sources

Top 5 Log Sources						 Log Sources
Name	Description	Group	Events/Flows	Offenses	Total Events/Flows	
Custom Rule Engine-8...	Custom Rule Engine		1	3	19	

Events/Flows:
The Custom Rule Engine
(CRE) created the only event
that contributes to the offense

© Copyright IBM Corporation 2015

Top 5 Log Sources

Top 5 Categories

QRadar SIEM sorted the event and the flows into categories

Top 5 Categories							 Categories
Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow		
Misc Malware		0	1	Aug 8, 2013 ...	Aug 8, 2013 ...		
Misc		0	16	Aug 8, 2013 ...	Aug 8, 2013 ...		
HTTP In Progress		1	158	Aug 8, 2013 ...	Aug 8, 2013 ...		
Web		0	20	Aug 8, 2013 ...	Aug 8, 2013 ...		
Multimedia		0	3	Aug 8, 2013 ...	Aug 8, 2013 ...		

© Copyright IBM Corporation 2015

Top 5 Categories

Last 10 Events

The Custom Rule Engine (CRE) created an event with information about the suspected botnet activity

Last 10 Events							Events
Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time	
Potential Botnet Activity	<div style="width: 100%;"> </div>	Custom Rule E...	Misc Malware	208.67.222.222	53	Aug...	

© Copyright IBM Corporation 2015

Last 10 Events

Last 10 Flows

This table provides information about what happened most recently

Double-click a row to open a window with details about the flow

Last 10 Flows						
Application	Source IP	Source Port	Destination IP	Dest... Port	Total Bytes	Last Packet Time
Web.Misc	10.20.0.80	58467	93.158.65.201	80	526	Aug 8, 2013 11:25:02 AM
Misc.domain	10.20.0.80	56196	208.67.222.222	53	174	Aug 8, 2013 11:25:02 AM
Misc.domain	10.20.0.80	64395	208.67.222.222	53	166	Aug 8, 2013 11:25:02 AM
Misc.domain	10.20.0.80	64199	208.67.222.222	53	184	Aug 8, 2013 11:25:02 AM
other	10.20.0.80	51954	86.3.249.91	10638	202	Aug 8, 2013 11:24:58 AM
P2P.BitTorrent	10.20.0.80	51898	190.58.212.103	28454	136	Aug 8, 2013 11:24:43 AM
other	10.20.0.80	51897	188.51.8.41	54713	125	Aug 8, 2013 11:24:43 AM
other	10.20.0.80	51969	190.213.79.246	38201	136	Aug 8, 2013 11:24:24 AM
other	10.20.0.80	54752	119.153.99.23	57396	68	Aug 8, 2013 11:24:15 AM
Misc.domain	10.20.0.80	64199	208.67.222.222	53	736	Aug 8, 2013 11:24:02 AM

© Copyright IBM Corporation 2015

Last 10 Flows

Annotations

- Annotations provide insight into why QRadar SIEM considers the event or traffic threatening
- QRadar SIEM can add annotations when it adds events and flows to an offense
- Read the oldest annotation because it was added when the offense was created
- Hold the mouse over an annotation to show the entire text

In this example, you learn about connections to a remote DNS server, which indicates connections to a botnet.

Top 5 Annotations

Annotation	Time	Weight
[2] "Destination/Event Analysis". The number of events this source generated during this attack.	Aug 8 2015 10:45:00 AM	6
"CRE_Event" CRE Rule description: [Potential Botnet Activity] Detected a host connecting to a DNS server on the Internet. This may indicate a host connecting to a Botnet. The host should be investigated for malicious code.	Aug 8 2015 10:45:00 AM	6

© Copyright IBM Corporation 2015

Annotations

Navigating flow details

Base information

Base information

Flow base information is similar to event base information

QRadar SIEM tries to extract custom flow properties from the payload

QRadar SIEM extracted only the HTTP version; QRadar SIEM administrators can increase the content capture length to provide more custom flow property data

Flow Information					
Protocol:	tcp_ip	Application:	Web Misc		
Magnitude:	6 (6)	Relevance:	10	Severity:	1 Credibility: 10
First Packet Time:	Aug 8, 2013 11:22:02 AM	Last Packet Time:	Aug 8, 2013 11:24:01 AM	Storage Time:	Aug 8, 2013 11:25:02 AM
Event Name:	Web				
Low Level Category:	Web				
Event Description:	Application detected with state based decoding				
HTTP Server (custom):	N/A				
HTTP Host (custom):	N/A				
HTTP Response Code (custom):	N/A				
HTTP Content-Type (custom):	N/A				
Google Search Terms (custom):	N/A				
HTTP User-Agent (custom):	N/A				
HTTP Version (custom):	1.1				
HTTP Referer (custom):	N/A				
HTTP GET Request (custom):	N/A				

© Copyright IBM Corporation 2015

Base information

Source and destination information

QRadar SIEM provides network connection details about the flow

Source and Destination Information			
Source IP:	10.20.0.80	Destination IP:	 93.158.65.201
Source Asset Name:	N/A	Destination Asset Name:	N/A
IPv6 Source:	0:0:0:0:0:0:0	IPv6 Destination:	0:0:0:0:0:0:0
Source Port:	58467	Destination Port:	80
Source Flags:	S,P,A	Destination Flags:	S,A
Source QoS:	Best Effort	Destination QoS:	Class 1
Source ASN:	0	Destination ASN:	0
Source If Index:	0	Destination If Index:	0
Source Payload:	3 packets, 260 bytes	Destination Payload:	3 packets, 266 bytes

© Copyright IBM Corporation 2015

Source and destination information

Layer 7 payload

This example shows the layer 7 payloads for an HTTP GET request and response; both show only the first 64 bytes of payload by default

Source Payload	Destination Payload
<p>utf hex base64</p> <p>Wrap Text</p> <pre>GET /torrent/CentOS-6.0-i386-bin-DVD/3184478934b9ab6edfc40a9b811</pre>	<p>utf hex base64</p> <p>Wrap Text</p> <pre>HTTP/1.1 200 OK Date: Thu, 08 Aug 2013 02:13:24 GMT Server: Apac</pre>

Note: QRadar SIEM administrators can increase the content capture length to provide more layer 7 payload

© Copyright IBM Corporation 2015

Layer 7 payload

Additional information

Additional Information			
Flow Type:	Standard Flow	Flow Source/Interface:	COE:eth0
Flow Direction:	L2R		
Custom Rules:	<u>BB:PortDefinition: Web Ports</u> <u>BB:CategoryDefinition: Any Flow</u> <u>BB:CategoryDefinition: Successful Communication</u> <u>Magnitude Adjustment: Destination Network Weight is Low</u> <u>Magnitude Adjustment: Context is Local to Remote</u> <u>Magnitude Adjustment: Source Network Weight is Low</u> <u>BB:NetworkDefinition: Client Networks</u> <u>BB:PortDefinition: Authorized L2R Ports</u> <u>BB:CategoryDefinition: Regular Office Hours</u> <u>Botnet: Potential Botnet Connection (DNS)</u>		
Custom Rules Partially Matched:	<u>System: Flow Source Stopped Sending Flows</u>		
Annotations:	Relevance has been decreased by 2 because the destination network weight is low. Relevance has been increased by 5 because the context is Local to Remote.		

© Copyright IBM Corporation 2015

Additional information

The **Flow Direction** field can include the following values:

- **L2L:** Traffic from a local network to another local network
- **L2R:** Traffic from a local network to a remote network
- **R2L:** Traffic from a remote network to a local network
- **R2R:** Traffic from a remote network to another remote network

False positives overview

Creating a false positive flow or event

- If an event or flow is legitimate, you can prevent it and similar events and flows from contributing to offenses
- In the top menu bar, click the **False Positive** icon



This option is rarely useful because it eliminates every occurrence of the above selection every time

The QID uniquely identifies the kind of application data that the flow transports



False Positive

False positive tuning allows you to prevent event/flow(s) from correlating into offenses.

Event/Flow Property

- Event/Flow(s) with a specific QID of 53268795 (*Web*)
- Any Event/Flow(s) with a low level category of *Web*
- Any Event/Flow(s) with a high level category of *Application*

Traffic Direction

- 10.20.0.80 to 93.158.65.201
- 10.20.0.80 to Any Destination
- Any Source to 93.158.65.201
- Any Source to any Destination

Cancel

Tune

© Copyright IBM Corporation 2015

Creating a false positive flow or event

Tuning a false positive flow or event

- Flows and events that you tagged as false positives perform in these ways
 - Contribute to reports
 - No longer contribute to offenses
 - Are still stored by QRadar SIEM
- QRadar SIEM administrators must perform these tasks
 - Keep the network hierarchy and Device Support Modules (DSM) up-to-date to prevent false alarm offenses
 - Disable rules that produce numerous unwanted offenses

© Copyright IBM Corporation 2015

Tuning a false positive flow or event

Investigating superflows

About superflows

QRadar SIEM aggregates flows with common characteristics into superflows that indicate common attack types

- Type A: Network sweep
one source IP address > many destination IP addresses
- Type B: Distributed denial of service (DDOS) attack
many source IP addresses > one destination IP address
- Type C: Portscan
one source IP address > many ports on one destination IP address

Flow Type

Flow Type	Source IP	Source Port	Destination IP	Des Por	Protoc	Application	Source Bytes
A	10.10.10.101	Multiple (41)	Multiple (41)	80	udp_ip	Web.Misc	110,208 (C)
B	Multiple (20)	Multiple (20)	24.10.10.200	53	tcp_ip	Misc.domain	3,840

© Copyright IBM Corporation 2015

About superflows

Superflow source and destination information

- Navigate to the flow details to investigate a superflow further
- This example shows a Type B Superflow that indicates a DDOS

Source and Destination Information			
Source(s)	Destination IP:	Protocol	Port
20 192.168.9.10:80 192.168.9.124:80 10.36.26.128:10000 10.36.15.9:10000 10.36.94.147:10000 192.168.9.204:80 192.168.9.224:80 192.168.9.94:80 ...	24.10.10.200:53	TCP	53

© Copyright IBM Corporation 2015

Superflow source and destination information

Superflow additional information

Flow Type:
The rules engine detected a denial of service (DoS), but QFlow collectors already aggregated the superflow

Flow Type

Additional Information

Flow Type:	Type B Superflow (DDOS)	Flow Source/Interface:	COE:eth0
Flow Direction:	L2R		
Custom Rules:	<u>BB:Flowshape: Outbound Only</u> <u>BB:CategoryDefinition: Suspicious Flows</u> <u>BB:CategoryDefinition: Suspicious Events</u> <u>BB:PortDefinition: DNS Ports</u> <u>BB:CategoryDefinition: Any Flow</u> <u>Botnet: Potential Botnet Connection (DNS)</u> <u>Magnitude Adjustment: Destination Network Weight is Low</u> <u>Magnitude Adjustment: Context is Local to Remote</u> <u>Magnitude Adjustment: Source Network Weight is Low</u> <u>o:Threats: DoS: Potential Multihost Attack</u> <u>Malware: Remote: Client Based DNS Activity to the Internet</u> <u>BB:NetworkDefinition: Client Networks</u> <u>BB:PortDefinition: Authorized L2R Ports</u>		

© Copyright IBM Corporation 2015

Superflow additional information

Investigating Security Incidents (Offenses)

B.3 Investigating an offense that is triggered by flows

- Viewing and grouping flows
- Using summary information to investigate an offense
- Navigating flow details
- False positives overview
- Investigating superflows



Hands-on Demo / Lab Exercises



Hands-on Demo / Lab Exercises

Hands-on Demo / Lab Exercises:

- Investigating a network offense (local DNS scanner offense)
- Looking for events that contribute to an offense
- Saving search criteria and search results
- Investigating event details
- Investigating an offense that is triggered by flows