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)

Temasek POLYTECHNIC

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

Creating and rating offenses

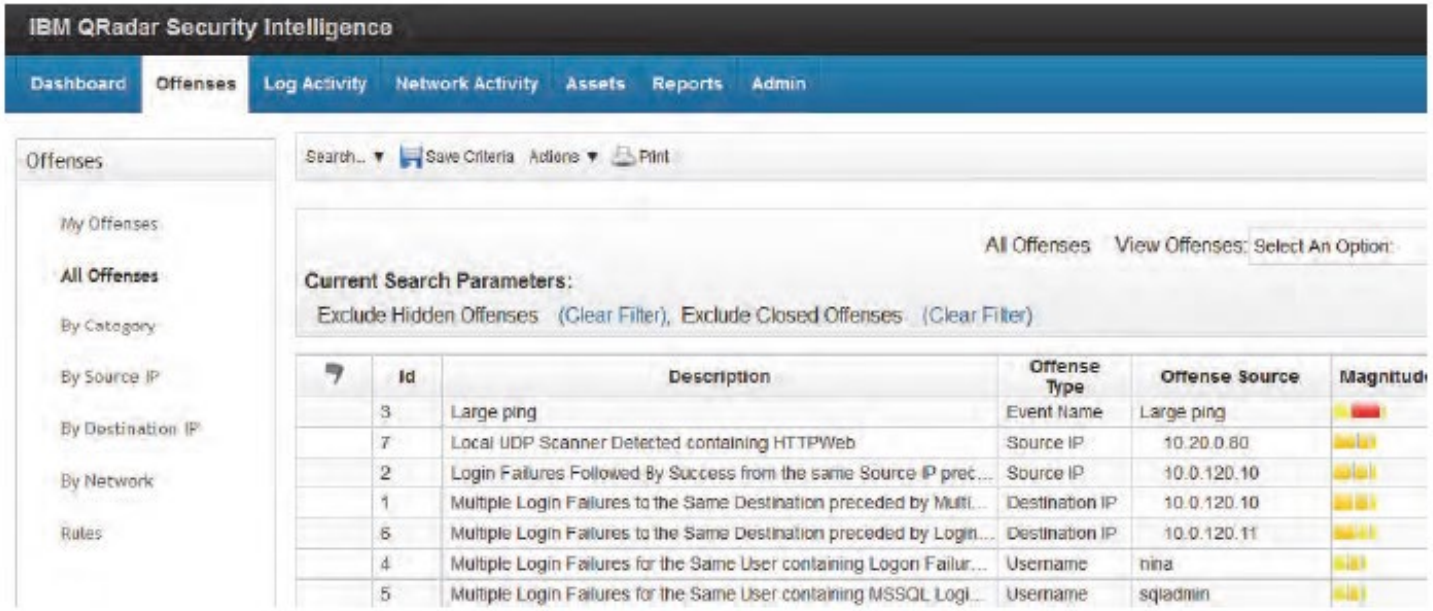
- QRadar SIEM creates an offense when events, flows, or both meet the test criteria specified in changeable **rules** that analyze the following information
  - Incoming events and flows
  - Asset information
  - Known vulnerabilities
- The **magistrate** in QRadar SIEM rates each offense by its **magnitude**,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

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



Selecting an offense to investigate

Selecting an offense to investigate (cont.)

This slide presents the **Offenses** tab:

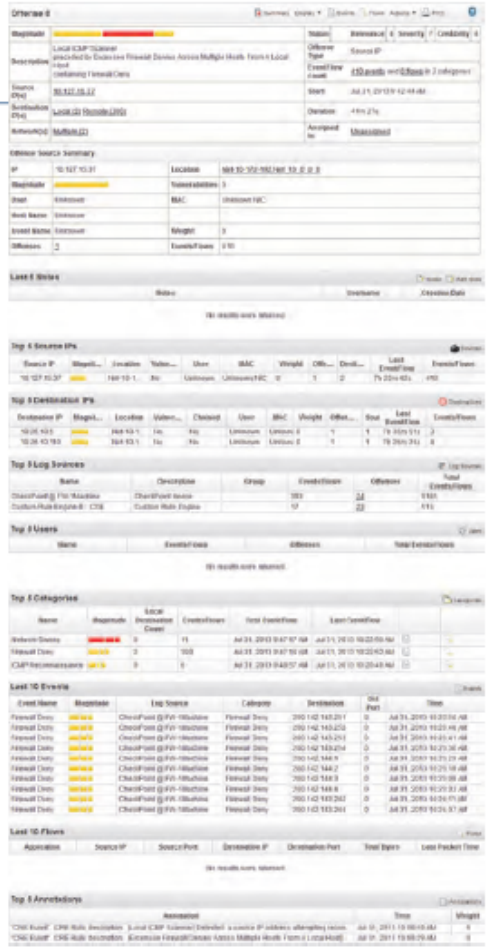
- The default view of the **Offenses** tab is called **Offense Manager**.
- Double-click an offense to view the detailed **Offense Summary** of that offense.
- Use the left navigation to view the offenses from different perspectives. For example, select **Offenses by Source IP** or **Offenses by Destination 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.



Offense Summary window

Offense Summary window (cont.)

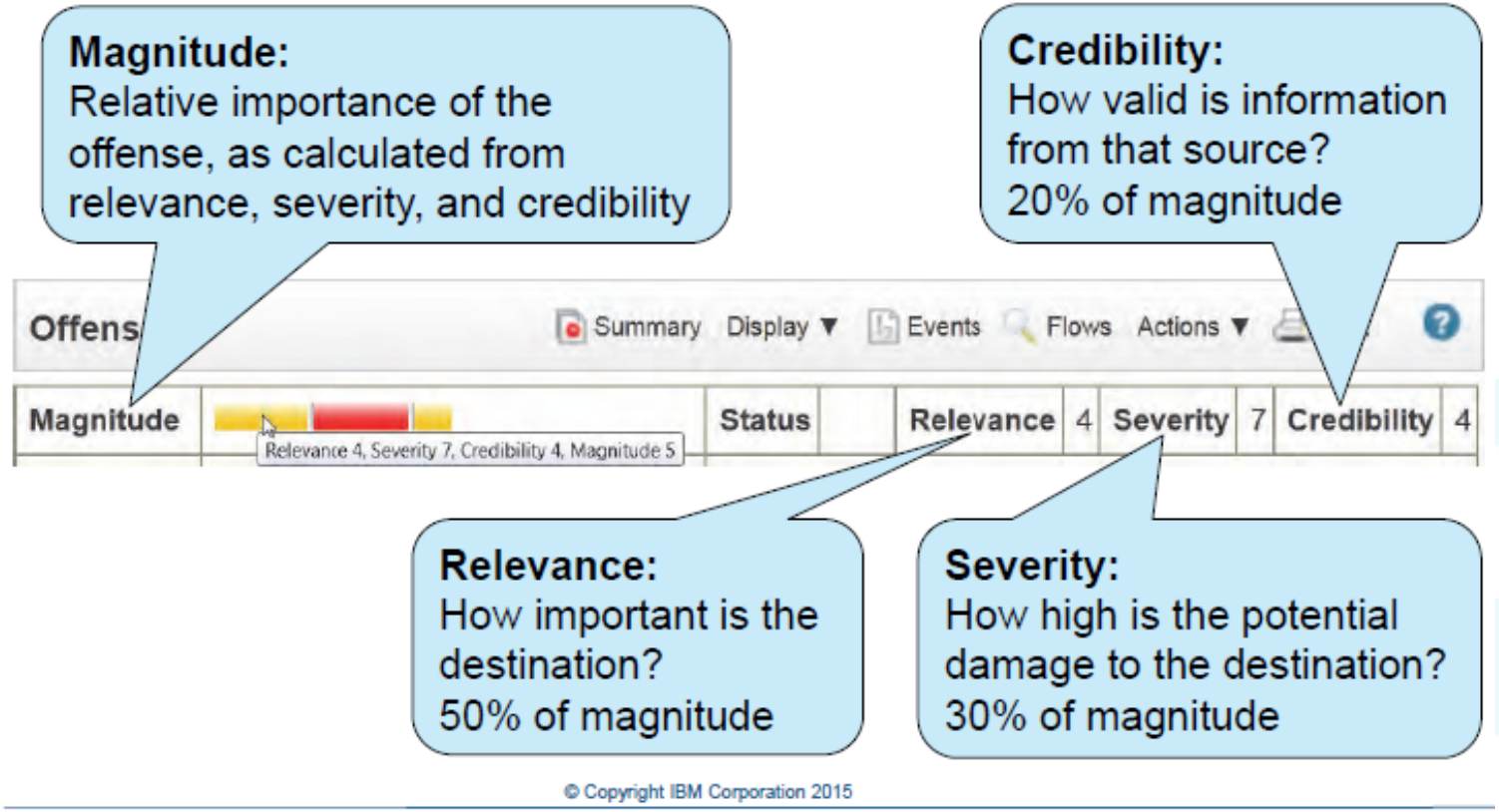
TheOffense Summary window includes these sections:

- 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.

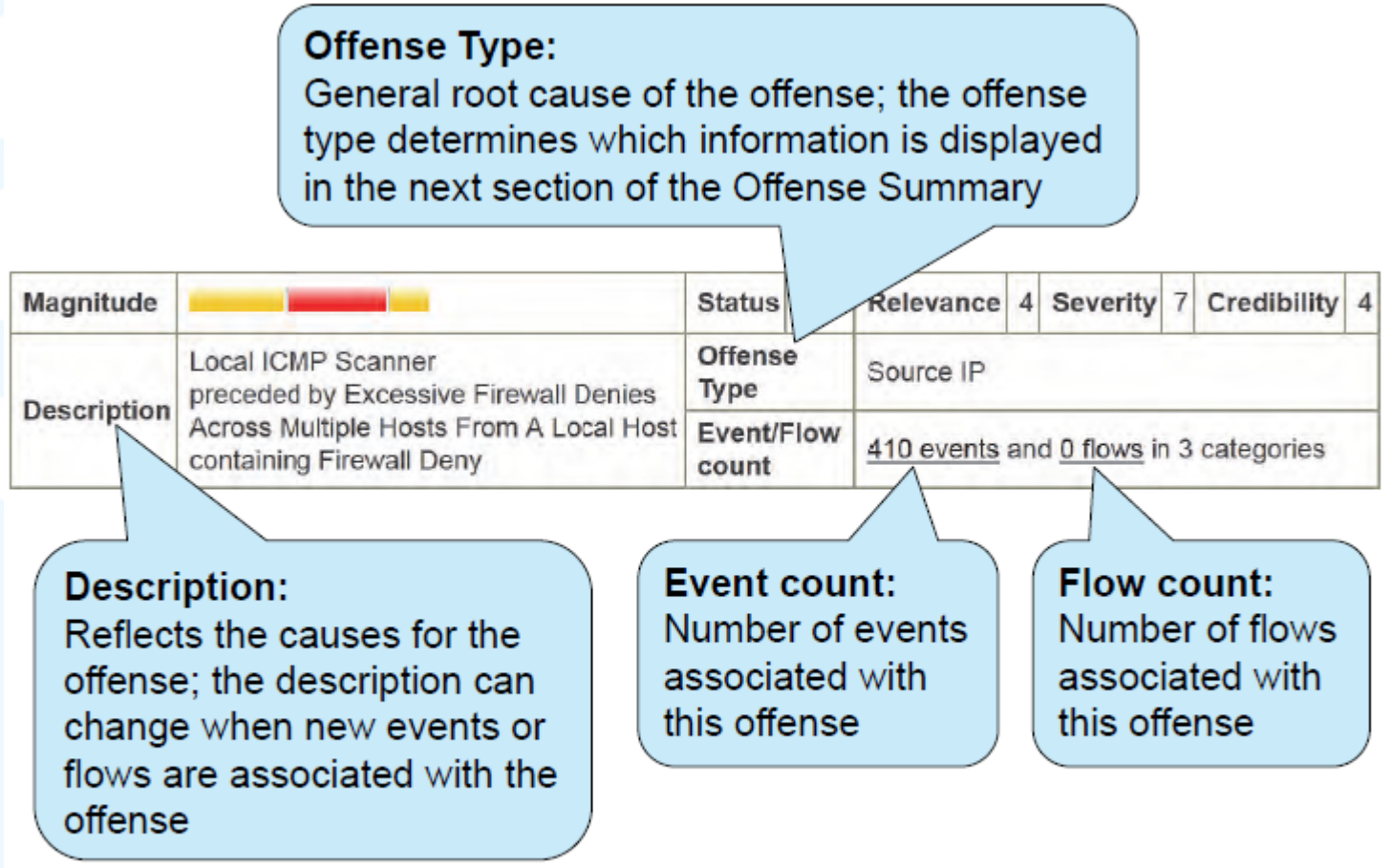
Offense parameters (1 of 4)

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



Offense parameters

Offense parameters (2 of 4)



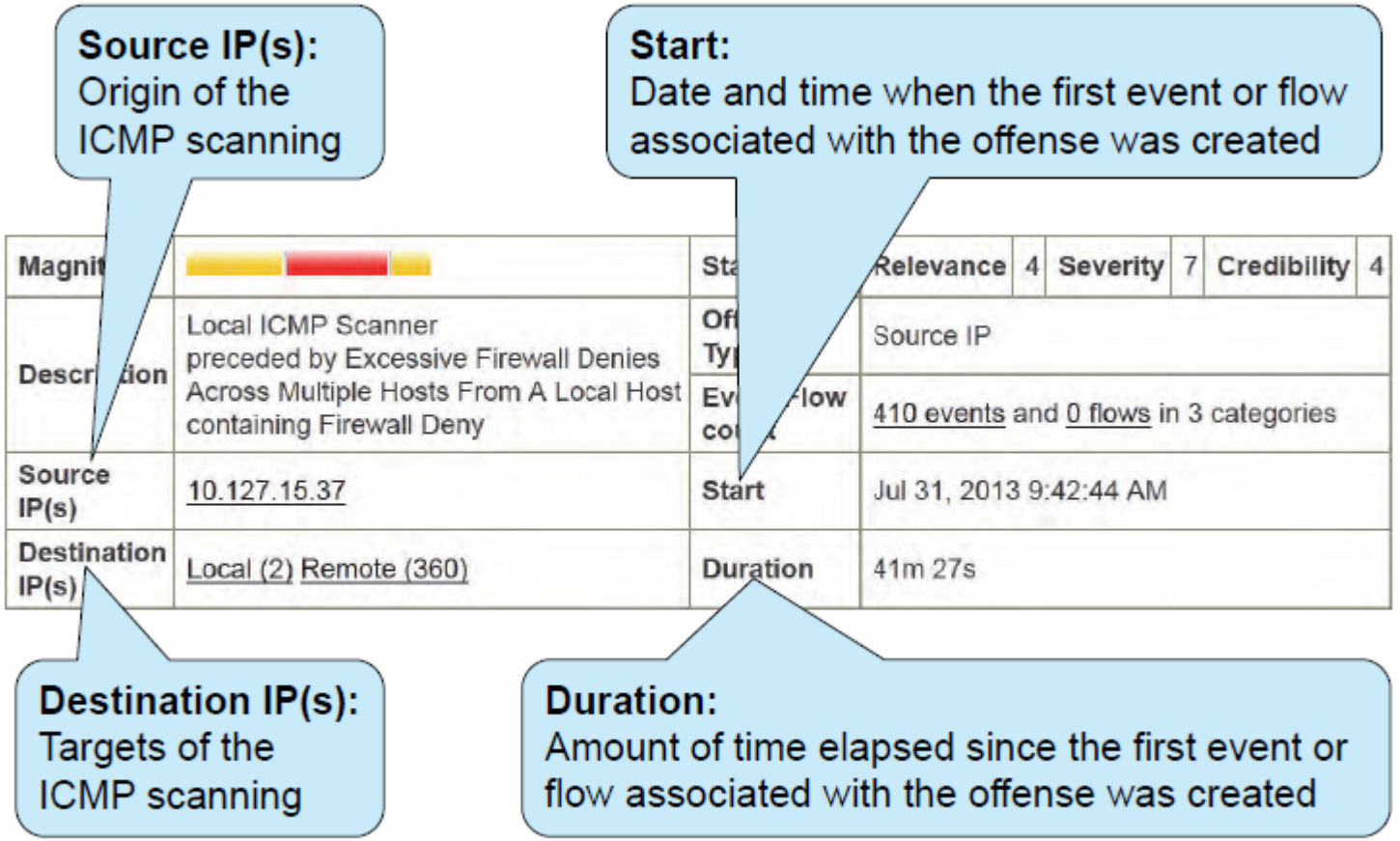
Offense parameters (2 of 4)

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)



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

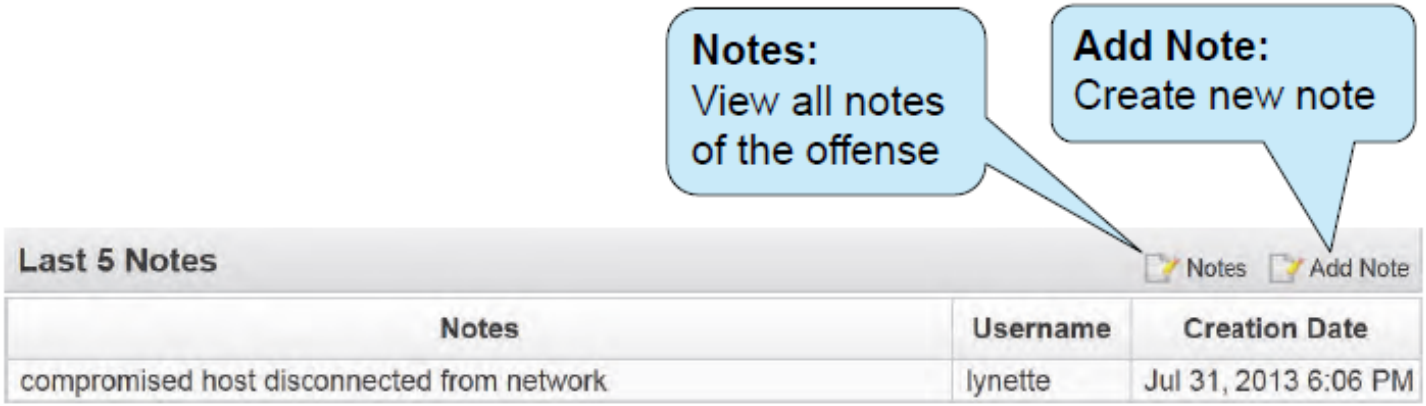
Offense parameters (4 of 4)

Investigating offense details

Notes

QRadar SIEM users can add notes to offenses

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



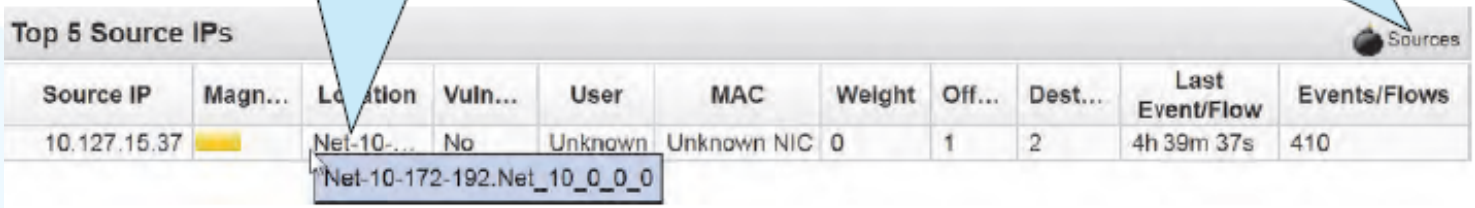
Notes

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

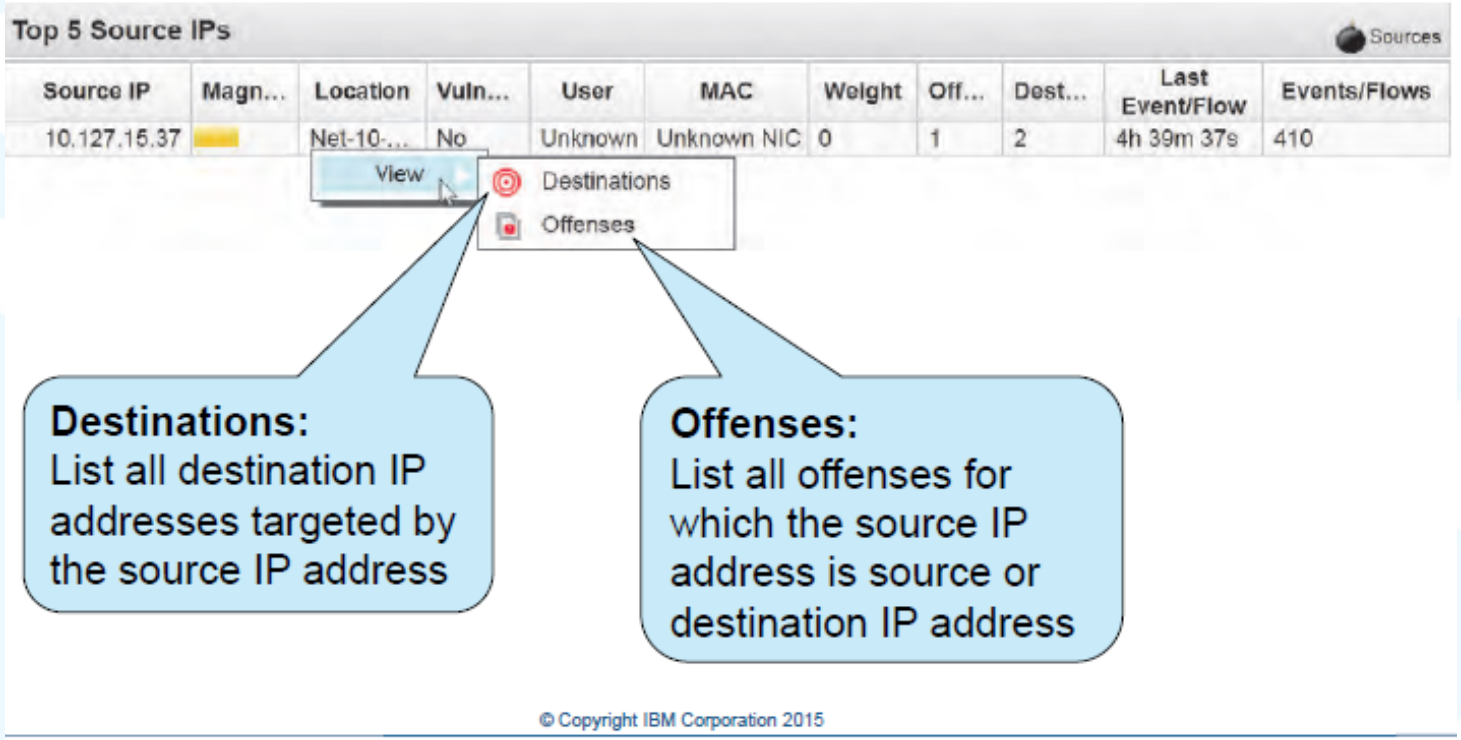


Note: The table contains only one row because the example offense has only one source IP address

Top 5 Source IPs

Top 5 Source IPs (cont.)

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



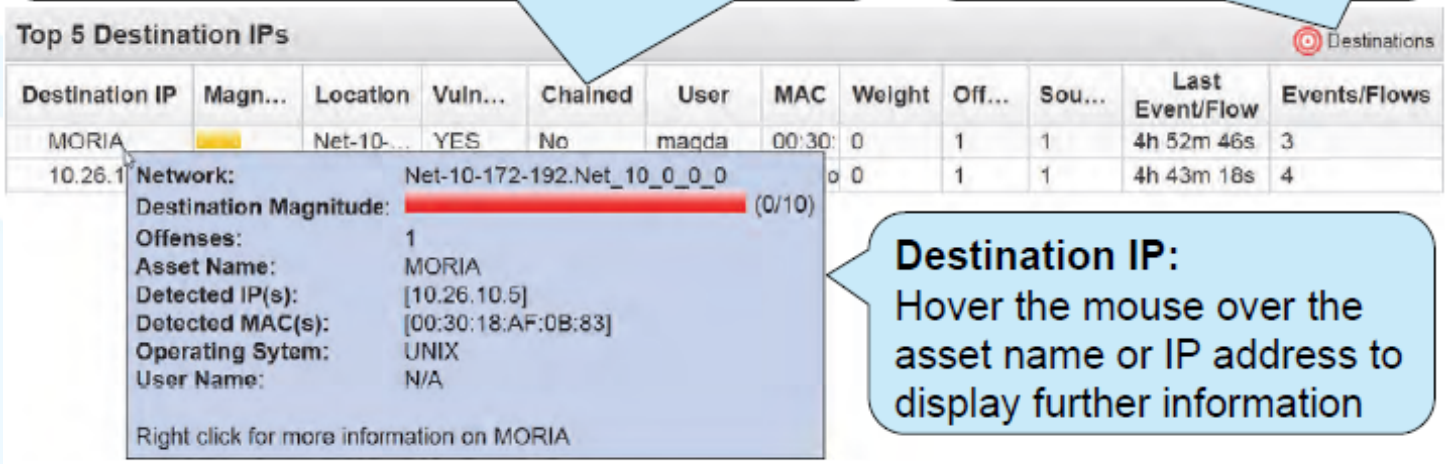
Top 5 Source IPs (continued)

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



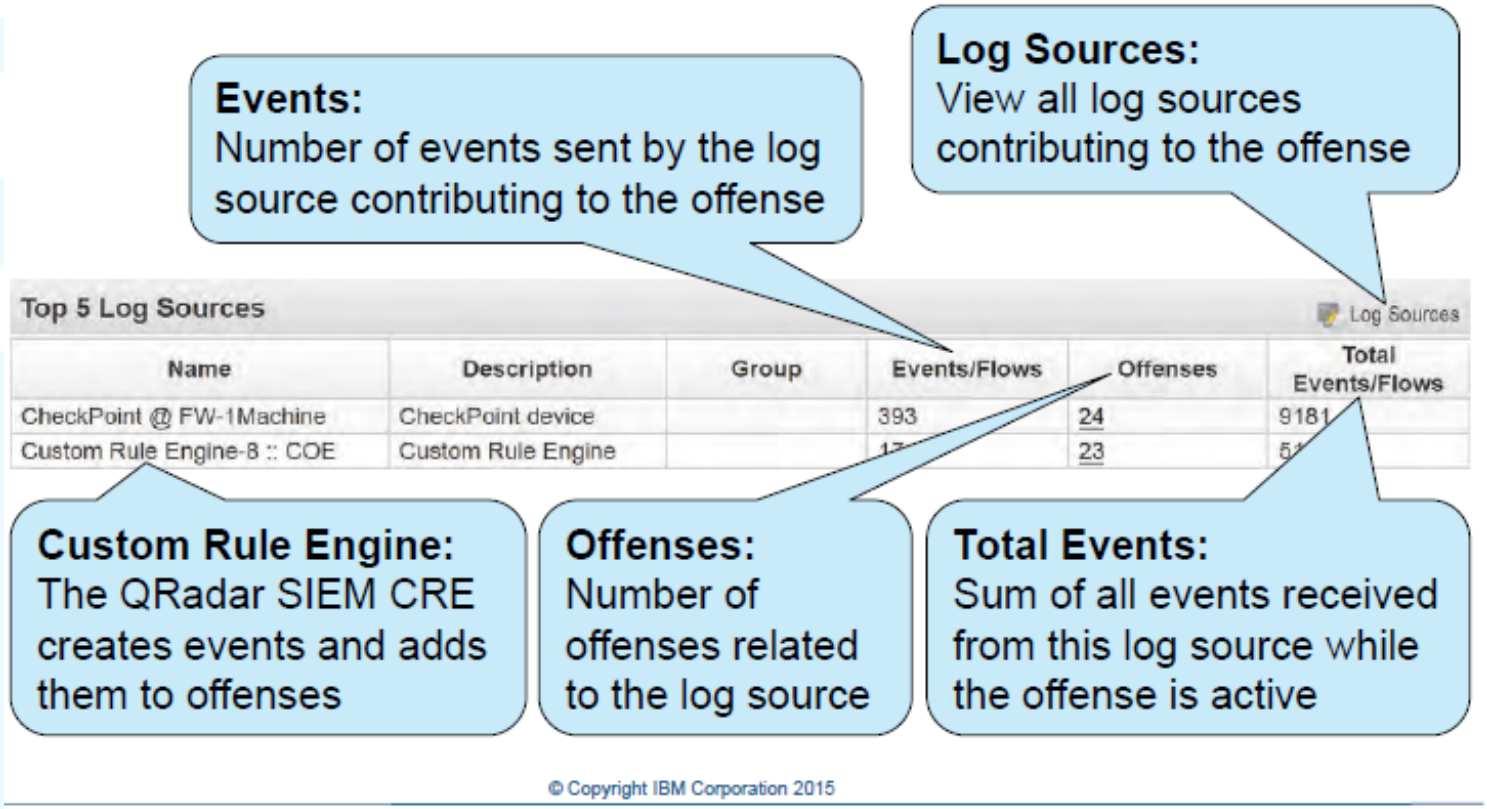
Destination IP:
Hover the mouse over the asset name or IP address to display further information

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

Top 5 Destination IPs

Top 5 Log Sources

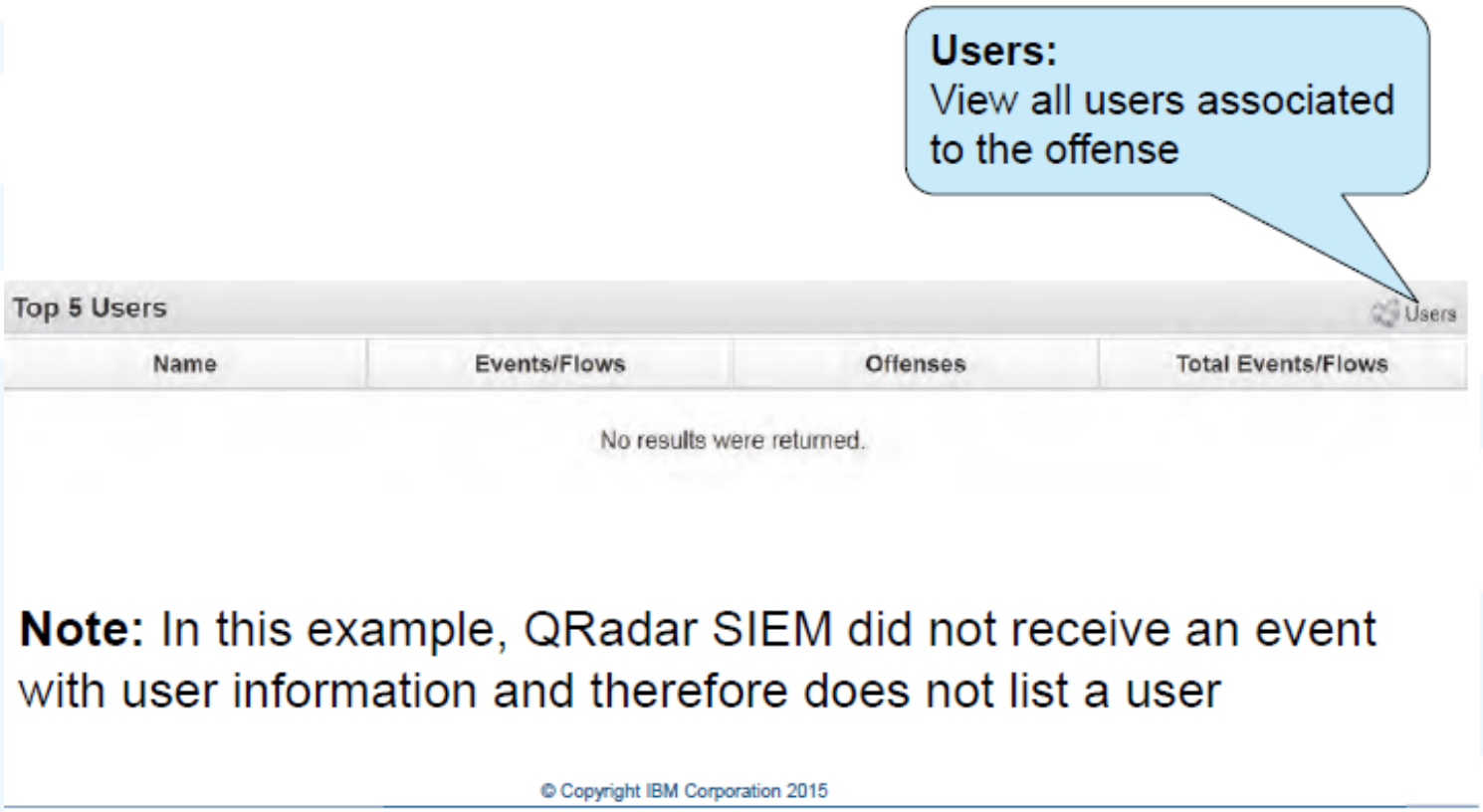
A firewall provided the log messages about firewall denies; this firewall is the major log source of the ICMP scanner offense



Top 5 Log Sources

Top 5 Users

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

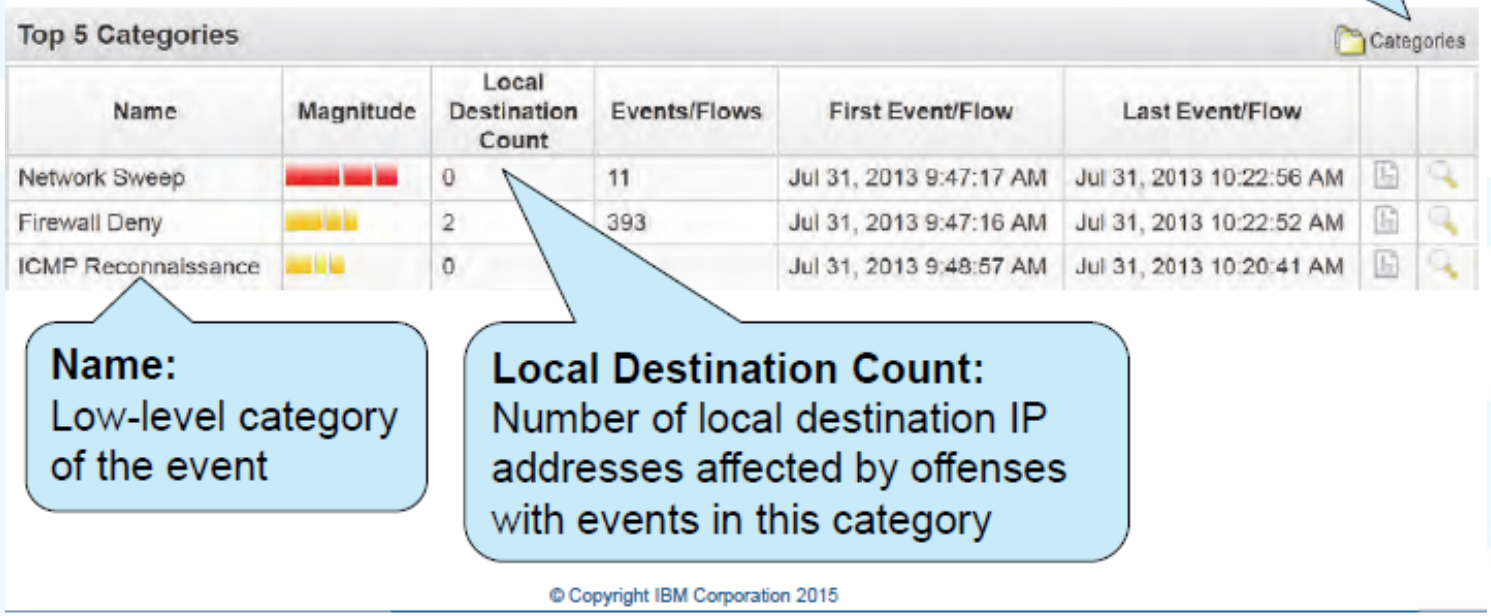


Top 5 Users

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

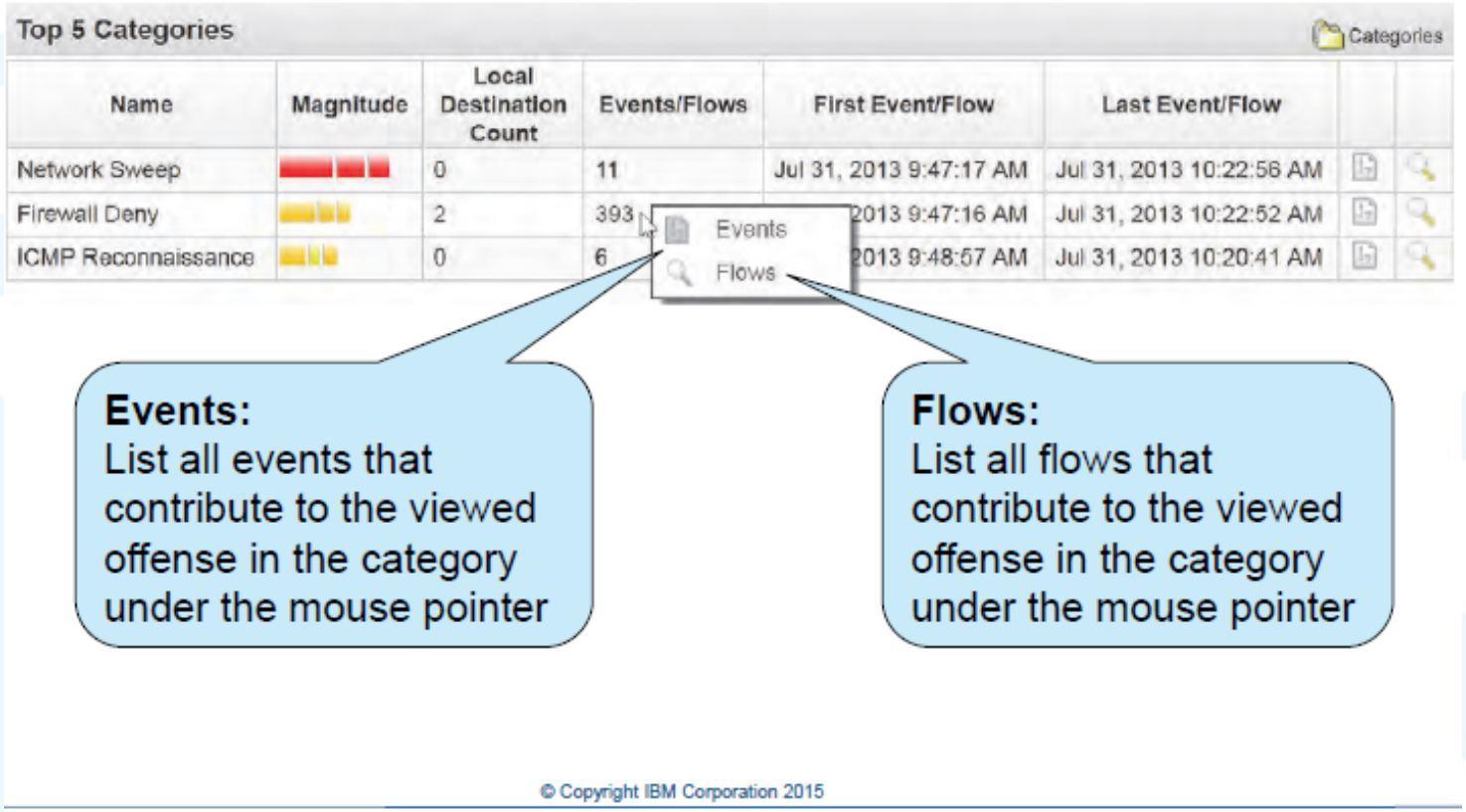
Categories:
View all low-level categories of the events contributing to the offense



Top 5 Categories

Top 5 Categories (cont.)

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



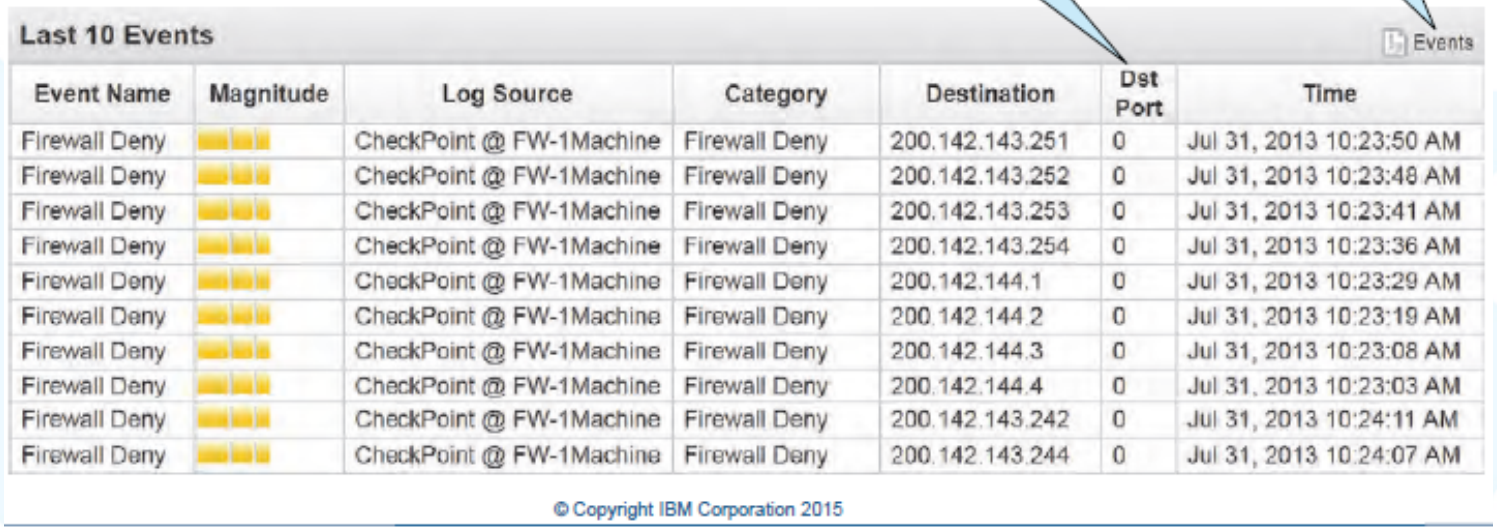
Top 5 Categories (continued)

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



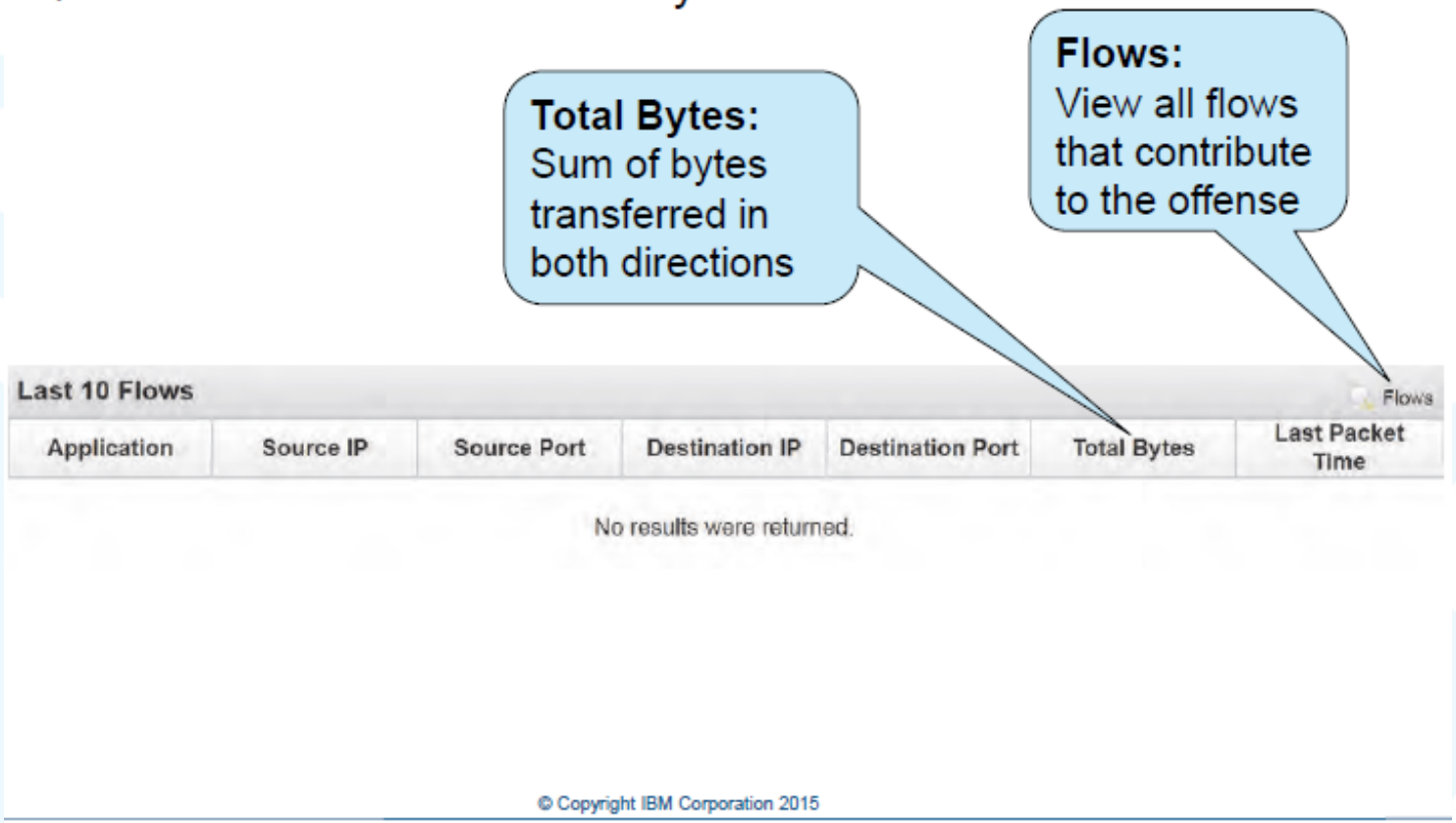
Last 10 Events — Events

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

Last 10 Events

Last 10 Flows

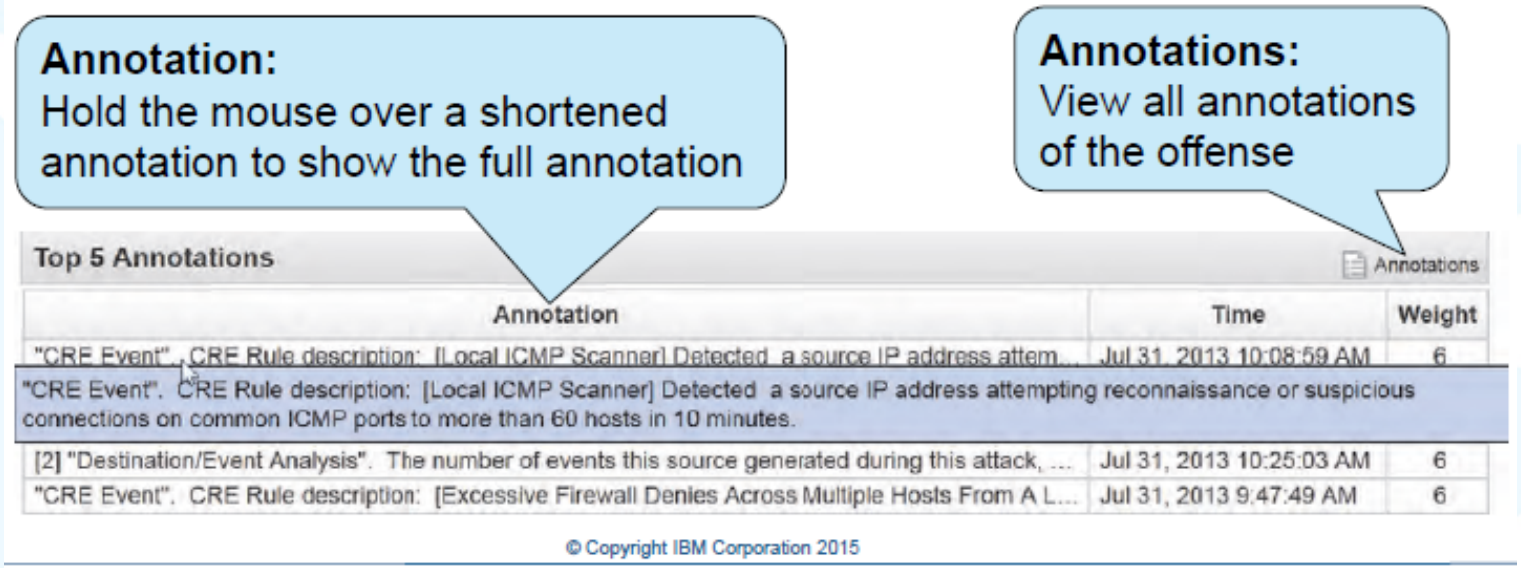
No flows contributed to the ICMP scanner offense; therefore, QRadar SIEM does not list any flows



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



Annotations

Offense Summary toolbar

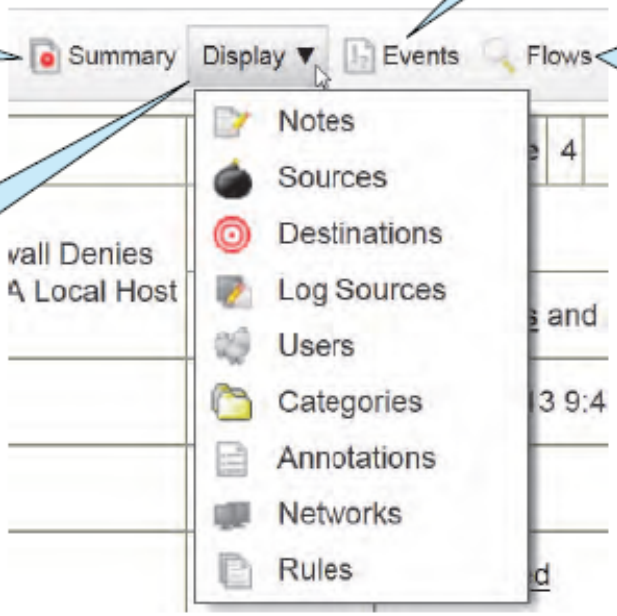
The Offense Summary toolbar provides direct links to the information that you just investigated

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

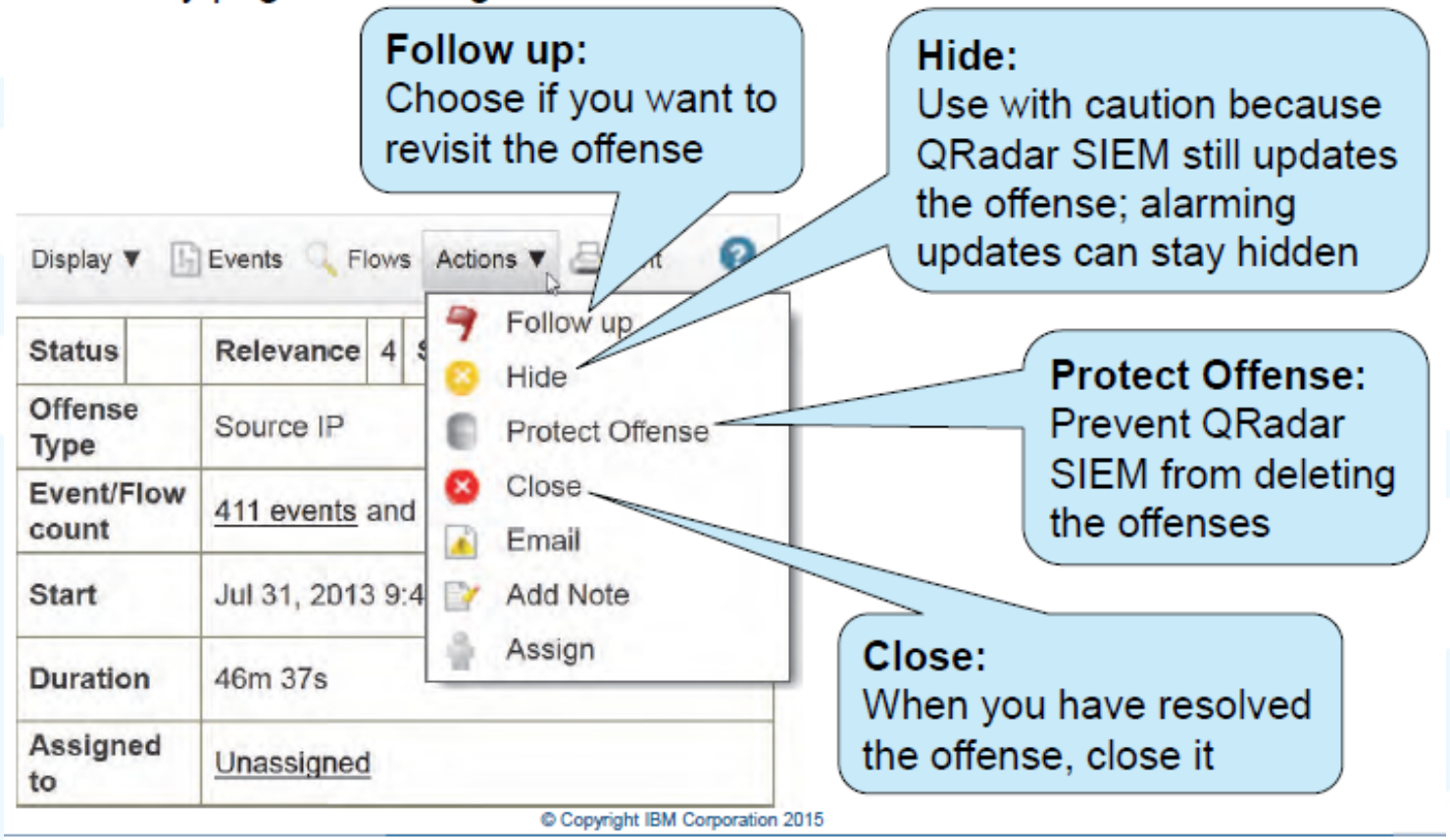


Offense Summary toolbar

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



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.

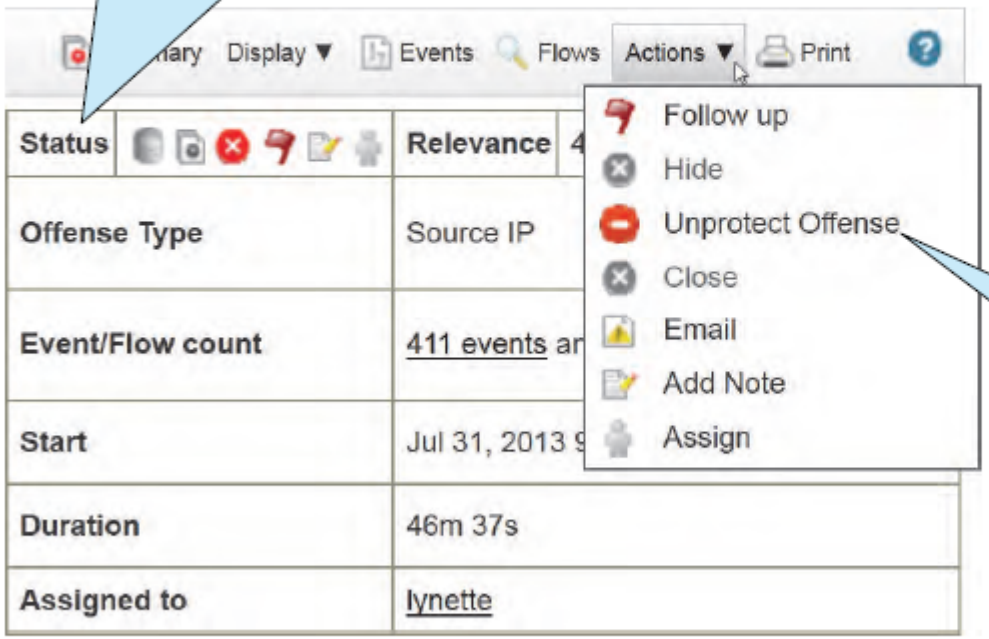
Offense actions (cont.)

- **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



Unprotect Offense: Allow QRadar SIEM to delete this protected offense

Offense status and flags

Summary

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

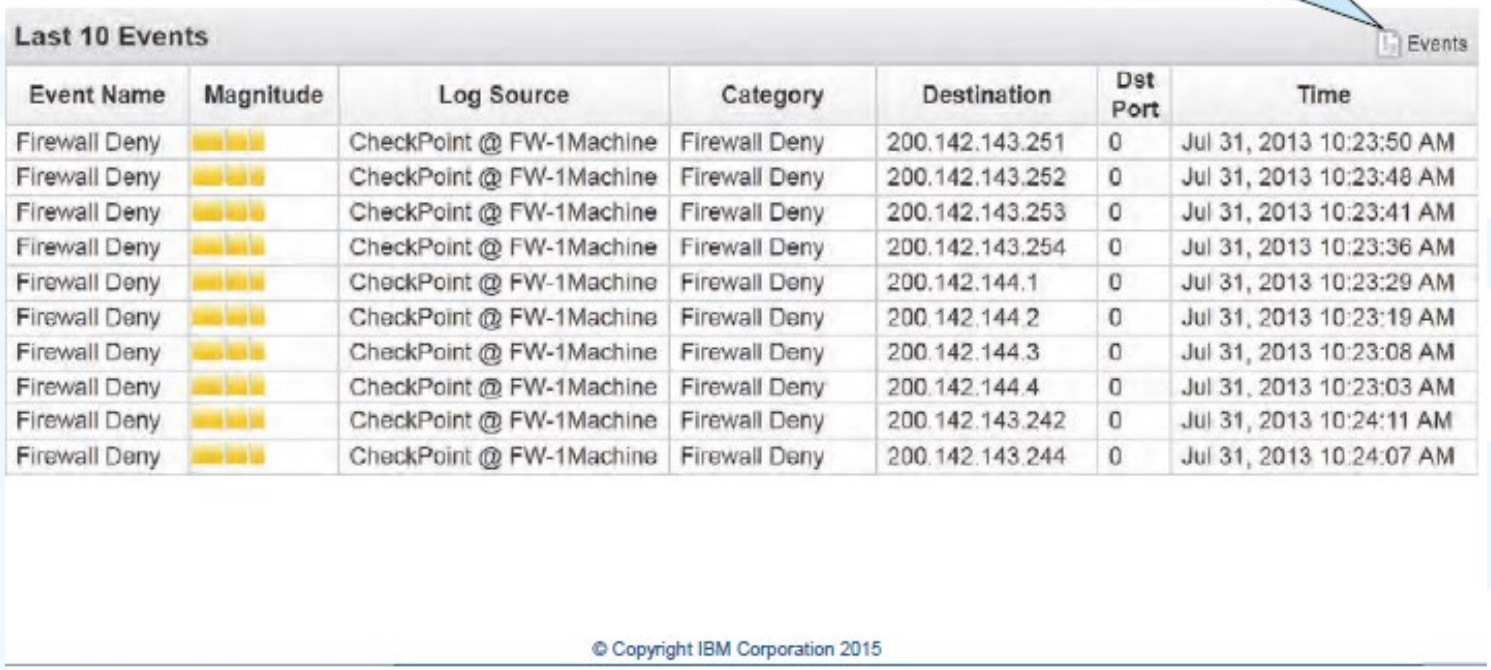
- Use the list of events to navigate event details
- Filter events included in an offense
- Group events to gain different perspectives
- Save a search that monitors a suspicious host
- Modify a saved search
- Add a search to the dashboard

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

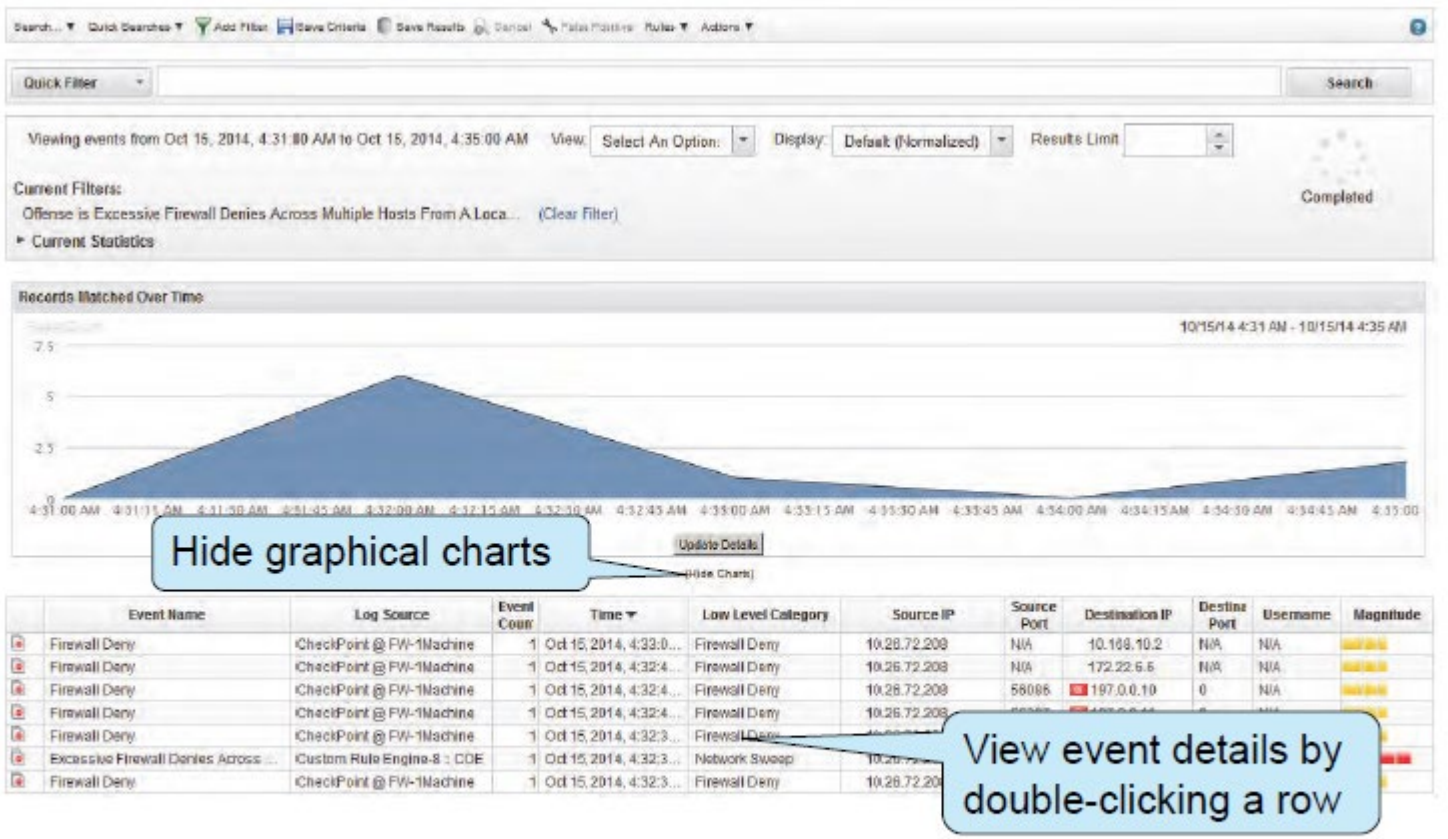


Last 10 Events

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

List of events

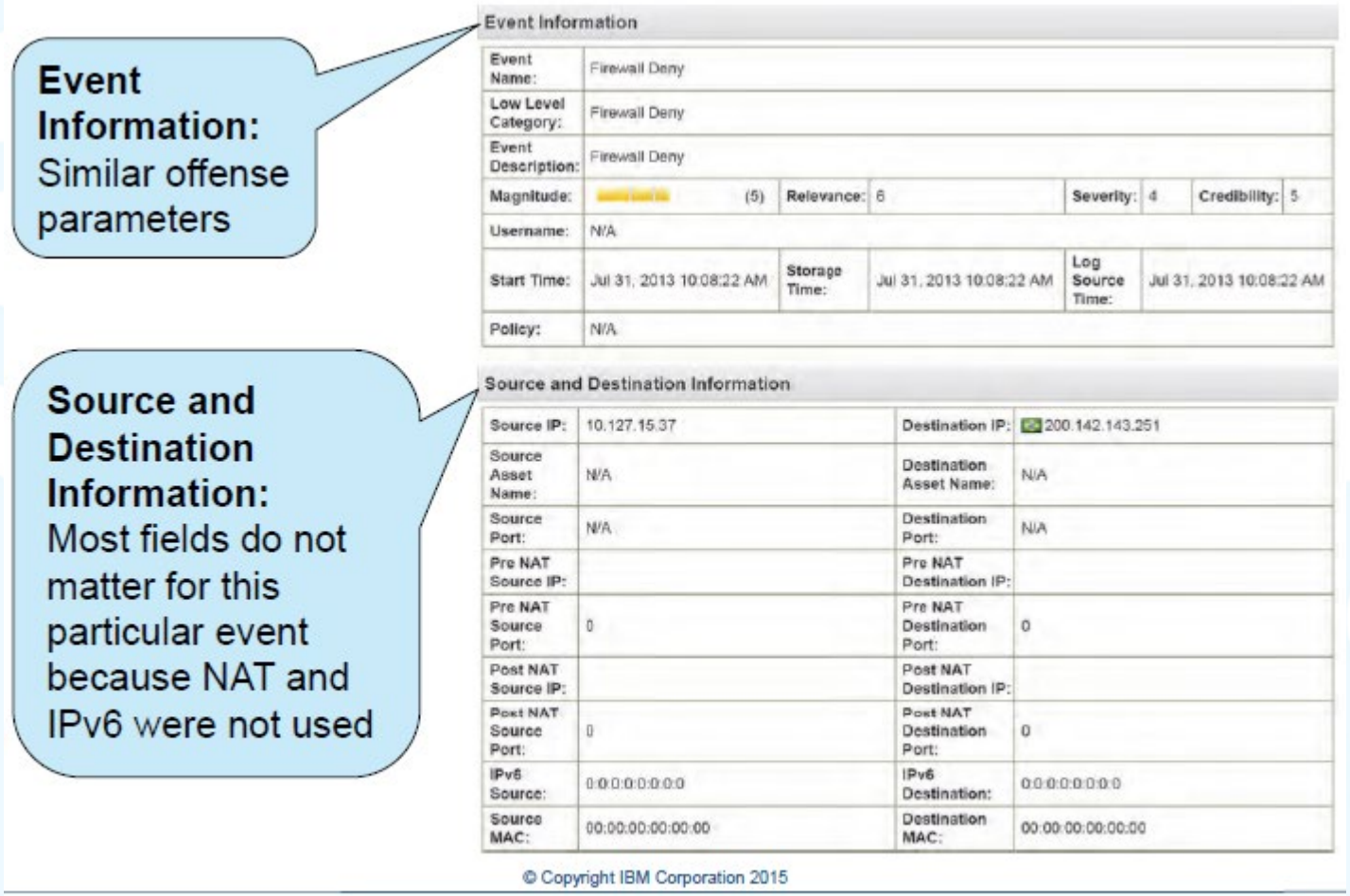


List of events

Event details: Base information

Event Information: Similar offense parameters

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



Event Information

Event Name:	Firewall Deny						
Low Level Category:	Firewall Deny						
Event Description:	Firewall Deny						
Magnitude:	[redacted] (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

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

Event details: Base information

Event details: Base information

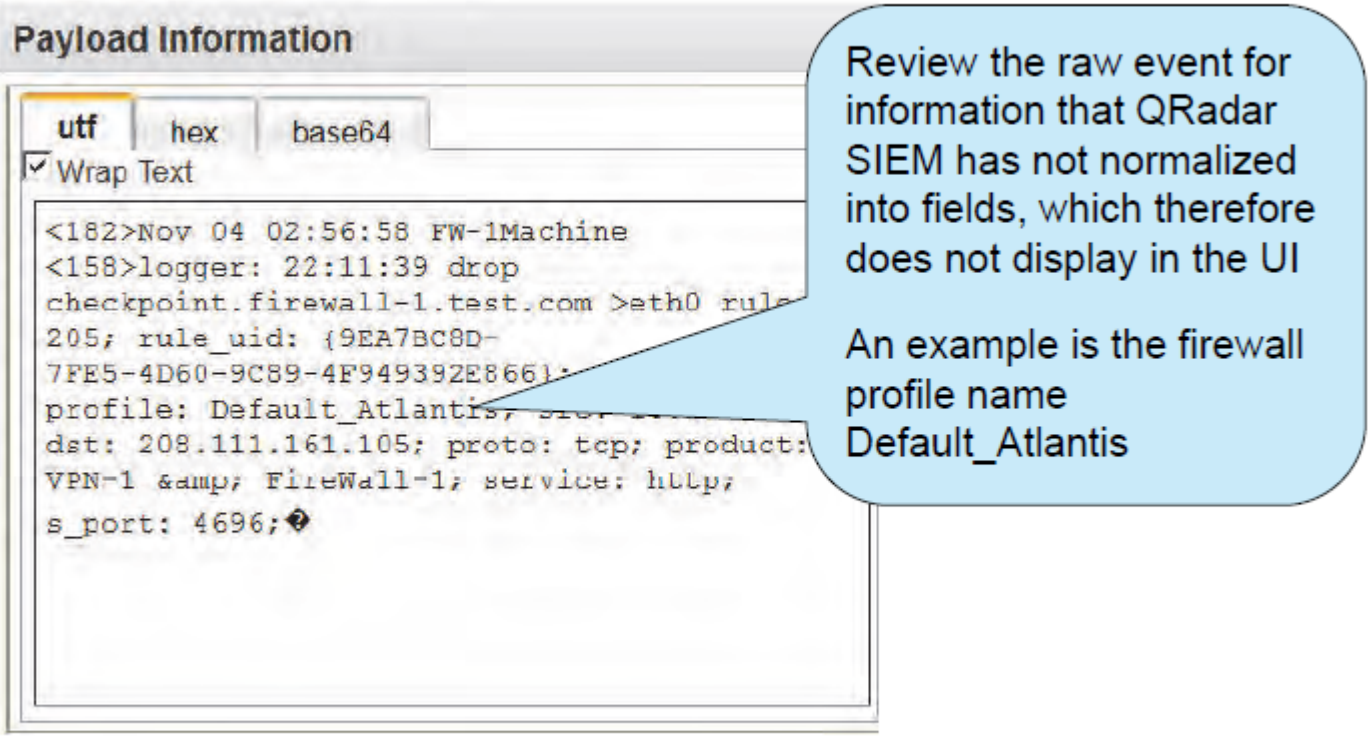
Event details: Base information

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

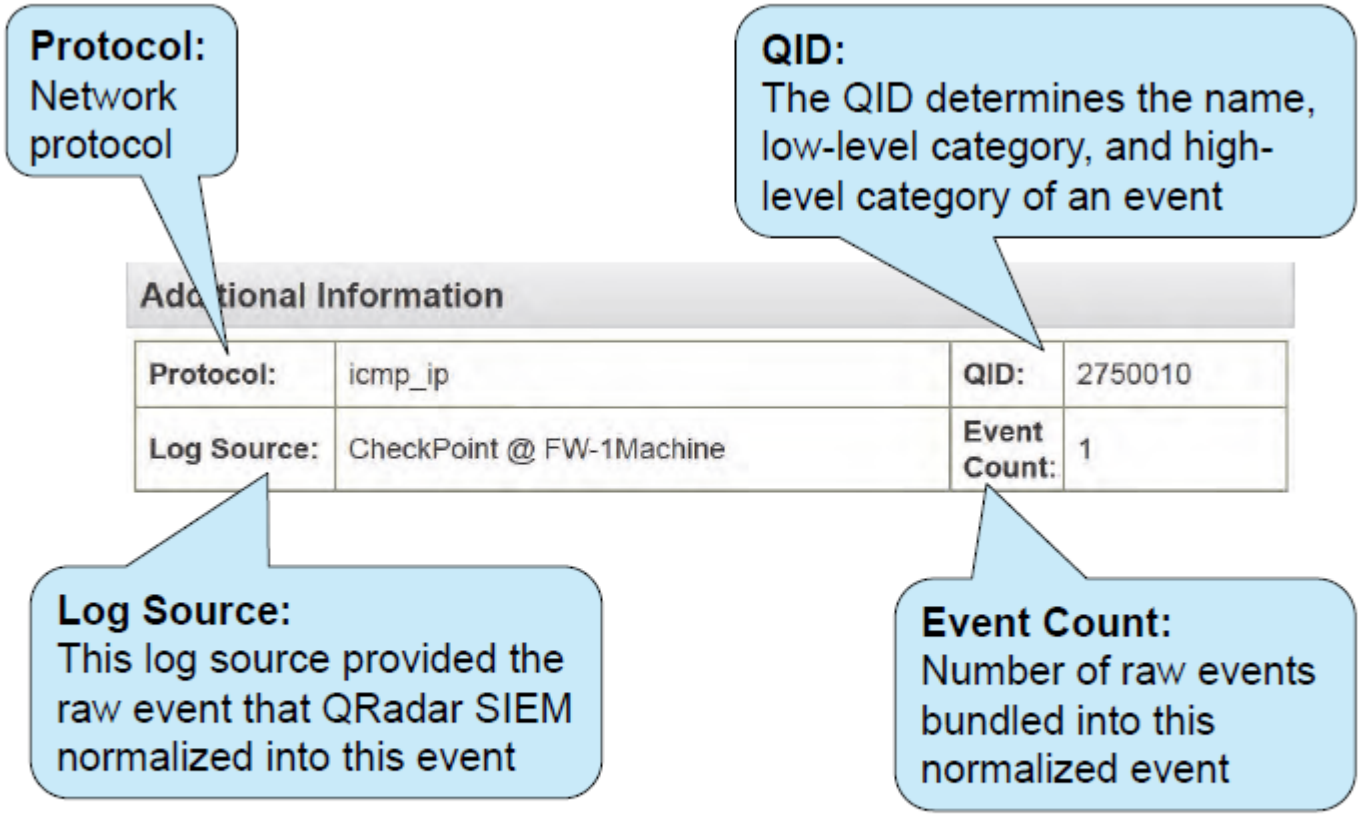
Event details: Reviewing the raw event

Each normalized event carries its raw event as the payload



Event details: Reviewing the raw event

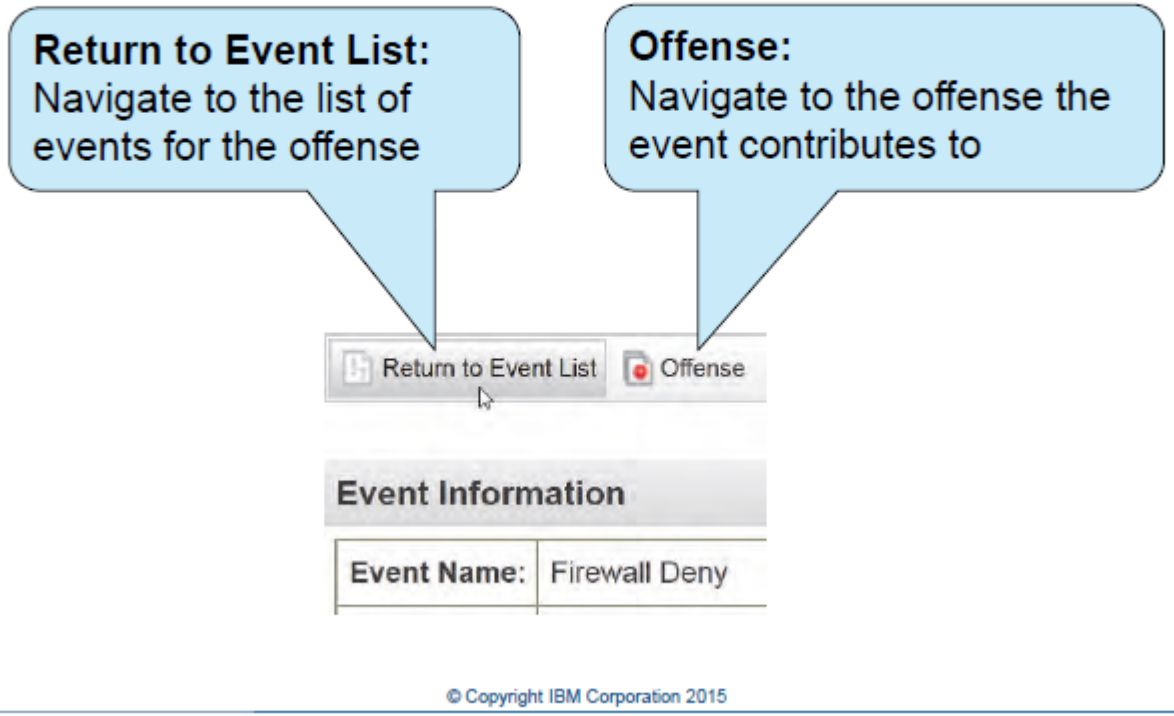
Event details: Additional details



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

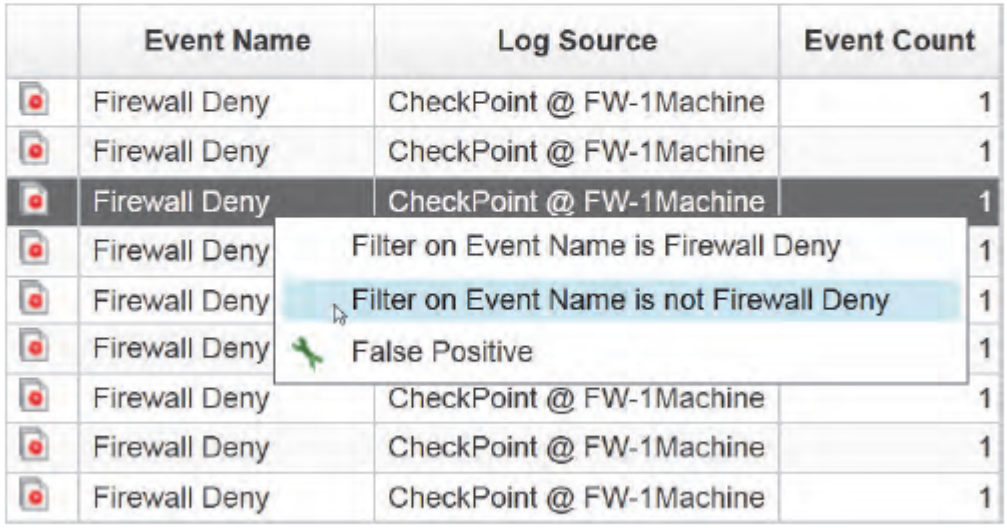


Returning to the list of events

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



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
	Local ICMP Scanner	Custom Rule Engine-8 :: COE
	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
	Local ICMP Scanner	Custom Rule Engine-8 :: COE
	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
	Excessive Firewall Denies Across Multiple Hosts From A Local Host	Custom Rule Engine-8 :: COE
	Local ICMP Scanner	Custom Rule Engine-8 :: COE

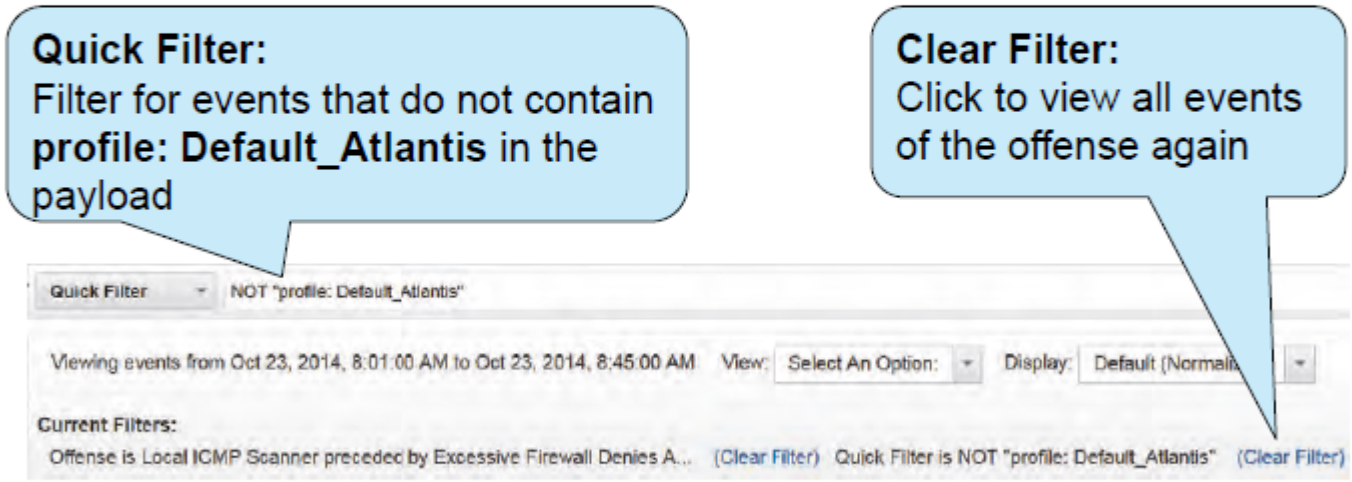
The Custom Rule Engine (CRE) in QRadar SIEM created the events in this list to alert you to suspicious activity

Filtering events (3 of 3)

Unlike searches, filters do not query each event processor

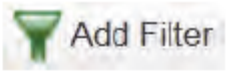
Applying a Quick Filter to the payload

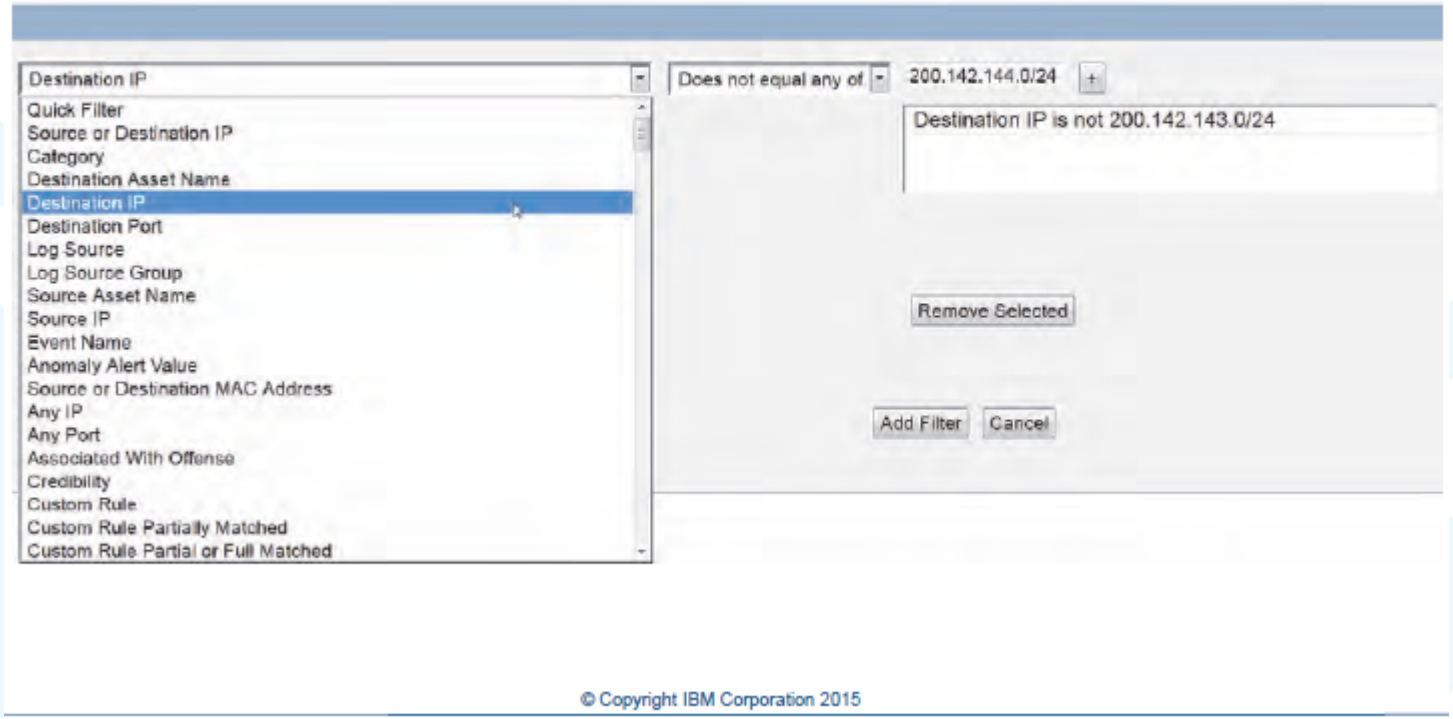
- The payload of an event contains the raw event that mentions the firewall profile that denied the connection
- To verify that the company's main profile, Atlantis, was always active, filter events without **profile: Default_Atlantis** in the payload



Applying a Quick Filter to the payload

Using another filter option

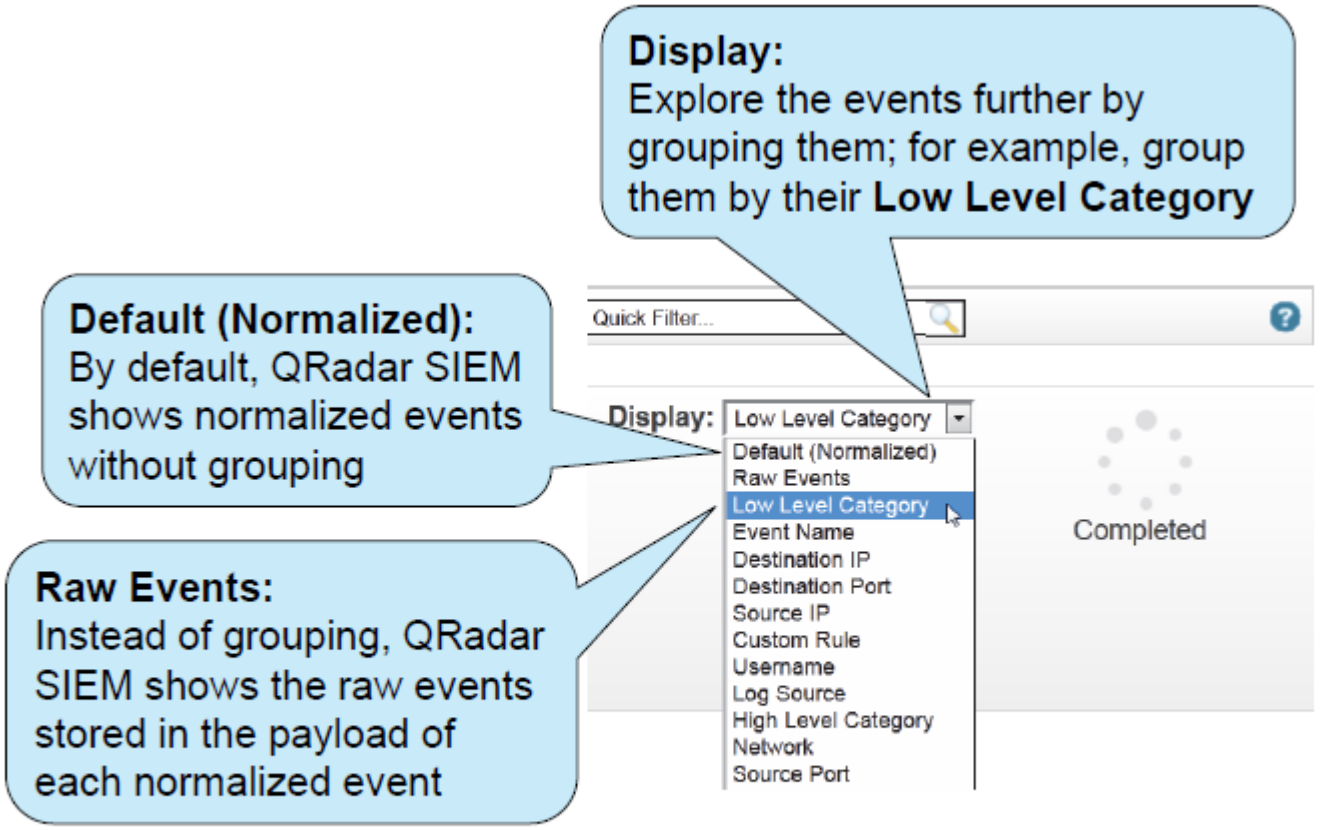
- You can use each event field as a filter
- To create a filter, in the top menu bar, click the icon 



Using another filter option

Using grouping to investigate events

Grouping events

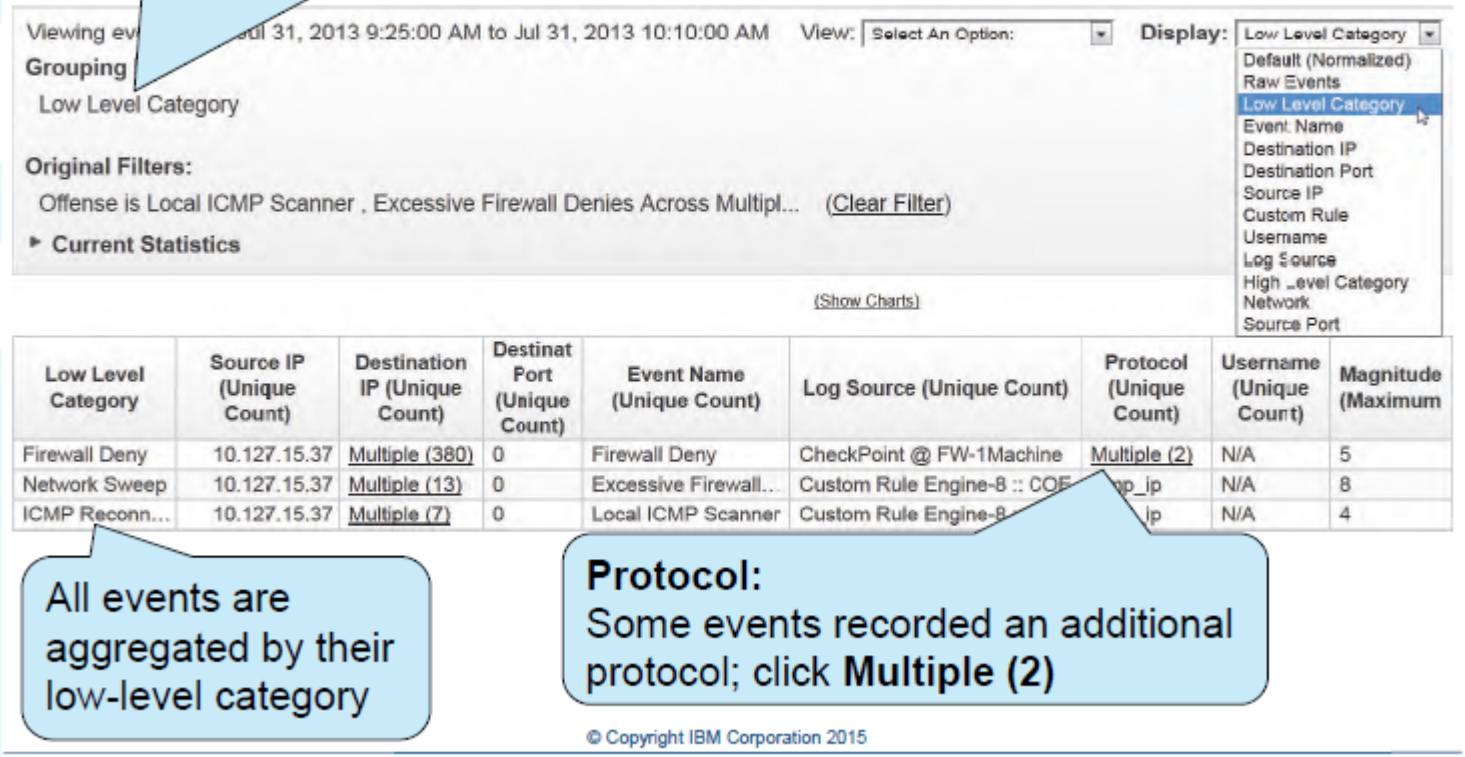


Grouping events

Grouping events by low-level category

Grouping By:
QRadar SIEM shows the currently selected grouping above the filters

In this example, exploring by grouping indicates a second protocol



All events are aggregated by their low-level category

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

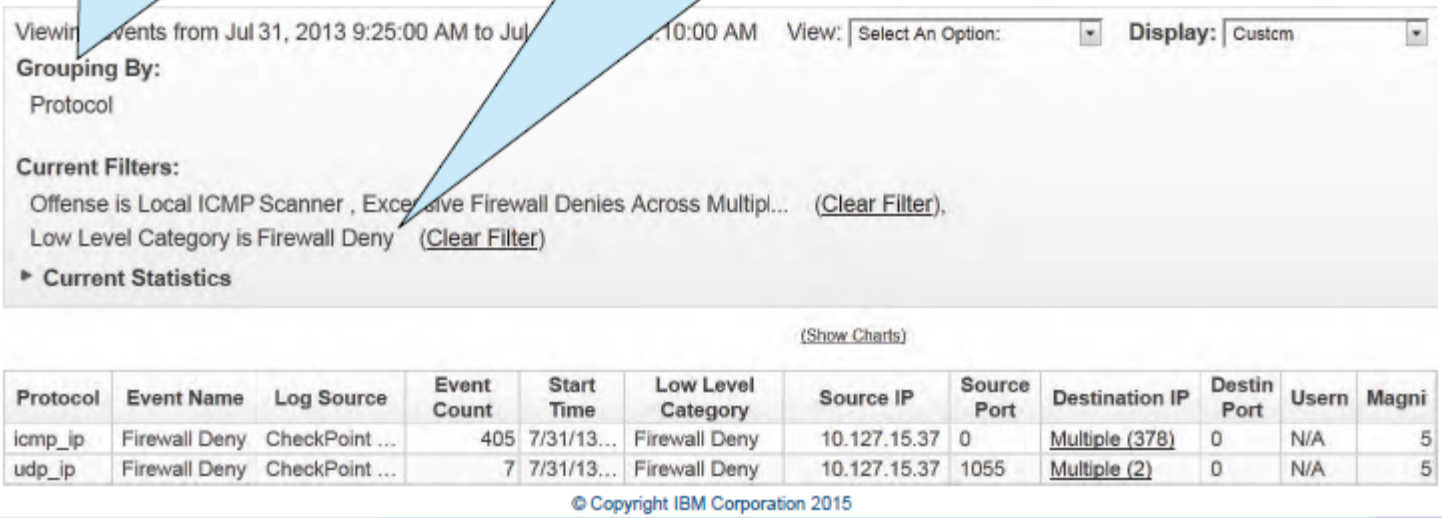
Grouping events by low-level category

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

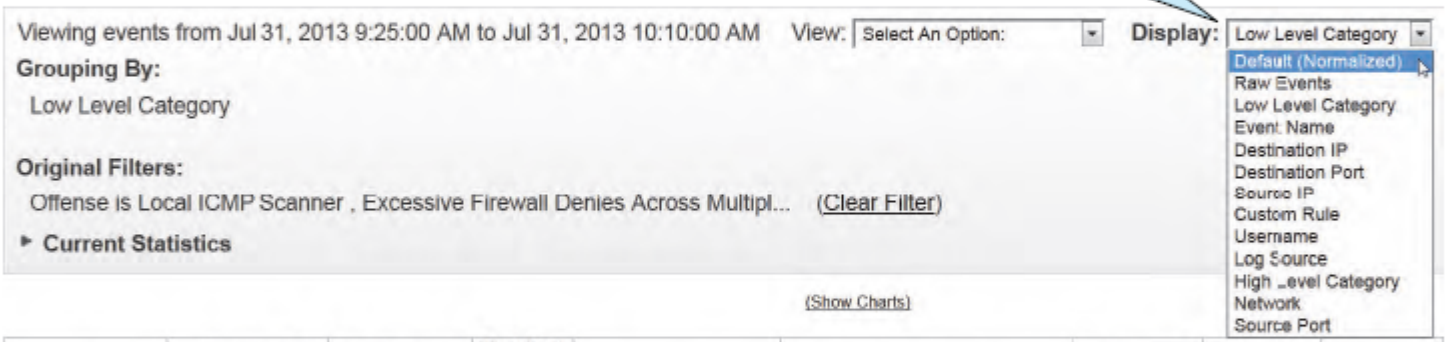
Current Filters:
The previous grouping, Low Level Category, became a filter



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

Removing grouping criteria

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



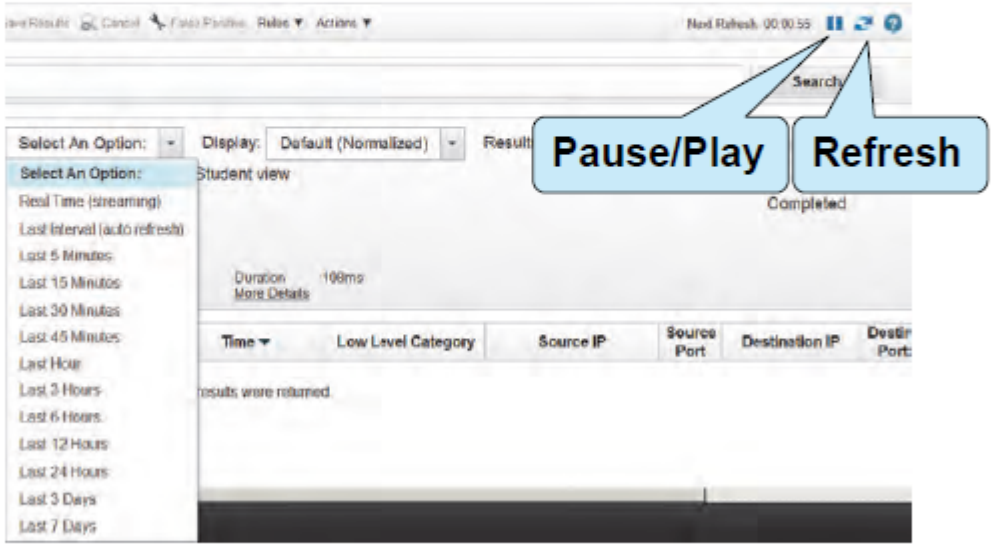
Low Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destinat Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum
Firewall Deny	10.127.15.37	Multiple (380)	0	Firewall Deny	CheckPoint @ FW-1Machine	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

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

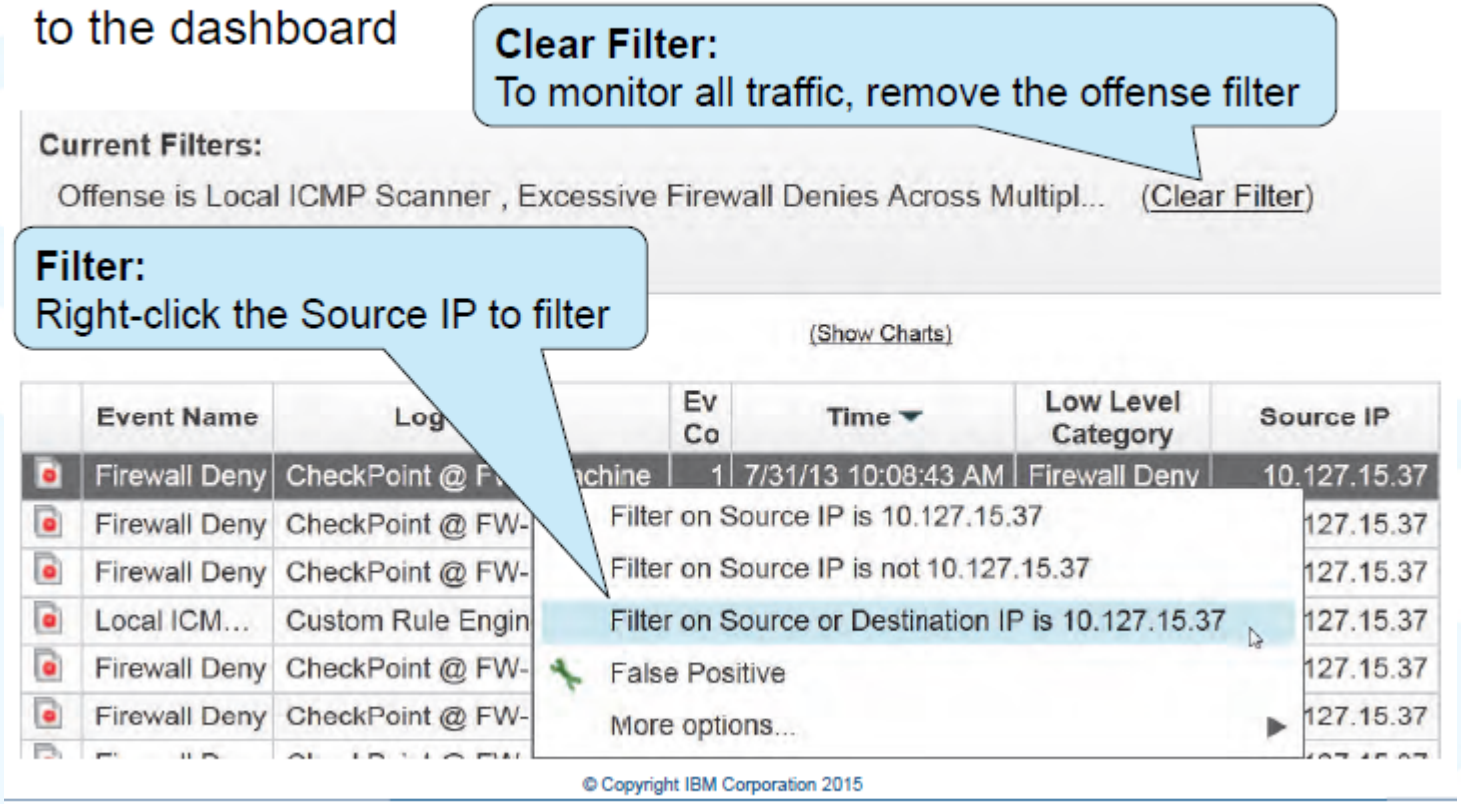


Viewing a range of events

Saving a search

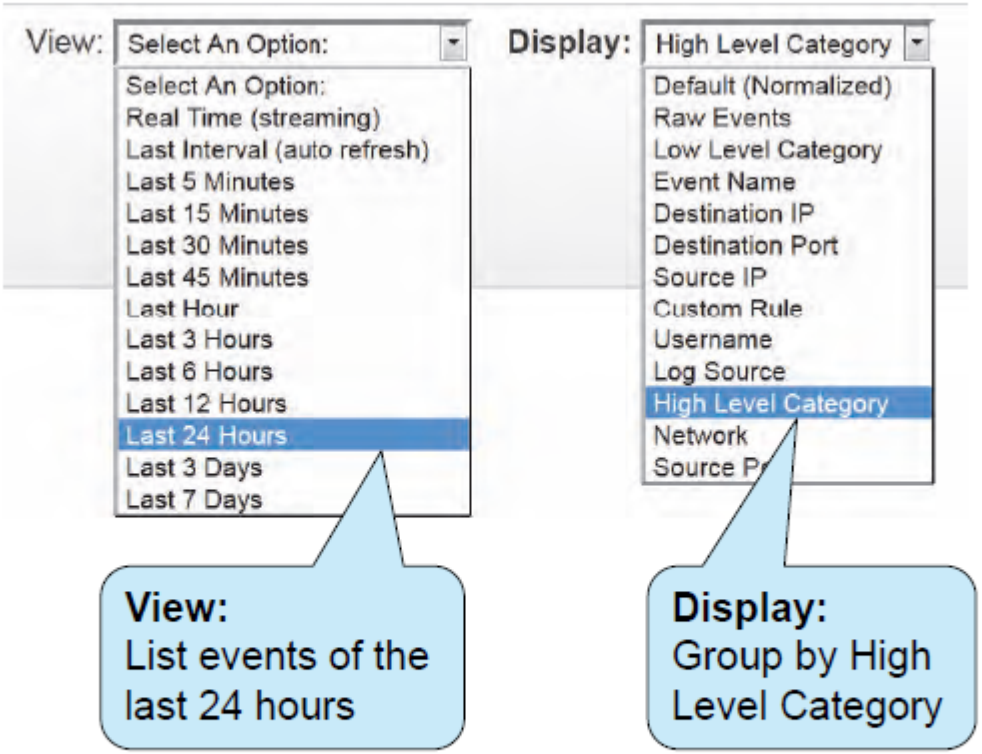
Monitoring the scanning host (1 of 3)

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



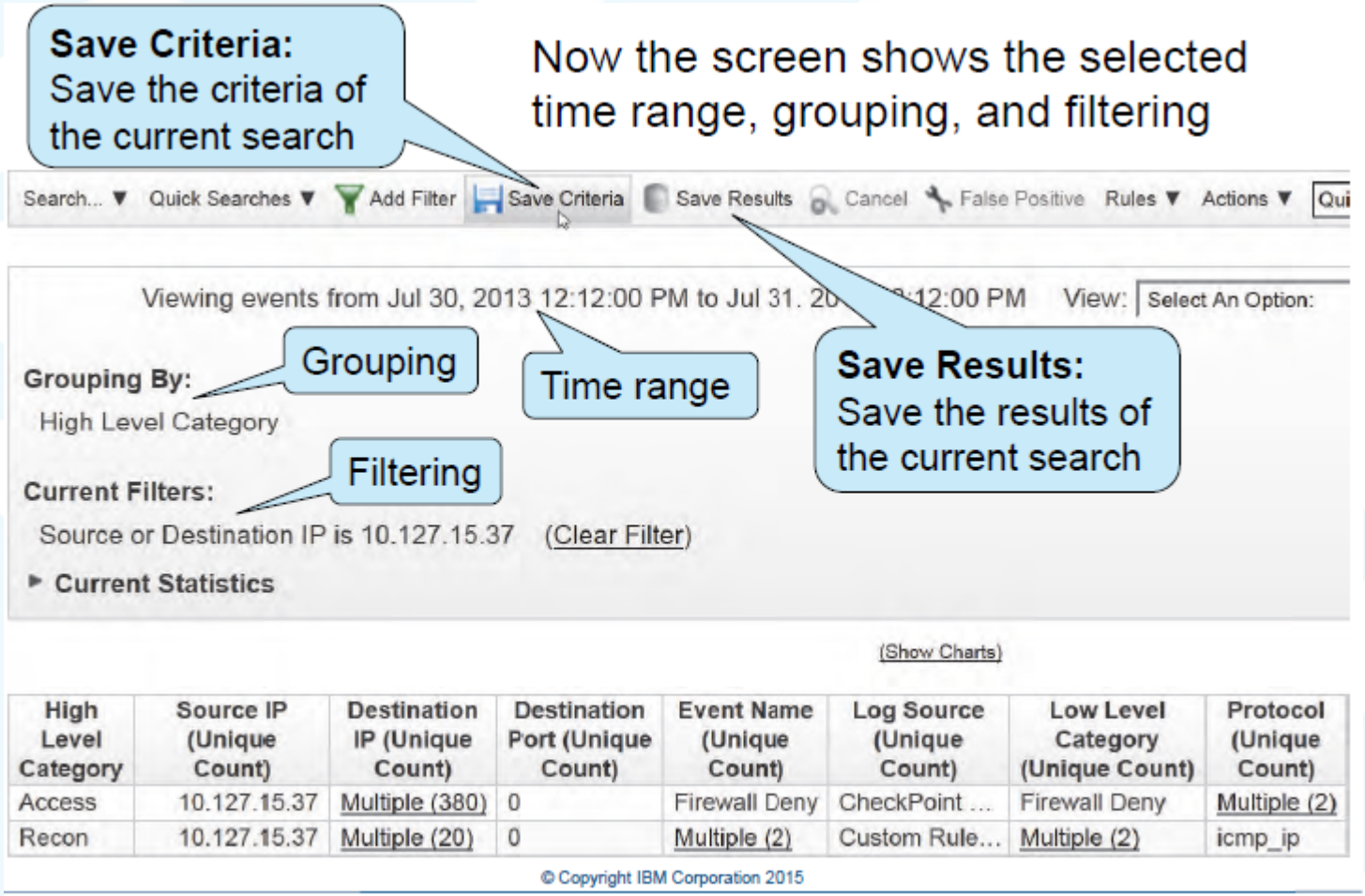
Monitoring the scanning host

Monitoring the scanning host (2 of 3)



Monitoring the scanning host (2 of 3)

Monitoring the scanning host (3 of 3)

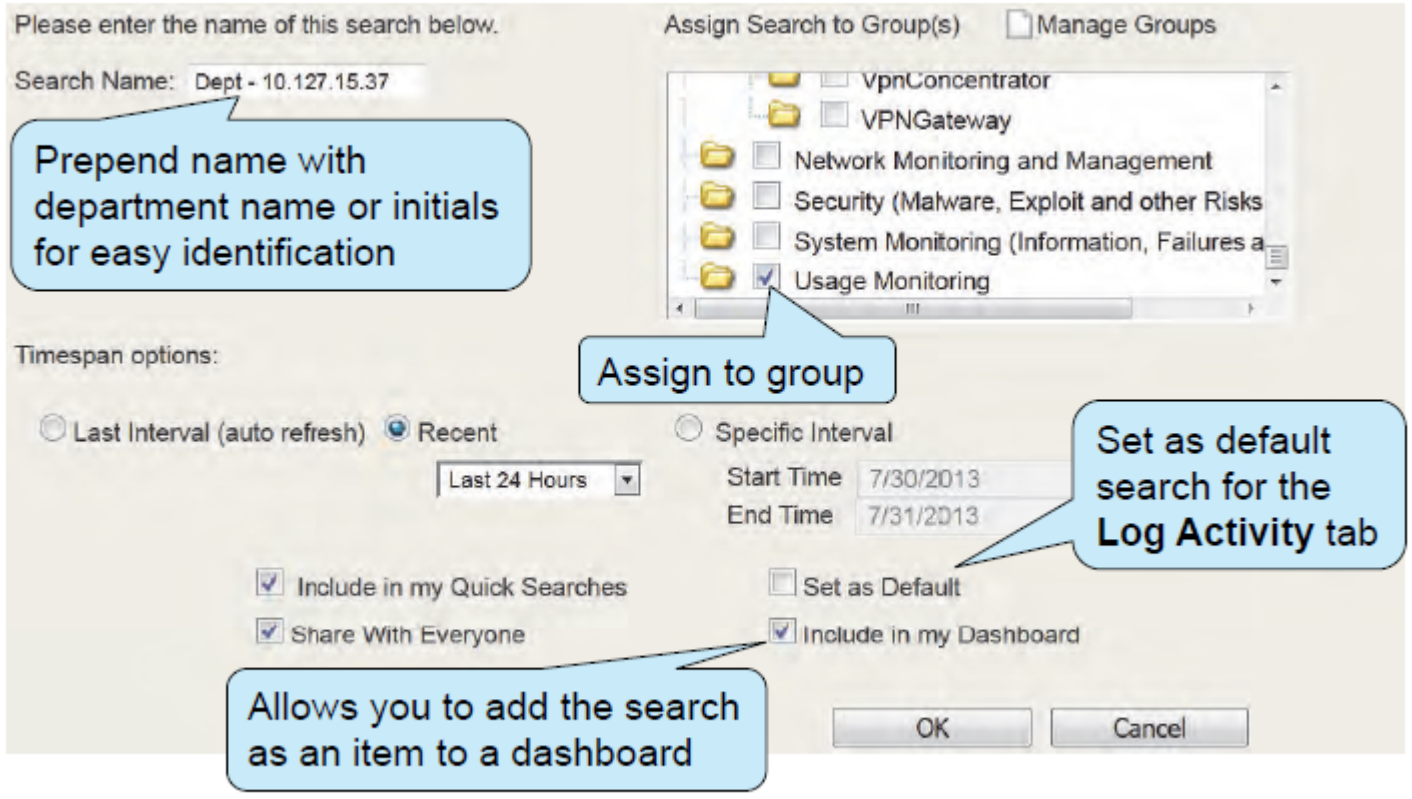


High Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)
Access	10.127.15.37	Multiple (380)	0	Firewall Deny	CheckPoint ...	Firewall Deny	Multiple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

Monitoring the scanning host (3 of 3)

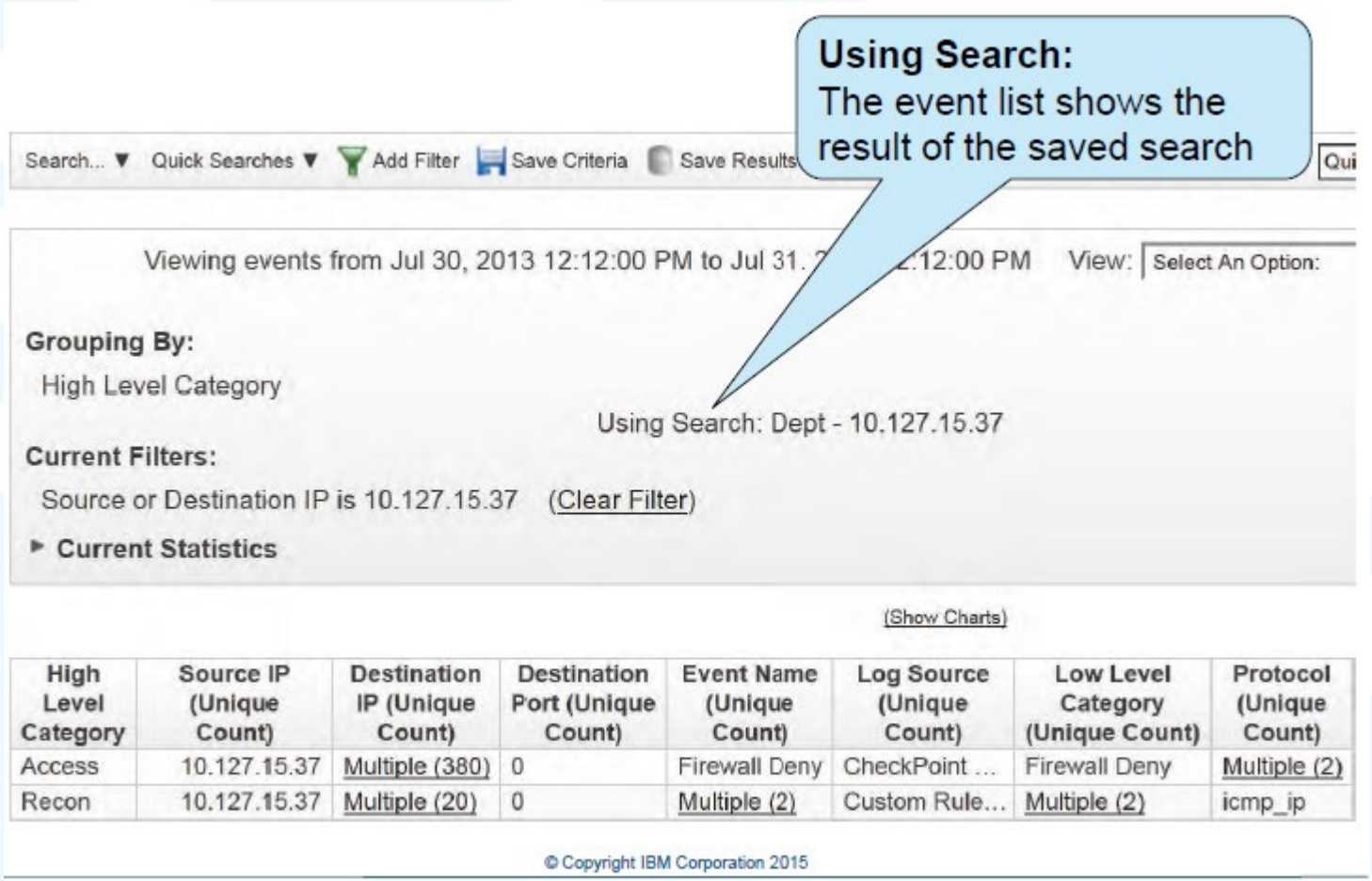
Saving search criteria

Save the search with the criteria specified



Saving search criteria

Event list using the saved search

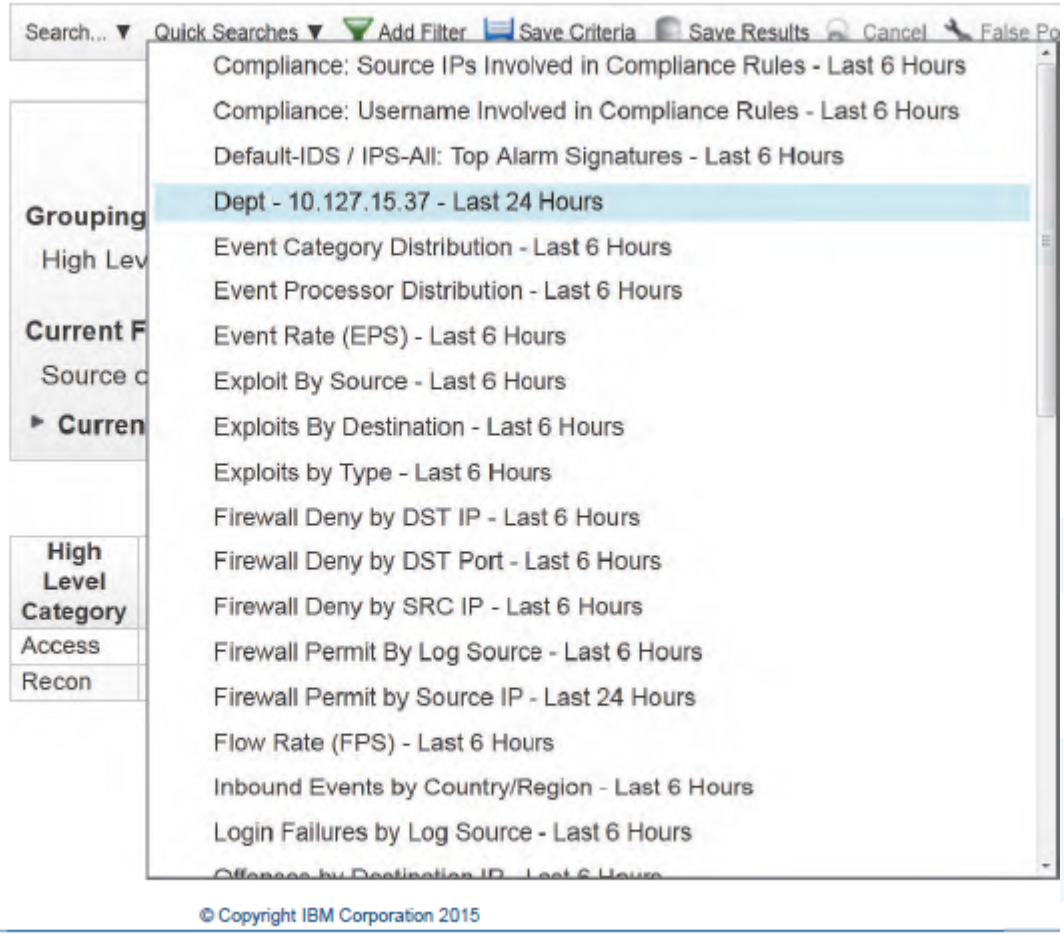


Event list using the saved search

Modifying saved searches

About Quick Searches

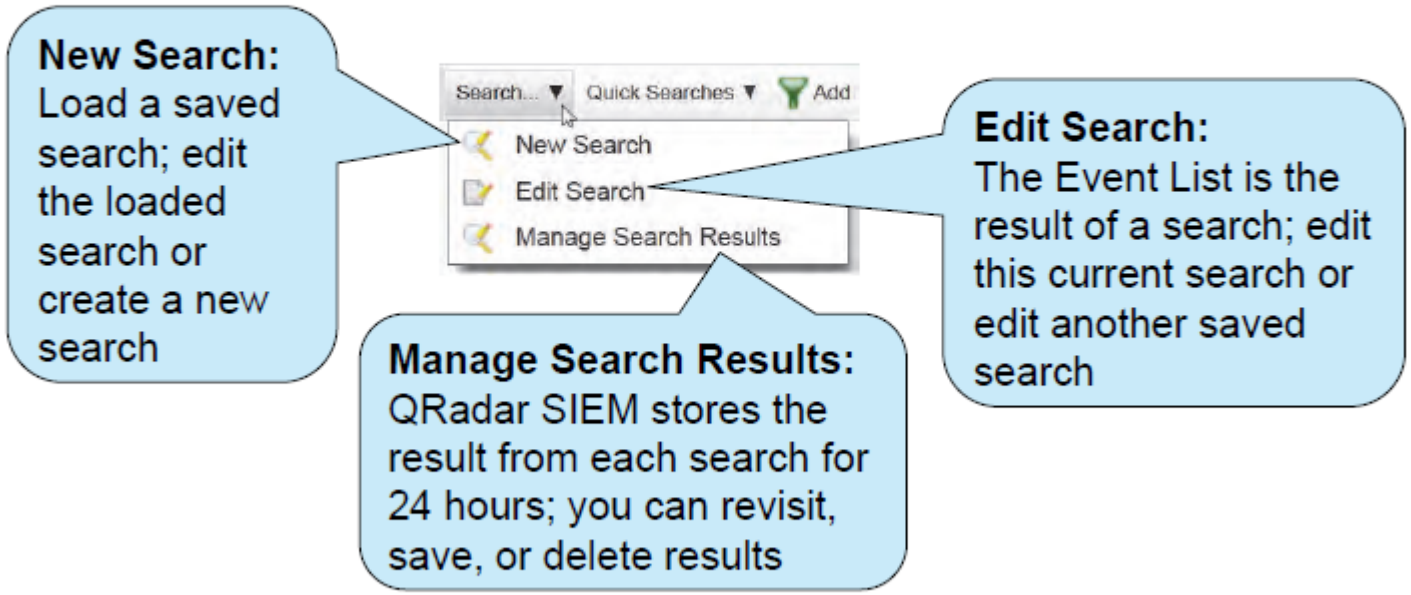
When you select **Include in my Quick Searches** when saving a search, QRadar SIEM lists the saved search in the predefined **Quick Searches** list



About Quick Searches

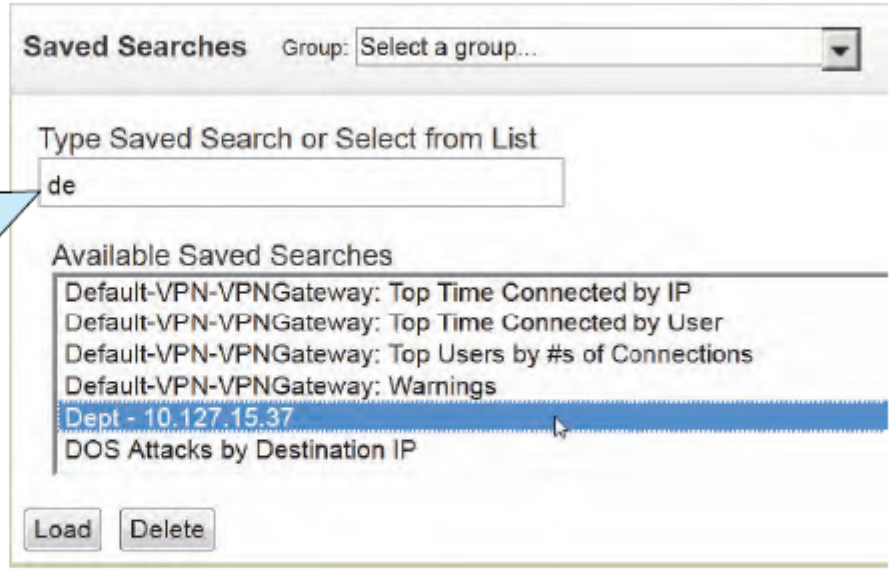
Using alternative methods to create and edit searches

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



Finding and loading a saved search

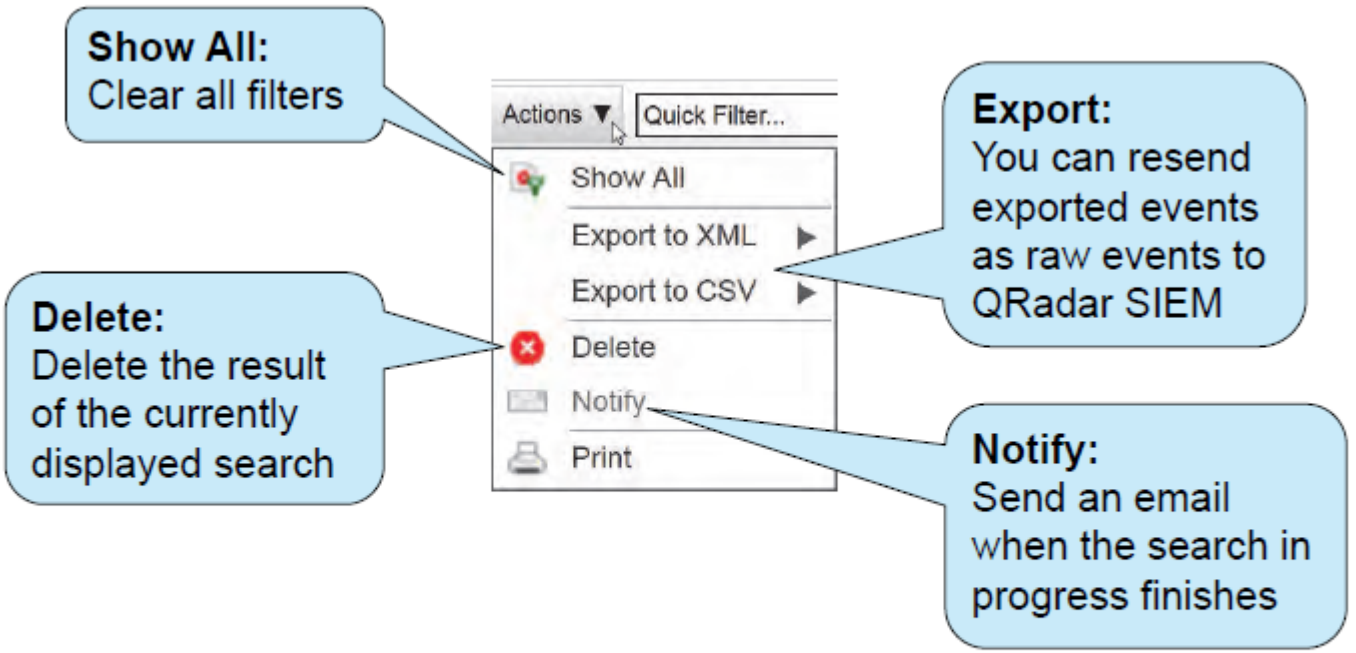
If you select **New Search** or **Edit Search**, the Event Search window opens



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

Finding and loading a saved search

Search actions

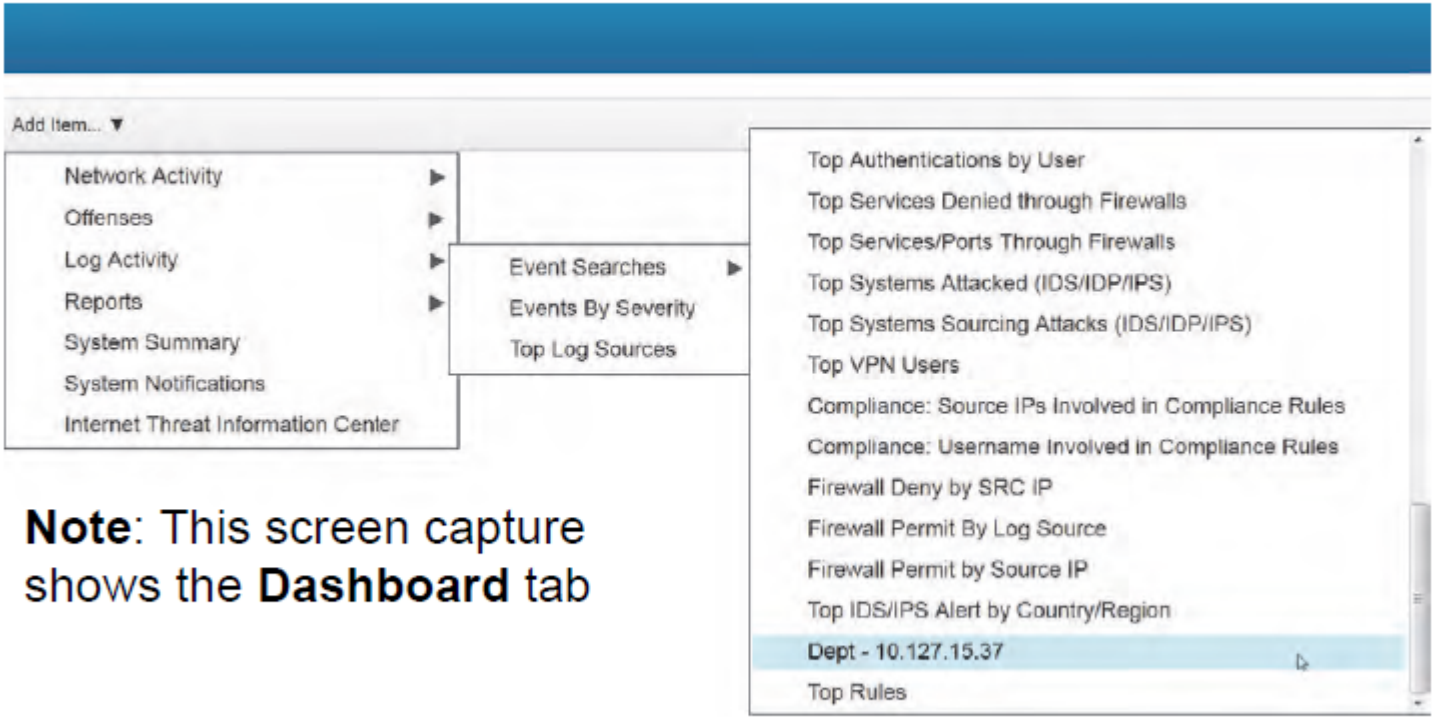


Search actions

Adding a search to the dashboard

Adding a saved search as a dashboard item

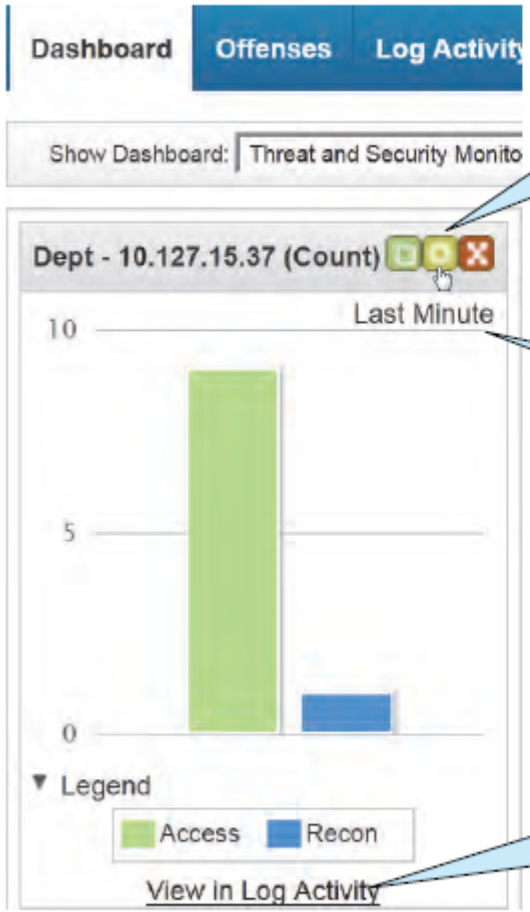
To watch the scanning IP address from the dashboard, add the saved search as a dashboard item



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

Adding a saved search as a dashboard item

Saving a search as a dashboard item



Settings button:
Modify the settings of an item

You can add only grouped searches as dashboard items

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

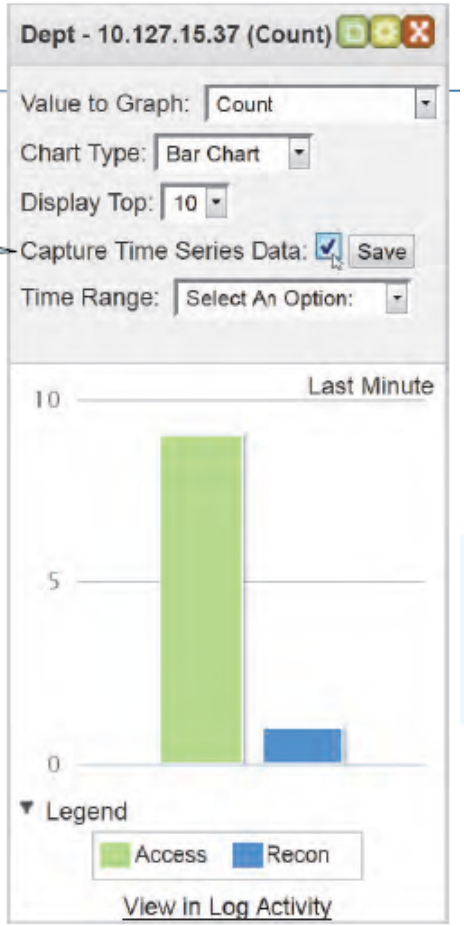
View in Log Activity:
Show the saved search with a 24-hour time range on **Log Activity** tab

Saving a search as a dashboard item

Enabling time-series data

Enabling time-series data

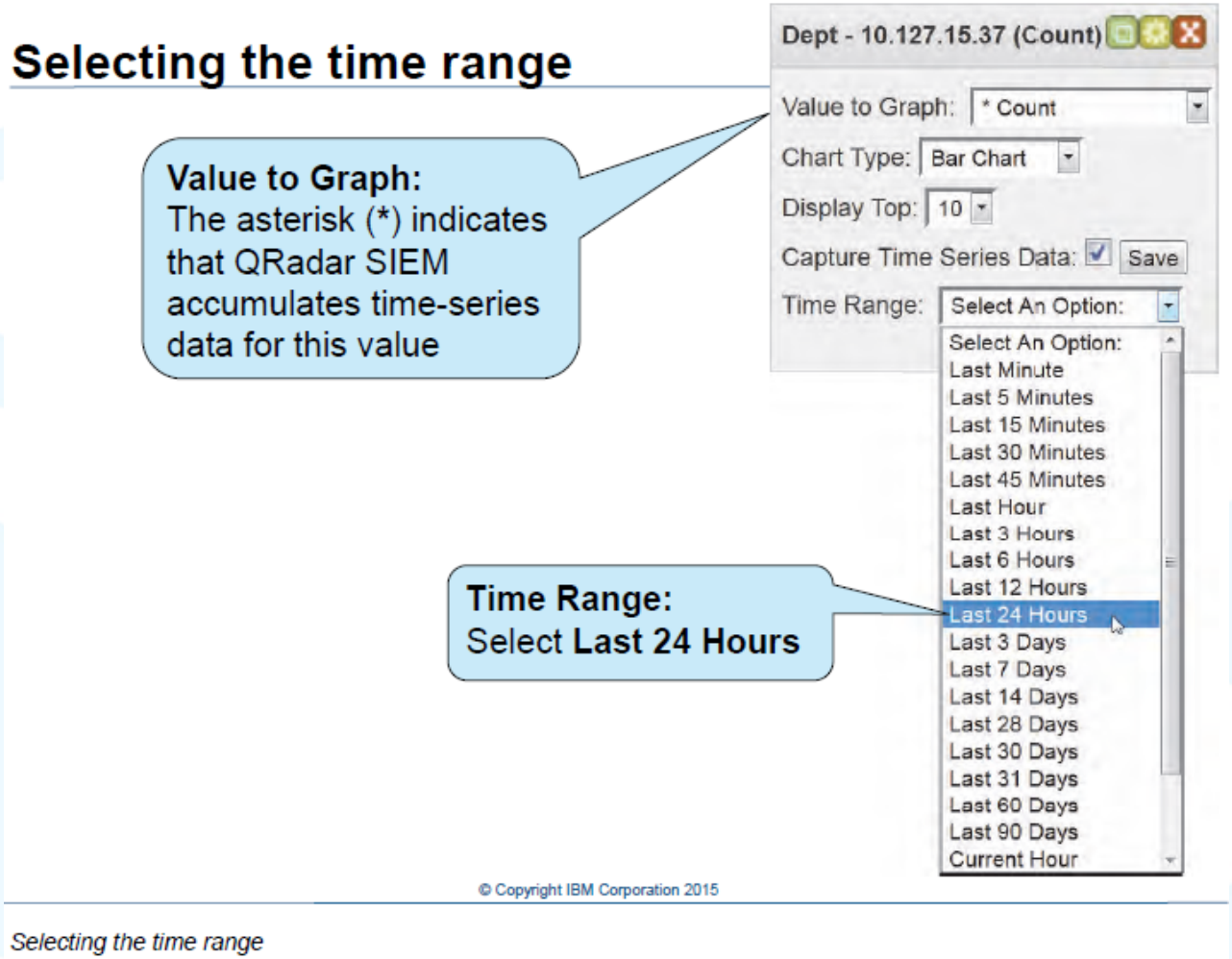
Capture Time Series Data:
Select to accumulate time-series data to count events and click **Save**



- 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

Enabling time-series data

Saving the time range



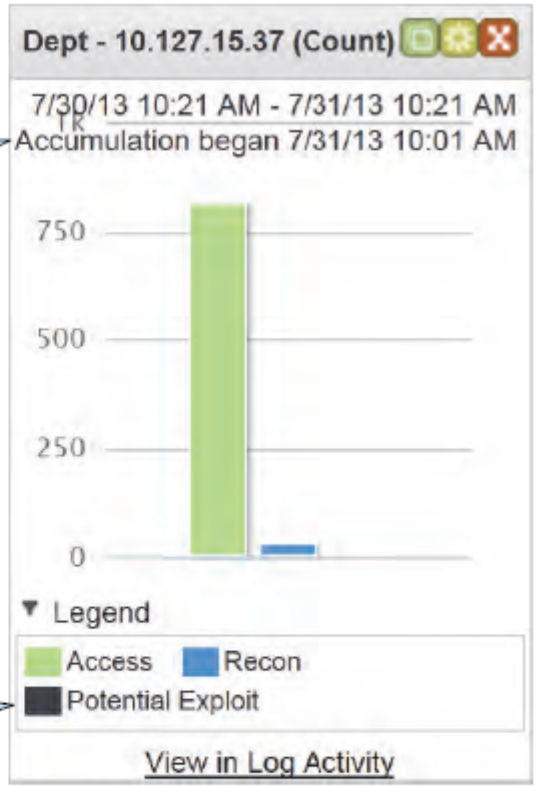
Selecting the time range

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



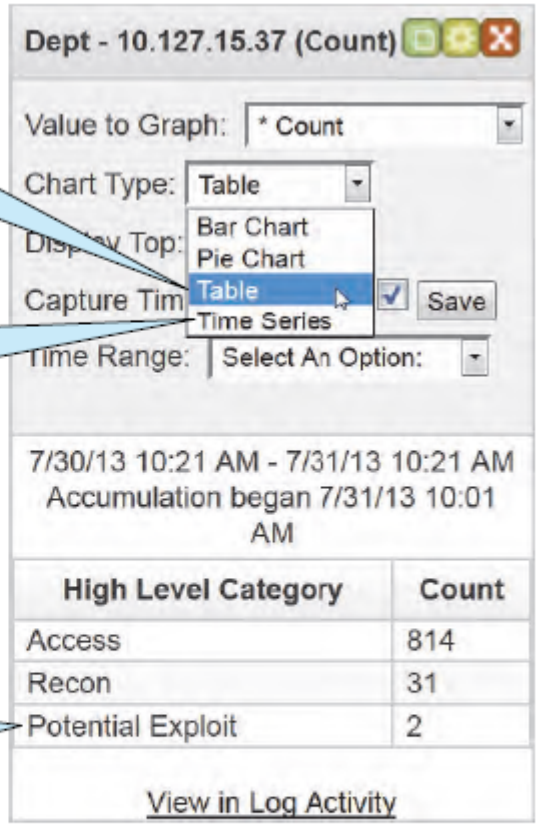
Displaying 24 hours in a dashboard item

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



Modifying items in the chart type table

Summary

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

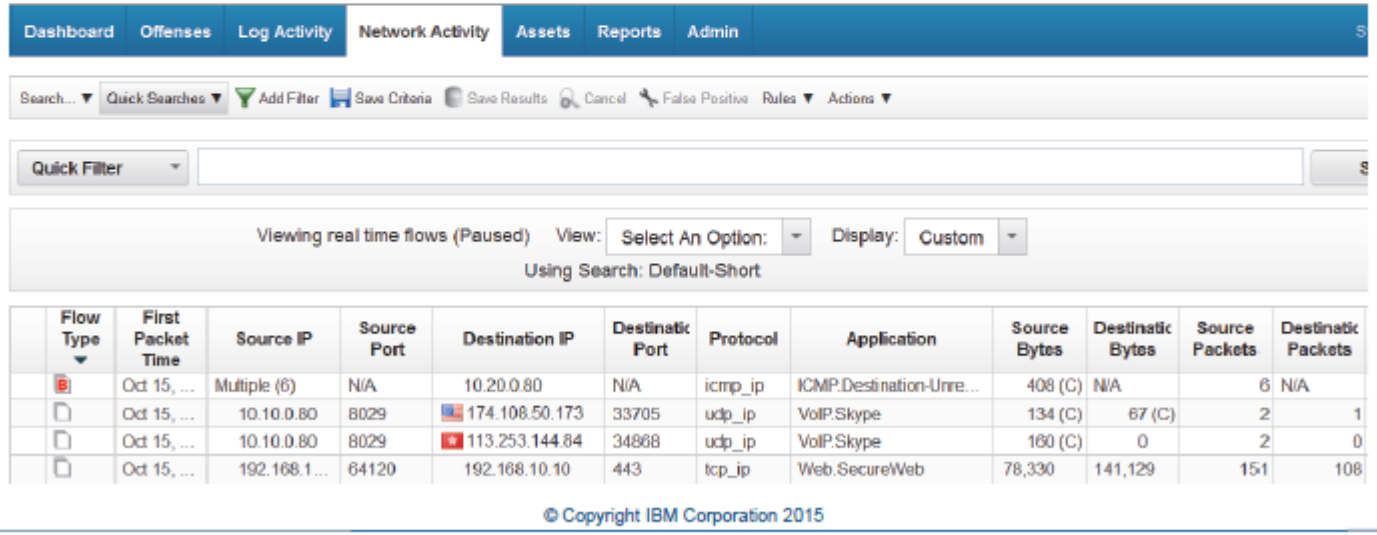
Viewing and grouping flows

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

Network Activity tab

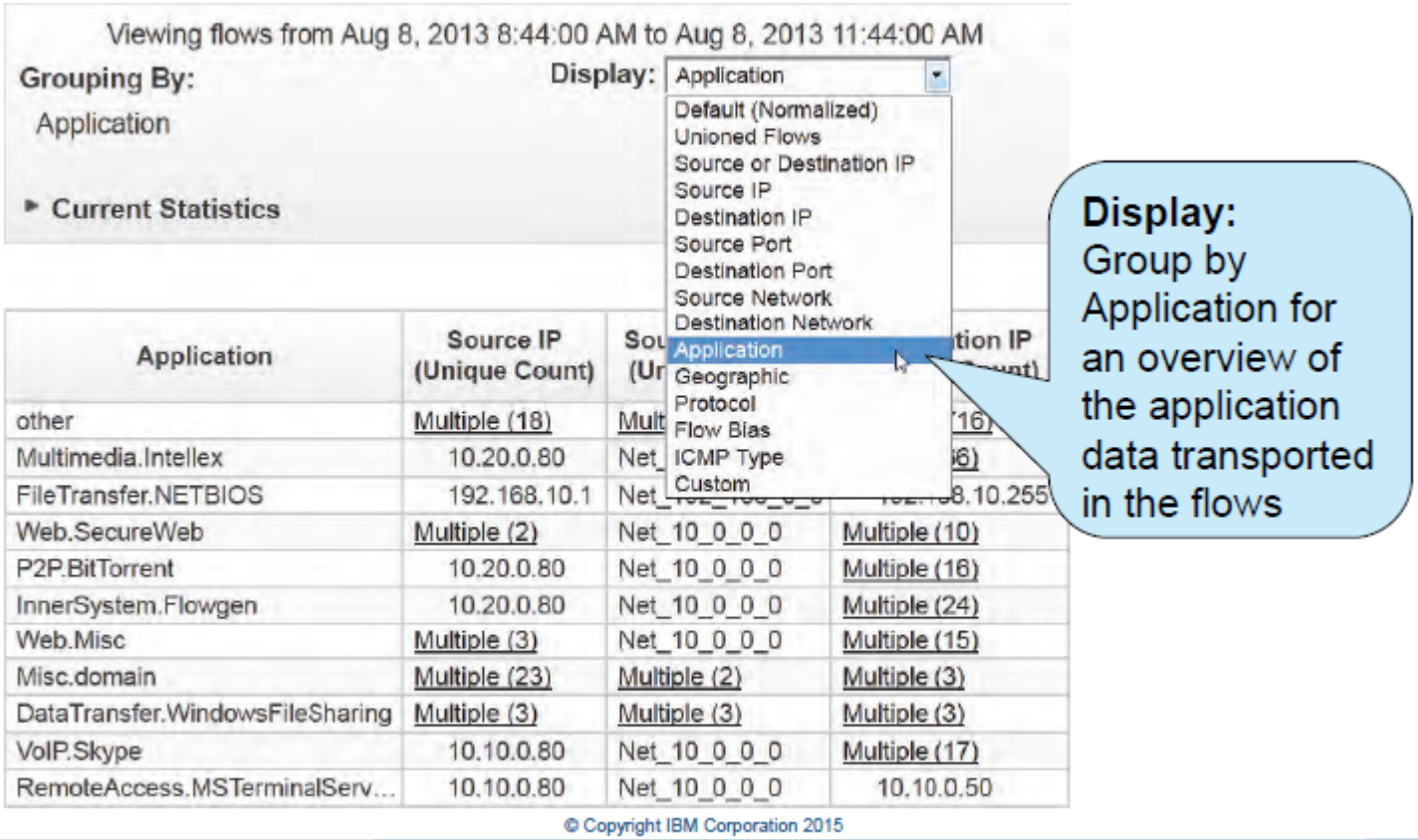
- Click the **Network Activity** tab to perform these tasks
  - Investigate flows sent to QRadar SIEM
  - Perform detailed searches
  - View network activity
- Flows on the **Network Activity** tab are shown in a similar way as events are on the **Log Activity** tab



Network Activity tab

Grouping flows

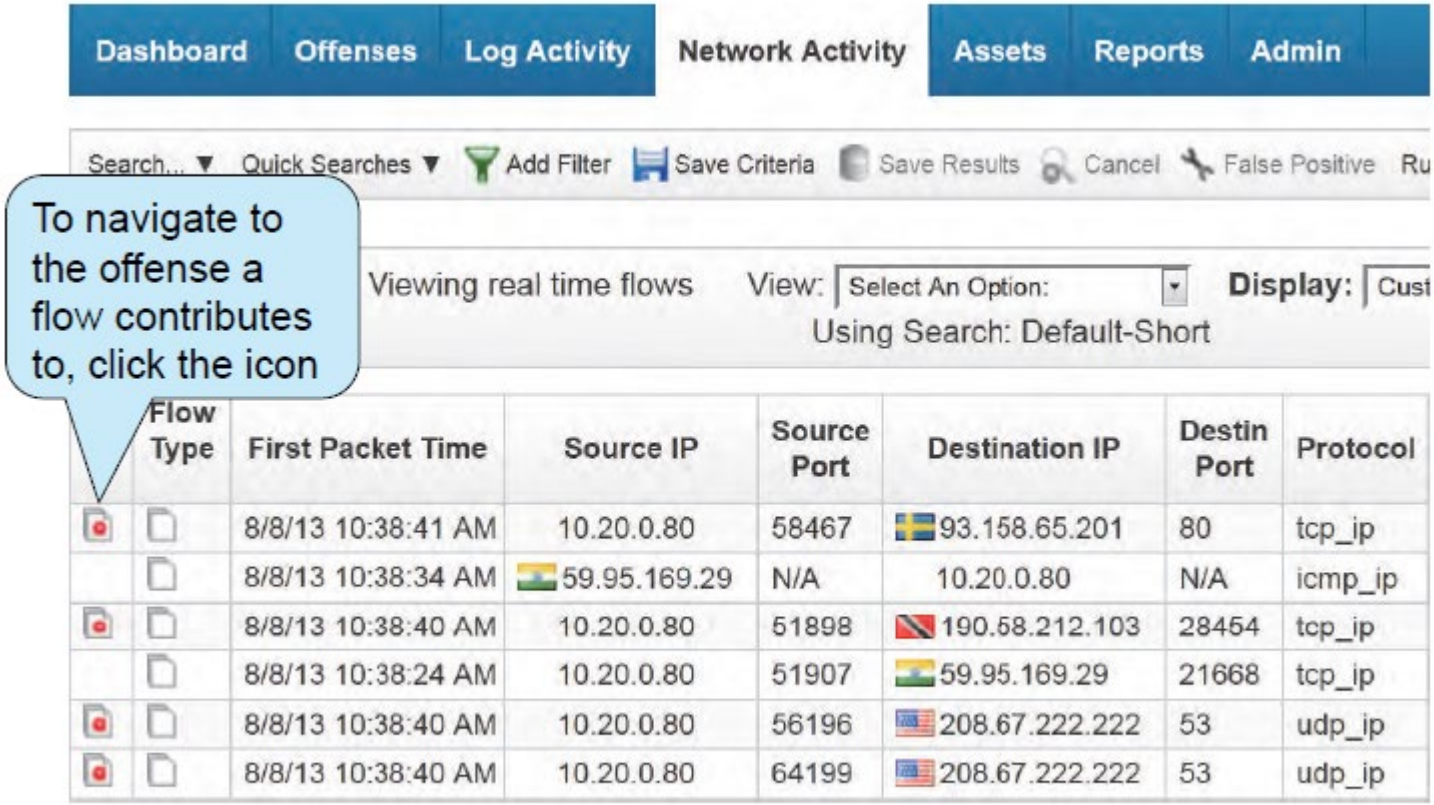
Some flow grouping options differ from event grouping options.



Grouping flows

Finding an offense

A red icon indicates that a flow contributes to an offense



Finding an offense

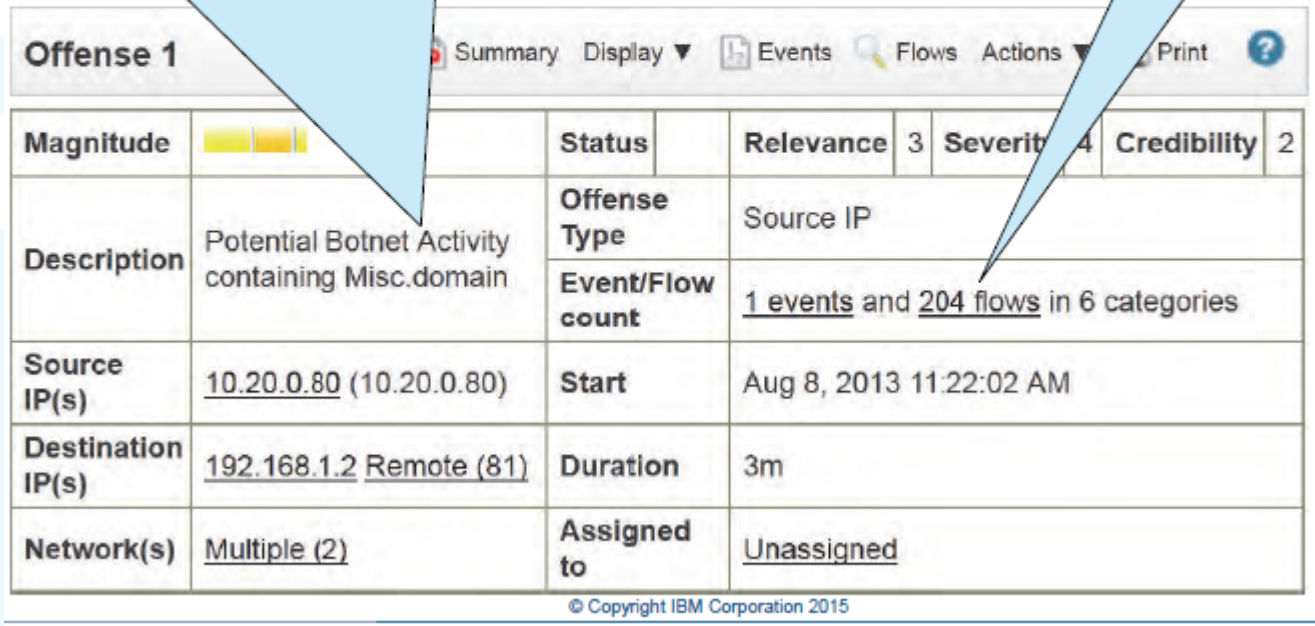
Using summary information to investigate an offense

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



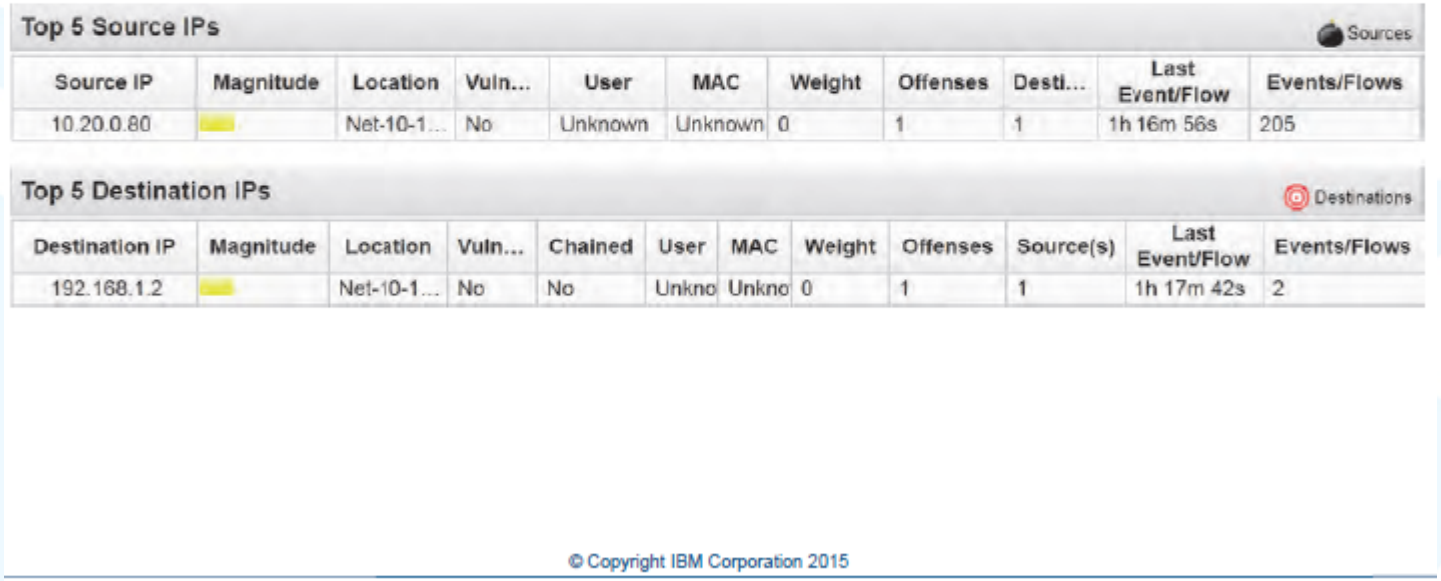
Offense 1 Summary Display ▼ Events Flows Actions ▼ Print

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)	10.20.0.80 (10.20.0.80)	**Start**	Aug 8, 2013 11:22:02 AM					
Destination IP(s)	192.168.1.2 Remote (81)	**Duration**	3m					
Network(s)	Multiple (2)	**Assigned to**	Unassigned					

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

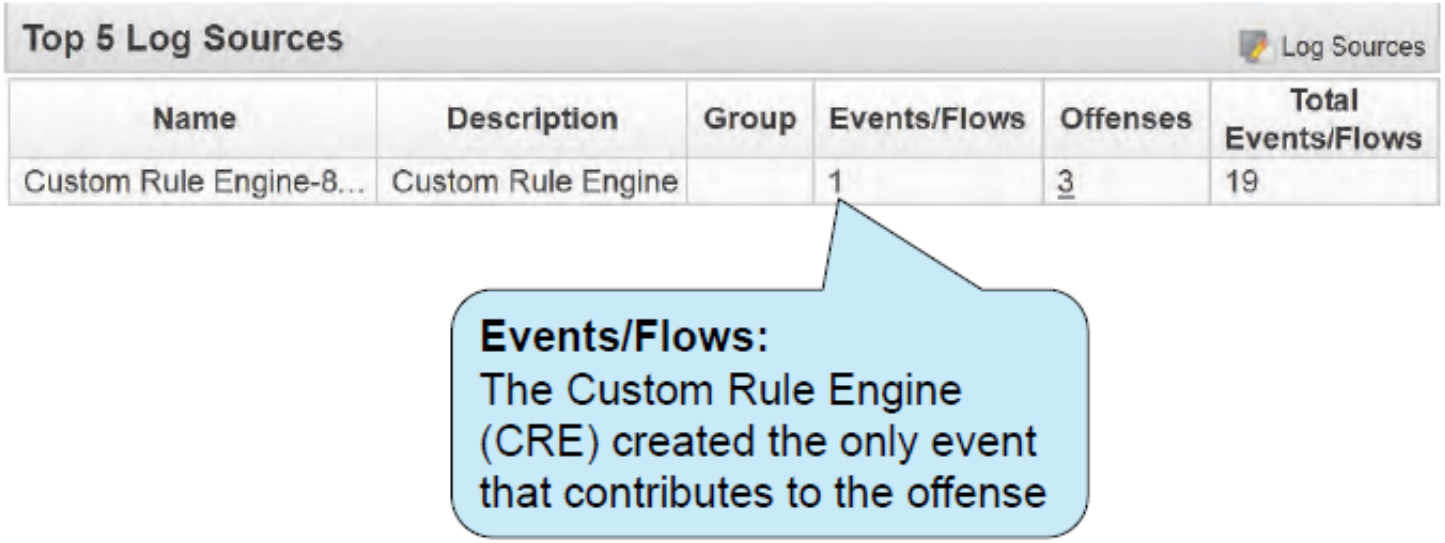
Source IP	Magnitude	Location	Vuln...	User	MAC	Weight	Offenses	Desti...	Last Event/Flow	Events/Flows
10.20.0.80		Net-10-1...	No	Unknown	Unknown	0	1	1	1h 16m 56s	205

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		Net-10-1...	No	No	Unkno	Unkno	0	1	1	1h 17m 42s	2

Top 5 Source and Destination IPs

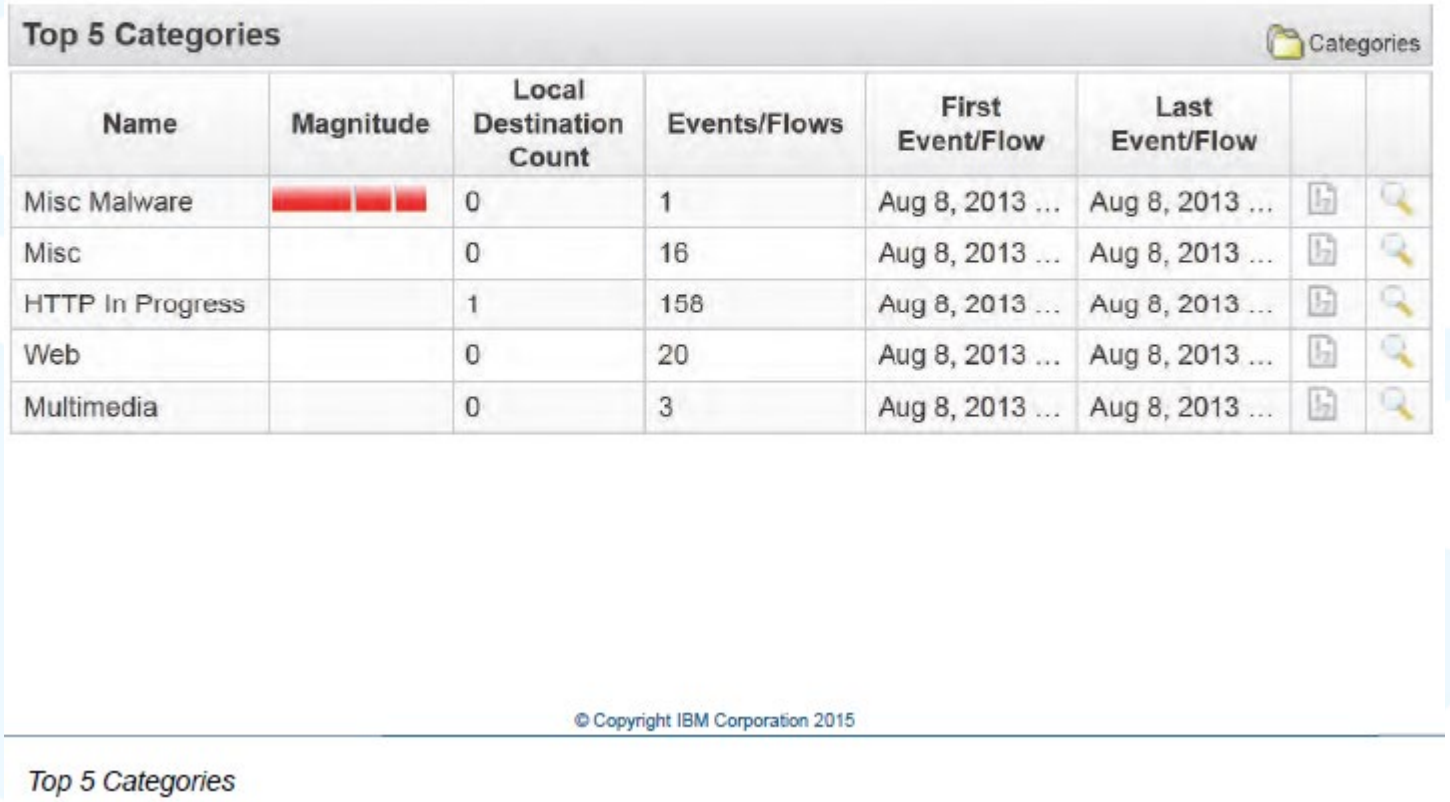
Top 5 Log Sources



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 ...		

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		Custom Rule E...	Misc Malware	208.67.222.222	53	Aug...

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 Flows

Application	Source IP	Source Port	...nation 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

Last 10 Flows

Annotations

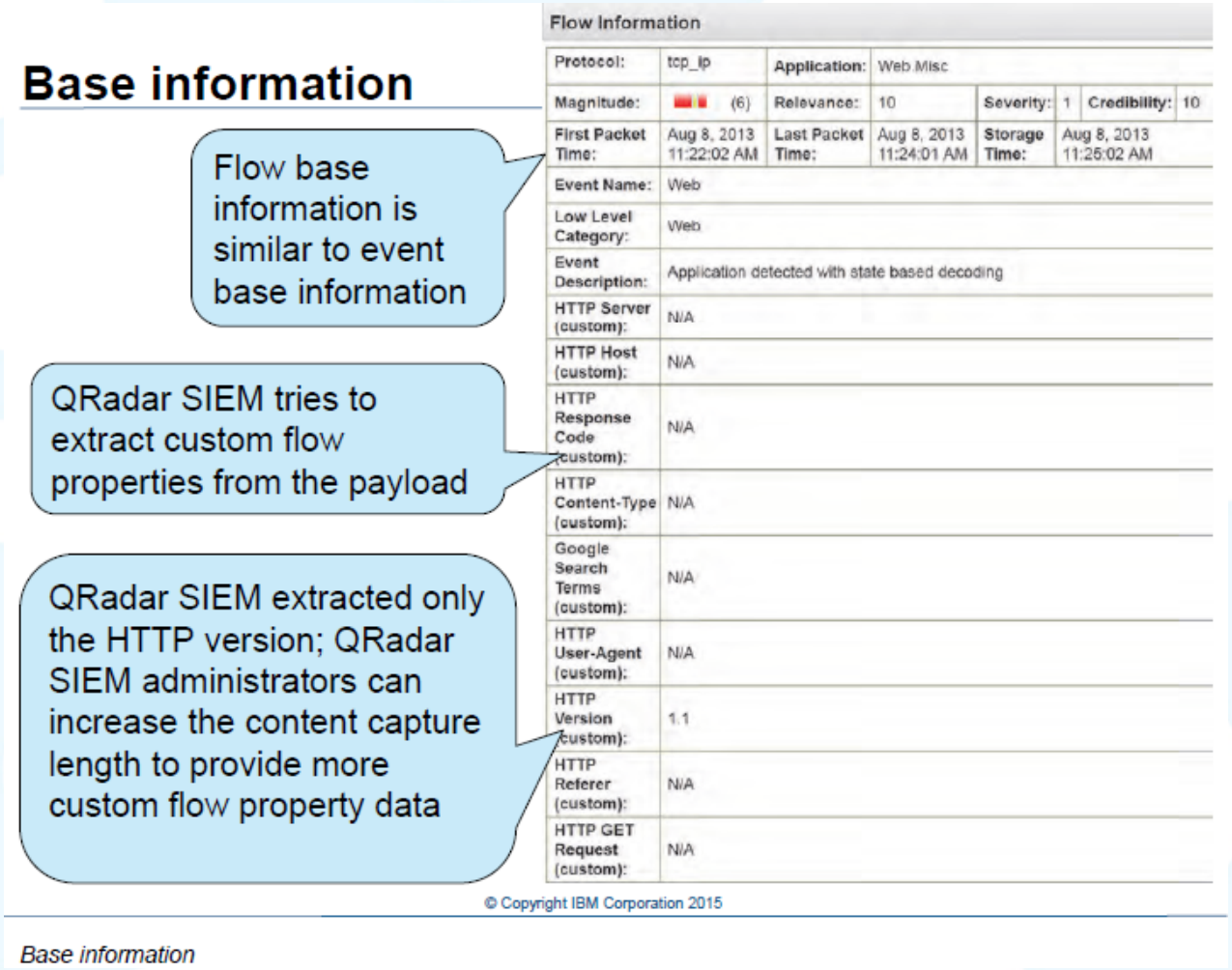
- Annotations provide insight into why QRadar SIEM considers the event or traffic threatening
- QRadar SIEM can add annotations when it adds events and flows to an offense
- Read the oldest annotation because it was added when the offense was created
- Hold the mouse over an annotation to show the entire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

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

Annotations

Navigating flow details

Base information



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:	0:0:0:0:0:0:0:0	**IPv6 Destination:**	0:0:0:0:0:0:0:0
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

Source and destination information

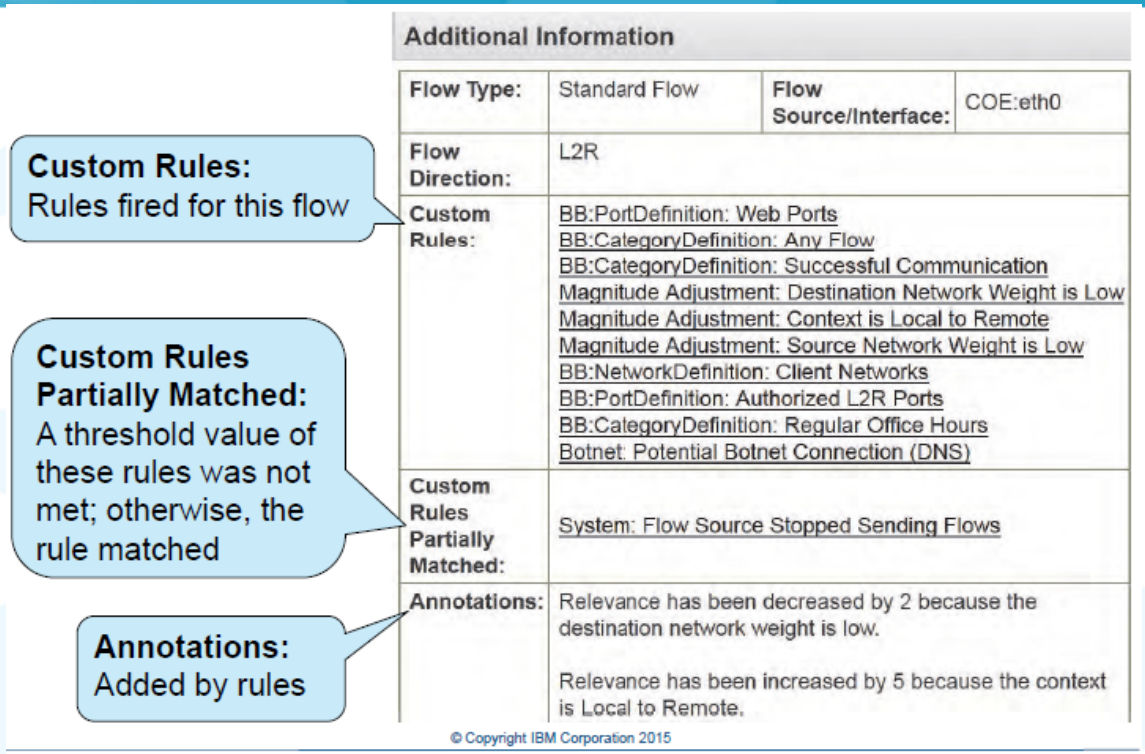
Layer 7 payload

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

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

Layer 7 payload

Additional information



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

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

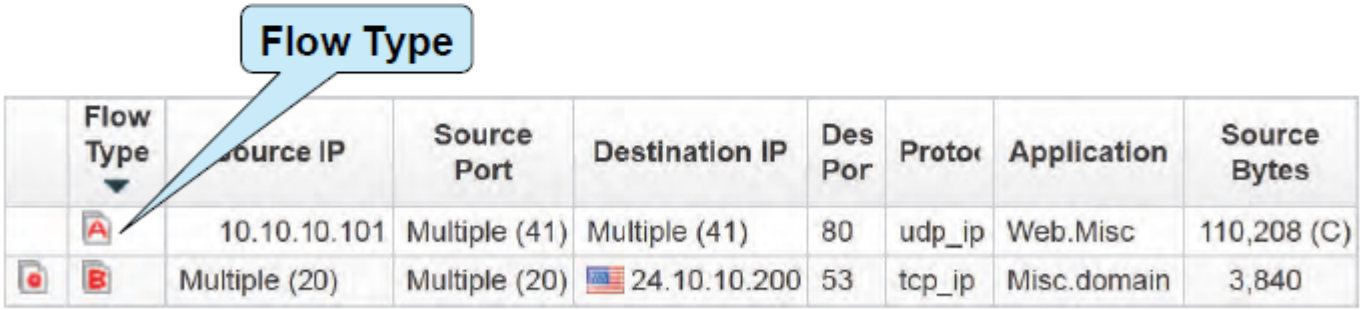
Tuning a false positive flow or event

Investigating superflows

About superflows

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

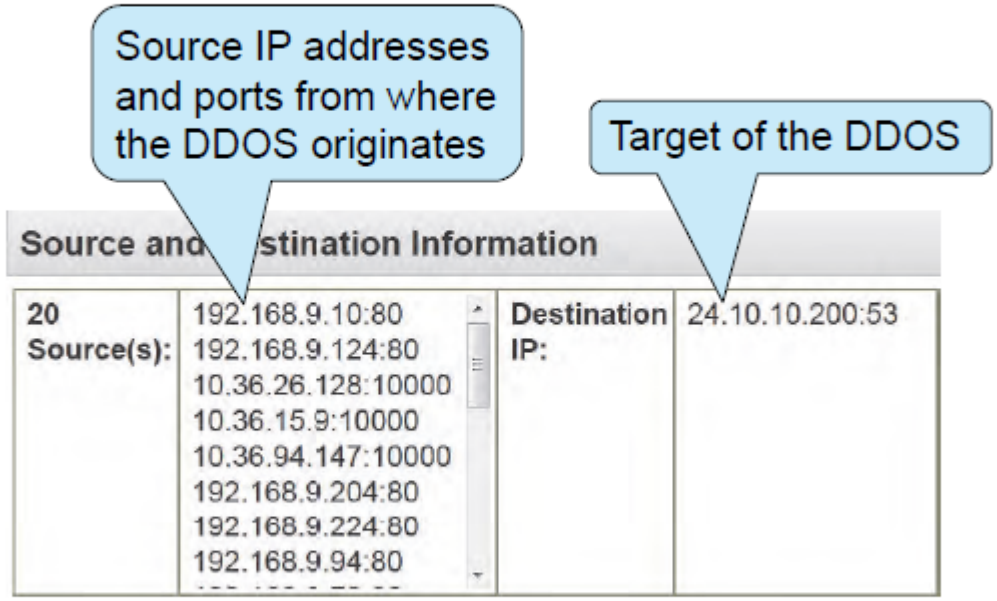
- Type A: Network sweep
  one source IP address > many destination IP addresses
- Type B: Distributed denial of service (DDOS) attack
  many source IP addresses > one destination IP address
- Type C: Portscan
  one source IP address > many ports on one destination IP address



About superflows

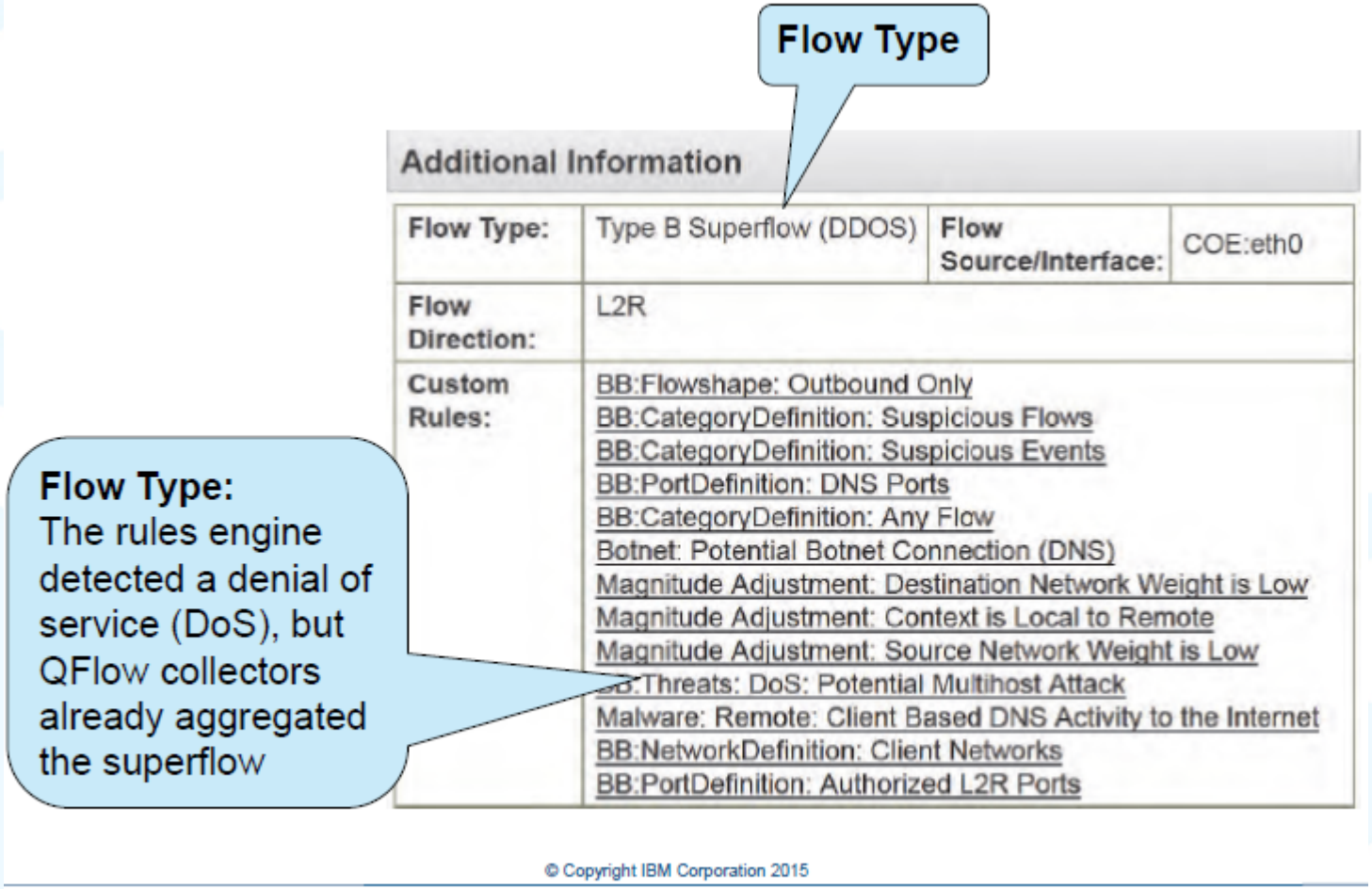
Superflow source and destination information

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



Superflow source and destination information

Superflow additional information



Superflow additional information

Summary

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