



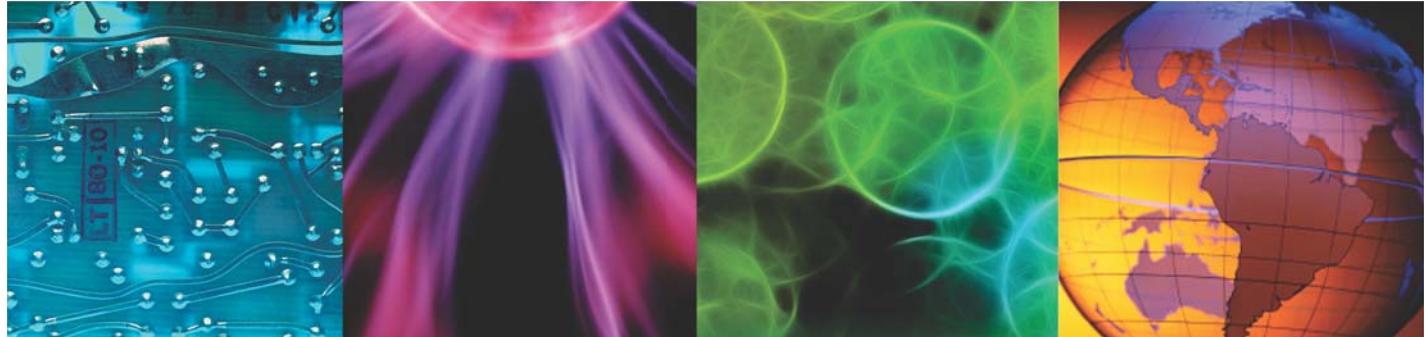
IBM Training

IBM Security QRadar SIEM Foundations

Student Notebook

Course code BQ102 ERC 1.0

January 2015



IBM Security Systems

All files and material for this course are IBM copyright property covered by the following copyright notice.

© Copyright IBM Corp. 2015. All Rights Reserved.

US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results.



Contents

About this course	8
1 Introduction to IBM Security QRadar SIEM	1
Objectives	2
Lesson 1 QRadar SIEM purpose	3
Purposes of QRadar SIEM	4
QRadar SIEM and the IBM Security Framework	5
Identifying suspected attacks and policy breaches	6
Providing context	7
Lesson 2 QRadar SIEM capabilities	8
Key QRadar SIEM capabilities	9
QRadar SIEM Console	11
Summary	12
2 How QRadar SIEM collects security data.....	13
Objectives	15
Lesson 1 Collecting and processing events and flows	16
Normalizing log messages to events	17
Event collection and processing	18
Flow collection and processing	20
Reporting	21
Lesson 2 Collecting and processing vulnerability data	22
Asset profiles	23
Active scanners	24
QRadar Vulnerability Manager scanner	25
Gathering asset information	26
Summary	27
3 Using the QRadar SIEM dashboard	28
Objectives	29
Lesson 1 Navigating the Dashboard tab	30
Dashboard overview	31
Instructor demonstration of the dashboard	32
Default dashboard	33
QRadar SIEM tabs	34
Other menu options	35
Context-sensitive help	36
Dashboard refresh	37
Lesson 2 Customizing a dashboard	38
Dashboard variety	39

Creating a custom dashboard	40
Items	41
Managing dashboard items	42
Student exercises	43
Summary	44
4 Investigating an offense that is triggered by events.....	45
Objectives	46
Lesson 1 Offenses overview	47
Introduction to offenses	48
Creating and rating offenses	49
Lesson 2 Using summary information to investigate an offense	50
Instructor demonstration of offense parameters	51
Selecting an offense to investigate	52
Offense Summary window	53
Offense parameters	54
Offense Source Summary	59
Lesson 3 Investigating offense details	64
Notes	65
Top 5 Source IPs	66
Top 5 Destination IPs	68
Top 5 Log Sources	69
Top 5 Users	70
Top 5 Categories	71
Last 10 Events	73
Last 10 Flows	74
Annotations	75
Offense Summary toolbar	76
Lesson 4 Acting on an offense	77
Offense actions	78
Offense status and flags	80
Student exercises	82
Summary	83
5 Investigating the events of an offense	84
Objectives	85
Lesson 1 Investigating event details	86
Navigating to the events	87
List of events	88
Event details: Base information	89
Event details: Reviewing the raw event	90
Event details: Additional details	91
Returning to the list of events	92
Lesson 2 Using filters to investigate events	93
Filtering events	94
Applying a Quick Filter to the payload	97
Using another filter option	98
Lesson 3 Using grouping to investigate events	99
Grouping events	100

Grouping events by low-level category	101
Removing grouping criteria	103
Viewing a range of events	104
Lesson 4 Saving a search	105
Monitoring the scanning host	106
Saving search criteria	109
Event list using the saved search	110
Lesson 5 Modifying saved searches	111
About Quick Searches	112
Using alternative methods to create and edit searches	113
Finding and loading a saved search	115
Search actions	116
Lesson 6 Adding a search to the dashboard	117
Adding a saved search as a dashboard item	118
Saving a search as a dashboard item	119
Enabling time-series data	120
Selecting the time range	121
Displaying 24 hours in a dashboard item	122
Modifying items in the chart type table	123
Student exercises	124
Summary	125
6 Using asset profiles to investigate offenses	126
Objectives	128
Lesson 1 Assets overview	129
About asset profiles	130
Creating asset profiles	131
Lesson 2 Investigating asset details	132
Navigating from an offense to an asset	133
Assets tab	134
Asset summary	135
Vulnerabilities	136
Services	138
Products	139
Summary	140
7 Investigating an offense that is triggered by flows	141
Objectives	142
Lesson 1 Viewing and grouping flows	143
About flows	144
Network Activity tab	145
Grouping flows	146
Finding an offense	148
Lesson 2 Using summary information to investigate an offense	149
Offense parameters	150
Top 5 Source and Destination IPs	151
Top 5 Log Sources	152
Top 5 Categories	153
Last 10 Events	154

Last 10 Flows	155
Annotations	156
Lesson 3 Navigating flow details	157
Base information	158
Source and destination information	159
Layer 7 payload	160
Additional information	161
Lesson 4 False positives overview	162
Creating a false positive flow or event	163
Tuning a false positive flow or event	164
Lesson 5 Investigating superflows	165
About superflows	166
Superflow source and destination information	167
Superflow additional information	168
Student exercises	169
Summary	170
8 Using rules and building blocks	171
Objectives	172
Lesson 1 Rules and build blocks overview	173
About rules and building blocks	174
About rules	175
About building blocks and functions	176
Lesson 2 Locating rules	177
Navigating to rules	178
Finding the rules that fired for an event or flow	181
Finding the rules that triggered an offense	182
Lesson 3 Using rule definitions during an investigation	183
Rule Wizard demonstration	185
Rule Wizard	186
Rule actions	187
Rule response	188
Student exercises	189
Summary	190
9 Creating QRadar SIEM reports	191
Objectives	192
Lesson 1 Navigating the Reports tab	193
Reporting introduction	194
Reporting demonstration	195
Reports tab	196
Finding a report	197
Running a report	198
Selecting the generated report	200
Viewing a report	201
Lesson 2 Creating a report template	202
Reporting demonstration	203
Creating a new report template	204
Choosing a schedule	205

Choosing a layout206
Defining report contents207
Configuring the upper chart208
Configuring the lower chart210
Verifying the layout preview212
Choosing a format213
Distributing the report214
Adding a description and assigning the group215
Verifying the report summary216
Viewing the generated report217
Best practices when creating reports218
Student exercises219
Summary220
10 Performing advanced filtering.....	.221
Objectives222
Lesson 1 Filtering scenarios223
Filtering demonstration224
Flows to external destinations225
Remote to Remote flows226
Scanning activity227
Applications not running on the correct port228
Data loss229
Flows to suspect Internet addresses230
Filtering on custom rules and building blocks231
Grouping by custom rules232
Lesson 2 Using Advanced Search filters233
Ariel Query Language234
Additional AQL examples235
Lesson 3 Using charts236
Charts on Log and Network Activity tabs: Grouping237
Charts on Log and Network Activity tabs: Time range238
Capturing time-series data239
Viewing time series charts: Zooming to focus240
Summary242



About this course



IBM Security QRadar SIEM Foundations



© Copyright IBM Corporation 2015

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

IBM Security QRadar SIEM provides deep visibility into network, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, assets, and vulnerabilities. QRadar SIEM classifies suspected attacks and policy breaches as offenses.

In this two-day course, you learn how to perform the following tasks:

- Describe how QRadar SIEM collects data to detect suspicious activities
- Navigate and customize the QRadar SIEM dashboard
- Investigate suspected attacks and policy breaches
- Search, filter, group, and analyze security data
- Investigate the vulnerabilities and services of assets
- Locate custom rules and inspect actions and responses of rules
- Use QRadar SIEM to create customized reports
- Use charts and apply advanced filters to examine specific activities in your environment

Using the skills taught in this instructor-led classroom course, you will be able to use QRadar SIEM to investigate threats and attacks, and configure the appropriate responses for your organization.

Course properties	Details
Delivery method	Classroom or instructor-led online (ILO)
Course level	ERC 1.0 This course is an update of the following previous course: • BQ101: IBM Security QRadar SIEM 7.2 Foundations ERC1.0
Product and version	IBM Security QRadar SIEM 7.2.3
Duration	Two days
Skill level	Basic

About the student

This course is designed for security analysts, security technical architects, offense managers, network administrators, and system administrators using QRadar SIEM. Before taking this course, make sure that you have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog

Learning objectives

Objectives

After completing this course, you should be able to perform the following tasks:

- Describe how QRadar SIEM collects data to detect suspicious activities
- Navigate and customize the QRadar SIEM dashboard
- Investigate suspected attacks and policy breaches
- Search, filter, group, and analyze security data
- Investigate the vulnerabilities and services of assets
- Locate custom rules and inspect actions and responses of rules
- Use QRadar SIEM to create customized reports
- Use charts and apply advanced filters to examine specific activities in your environment

© Copyright IBM Corporation 2015

Course agenda

The course contains the following units:

1. Introduction to IBM Security QRadar SIEM

This unit provides a high-level description of the purpose and capabilities of the QRadar SIEM licensed program.

2. How QRadar SIEM collects security data

QRadar SIEM collects and processes the event data and vulnerability assessment data that is gathered by the systems in your network. This unit provides a high-level description of how QRadar SIEM collects data and performs vulnerability assessment.

3. Using the QRadar SIEM dashboard

QRadar SIEM displays the Dashboard tab when you sign in. Multiple items on a dashboard display information about activities of systems in your network. The items enable you to focus on specific areas of interest such as security or network operations. You can customize each dashboard to meet the needs and responsibilities of the analyst. This unit teaches you how to navigate and customize the dashboard tab.

4. Investigating an offense that is triggered by events

QRadar SIEM correlates events and flows into an offense if it assumes suspicious activity. This unit teaches you how to investigate the information that is contained in an offense and respond to an offense.

5. Investigating the events of an offense

The investigation of an offense usually leads to the investigation of the events that contributed to the offense. This unit teaches you how to find, filter, and group events in order to gain critical insights about the offense. You also learn how to create and edit a search that monitors the events of suspicious hosts.

6. Using asset profiles to investigate offenses

QRadar SIEM stores security-relevant information about systems in your network in asset profiles. This unit teaches you how asset profiles are created and updated, and how to use them as part of an offense investigation.

7. Investigating an offense that is triggered by flows

QRadar SIEM correlates flows into an offense if it determines suspicious activities in network communications. This unit teaches you how to investigate the flows that contribute to an offense. You also learn how to create and tune false positives and investigate superflows.

8. Using rules and building blocks

Rules perform tests on the events, flows, and offenses in QRadar SIEM and respond if the test criteria is met. A building block is a rule without a response that is used as a common variable in

multiple rules or to build complex rules. This unit teaches you how to find custom rules in the QRadar SIEM console and how to assign actions and responses to the rule. You also learn how to configure rules.

9. Creating QRadar SIEM reports

Reports allow you to examine trends and statistical views on your network for various purposes, in particular to meet compliance requirements. This unit teaches you how to generate a report using a predefined template and create a report template.

10. Performing advanced filtering

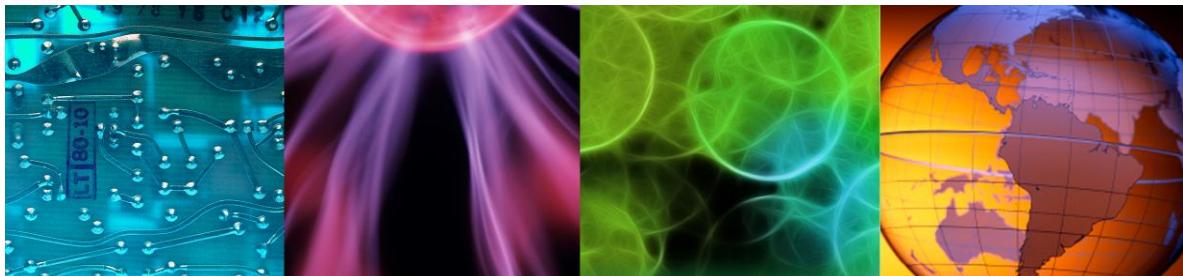
QRadar SIEM provides several filters that you can apply to identify suspicious or non-standard behavior. Bar, pie, table, and time-series charts visualize security data. This unit teaches you how to use charts and apply advanced filters to examine specific activities in your environment.



1 Introduction to IBM Security QRadar SIEM



Introduction to IBM Security QRadar SIEM



© Copyright IBM Corporation 2015
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit provides a high-level description of the purpose and capabilities of the QRadar SIEM licensed program.

This unit has no student exercises.

Objectives

In this unit, you learn to perform the following tasks:

- Describe the purpose of QRadar SIEM
- List the capabilities of QRadar SIEM

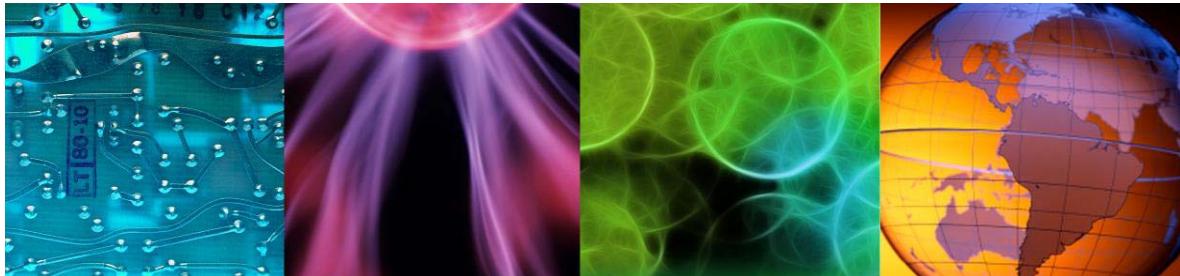
© Copyright IBM Corporation 2015

Objectives

Lesson 1 QRadar SIEM purpose



Lesson: QRadar SIEM purpose



© Copyright IBM Corporation 2015

QRadar SIEM alerts to suspicious activities and enables security analysts to investigate them. In this lesson, you are introduced to the purpose of the QRadar SIEM software application, including the following aspects of the application:

- The challenges QRadar SIEM addresses
- Where QRadar SIEM fits into the IBM Security Framework
- How QRadar SIEM helps to identify attacks and provides context to investigate them

Purposes of QRadar SIEM

The IBM Security QRadar SIEM licensed program performs these tasks

- Alerts to suspicious activities and policy breaches in the IT environment
- Provides deep visibility into network, user, and application activity
- Puts security-relevant data from various sources in context with each other
- Provides reporting templates to meet operational and compliance requirements
- Provides reliable, tamper-proof log storage for forensic investigations and evidentiary use

“Our most formidable challenge is getting companies to detect that they have been compromised.”

Kimberly K. Peretti,
Senior Counsel,
US Dept. of Justice (DoJ)

© Copyright IBM Corporation 2015

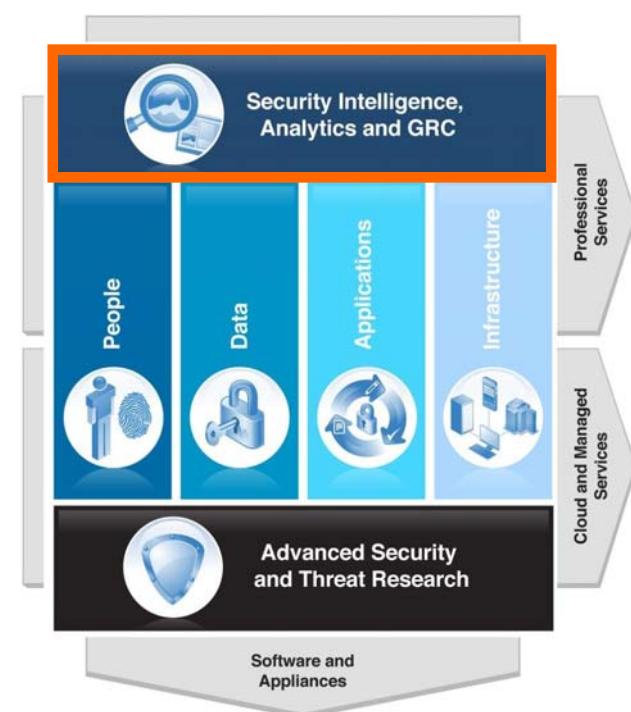
Purposes of QRadar SIEM

QRadar SIEM enables you to minimize the time gap between when a security incident occurs and when it is detected.



Note: SIEM = Security Information and Event Management

QRadar SIEM and the IBM Security Framework



In the IBM Security Framework, QRadar SIEM offers these capabilities

- Security Intelligence, Analytics and Governance, Risk Management, and Compliance (GRC)
- Insight into all domains of the IBM Security Framework

© Copyright IBM Corporation 2015

QRadar SIEM and the IBM Security Framework

Identifying suspected attacks and policy breaches

QRadar SIEM helps answer the following key questions

- What is being attacked?
- What is the security impact?
- Who is attacking?
- Where should the investigation be focused?
- When are the attacks taking place?
- How is the attack penetrating the system?
- Is the suspected attack or policy breach real or a false alarm?

© Copyright IBM Corporation 2015

Identifying suspected attacks and policy breaches

Providing context

To enable security analysts to perform investigations, QRadar SIEM correlates information such as these examples

- Point in time
- Offending users
- Origins
- Targets
- Vulnerabilities
- Asset information
- Known threats



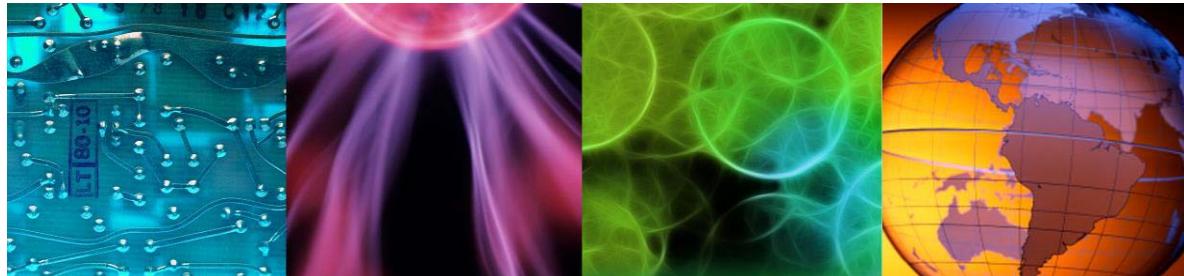
© Copyright IBM Corporation 2015

Providing context

Lesson 2 QRadar SIEM capabilities



Lesson: QRadar SIEM capabilities



© Copyright IBM Corporation 2015

QRadar SIEM helps your organization to identify attacks and policy breaches. This lesson provides a high-level description of the features of QRadar SIEM.

Key QRadar SIEM capabilities

- Ability to process security-relevant data from a wide variety of sources, such as these examples
 - Firewalls
 - User directories
 - Proxies
 - Applications
 - Routers
- Collection, normalization, correlation, and secure storage of raw events, network flows, vulnerabilities, assets, and threat intelligence data
- Layer 7 payload capture up to a configurable number of bytes from unencrypted traffic

© Copyright IBM Corporation 2015

Key QRadar SIEM capabilities

By default, QFlow captures the first 64 bytes of unencrypted layer 7 payloads. The user interface displays these bytes without further decoding. Payloads from encrypted traffic are not captured.

Key QRadar SIEM capabilities (continued)

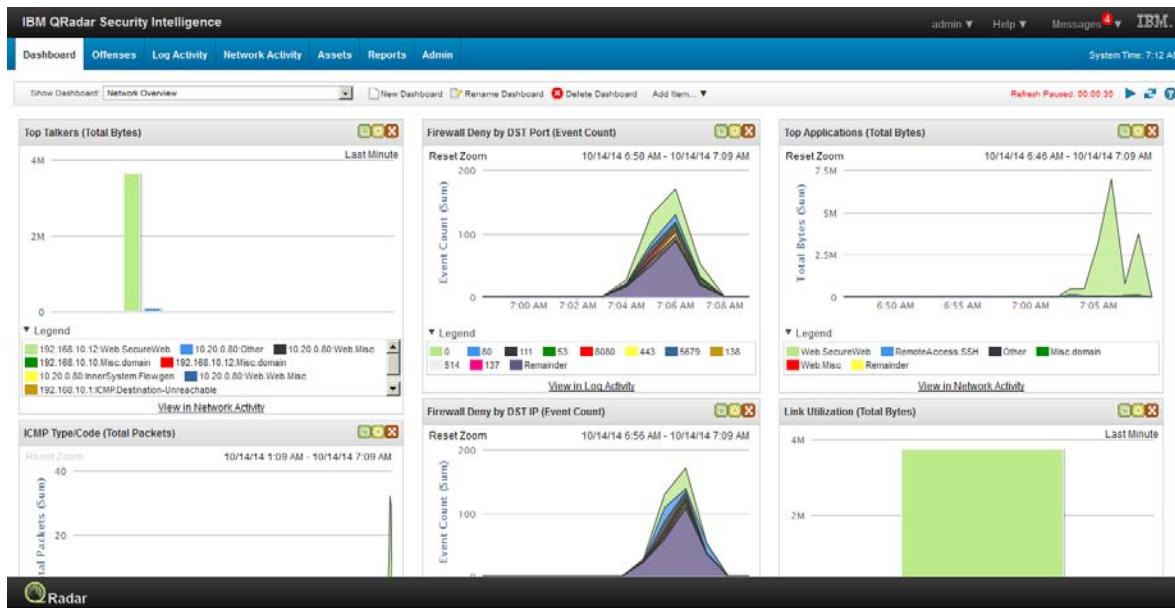
- Comprehensive search capabilities
- Monitor host and network behavior changes that could indicate an attack or policy breach such as these examples
 - Off hours or excessive usage of an application or network activity patterns inconsistent with historical profiles
 - Prioritization of suspected attacks and policy breaches
- Notification by email, SNMP, and others
- Many generic reporting templates included
- Scalable architecture to support large deployments
- Single user interface

© Copyright IBM Corporation 2015

Key QRadar SIEM capabilities (continued)

While QRadar SIEM alerts you to suspicious activities and facilitates their investigation, it does not respond automatically. For example, QRadar SIEM can detect services it suspects are targeted by an attack, but it does not change configurations or shut down such services. Such automatic changes can cause unwanted system outages.

QRadar SIEM Console



The console provides one integrated user interface for all tasks

© Copyright IBM Corporation 2015

QRadar SIEM Console

Summary

Now you should be able to perform the following tasks:

- Describe the purpose of QRadar SIEM
- List the capabilities of QRadar SIEM

© Copyright IBM Corporation 2015

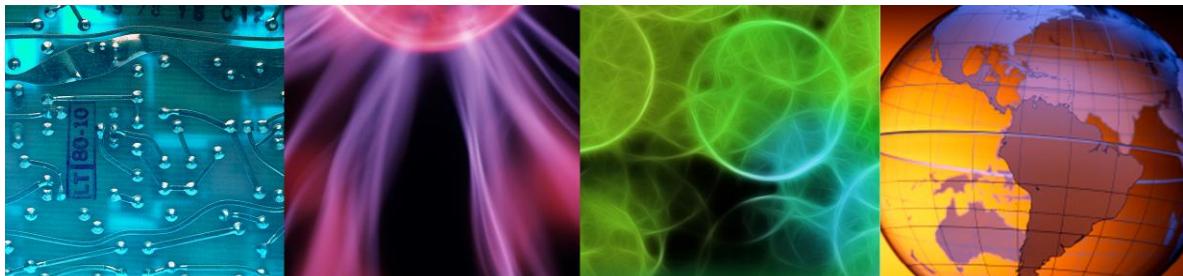
Summary



2 How QRadar SIEM collects security data



How QRadar SIEM collects security data



© Copyright IBM Corporation 2015
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

QRadar SIEM collects and processes the event data and vulnerability assessment data that is gathered by the systems in your network. This unit provides a high-level description of how QRadar SIEM collects data and performs vulnerability assessment.

References:

- *IBM Security QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar SIEM Administration Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar Log Sources User Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar WinCollect User Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar Adaptive Log Exporter Users Guide* <http://ibm.co/1wvpSEE>
- Microsoft Windows Management Instrumentation
<http://technet.microsoft.com/en-us/library/ee692942.aspx>
- *IBM Security QRadar Vulnerability Assessment Configuration Guide* <http://ibm.co/1wvpSEE>

This unit has no student exercises.

Objectives

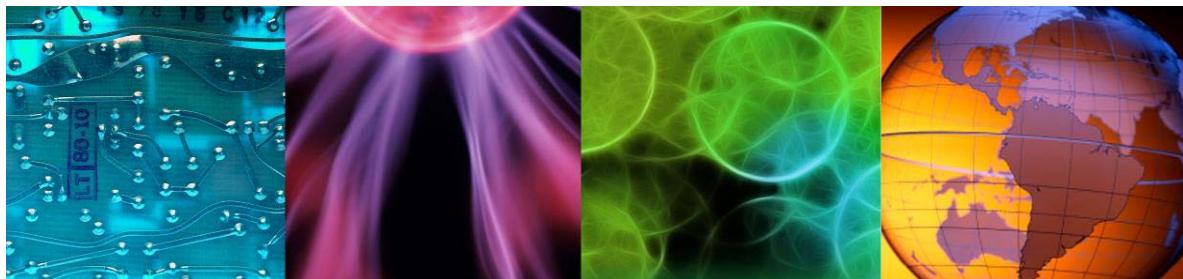
In this unit, you learn to perform the following tasks:

- Describe how QRadar SIEM collects and processes events and flows
- Describe how QRadar SIEM collects vulnerability data

Lesson 1 Collecting and processing events and flows



Lesson: Collecting and processing events and flows



© Copyright IBM Corporation 2015

In this lesson, you learn how QRadar SIEM collects and processes both events and flows.

References:

- *IBM Security QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar SIEM Administration Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar Log Sources User Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar WinCollect User Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar Adaptive Log Exporter Users Guide* <http://ibm.co/1wvpSEE>
- Microsoft Windows Management Instrumentation
<http://technet.microsoft.com/en-us/library/ee692942.aspx>
- *IBM Security QRadar Vulnerability Assessment Configuration Guide* <http://ibm.co/1wvpSEE>

Normalizing raw events

- An event is a record from a device that describes an action on a network or host
- QRadar SIEM normalizes the varied information found in raw events
 - Normalizing means to map information to common field names, for example
 - SRC_IP, Source, IP, and others are normalized to **Source IP**
 - user_name, username, login, and others are normalized to **User**
 - Normalized events are mapped to high-level and low-level categories to facilitate further processing
- After raw events are normalized, it is easy to search, report, and cross-correlate these normalized events

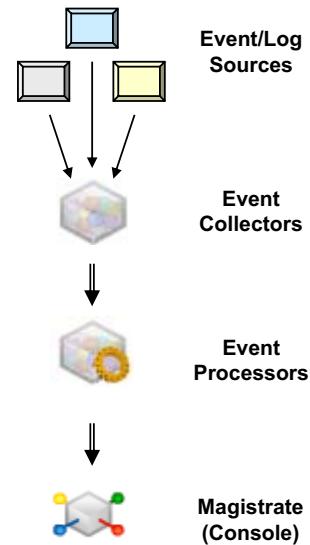
© Copyright IBM Corporation 2015

4

Normalizing log messages to events

Event collection and processing

- Log Sources typically send syslog messages, but they can use other protocols also
- Event Collectors receive raw events as log messages from a wide variety of external log sources
 - Device Support Modules (DSMs) in the event collectors parse and normalize raw events; raw log messages remain intact
- Event Processors receive the normalized events and raw events to analyze and store them
- Data Nodes (not pictured) provide additional storage for event and flow data
- Magistrate correlates data from event processors and creates offenses



© Copyright IBM Corporation 2015

5

Event collection and processing

To receive raw events from log sources, QRadar SIEM supports many protocols, such as those detailed in the following list:

- Syslog from operating systems, applications, firewalls, IPS/IDS, router, switches
- Other standard protocols, such as SNMP and SOAP
- Data from a database table or view, such as JDBC
- Proprietary vendor-specific messaging protocols, such as OPSEC/LEA from Checkpoint

Refer to the *IBM Security QRadar Log Sources User Guide* at <http://ibm.co/1wvPSEE>.

Collection methods

QRadar SIEM uses the following collection methods on variants of UNIX and Linux operating systems (licensed programs):

- Output from the operating system's **syslog** licensed program is the most common method.
- **Transfer of syslog files** to QRadar SIEM allows more secure communication.
- Third-party agents such as the **syslog-ng**, **Snare**, and **Splunk Universal Forwarder** licensed programs are also available.

QRadar SIEM uses the following collection methods on variants of Microsoft Windows operating systems (licensed programs):

- The **IBM Security QRadar WinCollect** licensed program collects events by running as a service on a Windows system. That agent can also collect events from other Windows servers where the agent is not installed. WinCollect is centrally managed from the QRadar SIEM user interface. Refer to the *IBM Security QRadar WinCollect User Guide* at <http://ibm.co/1wvpSEE>.
- The **Microsoft Windows Management Instrumentation (WMI)** licensed program can be used and administered through the QRadar SIEM user interface to collect events without an agent. However, WMI puts a major load on network and Windows servers. Domain controllers usually slow down when WMI is configured. For more information, refer to <http://technet.microsoft.com/en-us/library/ee692942.aspx>.
- Third-party agents such as the **syslog-ng**, **Snare**, **Splunk Universal Forwarder**, and **Adiscon EventReporter** licensed programs are also available.

About Event Collectors

Each Event Collector gathers events from local and remote sources. The Event Collector normalizes events and classifies them into low- and high-level categories. The Event Collector also bundles identical events to conserve system usage through a process that is known as *coalescing*.

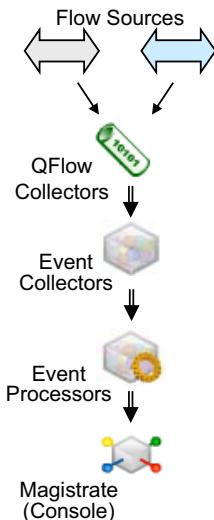
Event collectors use traffic analysis to discover which kind of device a log source is if a Device Support Module (DSM) for that kind of device is installed. In addition, the DSM for a device specifies how to map and normalize the device's raw events.

About Event Processors

Each Event Processor processes events from the Event Collectors and flow data. Event processors correlate the information. The Event Processor examines information gathered by QRadar SIEM to indicate behavioral changes or policy violations. Rules are applied to the events to search for anomalies.

Flow collection and processing

- A *flow* is a communication session between two hosts
- QFlow Collectors read packets from the wire or receive flows from other devices



- QFlow Collectors convert all gathered network data to flow records similar normalized events; they include such details as when, who, how much, protocols, and options.

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code
□	Oct 14, 2014, 7:00:13 AM	192.168....	61190	202.12.27.33	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
□	Oct 14, 2014, 6:59:59 AM	192.168...	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	380 (C)	3,376 (C)	4	4	N/A
□	Oct 14, 2014, 7:00:53 AM	0.0.0.0	546	0.0.0.0	547	udp_ip	Other	612 (C)	0	4	0	N/A
□	Oct 14, 2014, 6:59:59 AM	192.168....	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	3,016	64,432	40	52	N/A
□	Oct 14, 2014, 6:59:59 AM	192.168...	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	4,132	85,256	51	54	N/A
□	Oct 14, 2014, 7:00:09 AM	192.168....	61190	192.203.230.10	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
□	Oct 14, 2014, 7:00:53 AM	0.0.0.0	546	0.0.0.0	547	udp_ip	Other	459 (C)	0	3	0	N/A
□	Oct 14, 2014, 7:00:24 AM	192.168...	64348	192.168.10.10	443	tcp_ip	Web SecureWeb	3,669	24,010	10	23	N/A
□	Oct 14, 2014, 7:00:05 AM	192.168....	61709	192.168.10.1	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
□	Oct 14, 2014, 6:59:59 AM	192.168....	61097	192.168.99.1	53	udp_ip	Misc.domain	78	0	1	0	N/A
□	Oct 14, 2014, 7:00:01 AM	192.168...	64335	192.168.10.10	443	tcp_ip	Web SecureWeb	192	297	3	4	N/A
□	Oct 14, 2014, 7:00:05 AM	192.168....	N/A	192.168.10.12	N/A	icmp_ip	ICMP.Destination-Unreachable	129 (C)	0	1	0	Port Unreac...

© Copyright IBM Corporation 2015

6

Flow collection and processing

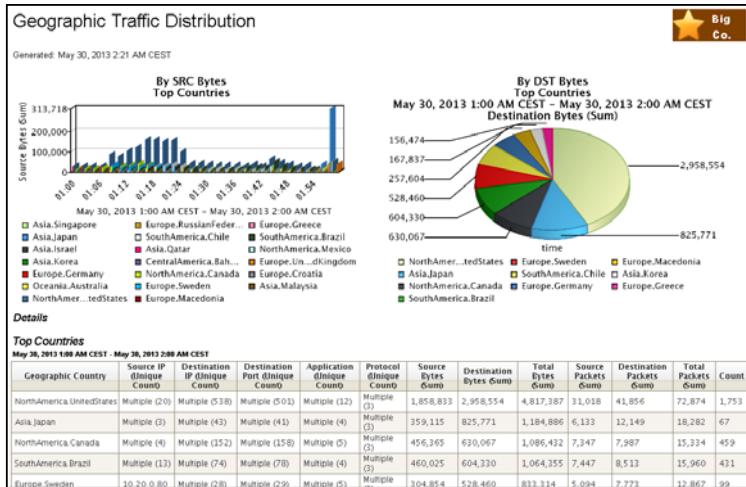
A *flow* is a record of a conversation between two devices on a network.

A network *flow record* provides information about a conversation between two devices using a specific protocol and can include many fields that describe the conversation. Examples include the source IP, the destination IP, the port, and other fields.

Up to a configurable number of bytes, QFlow provides layer 7 insights into the payload if it is unencrypted. Using a tap or span port, QFlow collects raw packets and places them into 60-second chunks. QFlow can also receive layer 4 flows from other network devices in IPFIX/NetFlow, sFlow, J-Flow, Packeteer, and Flowlog file accounting technologies.

Flows update asset profiles with the ports and services that are running on each host.

Reporting



- All collected information is available for reports
- Thousands of report templates are available
- With the report wizard, you can create new templates and change existing templates

© Copyright IBM Corporation 2015

7

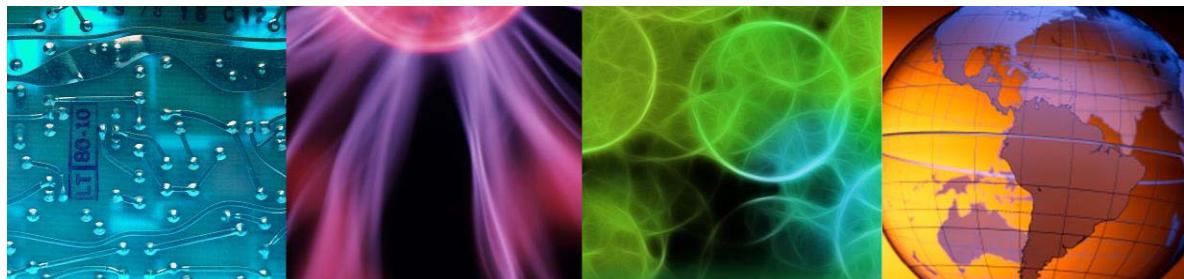
Reporting

Compliance reporting packages are available for PCI, SOX, FISMA, GLBA, and HIPAA, with reports based on control frameworks such as NIST, ISO, and CoBIT.

Lesson 2 Collecting and processing vulnerability data



Lesson: Collecting and processing vulnerability data



© Copyright IBM Corporation 2015

The more QRadar SIEM knows about vulnerabilities of hosts, the better it can detect and prioritize suspicious activities. This lesson introduces you to vulnerability scanning and detection, as well as tracking the found vulnerabilities in asset profiles.

Asset profiles

QRadar SIEM maintains asset profiles for systems in the network; the profiles track host details, such as these examples

- IP addresses
- Services listening on open ports
- Vulnerabilities

Id	IP Address	Asset Name	Aggregate CVSS Score	Vulnerabilities	Services
1030	10.111.219.138	10.111.219.138	0.0	0	0
1013	10.117.220.204	10.117.220.204	0.0	0	0
1014	10.117.220.205	10.117.220.205	0.0	0	0
1012	10.117.254.16	10.117.254.16	0.0	0	0
1011	10.117.254.36	10.117.254.36	0.0	0	0
1010	10.117.254.66	10.117.254.66	0.0	0	0
1009	10.15.20.140	10.15.20.140	0.0	0	0
1015	10.2.100.66	10.2.100.66	0.0	0	0
1018	10.20.0.80	10.20.0.80	0.0	0	0
1007	128.245.120.152	128.245.120.152	0.0	0	0
1019	172.16.254.2	chkpt1	0.0	0	0

© Copyright IBM Corporation 2015

9

Asset profiles

In addition to technical asset information, asset profiles track user logins to the asset if this information is provided to QRadar SIEM. QRadar SIEM automatically creates and updates asset profiles for systems that are found in the following areas:

- DHCP, DNS, VPN, proxy, firewall NAT, and wireless AP logs
- Passively gathered bidirectional flow
- Vulnerability data provided by active scanners

If this information is unavailable, QRadar SIEM does not create asset profiles automatically. You can still create asset profiles manually in the user interface or by import. Only flows and vulnerability data add and update information about ports and services to asset profiles.

Asset profile information is used for correlation purposes. For example, if an attacker attempts to compromise a certain service that is running on a specific asset, QRadar SIEM can determine whether the asset is vulnerable to this attack by correlating the attack to the asset profile.

Active scanners

For vulnerability assessment (VA) and maintaining asset profiles, QRadar SIEM integrates with many active scanners

- You can schedule Nessus, Nmap, and IBM Security QRadar Vulnerability Manager scanner directly in QRadar SIEM
- For other scanners, you schedule only the collection of scan results in QRadar SIEM but not the scan itself



© Copyright IBM Corporation 2015

10

Active scanners

Third-party scanners, such as Nessus and nCircle IP360, report vulnerabilities to QRadar SIEM using external references from the Open Source Vulnerability Database (OSVDB) and National Vulnerability Database (NVDB) to identify found vulnerabilities. Each vulnerability is assigned a unique reference identifier, an OSVDB ID. In addition, each vulnerability can be identified by external data references, such as a Common Vulnerability and Exposures (CVE) ID or Bugtraq ID.

QRadar Vulnerability Manager scanner

You can add the separate product IBM Security QRadar Vulnerability Manager licensed program with QRadar SIEM

It provides these benefits

- Active scanner present on all QRadar event and flow collectors and processors
- Detects 70,000+ vulnerabilities
- Processes results from IBM-hosted scanner to see a view from outside your firewall
- Tracks *Common Vulnerabilities and Exposures* (CVE)
- Third-party vulnerability data feeds

Source IP	Source Port	Destination IP	Destinati Port	Username
9.180.225.51	0	127.0.0.1	0	N/A
9.180.225.51	0	127.0.0.1	0	N/A

Filter on Source IP is 9.180.225.51
Filter on Source IP is not 9.180.225.51
Filter on Source or Destination IP is 9.180.225.51
False Positive
More Options... ▾

► Navigate Information Run QVM Scan

QRadar Vulnerability Manager scanner

The user interface shows the **Vulnerabilities** tab if your organization deployed a license for QRadar Vulnerability Manager.

Gathering asset information

Active scanners

QRadar Vulnerability Manager scanner, Nessus, Nmap, Qualys, and others

Provide:

- List of hosts with risks and potential vulnerabilities
- IP and MAC addresses
- Open ports
- Services and versions
- Operating system

Pros

- Detailed host information
- Policy and compliance information

Cons

- Out of date quickly
- Full network scans can take weeks
- Active scanners cannot scan past firewalls
- User can hide from active scans

Asset Profiles

Passive detection

Flows from QFlow, or other flow sources in accounting technologies such as IPFIX/NetFlow, sFlow, and others

Provide:

- IP addresses in use
- Open ports in use

Pros

- Real-time asset profile updates
- Firewalls have no impact
- End system cannot hide
- Policy and compliance information

Cons

- Not as detailed as active scans
- Does not detect installed but unused services or ports

© Copyright IBM Corporation 2015

12

Gathering asset information

A user can hide a system from active scans by connecting it to the network only for short periods of time.

Summary

Now you should be able to perform the following tasks:

- Describe how QRadar SIEM collects and processes events and flows
- Describe how QRadar SIEM collects vulnerability data



3 Using the QRadar SIEM dashboard



Using the QRadar SIEM dashboard



© Copyright IBM Corporation 2015
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

QRadar SIEM displays the **Dashboard** tab when you sign in. Multiple items on a dashboard display information about activities of systems in your network. The items enable you to focus on specific areas of interest such as security or network operations. You can customize each dashboard to meet the needs and responsibilities of the analyst. This unit teaches you how to navigate and customize the dashboard tab.

References:

- *IBM Security QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar SIEM Administration Guide* <http://ibm.co/1wvpSEE>

Objectives

In this unit, you learn to perform the following tasks:

- Navigate the default dashboard
- Customize dashboards

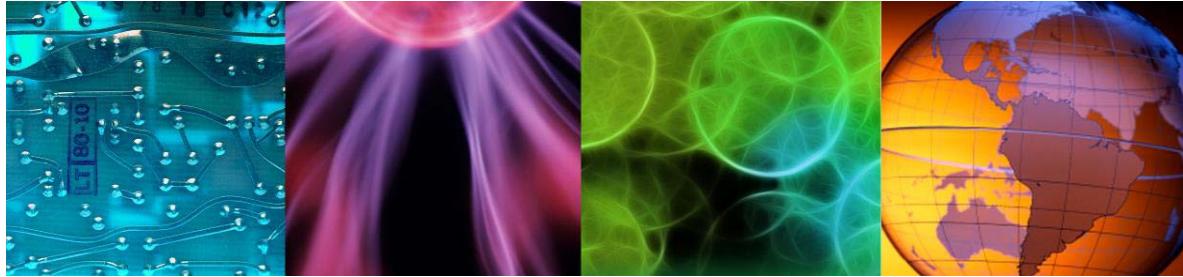
© Copyright IBM Corporation 2015

Objectives

Lesson 1 Navigating the Dashboard tab



Lesson: Navigating the Dashboard tab



© Copyright IBM Corporation 2015

The **Dashboard** tab is the default view when you sign in to QRadar SIEM. In this lesson, you learn how to navigate the QRadar SIEM user interface and **Dashboard** tab by performing the following tasks:

- Locate the tabs in QRadar SIEM
- Use QRadar SIEM menu options
- Access context-sensitive help
- Refresh the dashboard

References:

- *IBM Security QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar SIEM Administration Guide* <http://ibm.co/1wvpSEE>

Dashboard overview

- QRadar SIEM shows the **Dashboard** tab when you log in
- You can create multiple dashboards
- Each dashboard can contain items that provide summary and detailed information
- Seven default dashboards are available
- You can create custom dashboards to focus on your security or operations responsibilities
- Each dashboard is associated with a user; changes that you make to a dashboard do not affect the dashboards of other users

© Copyright IBM Corporation 2015

Dashboard overview

Instructor demonstration of the dashboard



© Copyright IBM Corporation 2015

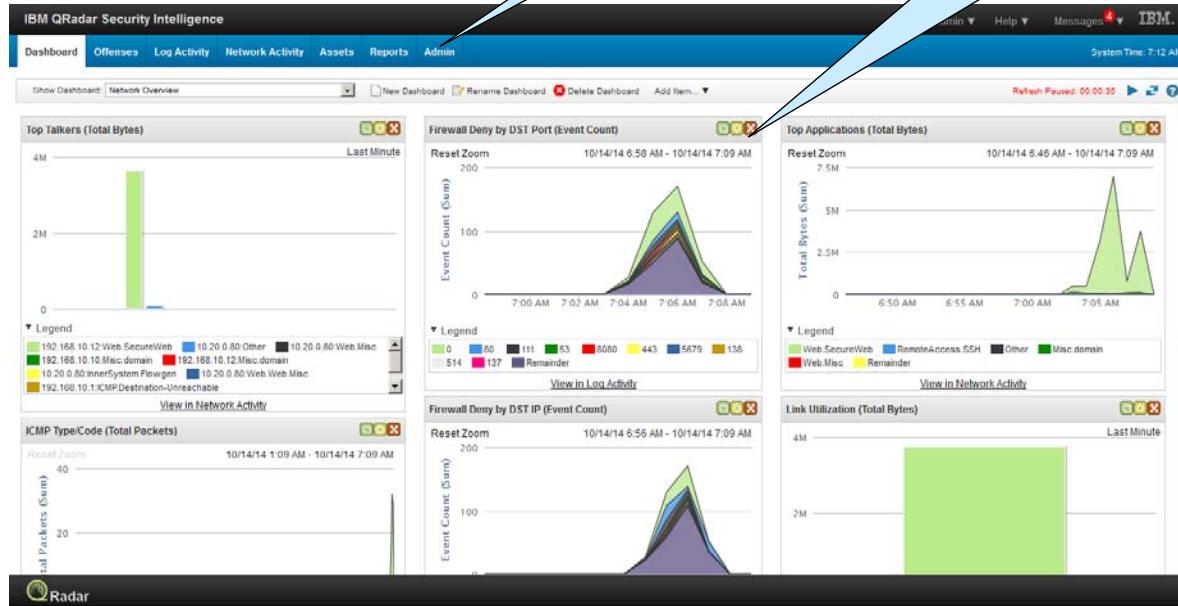
Instructor demonstration of the dashboard

Default dashboard

Click a tab to load it

Tabs

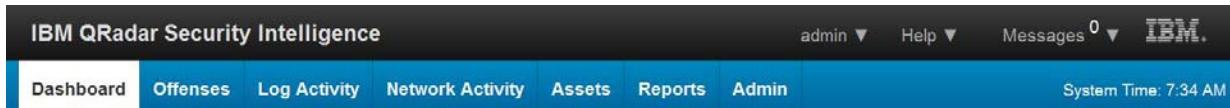
Tables and charts



© Copyright IBM Corporation 2015

Default dashboard

QRadar SIEM tabs



Use tabs to navigate the primary QRadar SIEM functions

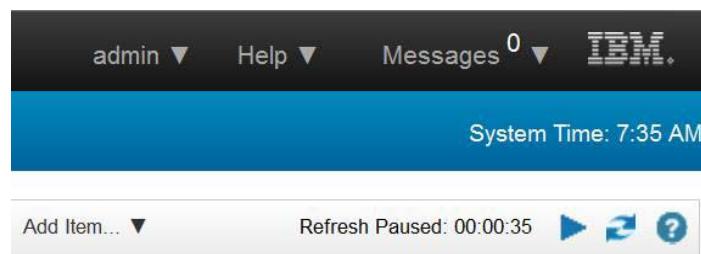
- **Dashboard:** The initial summary view
- **Offenses:** Displays offenses; list of prioritized incidents
- **Log Activity:** Query and display events
- **Network Activity:** Query and display flows
- **Assets:** Query and display information about systems in your network
- **Reports:** Create templates and generate reports
- **Admin:** Administrative system management

© Copyright IBM Corporation 2015

QRadar SIEM tabs

The user interface (UI) in QRadar SIEM includes a series of tabs that you use to navigate and focus on specific slices of the collected, analyzed, and displayed data.

Other menu options



The dashboard has the following additional menu options

- **User Preferences**
- **Help**
- **Log out**

Name:	admin
E-mail:	root@localhost
Current Password:	*****
New Password:	*****
Confirm New Password:	*****
Locale:	en_US
Enable Popup Notifications:	<input checked="" type="checkbox"/>

Save Cancel

© Copyright IBM Corporation 2015

Other menu options

You can see these additional menu options:

- **User Preferences:** Users can change their password here if they authenticate with the local system authentication of QRadar SIEM. Users cannot change the password here if QRadar SIEM uses RADIUS, TACACS, Active Directory, or LDAP for their authentication.

In most deployments, the user *admin* authenticates with the local system authentication of QRadar SIEM even if other users use external authentication. Therefore, user *admin* usually can change his or her password in the User Preferences of QRadar SIEM.

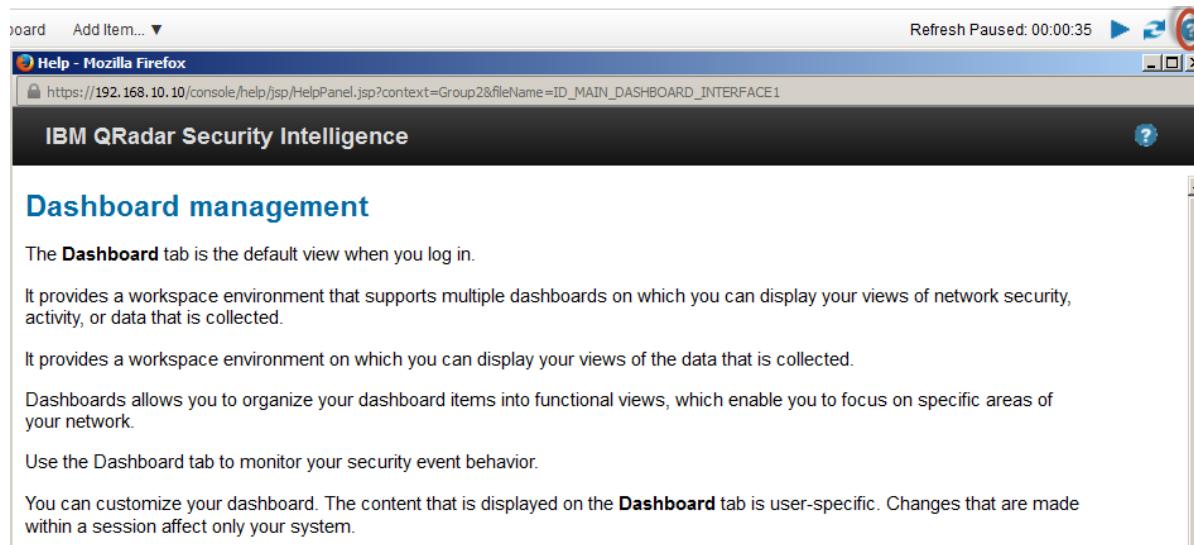


Note: Refer to the *IBM Security QRadar SIEM Administration Guide* (<http://ibm.co/1wvpSEE>) for further details.

- **Help:** Opens the page-level help documentation.
- **Log out:** Closes the web session and logs out the user.
- **Messages:** Opens the system notification center.

Context-sensitive help

Click the question mark in any window to access help for the current page



© Copyright IBM Corporation 2015

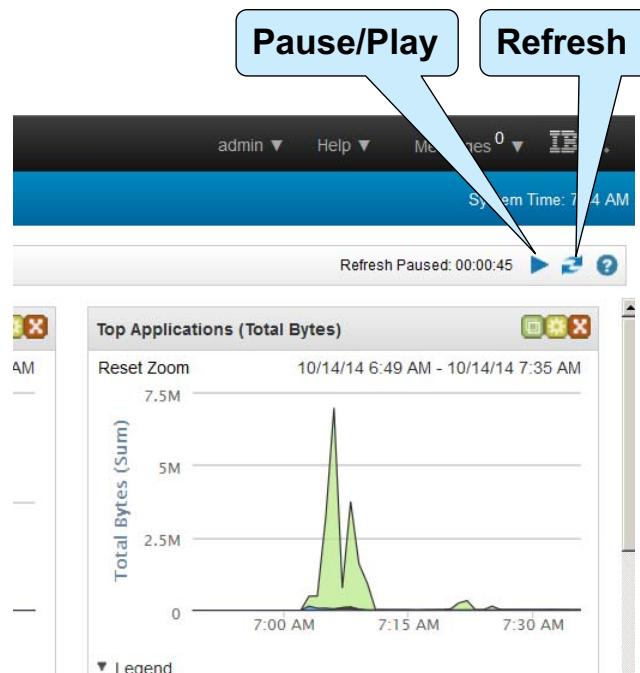
Context-sensitive help

You can access page-level help in the following ways:

- View the help text in the banner for an index of all help.
- Right-click the question mark icon (?) for context-sensitive help.

Dashboard refresh

- In the displayed dashboard, events and flows refresh every minute unless you click **Pause**
- Use the **Refresh** button to manually refresh the displayed data



© Copyright IBM Corporation 2015

Dashboard refresh

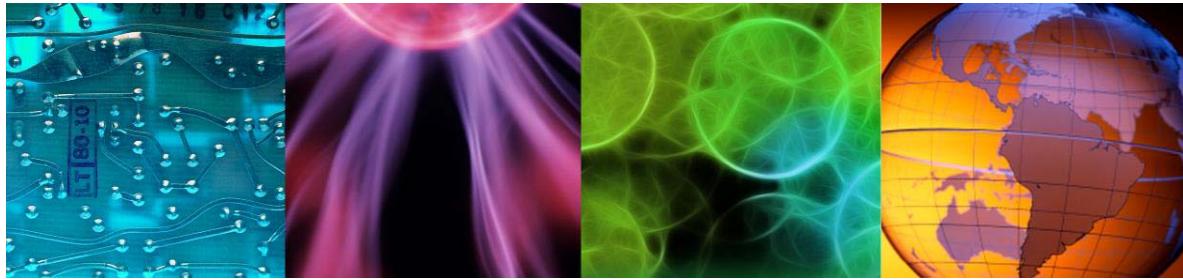
The dashboard can display table, bar, pie, and time-series charts. By default, QRadar SIEM refreshes data from the event and flow processors every minute. The user can manually refresh at any time, resetting the displayed countdown to 60 seconds, but data results returned are from the prior minute to match the system refresh cycle for the event and flow processors. If the refresh clock is, for example, at 55 seconds and the user manually refreshes, the data displayed still originates from the earlier cycle. QRadar SIEM always refreshes automatically at the 1-minute mark.

The **Pause** button stops only the display refresh. QRadar SIEM continues to update and process in the background.

Lesson 2 Customizing a dashboard



Lesson: Customizing a dashboard



© Copyright IBM Corporation 2015

You can customize dashboards to display user-specific information. In this lesson, you learn how to create a customized dashboard and manage dashboard items.

Dashboard variety

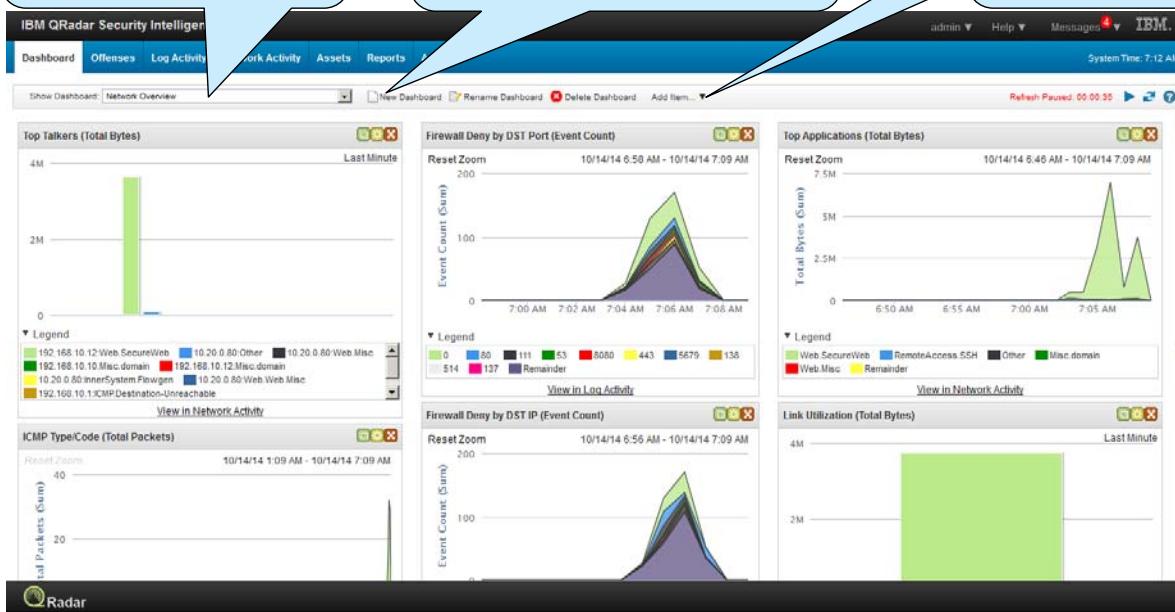
- QRadar SIEM includes the following default dashboards
 - Application Overview
 - Compliance Overview
 - Network Overview
 - System Monitoring
 - Threat and Security Monitoring
 - Virtual Cloud Infrastructure
 - Vulnerability Management
- Use multiple dashboards to better organize data; for example, a single user can have the following dashboards to show log and network activity of these systems
 - Databases
 - Critical Applications

© Copyright IBM Corporation 2015

Dashboard variety

Creating a custom dashboard

Show Dashboard:
Select a dashboard to view



New Dashboard:
Create a new dashboard empty of items

Add item:
Add an item to dashboard

Creating a custom dashboard

To create a custom dashboard, perform the following steps:

1. Click the **New Dashboard** icon.
A new Dashboard window opens.
2. In the **Name** field, enter a name. You can enter up to 65 characters.
3. In the **Description** field, enter a description. You can enter up to 255 characters.
4. Click **OK**.

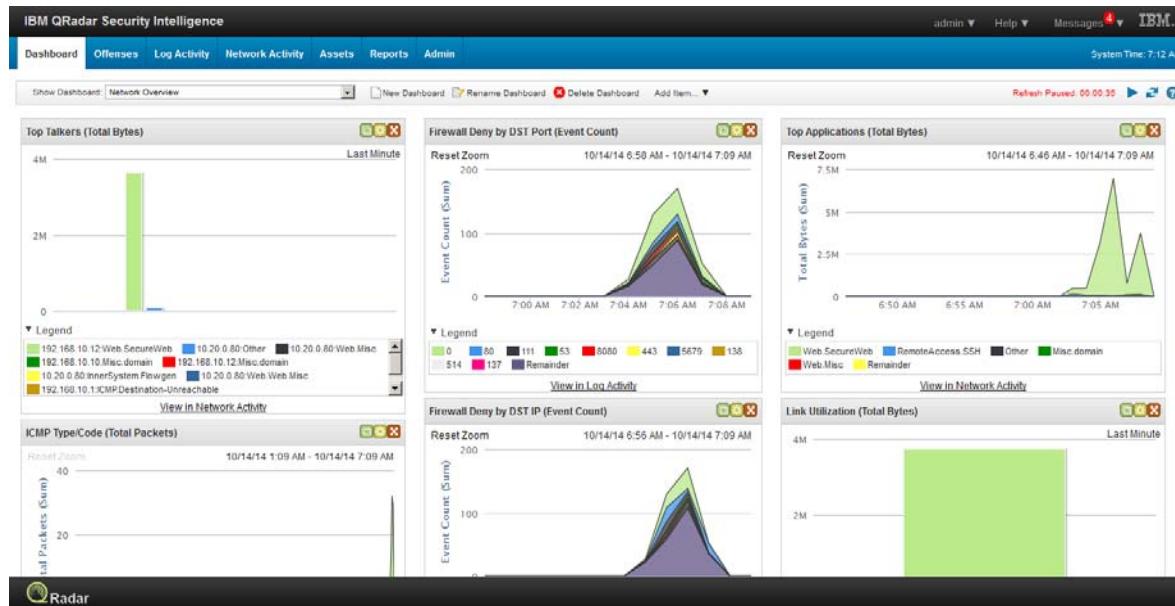
The new dashboard opens on the **Dashboard** tab and is listed in the **Show Dashboard** list.
The new dashboard is empty.

To add items to the new dashboard, perform the following steps:

1. From the **Show Dashboard** list, select the dashboard where you want the item added.
2. From the **Add Item** list, select an item.
The item displays on the dashboard.
3. Repeat until you have added all the items you want to the dashboard.

Items

Include no more than 15 items on each dashboard



© Copyright IBM Corporation 2015

Items

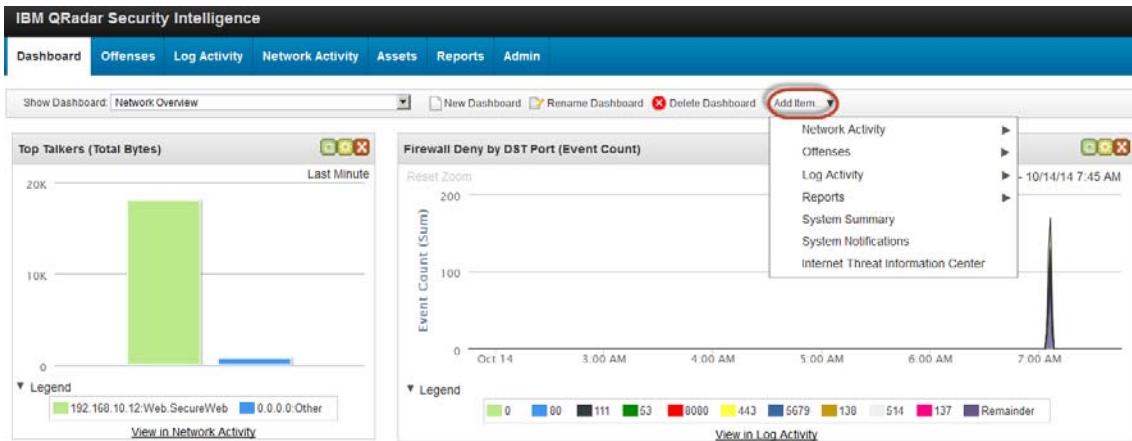
Managing dashboard items

Click **Add Item** to place additional objects on the dashboard

Click the green icon to detach the object from the interface to the desktop

Click the yellow icon to modify the settings of an object

Click the red icon to delete an object from the dashboard



© Copyright IBM Corporation 2015

Managing dashboard items

Student exercise

Use the procedures in the *Student Exercises Guide* to create a new dashboard



© Copyright IBM Corporation 2015

Student exercises

Perform the exercises for this unit.



Summary

Now you should be able to perform the following tasks:

- Navigate and customize the user interface
- Customize dashboards

© Copyright IBM Corporation 2015

Summary



4 Investigating an offense that is triggered by events



Investigating an offense that is triggered by events



© Copyright IBM Corporation 2015
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

QRadar SIEM correlates events and flows into an offense if it assumes suspicious activity. This unit teaches you how to investigate the information that is contained in an offense and respond to an offense.

References:

- QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>
- QRadar SIEM Administration Guide <http://ibm.co/1wvpSEE>



Objectives

In this unit, you learn to perform the following tasks:

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

© Copyright IBM Corporation 2015

Objectives

Lesson 1 Offenses overview



Lesson: Offenses overview



© Copyright IBM Corporation 2015

By creating an offense, QRadar SIEM alerts to suspicious activities. In this lesson, you learn the significance of offenses and what offenses represent, including common offenses and their priority rating.

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

The following list includes some of the most common offenses that a typical security analyst investigates:

- Clear Text Application Usage
- Remote Desktop Access from the Internet
- Connection to a remote proxy or anonymization service
- SSH or Telnet detected on Non-Standard Port
- Large Outbound Transfer
- Communication to a known Bot Command and Control
- Local IRC Server detected

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

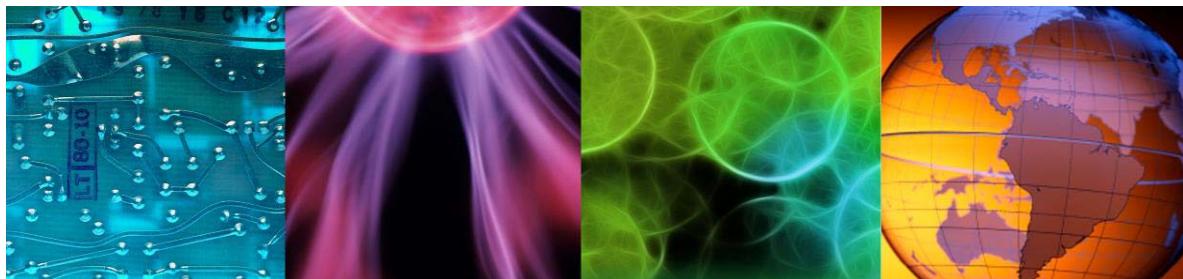
Creating and rating offenses

The magistrate reevaluates the offense magnitude at scheduled intervals and also when events are added to the offense.

Lesson 2 Using summary information to investigate an offense



Lesson: Using summary information to investigate an offense



© Copyright IBM Corporation 2015

An offense bundles a wealth of information about a suspicious activity. In this lesson, you learn how to use offense summary information to begin investigating an offense.

References:

- QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>
- QRadar SIEM Administration Guide <http://ibm.co/1wvpSEE>

Instructor demonstration of offense parameters



This demonstration uses an offense that alerts to a suspected ICMP scanner as an example

Investigating this kind of offense is a typical part of a security analyst's job

© Copyright IBM Corporation 2015

Instructor demonstration of offense parameters

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 dark header bar with the text "IBM QRadar Security Intelligence". Below it is a blue navigation bar with tabs: "Dashboard" (which is selected), "Offenses", "Log Activity", "Network Activity", "Assets", "Reports", and "Admin". On the left side, there's a sidebar with a "Offenses" section containing links: "My Offenses", "All Offenses" (which is selected), "By Category", "By Source IP", "By Destination IP", "By Network", and "Rules". 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's a section titled "Current Search Parameters" with buttons for "Exclude Hidden Offenses" and "Exclude Closed Offenses", both with "(Clear Filter)" links. To the right of this, there are buttons for "All Offenses" and "View Offenses" followed by a dropdown menu labeled "Select An Option". A table below lists offenses with columns: "Id", "Description", "Offense Type", "Offense Source", and "Magnitude". The table contains 8 rows of offense 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 Multi...	Source IP	10.0.120.10	Medium
1	Multiple Login Failures to the Same Destination preceded by Multi...	Destination IP	10.0.120.10	Medium
6	Multiple Login Failures to the Same Destination preceded by Login...	Destination IP	10.0.120.11	Medium
4	Multiple Login Failures for the Same User containing Logon Failur...	Username	nina	Medium
5	Multiple Login Failures for the Same User containing MSSQL Logi...	Username	sqladmin	Medium

© Copyright IBM Corporation 2015

Selecting an offense to investigate

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

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 several sections:

- Offense 8**: Shows offense details like Source IP (10.127.15.37), Destination (Local (2) Remote (260)), and Description (Local ICMP Scanner detected Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewall Deny).
- Last 5 Notes**: A table with columns: Notes, Username, and Creation Date. It shows one entry: "No results were returned."
- Top 5 Source IPs**: A table with columns: Source IP, Magnitude, Location, Value..., User, MAC, Weight, Offenses, and Last EventFlow. It shows two entries: 10.127.15.37 (Magnitude 10, Offenses 1) and 10.26.10.110 (Magnitude 10, Offenses 2).
- Top 5 Destination IPs**: A table with columns: Destination IP, Magnitude, Location, Value..., Channel, User, MAC, Weight, Offenses, and Last EventFlow. It shows two entries: 10.26.10.110 (Magnitude 10, Offenses 2) and 10.26.10.110 (Magnitude 10, Offenses 1).
- Top 5 Log Sources**: A table with columns: Name, Description, Group, Events/Flows, Offenses, and Last EventFlow. It shows two entries: CheckPoint @ FW-Machine (CheckPoint device, Group 383, Offenses 24) and Custom Rule Engine-6: CSE (Custom Rule Engine, Group 17, Offenses 22).
- Top 5 Users**: A table with columns: Name, Events/Flows, Offenses, and Total Events/Flows. It shows one entry: No results were returned.
- Top 5 Categories**: A table with columns: Name, Magnitude, Local Connection Count, Events/Flows, First EventFlow, and Last EventFlow. It shows three entries: Network Sweep (Magnitude 0, Offenses 11), Firewall Deny (Magnitude 2, Offenses 383), and ICMP Reconnaissance (Magnitude 0, Offenses 8).
- Last 10 Events**: A table with columns: Event Name, Magnitude, Log Source, Category, Destination, Duration, and Time. It lists 10 Firewall Deny events from Jul 31, 2013 to Aug 01, 2013.
- Last 10 Flows**: A table with columns: Application, Source IP, Source Port, Destination IP, Destination Port, Total Bytes, and Last Packet Time. It shows one entry: No results were returned.
- Top 5 Annotations**: A table with columns: Annotation, Time, and Weight. It shows two entries: "ICMP Event" (Time Jul 31, 2013 10:08:59 AM, Weight 0) and "ICRE Event" (Time Jul 31, 2013 10:09:29 AM, Weight 0).

© Copyright IBM Corporation 2015

Offense Summary window

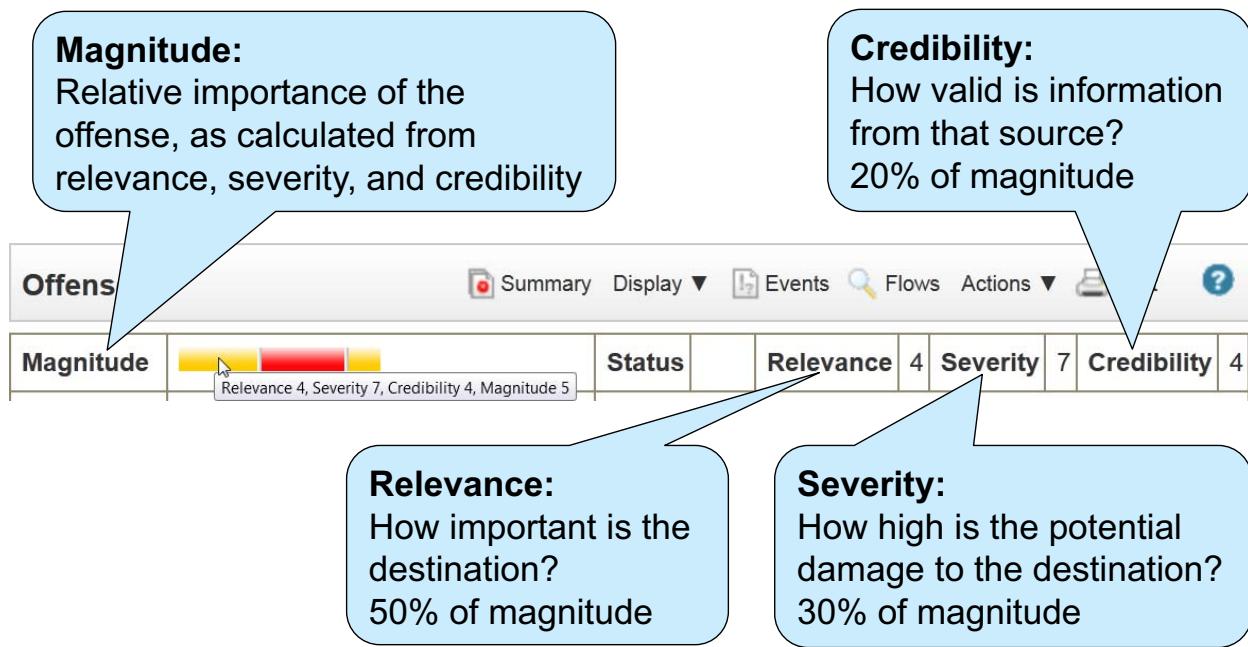
The Offense Summary window includes these sections:

- 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



© Copyright IBM Corporation 2015

Offense parameters

- **Magnitude:** Prioritizes offenses by importance. Security analysts cannot ignore less important offenses because they could indicate a real attack or policy breach.
- **Status:** The offense on the slide is in status *active*. QRadar SIEM does not display a status icon for the *active* status. Other statuses are indicated with an icon in the **Status** field.
- **Relevance:** Indicates the importance of the destination. Less important areas of the network have a lower relevance. QRadar SIEM determines the relevance by the weight of networks and assets. QRadar SIEM administrators configure the weight in the network hierarchy, remote networks, remote services, and asset profiles.
- **Severity:** Indicates the amount of threat an attack poses in relation to the vulnerability of the destination.
- **Credibility:** Indicates the reliability of the witness. Credibility increases if multiple sources report the same attack. QRadar SIEM administrators configure the credibility rating of log sources.

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		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 parameters (2 of 4)

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

ASN: An **Autonomous System Number (ASN)** uniquely identifies one or more IP networks that have a single, clearly defined external routing policy. An ASN is required only if the autonomous system exchanges routing information with other autonomous systems on the Internet.

Offense parameters (3 of 4)

Source IP(s): Origin of the ICMP scanning		Start: Date and time when the first event or flow associated with the offense was created	
Magnitude	 	Start	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
Source IP(s)	10.127.15.37	Event count	410 events and 0 flows in 3 categories
Destination IP(s)	Local (2) Remote (360)	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)

About Source IPs

- To get more information about the IP address, right-click, left-click, or hold the mouse over the address.
- Offenses of type **Source IP** always originate from only one source IP address. Offenses of other types can have more than one source IP address. In those cases, the **Source IP(s)** field displays **Multiple(n)**, where *n* indicates the number of source IP addresses.
- Left-click **Multiple(n)** to view a list of the source IP addresses.

About Destinations IPs

- If the offense has only one target, its IP address is displayed. To get more information about the IP address, right-click, left-click, or hold the mouse over it.
- If the offense has multiple targets, the following terms are displayed:
 - **Local (n)**: Local IP addresses that were targeted.
 - **Remote (n)**: Remote IP addresses that were targeted.
- Left-click an option to view a list of the local or remote IP addresses.

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)

About Networks

- QRadar SIEM considers all networks that are specified in the network hierarchy on the **Admin** tab as local.
- QRadar SIEM does not associate remote networks to an offense, even if they are specified as a Remote Network or Remote Service on the **Admin** tab.

Offense Source Summary (1 of 4)

To the security analyst, the **Offense Source Summary** provides information about the origin of the ICMP scanning

Offense Source Summary			
IP	10.127.15.37	Location	Net-10-172-192.Net 10 0 0 0
Magnitude	<div style="width: 100px; height: 10px; background-color: yellow;"></div>	Vulnerabilities	0

IP:
Origin of the ICMP scanning

Location:
Network of the source IP address if it is local

Magnitude:
Indication about the level of risk that an IP address poses relative to other IP addresses

Vulnerabilities:
A known vulnerability of a local host can have been exploited and turned into an attacker

© Copyright IBM Corporation 2015

Offense Source Summary

The example offense on the slide is of the type **Source IP**. For an offense of type **Destination IP**, the fields display information about the destination.

Offense Source Summary (2 of 4)

When you right-click the IP, you see navigation options for further investigation

Offense Source Summary			
IP	10.127.15.37	Location	Net-10-172-192.Net 10 0 0 0
Magnitude		Navigate	
User	Unknown	Information	View By Network View Source Summary View Destination Summary

© Copyright IBM Corporation 2015

Offense Source Summary (2 of 4)

If a valid license for IBM Security QRadar Vulnerability Manager is deployed, the right-click menu includes the **Run QVM Scan** menu item.

Offense Source Summary (3 of 4)

Offense Source Summary			
IP	10.127.15.37	Location	Net-10-172-192.Net 10_0_0_0
Magnitude	UNKNOWN	Navigate	▶
User	UNKNOWN	Information	▶
Host Name	Unknown	DNS Lookup	
Asset Name	Unknown	WHOIS Lookup	
Offenses	1	Port Scan	

Port Scan:
Nmap scans the IP address

WHOIS Lookup:
Find registered owner of the IP address

Search Flows:
Find flows associated with the IP address

© Copyright IBM Corporation 2015

Offense Source Summary (3 of 4)

- **WHOIS Lookup:** By default, whois.arin.net is configured as the WHOIS server. It does not have the owners of local IP addresses registered. QRadar SIEM must be able to reach whois.arin.net to look up registered owners of remote IP addresses.
- **Port Scan:**
 - On the Console, QRadar SIEM runs the command `nmap -A` for the IP address. All QRadar SIEM 7.2 installations include Nmap.
 - QRadar SIEM displays the Nmap scan results in a pop-up window. In addition to open ports and services, Nmap detects operating system versions and a few potential vulnerabilities, such as anonymous FTP login. However, Nmap does not check for vulnerabilities that are provided by threat intelligence feeds.
 - The result of the Port Scan does not create or update the asset profile in QRadar SIEM. Even if Nmap is configured as a vulnerability scanner, Port Scan still does not update asset profiles because Port Scan runs `nmap -A` only on the Console. To have Nmap or other scanners create and update asset profiles, a QRadar SIEM administrator must configure and run them as vulnerability assessment (VA) scanners. These VA scanners are not invoked by selecting the **Port Scan** menu.



Important: A QRadar SIEM user can run a Port Scan for a remote IP address, but the owner of the remote system could consider this scan an attack. Therefore, do not scan remote IP addresses.

- **Asset Profile:** The menu item is *inactive* on the slide because no asset profile exists for the IP address in QRadar SIEM.
- **Search Events:** Use this menu item to find events that are associated with the IP address.

Offense Source Summary (4 of 4)

Offense Source Summary			
IP	10.127.15.37	Location	Net-10-172-192.Net 10 0 0 0
Magnitude	<div style="width: 100px; height: 10px; background-color: yellow;"></div>	Vulnerabilities	0
User	Unknown	MAC	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	410

Weight:
Relevance of
the source IP
address

Offenses:
Number of offenses
associated with this
source IP address

Events/Flows:
Number of events and flows
associated with this offense

© Copyright IBM Corporation 2015

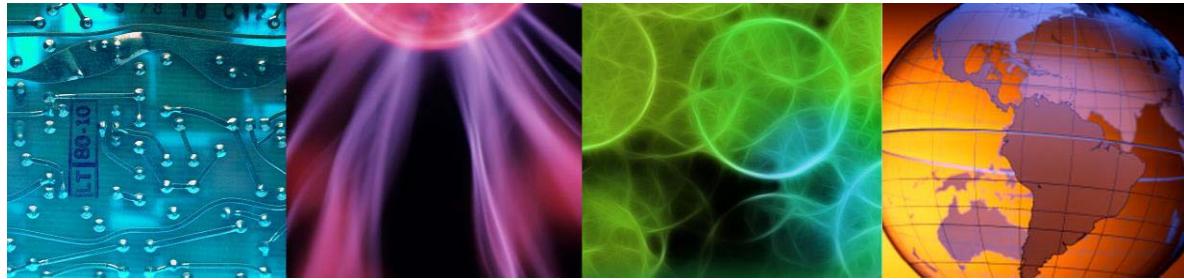
Offense Source Summary (4 of 4)

- **User:** User that is associated with this source IP address. If no user is identified, the field shows **Unknown**.
- **MAC:** MAC address with the source IP address when the offense began. If unknown, the field shows **Unknown NIC**.
- **Host Name:** Host name that is associated with the source IP address. If unidentified, the field shows **Unknown**.
- **Asset Name:** Asset name that is associated with the source IP address. If unidentified, the field shows **Unknown**.
- **Weight:** Relevance of the source IP address, as defined by QRadar SIEM administrators, in the asset profile. If no asset profile exists, the weight of the network hierarchy, remote network, or remote service determines the weight of the source IP address. The field in the user interface shows **0** in that case.

Lesson 3 Investigating offense details



Lesson: Investigating offense details



© Copyright IBM Corporation 2015

Many details help the security analyst to investigate an offense. In this lesson, you learn how to use further details to investigate an offense by performing the following tasks:

- View and add notes to an offense
- Investigate offense details
- View the annotations QRadar SIEM adds to an offense
- Use the Offense Summary toolbar

References:

- QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>
- QRadar SIEM Administration Guide <http://ibm.co/1wvpSEE>

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 table titled "Last 5 Notes" with three columns: "Notes", "Username", and "Creation Date". The first row contains the note "compromised host disconnected from network", created by "lynette" on "Jul 31, 2013 6:06 PM". Above the table, two callout boxes point to the "Notes" and "Add Note" buttons in the header. The "Notes" box says "View all notes of the offense". The "Add Note" box says "Create new note".

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

© Copyright IBM Corporation 2015

Notes

QRadar SIEM displays only the beginning of notes that are too long for one row on the Offense Summary window. Double-click the row to view the whole note.

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...	Locat...	Vuln...	User	MAC	Weight	Off...	Dest...	Last Event/Flow	Events/Flows	
10.127.15.37		Net-10-...	No	Unknown	Unknown NIC	0	1	2	4h 39m 37s	410	Net-10-172-192.Net_10_0_0_0

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

The example offense on this slide is of type **Source IP**. Therefore, the Offense Source Summary displays the same information as the columns in the Top 5 Source IPs. Refer to the previous lesson for explanations of the columns.

Top 5 Source IPs (continued)

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" with a single row. The 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. A tooltip for "View" shows two options: "Destinations" (represented by a target icon) and "Offenses" (represented by a document icon).

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													Destinations
Destination IP	Magn...	Location	Vuln...	Chained	User	MAC	Weight	Off...	Sou...	Last Event/Flow	Events/Flows		
MORIA	██████	Net-10-...	YES	No	magda	00:30:18:AF:0B:83	0	1	1	4h 52m 46s	3		
10.26.1	Network: 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

Chained: The field shows Yes if the destination IP address is the source IP address of other offenses. In such cases, an attacker has taken control over the system with this IP address and uses it to attack other systems. Click Yes to view the chained offenses.

Magnitude: The column displays the Aggregate CVSS Score if this value exists. If it does not exist, the column displays the highest offense magnitude of all the offenses that the IP address is a part of.

Destination Magnitude: The bar displays the Aggregate CVSS Score if this value exists. If it does not exist, a zero (0) is displayed.

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

The diagram illustrates the 'Top 5 Log Sources' table with several callout boxes explaining its columns:

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

- Events:** Number of events sent by the log source contributing to the offense
- Log Sources:** View all log sources contributing to the offense
- 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

- **Name and Description:** QRadar SIEM administrators choose the name and description of a log source. They also choose the credibility for events that are received from the log source.
- **Custom Rule Engine:** The Custom Rule Engine (CRE) in QRadar SIEM contributes events to offenses. The CRE creates these events and adds them to offenses if test criteria specified in rules match the incoming events.
- **Group:** Optionally, QRadar SIEM administrators can group log sources.
- **Events/Flows and Total Events/Flows:** Although the column titles indicate flows, QRadar SIEM totals only events.

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

QRadar SIEM classifies offenses into categories. Categories cannot be added, deleted, or renamed.



Hint: Refer to the QRadar SIEM Administration Guide (<http://ibm.co/1wvPSEE>) for a list of high-level categories (HLC) and low-level categories (LLC).

Rules that are applied by the Custom Rules Engine (CRE) noticed the suspicious Firewall Deny events. As an action of the rules, the CRE created the events in the Network Sweep and ICMP Reconnaissance categories, and created the ICMP scanner offense that ties these events together.

- **Local Destination Count:** Shows **0** if all destination IP addresses are remote.
- **Events/Flows:** Shows the number of events per low-level category that contributed to the offense.

Top 5 Categories (continued)

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

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)

The First Event/Flow and Last Event/Flow columns include the same menu items, **Events** and **Flows**, as the context menu.

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

The last 10 events added to the offense provide the security analyst information about the latest developments in the offense.

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							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
"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 10:25:03 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

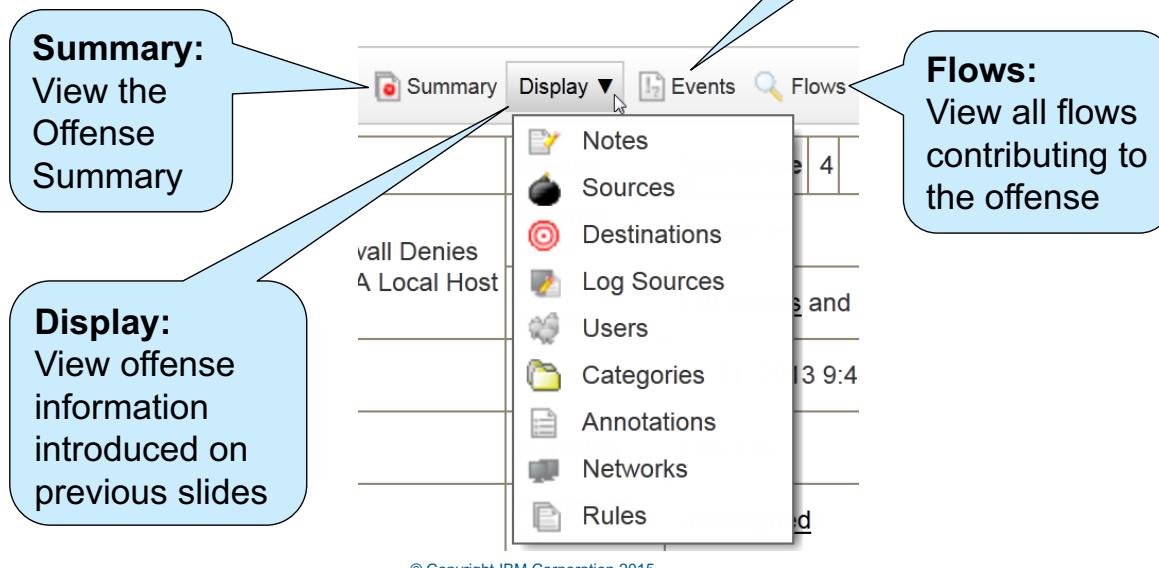
Annotations

QRadar SIEM rules and building blocks add annotations when they create or update an offense.

QRadar SIEM users cannot add, edit, or delete annotations.

Offense Summary toolbar

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

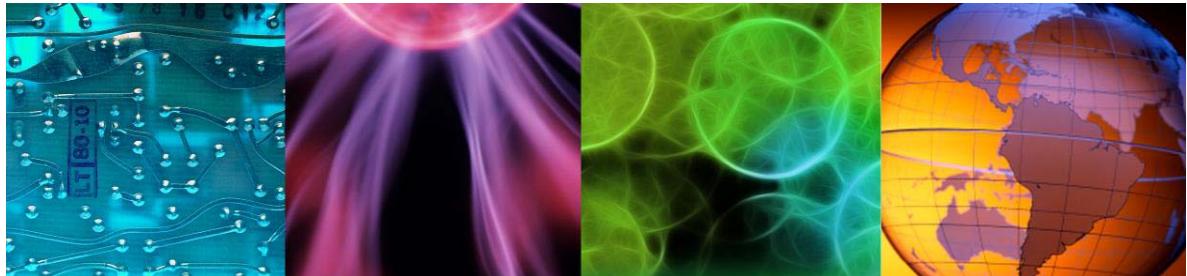


Offense Summary toolbar

Lesson 4 Acting on an offense



Lesson: Acting on an offense



© Copyright IBM Corporation 2015

Security analysts draw conclusions from investigating an offense and can act accordingly. In this lesson, you learn how to take action on an offense in QRadar SIEM.

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 Offense Summary page with various details like Status, Relevance, Offense Type (Source IP), Event/Flow count (411 events and 4 flows), Start date (Jul 31, 2013 9:46 AM), Duration (46m 37s), and Assigned to (Unassigned). A cursor is hovering over the 'Actions' button in the top navigation bar, which has a dropdown menu with the following items:

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

Callouts 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

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.

- **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 the QRadar SIEM interface for investigating an offense. At the top, there are tabs for 'Primary', 'Display ▼', 'Events', 'Flows', and 'Actions ▼'. Below the tabs is a table with offense details:

Status	Relevance
Source IP	4
Event/Flow count	411 events are
Start	Jul 31, 2013 9:46 AM
Duration	46m 37s
Assigned to	lynnette

An 'Actions' dropdown menu is open, listing the following options:

- 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

This slide displays the **Status** field and the **Actions** menu after you have performed the following actions:

- Follow up
- Protect Offense
- Close
- Add Note
- Assign

Field descriptions

- **Status:** No icon exists for status *active*. An icon exists for the status of *hidden*, but it is not displayed in the slide.
- **Follow up, Email, Add Note, and Assign:** These actions are available for *inactive* offenses. When you select **Follow up** for an offense with the **Follow up** flag that is already set, QRadar SIEM removes the flag.
- **Assigned to:** The offense is now assigned to a QRadar SIEM user.



Note: The **Actions** menu of the Offense Manager on the **Offenses** tab allows you to export offenses. You can export offenses to keep records outside of QRadar SIEM. Exported offenses cannot be imported back into QRadar SIEM.

Student exercise

Use the procedures in the *Student Exercises Guide* to investigate the local DNS scanner offense



© Copyright IBM Corporation 2015

Student exercises

Perform the exercises for this unit.

Summary

Now you should be able to perform the following tasks:

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

© Copyright IBM Corporation 2015

Summary



5 Investigating the events of an offense



Investigating the events of an offense



© Copyright IBM Corporation 2015

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

The investigation of an offense usually leads to the investigation of the events that contributed to the offense. This unit teaches you how to find, filter, and group events in order to gain critical insights about the offense. You also learn how to create and edit a search that monitors the events of suspicious hosts.

Reference: QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>



Objectives

In this unit, you learn to perform the following tasks:

- 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

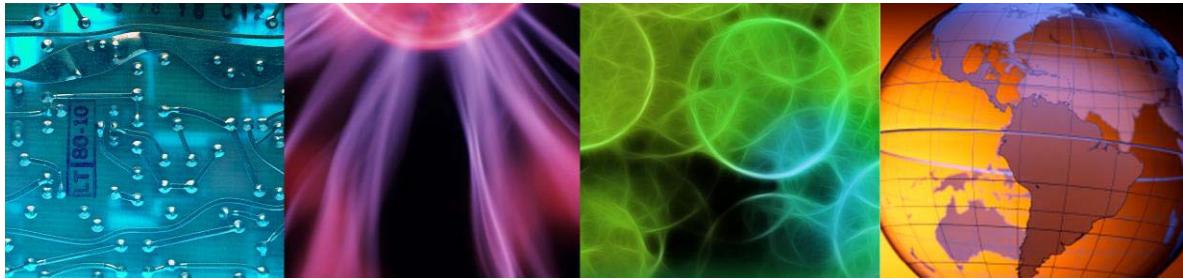
© Copyright IBM Corporation 2015

Objectives

Lesson 1 Investigating event details



Lesson: Investigating event details



© Copyright IBM Corporation 2015

One of the first steps when investigating the events of an offense is to examine the event data at a high level. In this lesson, you learn how to navigate the event details that are displayed in the list of events.

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



Note: You can also use the **Log Activity** tab to view events.

List of events

Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾

Quick Filter

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: Completed

Current Filters:
Offense is Excessive Firewall Denies Across Multiple Hosts From A Loca... [\(Clear Filter\)](#)

► Current Statistics

Records Matched Over Time

Reset Zoom 7.5 10/15/14 4:31 AM - 10/15/14 4:35 AM

[Update Details](#) [\(Hide Charts\)](#)

Hide graphical charts

	Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
	Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:33:0...	Firewall Deny	10.26.72.208	N/A	10.168.10.2	N/A	N/A	
	Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:4...	Firewall Deny	10.26.72.208	N/A	172.22.6.6	N/A	N/A	
	Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:4...	Firewall Deny	10.26.72.208	56086	197.0.0.10	0	N/A	
	Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:4...	Firewall Deny	10.26.72.208	56087	197.0.0.11	0	N/A	
	Excessive Firewall Denies Across ...	Custom Rule Engine-8 :: COE	1	Oct 15, 2014, 4:32:3...	Network Sweep	10.26.72.208	N/A	N/A	N/A	N/A	
	Firewall Deny	CheckPoint @ FW-1Machine	1	Oct 15, 2014, 4:32:3...	Firewall Deny	10.26.72.20	N/A	N/A	N/A	N/A	

View event details by double-clicking a row

© Copyright IBM Corporation 2015

List of events

To sort events, click a column header. To investigate suspicious activity, you must locate the information that is associated with the offense, such as its 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
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

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

The screenshot shows a 'Payload Information' panel with tabs for 'utf', 'hex', and 'base64'. The 'utf' tab is selected, and a checkbox for 'Wrap Text' is checked. The raw event data is displayed as follows:

```
<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-
7FE5-4D60-9C89-4F949392E8661
profile: Default_Atlantis, sic...
dst: 208.111.161.105; proto: tcp; product:
VPN-1 & FireWall-1; service: http;
s_port: 4696;
```

A callout bubble points to the word 'Default_Atlantis' in the raw data, with the following text:

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

QRadar SIEM normalizes data out of raw events automatically, including information such as:

- Date
- Time
- Source IP address
- Destination IP address
- Protocol

Event details: Additional details

The diagram illustrates the 'Additional Information' section of the Event Details window. It features four callout boxes pointing to specific fields:

- Protocol:** Network protocol (points to the 'Protocol' field: icmp_ip)
- QID:** The QID determines the name, low-level category, and high-level category of an event (points to the 'QID' field: 2750010)
- Log Source:** This log source provided the raw event that QRadar SIEM normalized into this event (points to the 'Log Source' field: CheckPoint @ FW-1Machine)
- Event Count:** Number of raw events bundled into this normalized event (points to the 'Event Count' field: 1)

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

© Copyright IBM Corporation 2015

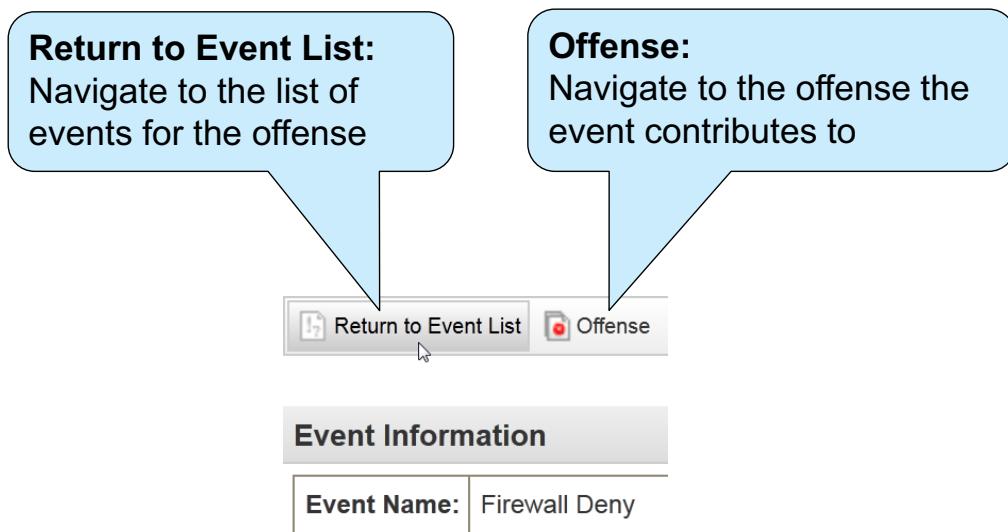
Event details: Additional details

The Event Details window provides more event information. This information is discussed in more depth later in this course.

- **Protocol:** In this example, the protocol is *icmp_ip*. ICMP is encapsulated into IP. Both are layer 3 protocols.
- **QID:** To normalize raw events, QRadar SIEM maps them to unique QIDs.
- **Log Source:** A system on your network is a log source if QRadar SIEM receives raw events from it.
- **Event Count:** For each individual log source, QRadar SIEM administrators can enable or disable **coalescing** of multiple similar raw event into one normalized event. The number indicates how many raw events have been coalesced into one normalized event. A coalesced, normalized event contains only the first raw event in the payload.

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



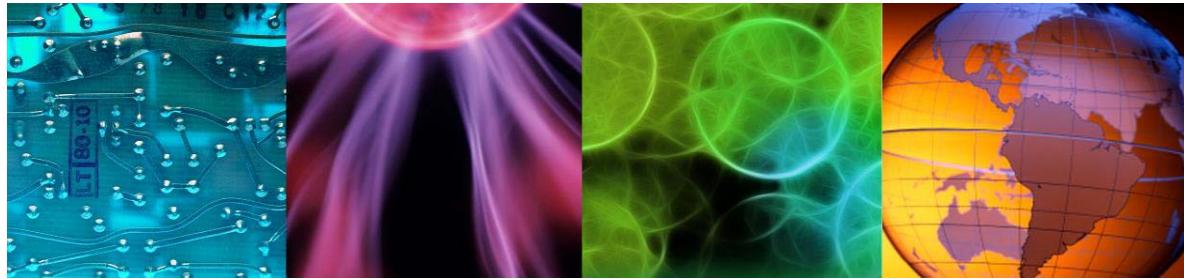
© Copyright IBM Corporation 2015

Returning to the list of events

Lesson 2 Using filters to investigate events



Lesson: Using filters to investigate events



© Copyright IBM Corporation 2015

Filters can temporarily hide events from the user interface, which makes it easier to focus on more significant events. When investigating events, it can be helpful to filter the events. In this lesson, you learn how to filter events.

Reference: QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>

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
1	Firewall Deny	CheckPoint @ FW-1Machine	1
2	Firewall Deny	CheckPoint @ FW-1Machine	1
3	Firewall Deny	CheckPoint @ FW-1Machine	1
4	Firewall Deny	Filter on Event Name is Firewall Deny	
5	Firewall Deny	Filter on Event Name is not Firewall Deny	
6	Firewall Deny	False Positive	
7	Firewall Deny	CheckPoint @ FW-1Machine	1
8	Firewall Deny	CheckPoint @ FW-1Machine	1
9	Firewall Deny	CheckPoint @ FW-1Machine	1

© Copyright IBM Corporation 2015

Filtering events

You can right-click most fields to filter them. Use the **False Positive** option to prevent this and similar events from contributing to an offense.

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

After filtering the **Firewall Deny** events, the List of Events displays the events created by the Custom Rule Engine (CRE) in QRadar SIEM. These events do not carry a payload because they are not based on a raw event.

In the example on the slide, the filtered **Firewall Deny** events sent by the **CheckPoint @ FW-1Machine** log source. The Low Level Category column (not displayed on the slide) indicates that QRadar SIEM classified those events into the ICMP Reconnaissance and Network Sweep categories.

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
	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

Unlike searches, filters do not query each event processor

© Copyright IBM Corporation 2015

 **Note:** Searches are introduced later in this course.

Applying a Quick Filter to the payload

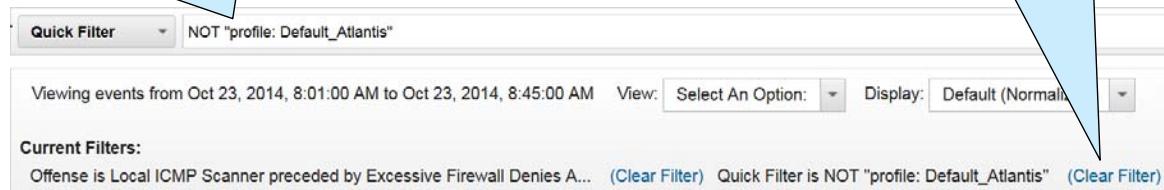
- The payload of an event contains the raw event that mentions the firewall profile that denied the connection
- To verify that the company's main profile, Atlantis, was always active, filter events without **profile: Default_Atlantis** in the payload

Quick Filter:

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

Clear Filter:

Click to view all events of the offense again



© Copyright IBM Corporation 2015

Applying a Quick Filter to the payload

Quick Filter supports expressions with AND, OR, and NOT. For example, when you apply the **NOT "profile: Default_Atlantis"** Quick Filter and no events show, you can assume that all of the event's payloads mention the firewall profile **Default_Atlantis** because no other firewall profile was active.



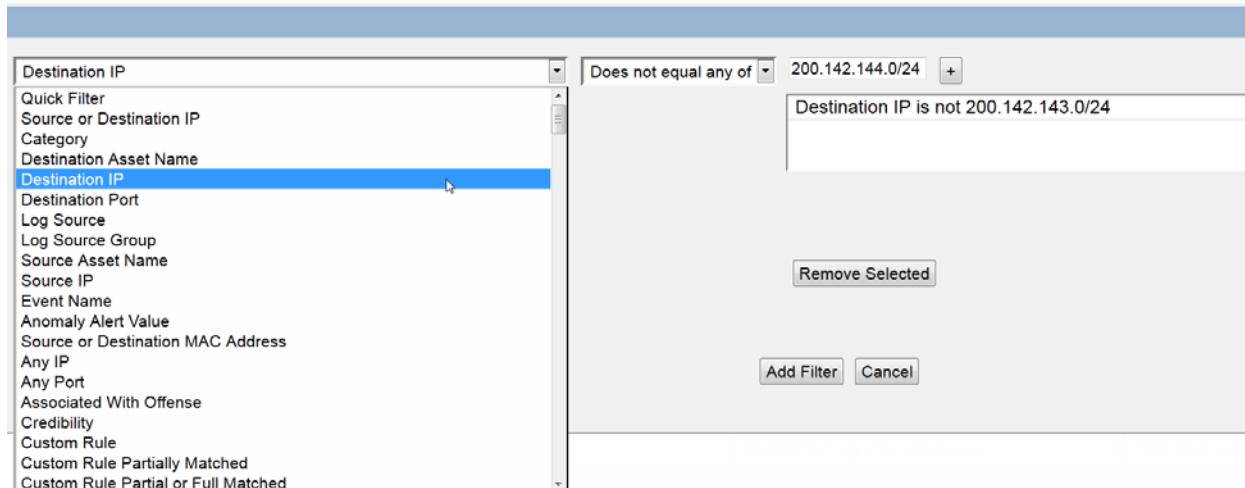
Note: Refer to the *QRadar SIEM Users Guide* (<http://ibm.co/1wvpSEE>) for more information about the expressions that Quick Filter supports.

A coalesced event contains only the payload of one of the raw events that are bundled. Therefore, quick filtering looks into only that one 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

Other filter options are available:

- Instead of an IP address, you can enter a range of IP addresses, in CIDR notation, such as 10.100.0.016.
- To include multiple filters, write **AND** between each one.
- To build an OR expression, use **Equals any of**.
- To search the payload for something that is not normalized, use **Payload contains** and **Payload Matches Regular Expression**. To find these menu items, scroll to the end of the list.

Lesson 3 Using grouping to investigate events



Lesson: Using grouping to investigate events



© Copyright IBM Corporation 2015

Grouping events arranges the events so you can view them from different perspectives. In this lesson, you learn how to group the events of an offense.

Grouping events

The screenshot shows the QRadar SIEM interface with a 'Display' dropdown menu open. The menu includes options like 'Default (Normalized)', 'Raw Events', and 'Low Level Category'. The 'Low Level Category' option is highlighted with a blue arrow pointing from the 'Raw Events' callout. Other options in the menu include Event Name, Destination IP, Destination Port, Source IP, Custom Rule, Username, Log Source, High Level Category, Network, and Source Port.

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

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

© Copyright IBM Corporation 2015

Grouping events

After changing the grouping, events are organized accordingly. All filters are retained.

Grouping events by low-level category

Grouping By:

QRadar SIEM shows the currently selected grouping above the filters

Viewing events from Jul 31, 2013 9:25:00 AM to Jul 31, 2013 10:10:00 AM View: Select An Option: Display: Low Level Category ▾

Grouping Raw Events Low Level Category Event Name Destination IP Destination Port Source IP Custom Rule Username Log Source High Level Category Network Source Port

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 :: COF	tcp_ip	N/A	8
ICMP Reconn...	10.127.15.37	Multiple (7)	0	Local ICMP Scanner	Custom Rule Engine-8	ip	N/A	4

All events are aggregated by their low-level category

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

In this example, exploring by grouping indicates a second protocol

Grouping events by low-level category

Grouping summarizes all events by the chosen field. In this example, grouping events by **Low Level Category** displays a column of all the unique low-level categories and summary information of the other columns, such as the number of unique protocols for each low-level category.

In the Protocol column, **Multiple (x)** is displayed, where x is the number of unique protocols. If only one protocol exists for a low-level category, that value displays instead of **Multiple (x)**. When you double-click the **Multiple (x)** protocols, a browser window that groups these protocols opens. The new window displays the unique protocols summarized by the previous grouping of 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

The screenshot shows the QRadar SIEM interface with the following details:

- Header: Viewin... 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 Multipl... ([Clear Filter](#))
 - Low Level Category is Firewall Deny ([Clear Filter](#))
- ▶ Current Statistics
- Table:

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

To explore the event further, click **Multiple (2)** to view the two destinations IP addresses that the source IP address wanted to contact using **udp_ip**. When finished, close the window.

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: Select An Option: Display: Low Level Category Default (Normalized) 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

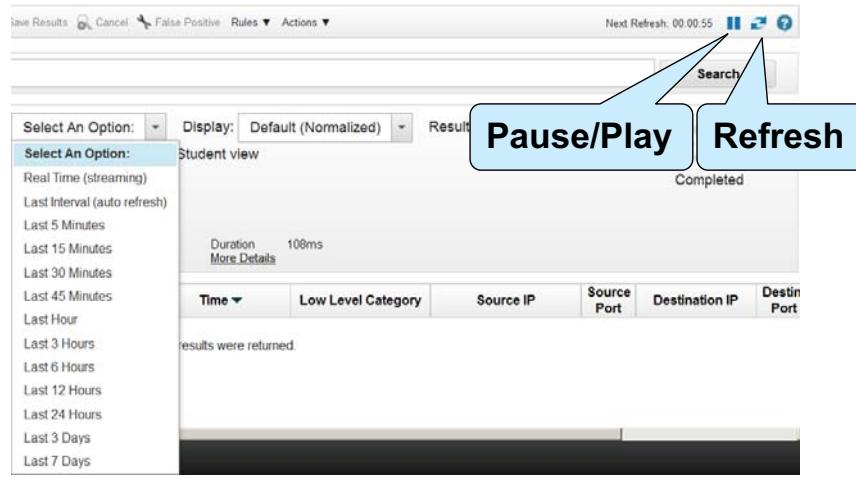
© Copyright IBM Corporation 2015

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



Viewing a range of events

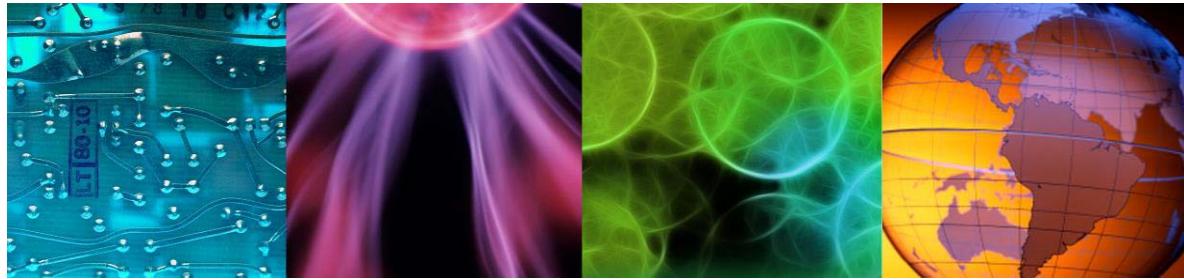
In addition to viewing incoming events, you can select a time range from the **View** list. When you open the List of events window from the Offense Summary, QRadar SIEM automatically includes all events added to the offense.

- **Last Interval (auto refresh):** The last minute of events can be delayed by up to one minute from the time the event reached the Event Processor refresh cycle.
- **Real Time (streaming):** To view the details of an event, pause streaming and double-click the event.
- **Real Time (streaming) and Last Interval (auto refresh):** Quick Filter on payloads allows filtering on simple words and phrases but not on expressions with AND, OR, and NOT.

Lesson 4 Saving a search



Lesson: Saving a search



© Copyright IBM Corporation 2015

The event list is the result of the search criteria that you chose. In this lesson, you learn how to save a search and use it to investigate the events that are included in an offense. The scenario that is used as an example in this lesson monitors a suspicious host.

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

[\(Show Charts\)](#)

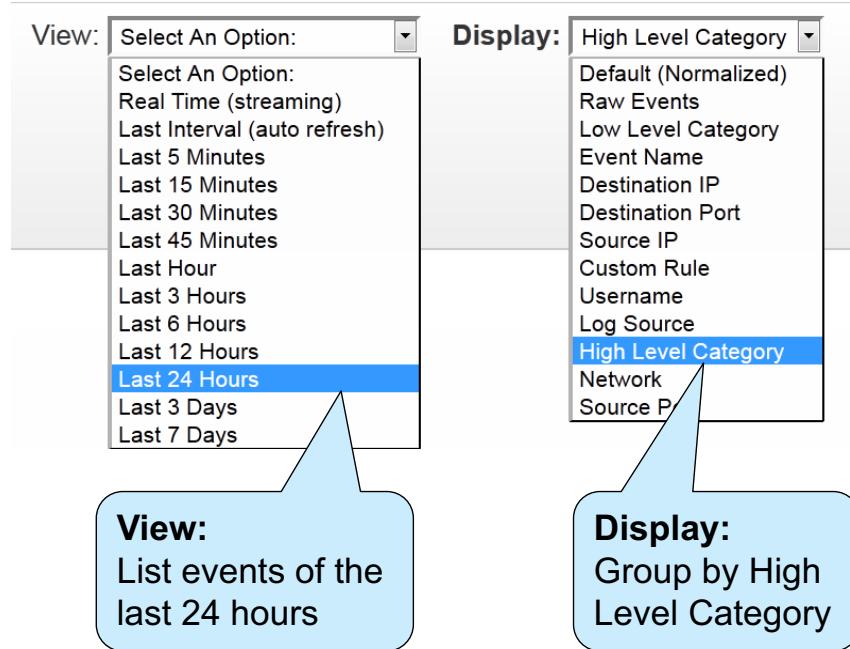
	Event Name	Log	Ev Co	Time ▼	Low Level Category	Source IP
1	Firewall Deny	CheckPoint @ FW- Machine	1	7/31/13 10:08:43 AM	Firewall Deny	10.127.15.37
2	Firewall Deny	CheckPoint @ FW-		Filter on Source IP is 10.127.15.37		127.15.37
3	Firewall Deny	CheckPoint @ FW-		Filter on Source IP is not 10.127.15.37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

© Copyright IBM Corporation 2015

Monitoring the scanning host

To monitor a scanning host, filter on the IP address and then clear the offense filter. If you clear the offense filter first, all of the events in the given time range show, making it difficult to find the IP address of interest.

Monitoring the scanning host (2 of 3)



© Copyright IBM Corporation 2015

Monitoring the scanning host (2 of 3)

Monitoring the scanning host (3/3)

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:

- Top navigation bar: Search..., Quick Searches, Add Filter, Save Criteria, Save Results, Cancel, False Positive, Rules, Actions, Quit.
- Time range: 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 (Filtering). (Clear Filter).
- Statistics section: ▶ Current Statistics (Show Charts).
- Table of search results:

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

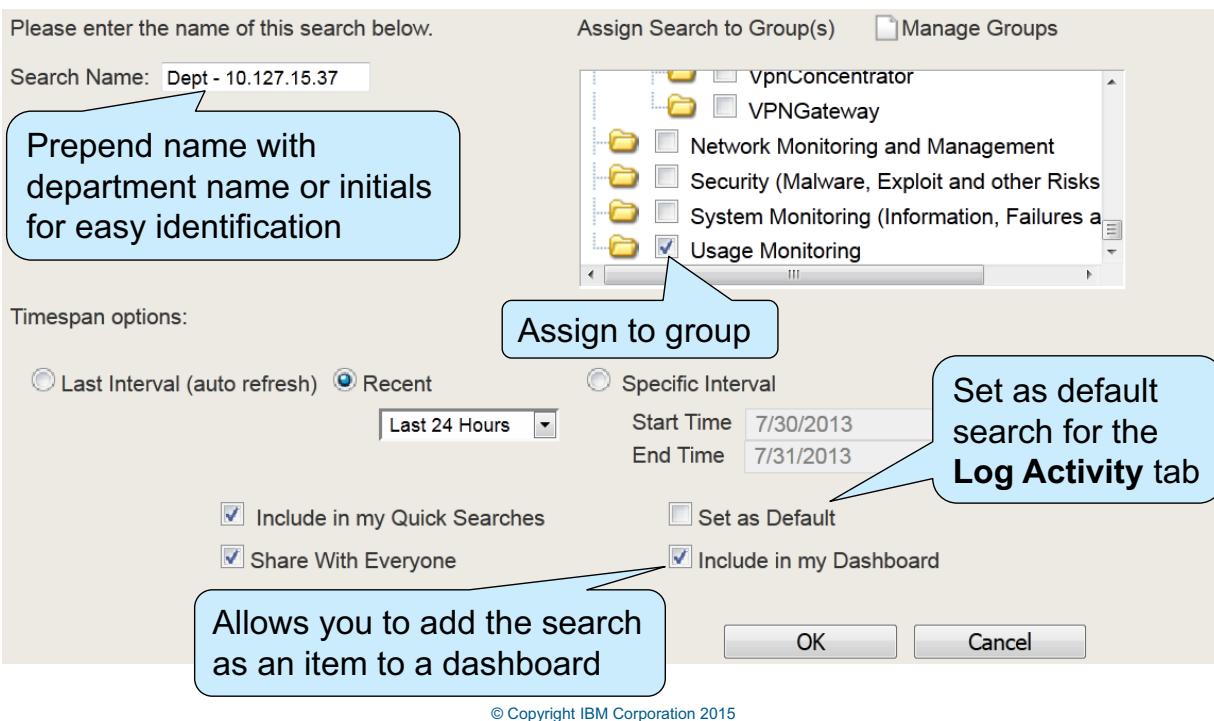
© Copyright IBM Corporation 2015

Monitoring the scanning host (3 of 3)

The key components of a search are time range, grouping, and filtering. You can save the search criteria, the results, or both. To save the displayed search, click **Save Criteria**.

Saving search criteria

Save the search with the criteria specified



Saving search criteria

You can include the criteria shown in the following list in your saved search:

- **Manage Groups:** Add, edit, or remove search groups.
- **Include in Quick Searches:** Add the saved search to the **Quick Searches** menu.
- **Share with Everyone:** Include this search in other users' lists of available searches.
- **Set as Default:** Show the result of this search by default on the **Log Activity** tab.
- **Include in my Dashboard:** Note that only grouped searches can be included in the dashboard.

Event list using the saved search

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

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

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
Using Search: Dept - 10.127.15.37

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

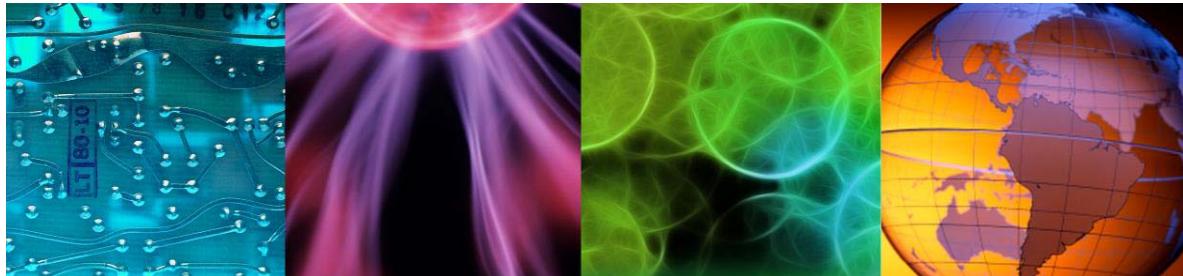
© Copyright IBM Corporation 2015

Event list using the saved search

Lesson 5 Modifying saved searches



Lesson: Modifying saved searches



© Copyright IBM Corporation 2015

To use QRadar SIEM effectively, manage and modify saved searches. In this lesson, you learn how to work with 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 a user interface for managing quick searches. At the top, there is a toolbar with buttons for 'Search...', 'Quick Searches' (with a dropdown arrow), 'Add Filter', 'Save Criteria', 'Save Results', 'Cancel', and 'False Positives'. Below the toolbar, a list of saved searches is displayed. One search, 'Dept - 10.127.15.37 - Last 24 Hours', is highlighted with a blue background. To the left of the search list, there is a sidebar titled 'Grouping' which includes 'High Level' and 'Current F...' sections. Under 'Current F...', there is a '► Current' section. Below these sections is a table titled 'High Level Category' with three rows: 'Access' and 'Recon'. The 'Access' row is currently selected. The main search list contains numerous items, such as 'Compliance: Source IPs Involved in Compliance Rules - Last 6 Hours', 'Default-IDS / IPS-All: Top Alarm Signatures - Last 6 Hours', and various network and security metrics.

© Copyright IBM Corporation 2015

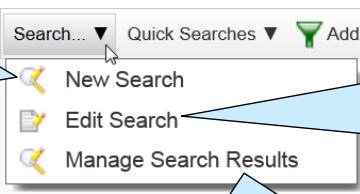
About Quick Searches

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



Edit Search:

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

Manage Search Results:

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

© Copyright IBM Corporation 2015

Using alternative methods to create and edit searches

Use the following options on the **Search** menu:

- The **New Search** and **Edit Search** menu items are about search criteria.
- The **Manage Search Results** menu item is about search results.

Managing search results

You can use the **Manage Search Results** option to complete the following tasks:

- Save results for auditing or forensics
- Delete previously saved search results
- Cancel long-running searches
- Send an email when the search in progress finishes



Note: Users see only the searches they create in the Manage Search Results window. Administrators see all searches.

Cancelling a search

QRadar SIEM might delete unsaved search results earlier than 24 hours if it requires the disk space.

When a search is queued or in progress, you can cancel the search in Manage Search Results or by clicking the **Cancel** button in the top menu bar. Search results accumulated before the cancellation are maintained.

How QRadar SIEM processes searches

Searches run concurrently in the background. The maximum number of concurrent searches depends on the search and the appliance in use. Subsequent searches above the maximum number are queued. Details of the three search queues are as follows:

- The **low-priority queue** includes searches that generate reports.
- The **normal-priority queue** includes searches created by users.
- The **high-priority queue** includes searches for dashboard items such as graphs and searches for the view Last interval (auto refresh).

Finding and loading a saved search

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

The screenshot shows the 'Saved Searches' interface. At the top, there is a group dropdown labeled '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, 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** (highlighted with a blue selection bar)
- DOS Attacks by Destination IP

At the bottom of the interface are two buttons: 'Load' and 'Delete'.

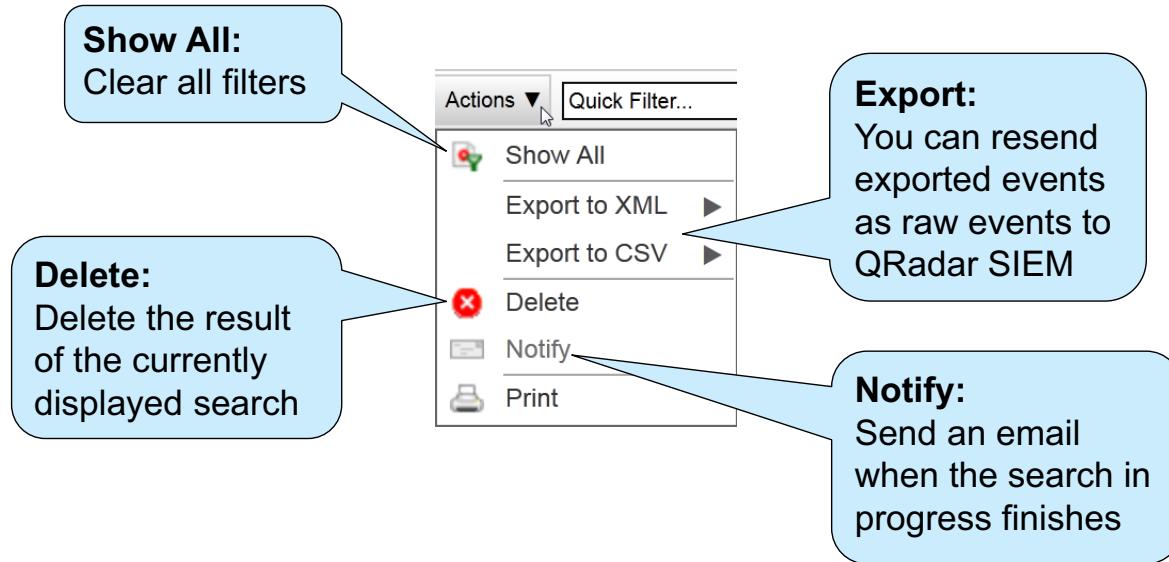
Type Saved Search:
To find saved searches easily, type your department name, if you prepended your saved searches with it

© Copyright IBM Corporation 2015

Finding and loading a saved search

The Event Search window provides more search features, such as custom time ranges, grouping by two or more fields, and column arrangement for the results.

Search actions



© Copyright IBM Corporation 2015

Search actions

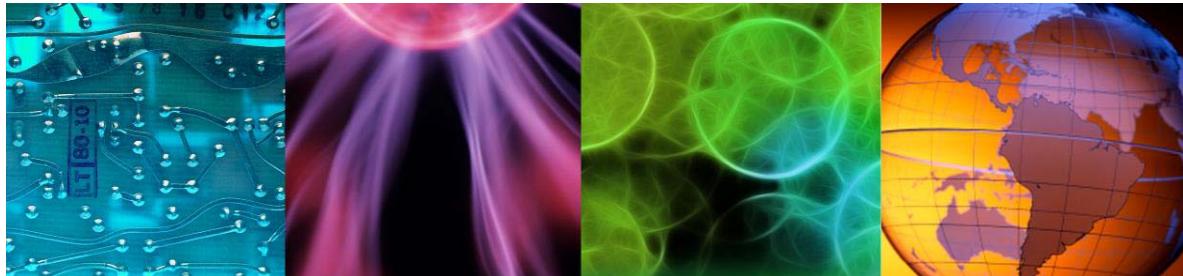
The following actions are available on the Quick Filter Search's **Action** menu:

- **Export to XML, Export to CSV, and Print:** These menu items are not available when viewing *Real Time (streaming)* or viewing partial results from a canceled search.
- **Delete:** This menu item is available only when no search is in progress.
- **Notify:** This menu item is available only when a search is in progress.

Lesson 6 Adding a search to the dashboard



Lesson: Adding a search to the dashboard



© Copyright IBM Corporation 2015

Dashboard items display the results of searches. In this lesson, you learn how to add and edit a saved 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 managing dashboard items. On the left, there's a sidebar with links like 'Network Activity', 'Offenses', 'Log Activity', 'Reports', 'System Summary', 'System Notifications', and 'Internet Threat Information Center'. A dropdown menu is open under 'Reports', showing options: 'Event Searches', 'Events By Severity', and 'Top Log Sources'. The main pane lists various search results, such as 'Top Authentications by User', 'Top Services Denied through Firewalls', etc. A specific search result, 'Dept - 10.127.15.37', is highlighted with a blue bar at the bottom. A note in the center-left says: 'Note: This screen capture shows the Dashboard tab'.

Add Item... ▾

- Network Activity
- Offenses
- Log Activity
- Reports
- System Summary
- System Notifications
- Internet Threat Information Center

Event Searches ▾

- Events By Severity
- Top Log Sources

- 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

Dept - 10.127.15.37

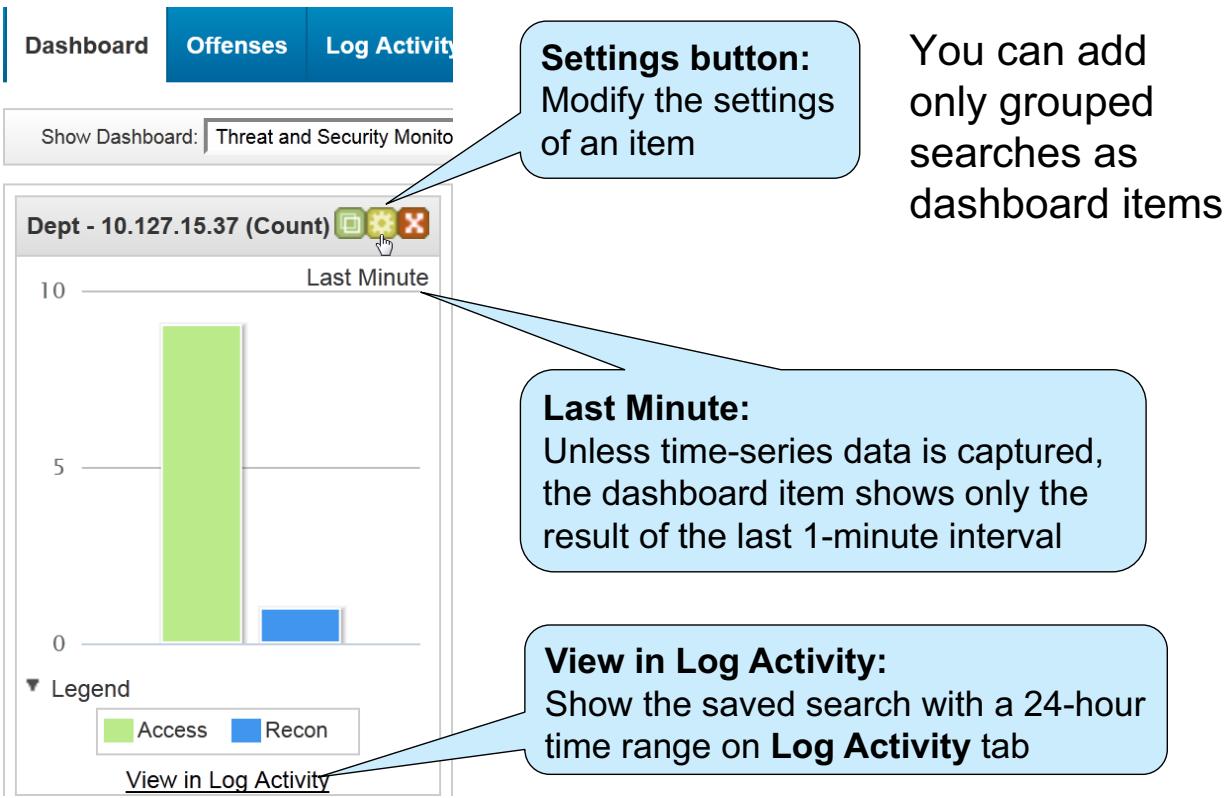
Top Rules

© Copyright IBM Corporation 2015

Adding a saved search as a dashboard item

If you select **Include in my Dashboard** when saving the search, you can add it as dashboard item. Dashboard items can display only searches with grouping.

Saving a search as a dashboard item



You can add only grouped searches as dashboard items

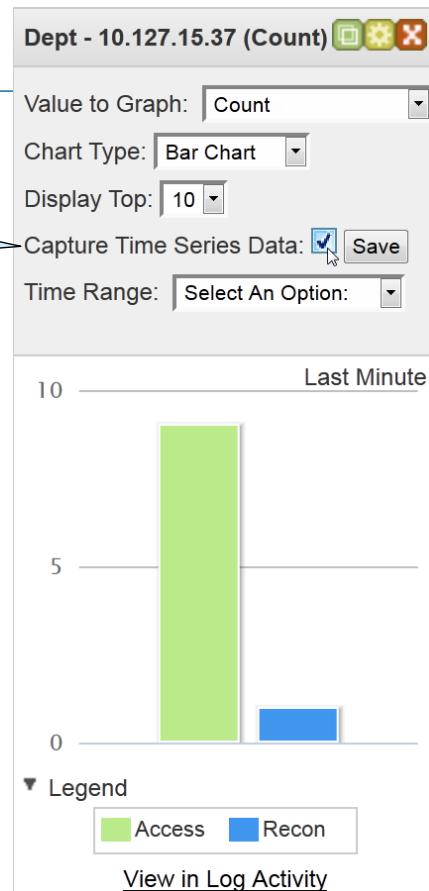
Saving a search as a dashboard item

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



Note: User permissions control the ability to configure and view time-series data.

Two options are in the **Value to Graph** list:

- **Count:** Number of events **before** coalescing bundles several raw events into one normalized event.
- **Event Count:** Number of events **after** coalescing has bundled several raw events into one normalized event.

Selecting the time range

Value to Graph:

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

Dept - 10.127.15.37 (Count)   

Value to Graph: * Count

Chart Type: Bar Chart

Display Top: 10

Capture Time Series Data: Save

Time Range: Select An Option:

- Select An Option:
- Last Minute
- 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
- Last 14 Days
- Last 28 Days
- Last 30 Days
- Last 31 Days
- Last 60 Days
- Last 90 Days
- Current Hour

Time Range:
Select Last 24 Hours

© Copyright IBM Corporation 2015

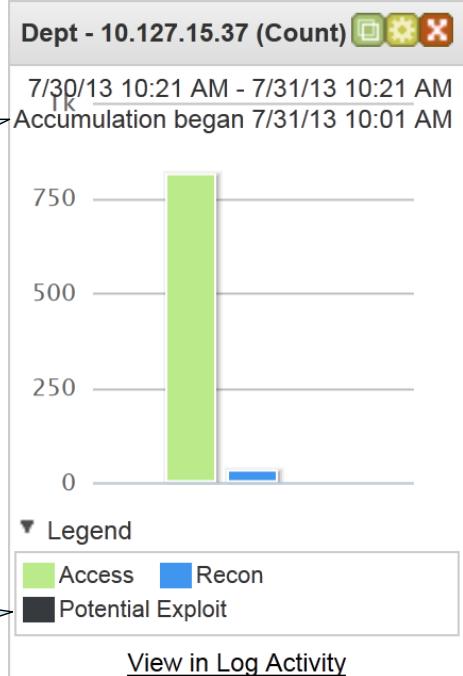
Selecting the time range

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

The screenshot shows a QRadar Log Activity window titled "Dept - 10.127.15.37 (Count)". The "Value to Graph" dropdown is set to "* Count". The "Chart Type" dropdown is open, showing options: Bar Chart, Pie Chart, Table (which is selected), and Time Series. Below the dropdown, the "Capture Time" and "Save" buttons are visible. The "Time Range" dropdown is set to "Select An Option". The main area displays a table of high-level categories and their counts:

High Level Category	Count
Access	814
Recon	31
Potential Exploit	2

At the bottom right of the table area is a link labeled "View in Log Activity".

© Copyright IBM Corporation 2015

Modifying items in the chart type table

Student exercises

Use the procedures in the *Student Exercises Guide* to perform these tasks

- Look for events contributing to an offense
- Save search criteria and search results
- Investigate event details



© Copyright IBM Corporation 2015

Student exercises

Perform the exercises for this unit.



Summary

Now you should be able to perform the following tasks:

- 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

© Copyright IBM Corporation 2015

Summary



6 Using asset profiles to investigate offenses



Using asset profiles to investigate offenses



© Copyright IBM Corporation 2015

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

QRadar SIEM stores security-relevant information about systems in your network in asset profiles. This unit teaches you how asset profiles are created and updated, and how to use them as part of an offense investigation.

References:

- *QRadar SIEM Vulnerability Assessment Configuration Guide* <http://ibm.co/1wvpSEE>
- *QRadar SIEM Administration Guide* <http://ibm.co/1wvpSEE>
- *PCI Security Standards Council* <https://www.pcisecuritystandards.org>

This unit has no student exercises.

Objectives

In this unit, you learn to perform the following tasks:

- Describe the purpose of an asset profile
- Investigate asset profile details

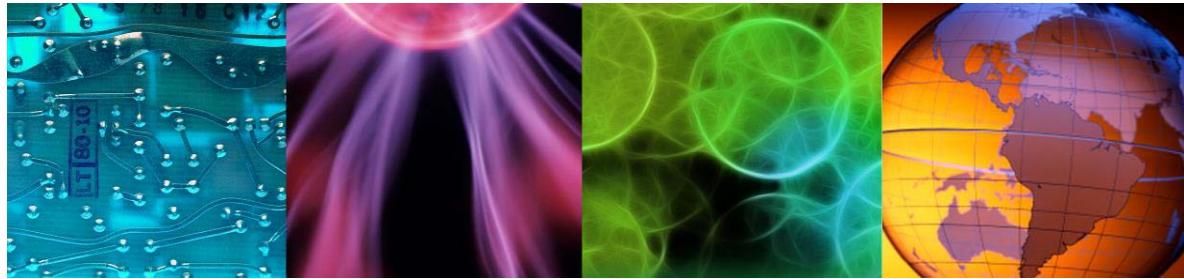
© Copyright IBM Corporation 2015

Objectives

Lesson 1 Assets overview



Lesson: Assets overview



© Copyright IBM Corporation 2015

The asset profiles of QRadar SIEM store security-relevant data of systems in your network. In this lesson, you are introduced into asset profiles and also learn how QRadar SIEM creates and updates asset profiles.

About asset profiles

- An asset is any type of system or host in the network
- Asset profiles store a wealth of information about the system resources, such as these examples
 - Name
 - IP addresses
 - MAC addresses
 - Operating system
 - Vulnerabilities
 - Services
 - Other resource information
- Use asset profiles to investigate each source and destination IP address of an offense

© Copyright IBM Corporation 2015

About asset profiles

Asset information is used throughout QRadar SIEM. For example, if a source attempts to attack a specific service running on a specific asset, QRadar SIEM can determine if the asset is vulnerable to this attack by correlating the attack to the asset profile.



Note: QRadar SIEM is not a full-fledged asset management system. For example, it does not show which computer hosts a virtual machine. QRadar SIEM also cannot represent storage in asset profiles.

Creating asset profiles

- QRadar SIEM automatically creates and updates asset profiles for systems found in these locations
 - DHCP, DNS, VPN, proxy, firewall NAT, and wireless access point logs
 - Passively gathered bidirectional flows
 - Vulnerability data provided by active scanners
- Only flows and vulnerability data add and update information about ports, services, and products to asset profiles
- QRadar SIEM administrators can create assets by using these methods
 - Manually in the user interface
 - By importing a CSV file in this format
IP address, Name, Weight (1-10), Description
Administrators can use the REST API to import other properties

© Copyright IBM Corporation 2015

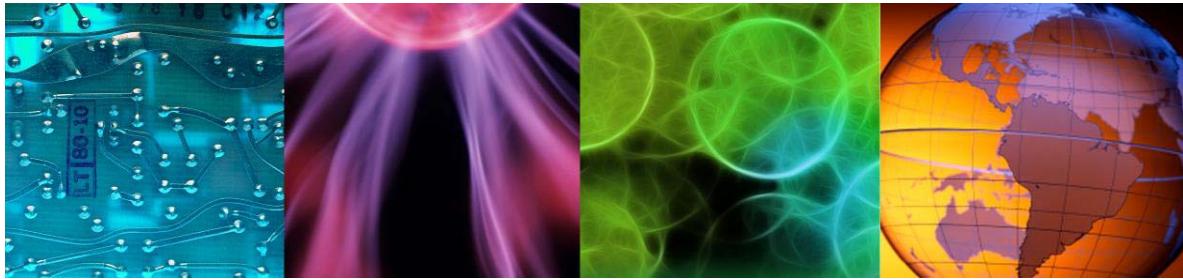
Creating asset profiles

QRadar SIEM administrators can delete asset profiles. A deleted asset profile is recreated if an active scanner finds the system or QRadar SIEM detects it in flow data.

Lesson 2 Investigating asset details



Lesson: Investigating asset details



© Copyright IBM Corporation 2015

Information regarding a system in your network is often beneficial to an offense investigation. In this lesson, you learn how to locate asset profiles and find details about an asset.

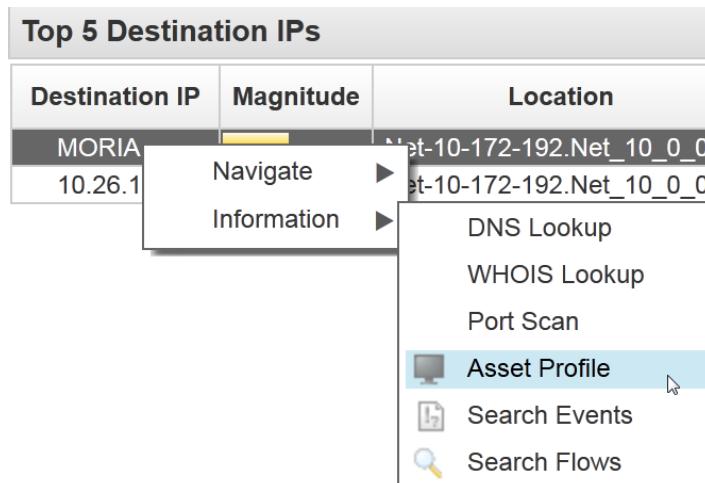
References:

- QRadar SIEM Vulnerability Assessment Configuration Guide <http://ibm.co/1wvpSEE>
- QRadar SIEM Administration Guide <http://ibm.co/1wvpSEE>
- PCI Security Standards Council <https://www.pcisecuritystandards.org>

Navigating from an offense to an asset

In the Offense Summary, you can navigate to the asset profile of any source or destination by this method

1. Right-click the IP address or asset name
2. Click **Information > Asset Profile**



© Copyright IBM Corporation 2015

Navigating from an offense to an asset

Assets tab

- You can also click the **Assets** tab to locate asset profiles
- You can search, filter, and sort asset profiles in a similar way as events

The screenshot shows the QRadar SIEM interface with the Assets tab selected. The top navigation bar includes tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets (selected), Reports, and Admin. On the left, a sidebar lists Asset Profiles, Server Discovery, and VA Scan. The main content area is titled 'Assets' and contains a table with the following data:

ID	IP Address	Asset Name	Aggregate CVSS Score	Vulnerabilities	Services
1008	10.26.10.5	MORIA	19.5	9	5
1001	192.168.1.1	192.168.10.10	0.0	0	21

A callout box with a blue arrow points to the first row of the table, containing the ID 1008, IP 10.26.10.5, and Asset Name MORIA. The text inside the callout box reads: "To investigate the asset profile of a target of the ICMP scanner offense, double-click the row".

© Copyright IBM Corporation 2015

Assets tab

Use the **Assets** tab to work with the following aspects of the asset management system within QRadar SIEM:

- **Asset Profiles:** If a system has two IP addresses on two different networks and a QRadar SIEM user is granted permission to view only one of the networks, the user will not see the system's asset profile at all.
- **Server Discovery:** QRadar SIEM administrators can discover different server types, such as mail, web, and Windows servers. QRadar SIEM classifies a server of a specific type if one or more open ports match the standard port for that server type. QRadar SIEM does not probe open server ports but uses the passively gathered network flows to determine open ports. Refer to the *QRadar SIEM Administration Guide* (<http://ibm.co/1wvSEE>) for more information about Server Discovery.
- **VA Scan:** QRadar SIEM administrators can schedule active scans for vulnerability assessments (VA) of systems on the network. Refer to the *QRadar SIEM Vulnerability Assessment Configuration Guide* (<http://ibm.co/1wvSEE>) for more information about VA Scan.

Asset summary

Double-click an asset to open the asset details

The screenshot shows the 'Asset Summary' section of the QRadar interface. At the top, there are several navigation links: Display ▾, Edit Asset, View By Network, View Source Summary, View Destination Summary, History, Applications, and Actions ▾. Below this is a section titled 'Asset Summary' with a table of asset information:

Asset ID	1008	IP Address	10.26.10.5 (Current DNS: 10.26.10.5)	MAC Address	00:30:18:AF:0B:83
Network	Net-10-172-192.Net_192_168_0_0	NetBIOS Name	MORIA	DNS Name	
Given Name		Group Name		Last User	magda (All Users)
Operating System	UNIX	Weight		Aggregate CVSS Score	19.5

A callout box points to the 'Aggregate CVSS Score' field, which contains the value '19.5'. The callout box contains the text: 'Aggregate CVSS Score: Level of concern about this asset in comparison to others'. Another callout box points to the 'Last User' field, which contains 'magda (All Users)'. This callout box contains the text: 'All Users: Display previous users of the asset'.

© Copyright IBM Corporation 2015

Asset summary

An asset can have many MAC addresses, IP addresses, DNS names, and NetBIOS names.

Either of the following statements can be true about a MAC Address:

- It is manually entered by a QRadar administrator.
- It is populated by an active scanner.

QFlow and other accounting technologies do not capture the MAC address.

The asset **Weight** measures the importance of the asset. The levels range from 0 (not important) to 10 (very important).

Vulnerabilities

Verify the vulnerabilities of the asset to determine whether the investigated offense is a concern

Severity:

Payment Card Industry (PCI) severity level

Risk:

Threat level

Risk Score:

Level of concern about this vulnerability in comparison to others

ID	Severity	Risk ▲	Service	Port	Vulnerability	Details	Risk Score
101656	High	Warning		445	Netbios - NULL Session - Information Loss		6.70
101657	High	Warning		445	Netbios - NULL Session - User.Group Enumeration - Information Loss		6.70
95325	Low	Warning			ICMP Timestamp Request		0.00
6529	Medium	Low		137	Information Leak - Computer Names are Visible		0.00
4346	High	Medium		445	Veritas - Backup Exec - Information-Disclosure Vulnerability		3.70
95002	Urgent	High		445	Files are Accessible From the Network		7.50
57157	Urgent	High		445	2009-3103 - MS09-050 - Microsoft - Windows - Denial of Service Issue		8.30
156	Urgent	High		445	MS Windows 2000, Admin Access w/o Password before Installation Reb...		10.00
109322	High	High		445	1999-0504 - Microsoft - Windows NT - Unspecified Issue		7.50
99623	Critical	High		445	IBM - OEM Microsoft Windows XP And Windows XP SP1 - Default Admi...		8.70
109323	High	High		445	1999-0505 - Microsoft - Windows NT - Unspecified Issue		7.10

© Copyright IBM Corporation 2015

Vulnerabilities

Following are the Severity levels:

- Low
- Medium
- High
- Critical
- Urgent

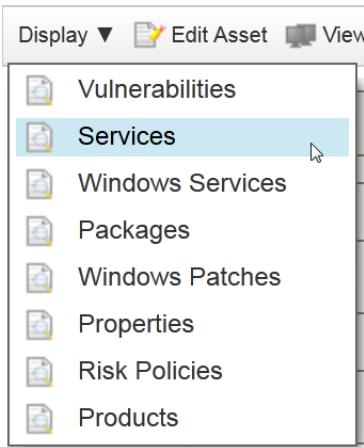


Hint: Refer to the PCI Security Standards Council (<https://www.pcisecuritystandards.org>) for more information about PCI severity levels.

Following are the Risk levels:

- Warning
- Low
- Medium
- High

Services



- By default, the asset details display the vulnerabilities of the asset
- In the **Display** menu, click **Services** to investigate the known services of the asset

Last Seen Passive:
Services detected in passively gathered network flows

Last Seen Active:
Services detected actively by scanners

▼ Services								
Service	Product	Port	Proto	Last Seen Passive	Last Seen Active	Service Default Ports	Vulnerabilities	
NetBIOS-IP		137	udp	2013-07-25 14:07:51.0		137	0	
NETBIOS	Samba Samba 3.6.3	Multiple (2)	tcp		2013-07-25 20:53:45.771	137,138,139	5	
UPnP		49152	tcp		2013-07-25 20:44:24.997	1900,5000	0	
SSH	OpenSSH OpenSSH...	22	tcp		2013-07-25 20:52:55.535	22	0	
Misc	Apache Software F...	80	tcp	2013-07-25 21:03:26.891	2013-07-25 20:59:57.114		3	

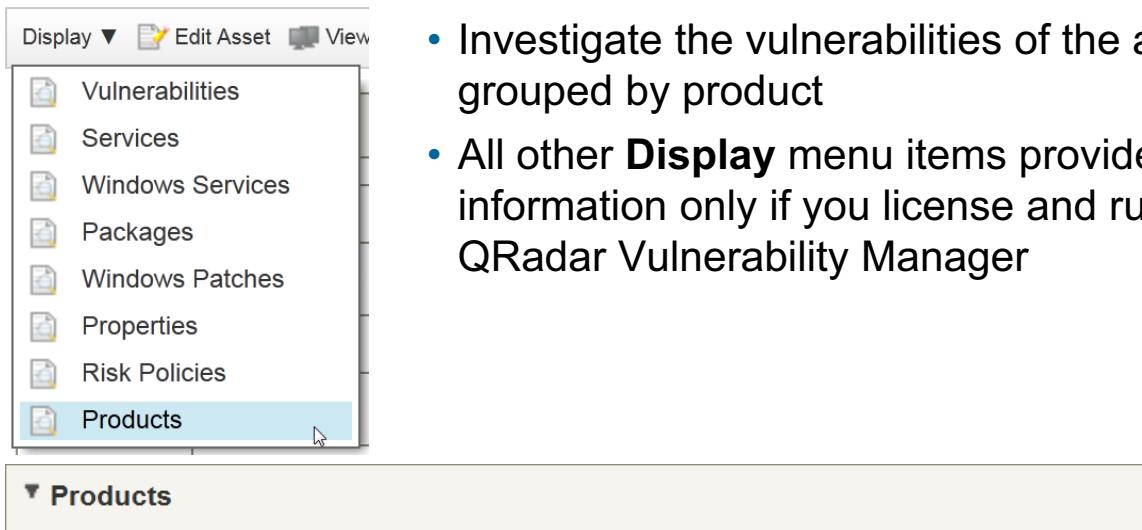
© Copyright IBM Corporation 2015

Services



Note: The vulnerabilities count is always 0 for open ports with unknown services.

Products



The screenshot shows a software interface with a top navigation bar containing 'Display ▾', 'Edit Asset', and 'View'. A vertical sidebar on the left lists several categories: 'Vulnerabilities', 'Services', 'Windows Services', 'Packages', 'Windows Patches', 'Properties', 'Risk Policies', and 'Products'. The 'Products' item is highlighted with a blue selection bar at the bottom. Below this, a main content area has a title 'Products' with a downward arrow icon. A table follows, displaying information about various products:

Product	Port	Vulnerability	Vulnerability ID
UNIX			
Samba Samba 3.6.3	445	Multiple (4)	Multiple (4)
OpenSSH OpenSSH 28.0.150	22		
Apache Software Foundation Apache 2.2...	80	Multiple (3)	Multiple (3)

© Copyright IBM Corporation 2015

Products

Summary

Now you should be able to perform the following tasks:

- Describe the purpose of an asset profile
- Investigate asset profile details

© Copyright IBM Corporation 2015

Summary



7 Investigating an offense that is triggered by flows



Investigating an offense that is triggered by flows



© Copyright IBM Corporation 2015
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

QRadar SIEM correlates flows into an offense if it determines suspicious activities in network communications. This unit teaches you how to investigate the flows that contribute to an offense. You also learn how to create and tune false positives and investigate superflows.

References:

- *QRadar SIEM Administration Guide* <http://ibm.co/1wvpSEE>
- *QRadar SIEM Application Configuration Guide* <http://ibm.co/1wvpSEE>

Objectives

In this unit, you learn to perform the following tasks:

- 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

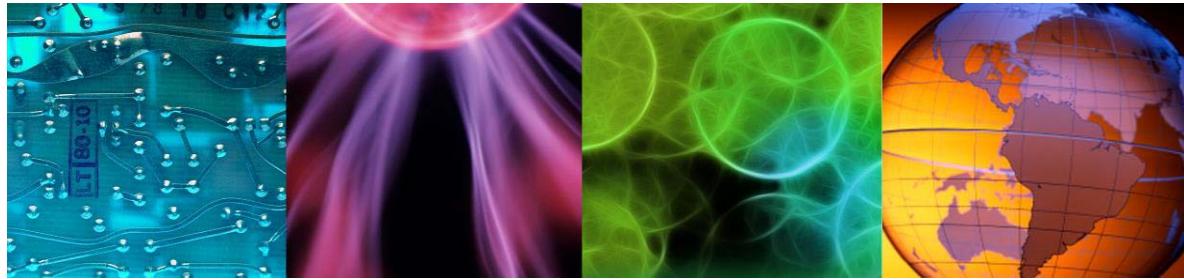
© Copyright IBM Corporation 2015

Objectives

Lesson 1 Viewing and grouping flows



Lesson: Viewing and grouping flows



© Copyright IBM Corporation 2015

A flow provides information about a network conversation between two systems. In this lesson, you learn how to use the **Network Activity** tab to view and group flows.

Reference: QRadar SIEM Application Configuration Guide <http://ibm.co/1wvpSEE>

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

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

© Copyright IBM Corporation 2015

Network Activity tab

The following information pertains to the Source Bytes and Destination Bytes columns:

- The **(C)** behind the number of bytes indicates that the flow contains captured layer 7 payload.
- The number of captured bytes is not displayed. By default, QRadar SIEM captures 64 bytes in each direction.
- The number of bytes in the Source Bytes and Destination Bytes columns indicates how many bytes the source and destination sent.

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	Source IP (Unique Count)	Source IP (Unique Count)
other	Multiple (18)	Multiple (16)
Multimedia.Intellex	10.20.0.80	Net_10_0_0_0
FileTransfer.NETBIOS	192.168.10.1	Net_192_168_1_0
Web.SecureWeb	Multiple (2)	Net_10_0_0_0
P2P.BitTorrent	10.20.0.80	Net_10_0_0_0
InnerSystem.Flowgen	10.20.0.80	Net_10_0_0_0
Web.Misc	Multiple (3)	Net_10_0_0_0
Misc.domain	Multiple (23)	Multiple (2)
DataTransfer.WindowsFileSharing	Multiple (3)	Multiple (3)
VoIP.Skype	10.10.0.80	Net_10_0_0_0
RemoteAccess.MSTerminalServ...	10.10.0.80	Net_10_0_0_0

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

© Copyright IBM Corporation 2015

Grouping flows

The following information describes some of the **Display** options available for flow grouping:

- **Display > Default (Normalized):** To remove a grouping, select **Default (Normalized)**.
- **Display > Unioned Flows:** QRadar SIEM works in 1-minute cycles. When the minute is over, the event processors send the events and flows they processed to the console (only if they are needed on the console). Therefore, QRadar SIEM cuts off flows even if the real network flows have not actually terminated. QRadar SIEM creates a new flow record during the next 1-minute cycle for such a flow. To merge these flow-slices into one flow representing the real network flow, group by **Unioned Flows**. Otherwise, one real network flow can be represented by more than one flow in QRadar SIEM.
- **Display > Application:** QRadar SIEM detects the kind of application data transported in flows. QFlow detects applications by performing traffic analysis on network packets. If you do not use QFlow, QRadar SIEM determines the type of application from the destination port.

Refer to the *QRadar SIEM Application Configuration Guide* (<http://ibm.co/1wvpSEE>) for further information.

- **Display > Geographic:** To summarize flows by the geographic country/region of their destination IP addresses, group by **Geographic**.
- **Display > Flow Bias:** To summarize flows by the flow direction, group by **Flow Bias**.

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
█ (red)	8/8/13 10:38:41 AM	10.20.0.80	58467	93.158.65.201	80	tcp_ip
█ (white)	8/8/13 10:38:34 AM	59.95.169.29	N/A	10.20.0.80	N/A	icmp_ip
█ (red)	8/8/13 10:38:40 AM	10.20.0.80	51898	190.58.212.103	28454	tcp_ip
█ (white)	8/8/13 10:38:24 AM	10.20.0.80	51907	59.95.169.29	21668	tcp_ip
█ (red)	8/8/13 10:38:40 AM	10.20.0.80	56196	208.67.222.222	53	udp_ip
█ (red)	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

In addition to the **Dashboard** and **Offenses** tabs, you find offenses on the **Network Activity** and **Log Activity** tabs.

Lesson 2 Using summary information to investigate an offense



Lesson: Using summary information to investigate an offense



© Copyright IBM Corporation 2015

An offense bundles information about a suspicious activity, including flows. In this lesson, you learn how to use offense summary information related to flows to begin your offense investigation.

References:

- QRadar SIEM Administration Guide <http://ibm.co/1wvpSEE>
- QRadar SIEM Application Configuration Guide <http://ibm.co/1wvpSEE>

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						
Magnitude	■■■	Status	Relevance	3	Severity	4
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			

© Copyright IBM Corporation 2015

Offense parameters



Note: Description: *Misc.domain* refers to domain name resolution traffic. Refer to the *QRadar SIEM Application Configuration Guide* (<http://ibm.co/1wvpSEE>) for further information.

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

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

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	<u>3</u>	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

In the example on the slide, no events created from log messages contribute to the offense.

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



Hint: Refer to the QRadar SIEM Administration Guide (<http://ibm.co/1wvpSEE>) for a list of high-level categories (HLC) and low-level categories (LLC).

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...	

© 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							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 att. "CRE_Event" CRE Rule description: [Potential Botnet Activity] Detected a host connecting or attempting to connect 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...	6
"CRE Event". CRE Rule description: [Potential Botnet Activity] Detected a host connecting or attempting to connect 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...	6

© Copyright IBM Corporation 2015

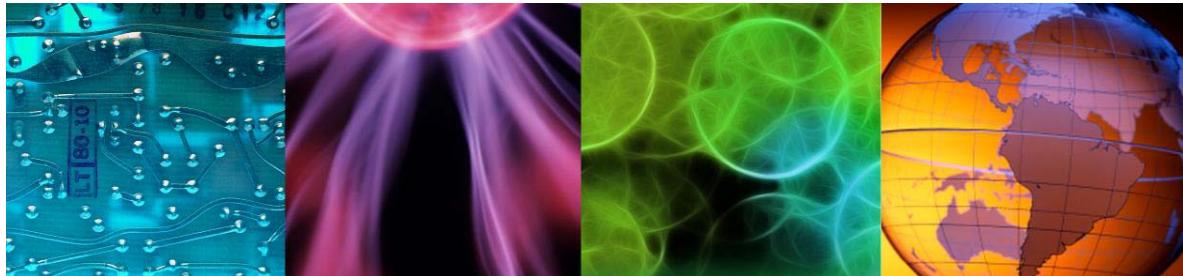
Annotations

QRadar SIEM rules and building blocks add annotations when they create or update an offense. QRadar SIEM users cannot add, edit, or delete annotations.

Lesson 3 Navigating flow details



Lesson: Navigating flow details



© Copyright IBM Corporation 2015

A flow in QRadar SIEM provides much information about the network conversation it represents. In this lesson, you learn how to navigate the details of a flow, such as base, source, and destination information, and layer 7 payload.

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)	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

In the example on the slide, the Event Description, **Application detected with state based decoding**, means that the state-based decoder QRadar SIEM uses determined the application of this flow.

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><input type="checkbox"/> Wrap Text</p> <pre>GET /torrent/CentOS-6.0-i386-bin-DVD/3184478934b9ab6edfc40a9b811</pre>	<p>utf hex base64</p> <p><input type="checkbox"/> 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

A content capture length greater than 1024 bytes negatively impacts the performance of QRadar SIEM.

Additional information

Additional Information					
Flow Type:	Standard Flow	Flow Source/Interface:	COE:eth0		
Flow Direction:	L2R				
Custom Rules: Rules fired for this flow	<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: A threshold value of these rules was not met; otherwise, the rule matched	<u>System: Flow Source Stopped Sending Flows</u>				
Annotations: Added by rules	<p>Relevance has been decreased by 2 because the destination network weight is low.</p> <p>Relevance has been increased by 5 because the context is Local to Remote.</p>				

© Copyright IBM Corporation 2015

Additional information

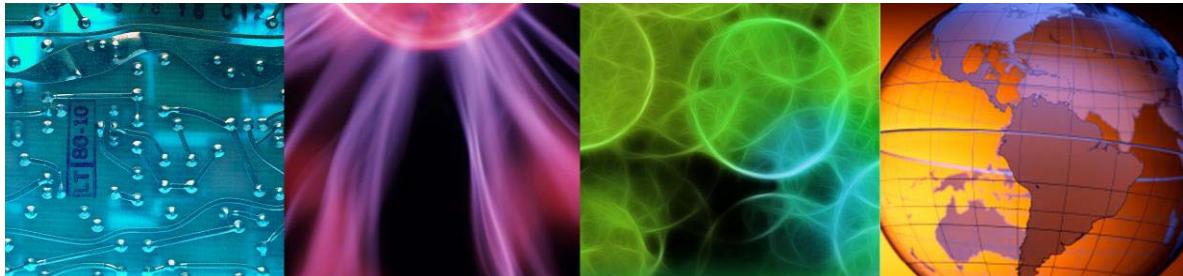
The **Flow Direction** field can include the following values:

- **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

Lesson 4 False positives overview



Lesson: False positives overview



© Copyright IBM Corporation 2015

Each organization has legitimate network traffic that can trigger false positive flows and events. This traffic creates noise that makes it difficult to identify true security incidents. In this lesson, you learn how to tune a flow or event as false positive.

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

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



False Positive

False positive tuning allows you to prevent specific 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

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

Creating a false positive flow or event

The example on the slide removes any event and flow that includes the specified QID and targets the 93.158.65.201 IP address without regard for the origin.

For events, the QID uniquely identifies a specific action of a device. For example, firewall denies issued from different firewall models have different QIDs. For flows, the QID uniquely identifies which kind of application data is transported by the flow.

To edit a false positive, edit the **User-BB-FalsePositive: User Defined False Positives Tunings** building block. To locate this building block, navigate to **Rules** on the **Offenses** tab.

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

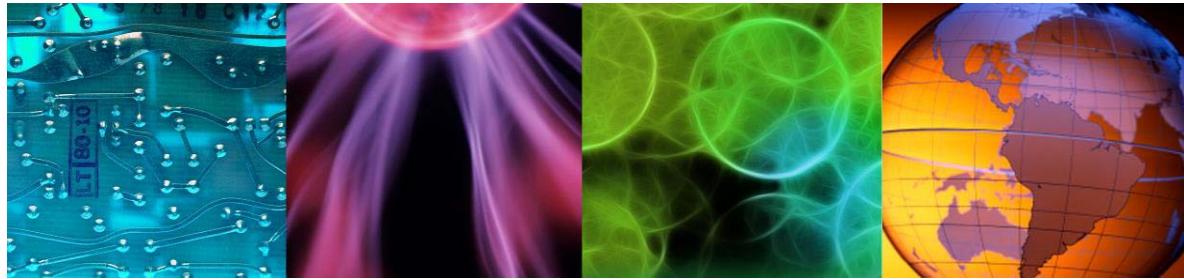
QRadar SIEM considers all networks in the network hierarchy local. You find the network hierarchy on the **Administration** tab.

By default, QRadar SIEM has many rules disabled. In a production environment, it can be necessary to enable some rules. In most deployments, a professional services consultant performs initial tuning for a new QRadar SIEM deployment.

Lesson 5 Investigating superflows



Lesson: Investigating superflows



© Copyright IBM Corporation 2015

A superflow is a flow that is an aggregate of a number of flows that have a similar set of elements. In this lesson, you learn how to find the information stored in a superflow.

Reference: QRadar SIEM Administration Guide <http://ibm.co/1wvpSEE>

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	Protocol	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

Following are some of the benefits of superflows:

- Reduced traffic from QFlow collectors
- Store only a single flow to disk

QRadar SIEM administrators can enable or disable the creation of superflows in the QFlow configuration.

Refer to the *QRadar SIEM Administration Guide* (<http://ibm.co/1wvpSEE>) for the criteria flows must meet so that QRadar SIEM can aggregate them into 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	
20 Source(s): 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	Destination IP: 24.10.10.200:53

© Copyright IBM Corporation 2015

Superflow source and destination information

Superflow additional information

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



Student exercises

Use the procedures in the *Student Exercises Guide* to investigate an offense that is triggered by flows



© Copyright IBM Corporation 2015

Student exercises

Perform the exercises for this unit.

Summary

Now you should be able to perform the following tasks:

- 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

© Copyright IBM Corporation 2015

Summary



8 Using rules and building blocks



Using rules and building blocks



© Copyright IBM Corporation 2015

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Rules perform tests on the events, flows, and offenses in QRadar SIEM and respond if the test criteria is met. A building block is a rule without a response that is used as a common variable in multiple rules or to build complex rules. This unit teaches you how to find custom rules in the QRadar SIEM console and how to assign actions and responses to the rule. You also learn how to configure rules.

References:

- *QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>
- *QRadar SIEM Administration Guide* <http://ibm.co/1wvpSEE>



Objectives

In this unit, you learn to perform the following tasks:

- Describe rules and building blocks
- Locate the rules that fired for events, flows, and offenses
- Use the Rule Wizard to examine a rule action and response

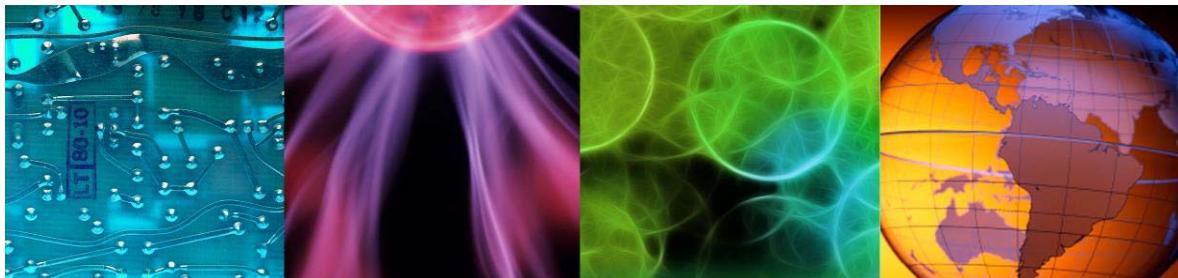
© Copyright IBM Corporation 2015

Objectives

Lesson 1 Rules and build blocks overview



Lesson: Rules and building blocks overview



© Copyright IBM Corporation 2015

Rules perform tests on events, flows, and offenses and respond if the test criteria is met. A building block is a rule without a response and can be used as a variable in multiple rules. In this lesson, you learn about rules and building blocks.

About rules and building blocks

- Rules and building blocks are a collection of tests
- Rules and building blocks test incoming events, flows, and offenses such as the following examples
 - Events
Example: when the user name matches the following regex ...
 - Flows
Example: when the destination TCP flags are exactly these flags ...
 - Offenses
Example: when the number of categories involved in the offense is greater than ...

© Copyright IBM Corporation 2015

About rules and building blocks

About rules

- If the tests of a rule match, the rule generates the configured actions and responses, such as these examples
 - Creating an offense
 - Adding an annotation
 - Sending an email
 - Generating system notifications shown on the dashboard
- Rules on offenses do not create new events or offenses; they perform only these tasks
 - Send notifications
 - Annotate the triggering offense
 - Name the triggering offense
- The Custom Rule Engine (CRE) performs all tests, actions, and responses specified in rules

© Copyright IBM Corporation 2015

About rules

About building blocks and functions

- A building block is a collection of tests without actions and responses
- Building blocks group commonly used tests to build complex logic that enables the building block to be reused in rules
- Building blocks often test for IP addresses, privileged user names, or collections of event names; for example, if a building block includes the IP addresses of all DNS servers, rules can then use this building block
- The CRE evaluates a building block only if a rule test uses it
- Functions allow rule tests with building blocks, for example:
when an event matches any|all of the following
BB:HostDefinition: DNS Servers

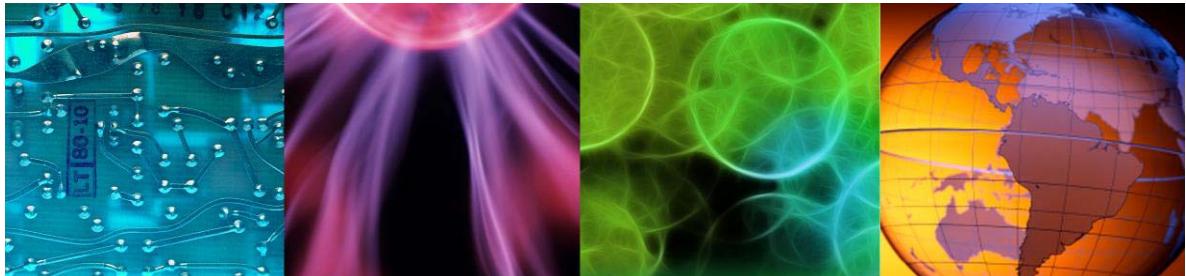
© Copyright IBM Corporation 2015

About building blocks and functions

Lesson 2 Locating rules



Lesson: Locating rules



© Copyright IBM Corporation 2015

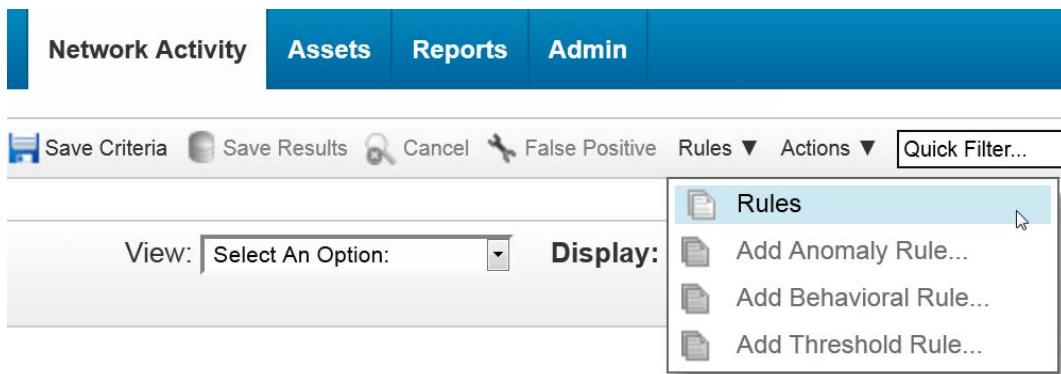
QRadar SIEM offers various options to navigate and list rules. In this lesson, you learn how to locate rules in general and find specific rules that fired for an event, flow, and offense.

References:

- QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>
- QRadar SIEM Administration Guide <http://ibm.co/1wvpSEE>

Navigating to rules

Select **Rules** by clicking either the **Log Activity** tab or **Network Activity** tab



© Copyright IBM Corporation 2015

Navigating to rules

The **Rules** list opens in a separate window.

This unit addresses only **custom rules**. They test the incoming events, flows, and offenses. QRadar SIEM includes four custom rule types:

1. Event rules that test only events
2. Flow rules that test only flows
3. Common rule that tests events and flows
4. Offense rule that tests only offenses

In addition, QRadar SIEM includes three **anomaly detection** rule types:

1. Anomaly detection rules that test the results of saved flow or event searches to detect when unusual traffic patterns occur in your network
2. Behavioral rules that test event and flow traffic according to seasonal traffic levels and trends
3. Threshold rules that test event and flow traffic for activity less than, equal to, or greater than a configured threshold or within a specified range



Hint: Refer to the *QRadar SIEM Users Guide* (<http://ibm.co/1wvpSEE>) for more information about anomaly detection rules.

Navigating to rules (continued)

Select **Rules** in the **Display** list on the **Offenses** tab to navigate to all rules and building blocks

Rule Name	Group	Rule Categ...	Rule Type	Enabled	Response ▾
System: Notification	System	Custom Rule	EVENT	true	Notification
Default-Response-Syslog: Of...	Respo...	Custom Rule	OFFENSE	false	Log
Default-Response-E-mail: Of...	Respo...	Custom Rule	OFFENSE	false	Email
System: Flow Source Stoppe...	System	Custom Rule	FLOW	true	Dispatch New Event
Anomaly: Long Duration Flo...	Anomaly	Custom Rule	FLOW	false	Dispatch New Event
Anomaly: Long Duration ICM...	Anomaly	Custom Rule	FLOW	false	Dispatch New Event
Anomaly: Remote Inbound C...	Anomaly	Custom Rule	FLOW	false	Dispatch New Event
DDoS: Potential DDoS Again...	D\\DoS	Custom Rule	FLOW	false	Dispatch New Event
DDoS: Potential DDoS Again...	D\\DoS	Custom Rule	FLOW	false	Dispatch New Event
DDoS: Potential DDoS Again...	D\\DoS	Custom Rule	FLOW	true	Dispatch New Event
DDoS: Potential DDoS Again...	D\\DoS	Custom Rule	FLOW	false	Dispatch New Event

© Copyright IBM Corporation 2015

Navigating to rules (continued)

You can click the column headers to sort rules.



Hint: Refer to the *QRadar SIEM Administration Guide* (<http://ibm.co/1wvpSEE>) for a list of all rules and more information about managing rules.

Finding the rules that fired for an event or flow

QRadar SIEM shows the rules and building blocks that fired for an event or flow on its details page

This rule added the first annotation below

This rule created the offense this flow contributes to

The rules listed above added the annotations

Additional Information					
Flow Type:	Standard Flow	Flow Source/Interface:	COE:eth0		
Flow Direction:	L2R	BB means building block			
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

Finding the rules that fired for an event or flow

In the example on the slide, **Botnet: Potential Botnet Connection (DNS)** created the offense. The other rules (Magnitude Adjustment) adjusted only the magnitude, and building blocks do not trigger offenses.

Finding the rules that triggered an offense

Select **Rules** in the **Display** menu of the Offense Summary to navigate to the rules that triggered the offense

The screenshot shows the QRadar SIEM interface. At the top, there's a navigation bar with 'Summary', 'Display ▾', 'Events', 'Flows', 'Actions ▾', 'Print', and a help icon. Below the navigation bar is an 'Offense 1' summary card. The card includes fields for 'Magnitude' (yellow), 'Description' (Potential Botnet Activity containing Misc.domain), 'Source IP(s)' (10.20.0.80), 'Destination IP(s)' (192.168.1.2 Remote (81)), and 'Network(s)' (Multiple (2)). To the right of the card is a small table showing 'Severity' (3), 'Credibility' (4), and a value of 2. A context menu is open over the offense card, listing options like 'Notes', 'Sources', 'Destinations', 'Log Sources', 'Users', 'Categories', 'Annotations', 'Networks', and 'Rules'. The 'Rules' option is highlighted with a blue background. A callout bubble points to the 'Rules' option with the text: 'To navigate to the rule details, double-click the row'. Below the summary card is a section titled 'List of Rules Contributing to Offense' with a table. The table has columns for a magnifying glass icon, 'Rule Name', 'Events/Flows', 'First Event/Flow', and 'Last Event/Flow'. One row is shown: 'Botnet: Potential Botnet Connection (DNS)' with 205 events/flows, first event at 24m 13s, and last event at 23m 21s.

	Rule Name	Events/Flows	First Event/Flow	Last Event/Flow
	Botnet: Potential Botnet Connection (DNS)	205	24m 13s	23m 21s

Finding the rules that triggered an offense

Using the navigation path on the slide, QRadar SIEM displays only rules and does not display the building blocks. To view and manage rules, the user must have the **View Custom Rules** or **Maintain Custom Rules** role permissions.

Lesson 3 Using rule definitions during an investigation



Lesson: Using rule definitions during an investigation



© Copyright IBM Corporation 2015

As part of an offense investigation, you might need to find out in detail why rules triggered an offense. The Rule Wizard allows you to view and modify tests, actions, and responses of rules. In this lesson, you learn how to examine a rule in the Rule Wizard.

Reference: QRadar SIEM Administration Guide <http://ibm.co/1wvpSEE>

Rule Wizard demonstration



© Copyright IBM Corporation 2015

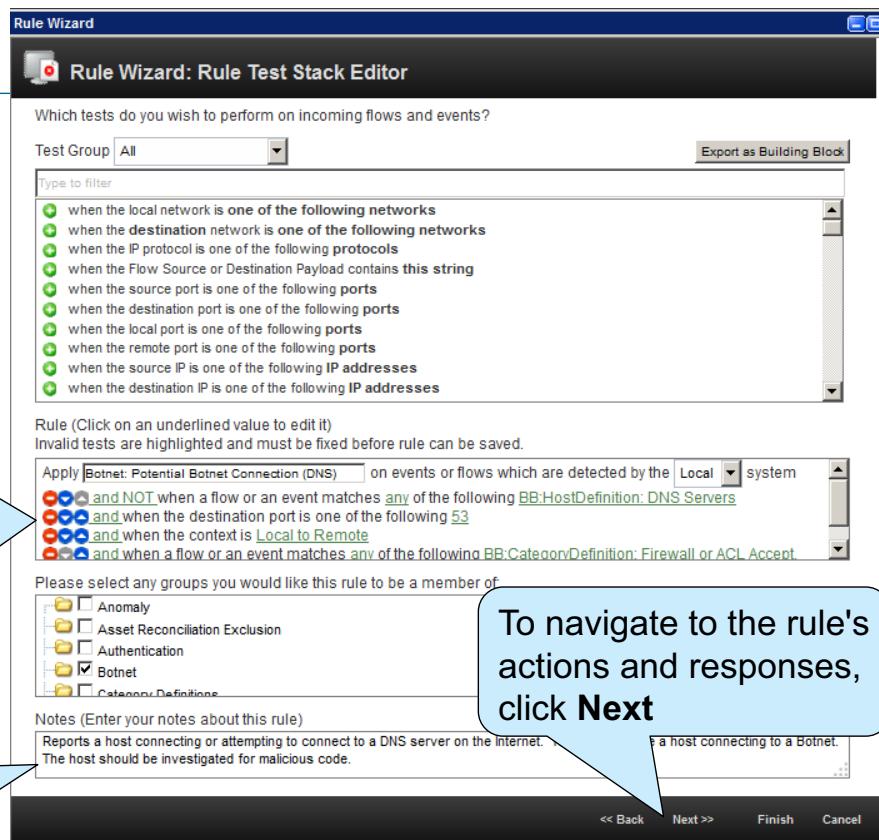
Rule Wizard demonstration

Rule Wizard

To find out in detail why a rule fired, investigate the rule

Learn from the rule's tests that it detects flows contacting remote DNS servers

Learn about the rule's purpose and tests



© Copyright IBM Corporation 2015

Rule Wizard

If you have the **Maintain Custom Rules** permission, QRadar SIEM opens the Rule Test Stack Editor to edit the rule as displayed on the slide. If you have the **View Custom Rules** permission, but not the **Maintain Custom Rules** permission, QRadar SIEM displays the rule summary as read only.

To add or remove a test:

- Click the green + to add the test.
- Click the red – to remove the test.



Hint: Refer to the *QRadar SIEM Administration Guide* (<http://ibm.co/1wvpSEE>) for more information about developing rules.

Rule actions

When a rule fires, QRadar SIEM executes its actions

The screenshot shows the 'Rule Wizard' interface with the title 'Rule Wizard - Rule Response'. Under the heading 'Rule Action', it says 'Choose the action(s) to take when an event or flow occurs that triggers this rule'. There are several options with checkboxes:

- Severity (Set to 0)
- Credibility (Set to 0)
- Relevance (Set to 0)
- Ensure the detected flow is part of an offense (Index offense based on Source IP, Annotate this offense: [])
- Include detected flows by Source IP from the point forward, for 300 second(s), in the offense

Three callout boxes highlight specific actions:

- A blue callout box points to the 'Ensure the detected flow is part of an offense' checkbox with the text 'The rule triggers an offense if it does not already exist'.
- A blue callout box points to the 'Include detected flows by Source IP from the point forward, for 300 second(s), in the offense' checkbox with the text 'A rule can change the magnitude of the event or flow'.
- A blue callout box points to the 'Index offense based on Source IP' dropdown with the text 'The rule specifies the offense type'.

© Copyright IBM Corporation 2015

Rule actions

The rule can also annotate the offense or flow.

Some of the rules that come with QRadar SIEM do not have defined actions and responses. QRadar SIEM still tags the event or flow as meeting the test criteria specified in the rule. This information can be used later in searches, reports, and other rules. Following are some examples of how this information could be used:

- Anomaly: Single IP with Multiple MAC Addresses
- Policy: Host has SANS Top 20 Vulnerability
- Recon: Single Merged Recon Events Remote Scanner
- System: Host Based Failures
- System: Critical System Events

Rule response

Again, the rule triggers an offense if it does not already exist

Rule Wizard

Rule Response
Choose the response(s) to make when an event or flow triggers this rule

Dispatch New Event
Enter the details of the event to dispatch

Event Name Potential Botnet Activity

Event Description Detected a host connecting or attempting to connect to a DNS server on the Internet. This may indicate a host connecting to a Botnet. The host should be investigated for malicious code.

Event Details

Severity 8 Credibility 5 Relevance 6

High-Level Category Malware Low-Level Category Misc Malware

Annotate this offense:

Ensure the dispatched event is part of an offense
Index offense based on Source IP

Include detected flows by Source IP from this point forward, for 300 second(s), in the offense

Offense Naming

This information should contribute to the name of the associated offense(s)
 This information should set or replace the name of the associated offense(s)
 This information should not contribute to the naming of the associated offense(s)

Email
 Send to Local SysLog
 Send to Forwarding Destinations
 Notify
 Add to a Reference Set
 Add to Reference Data

© Copyright IBM Corporation 2015

To alert, the rule makes the CRE create a new event

Rule response

The Custom Rule Engine (CRE) is the log source of the new event because the CRE creates all events that are triggered by rules.

Student exercises

Use the procedures in the *Student Exercises Guide* to perform the following tasks

- Create an event rule
- Analyze the rule that contributed to the Local DNS Scanner offense
- Work with rule parameters
- Delete changes made to a rule
- Search for a rule



© Copyright IBM Corporation 2015

Student exercises

Perform the exercises for this unit.

Summary

Now you should be able to perform the following tasks:

- Describe the rules and building blocks
- Locate the rules that fired for events, flows, and offenses
- Use the Rule Wizard to examine a rule action and response

© Copyright IBM Corporation 2015

Summary



9 Creating QRadar SIEM reports



Creating QRadar SIEM reports



© Copyright IBM Corporation 2015
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Reports allow you to examine trends and statistical views on your network for various purposes, in particular to meet compliance requirements. This unit teaches you how to generate a report using a predefined template and create a report template.

Reference: *QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>

Objectives

In this unit, you learn to perform the following tasks:

- Navigate and use the **Reports** tab
- Generate and view a report
- Use the Report Wizard to create a custom report template

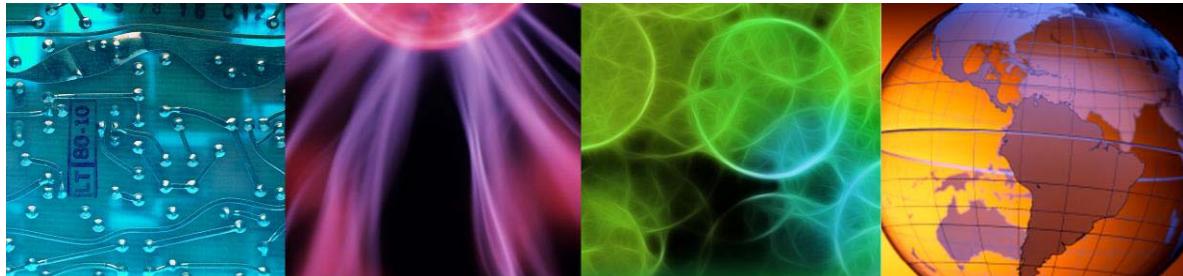
© Copyright IBM Corporation 2015

Objectives

Lesson 1 Navigating the Reports tab



Lesson: Navigating the Reports tab



© Copyright IBM Corporation 2015

QRadar SIEM provides over one thousand templates you can use to generate reports. In this lesson, you learn how to access the report templates and generate a report.

Reference: QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>

Reporting introduction

- A QRadar SIEM report is a means of scheduling and automating one or more *saved searches*
- QRadar SIEM reports perform the following tasks
 - Present measurements and statistics derived from events, flows, and offenses
 - Provide users the ability to create custom reports
 - Can brand reports and distribute them
- Predefined report templates serve a multitude of purposes, such as the following examples
 - Regulatory compliance
 - Authentication activity
 - Operational status
 - Network status
 - Executive summaries

© Copyright IBM Corporation 2015

Reporting introduction

QRadar SIEM supports the following regulatory schemas:

- **HIPAA:** Health Insurance Portability and Accountability Act
- **COBIT:** Control Objectives for Information and Related Technology
- **SOX:** Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act
- **PCI:** Visa Payment Card Industry Data Security Standard
- **GLBA:** Gramm-Leach-Bliley Privacy Act
- **FISMA:** Federal Information Security Management Act
- **NERC:** The North American Electric Reliability Council
- **GSX:** Government Secure Extranet

Reporting demonstration



© Copyright IBM Corporation 2015

Reporting demonstration

Reports tab

You can search and sort report templates in a similar way as events and flows

	Report Name ▾	Group	Schedule	Next Run Time
	Weekly User Authentication Activity	Authentication, Identity and User Activity...	Weekly	4 days 11 hours 53
	Weekly PCI Compliance Failures	Vulnerability Management	Manual	Manual
	Weekly Firewall Deny Activity	Network Management, Security, Usage ...	Weekly	4 days 11 hours 53
	Weekly Firewall Allow Activity	Network Management, Security, Usage ...	Weekly	4 days 11 hours 53
	Vulnerability Overview	Vulnerability Management	Manual	Manual
	Top IDS/IPS Alerts by Geography...	Security	Weekly	4 days 11 hours 53
	Top IDS/IPS Alerts (Weekly)	Security	Weekly	4 days 11 hours 53
	Top IDS/IPS Alerts (Daily)	Security	Daily	11 hours 53 minute
	Top Applications (Internet)	Network Management	Daily	11 hours 53 minute
	Top Applications (Internet)	Network Management	Weekly	3 days 11 hours 53
	PCI Compliance Failures	Vulnerability Management	Manual	Manual

© Copyright IBM Corporation 2015

Reports tab

Select **Branding** in the left column to upload logos for your reports. Once a logo is uploaded, users can use the log when creating or editing report templates.

Finding a report

QRadar SIEM includes more than 1500 report templates; before you create a new template, check the predefined templates



© Copyright IBM Corporation 2015

Finding a report

Inactive reports: QRadar SIEM does not automatically generate reports for inactive templates.

Active reports: QRadar SIEM generates reports for active templates automatically according to the schedule, unless the schedule is set to manual. QRadar SIEM lists active templates with a manual schedule if the **Hide Inactive Reports** check box is enabled.

Running a report

Run Report:

Run selected report template immediately, regardless of its schedule or active or inactive state

Run Report on Raw Data:

Generate the report on raw data if QRadar SIEM has not captured the required time-series data

Toggle scheduling:

Toggle the active and inactive state of the template

The screenshot shows a list of reports in a table format. The columns include Report Name, Type, and Sub-Type. A context menu is open over the second row, which contains the report 'Daily Firewall Deny Activity'. The menu items are: Create, Edit, Duplicate, Assign Groups, Share, Run Report, Run Report on Raw Data, Toggle Scheduling, Cancel Report Generation, Delete Report, and Delete Generated Content. The 'Run Report' option is highlighted with a blue background and a cursor arrow pointing to it. The menu also includes a 'Run Time' section with 'Active' and 'Inactive' options, and a timestamp '8 hours 14 mi...'. The bottom of the menu has a note: '© Copyright IBM Corporation 2015'.

Report Name	Type	Sub-Type
Daily Firewall Allow Activity	Network Management	
Daily Firewall Deny Activity	Network Management	
Daily Most Active Devices	Log Sources, Security	
Geographic Traffic Distrib...	Network Management	
Large Outbound File Tra...	Network Management	
Monthly Most Active Devi...	Network Management	
Network Traffic Volume	Compliance, Executive	
Network Traffic Volume	Compliance, Executive	
Top Talkers (Weekly)	Network Management	
Top URL Reports	Network Management	

Running a report

The left-most column with the exclamation point includes an error icon when a report fails to generate.

About the Run Report option

Reports scheduled to run daily, weekly, and monthly use accumulated time-series data. When a report is scheduled or created, the time-series data accumulations begins:

- If no accumulated data is available when the report runs, the generated report displays the message that accumulated data is not available.
- Hourly reports use accumulated time-series data if it is available. If accumulated time-series data is not available, an hourly report automatically uses raw data to generate the report.
- Manually scheduled reports use accumulated data if it is available; however, they do not start the time-series data accumulation process.

About the Run Report on Raw Data option

You can choose this option if QRadar SIEM has not accumulated time-series data for your required reporting period. When a report runs on raw data, QRadar SIEM queries the data in its datastore to

generate the report. Running a report on raw data takes a longer time to process than running a report on accumulated time-series data.

Selecting the generated report

Next Run Time	Last Modified	Owner	Author	Generated Reports	Formats
Inactive	Sep ...	admin	admin	None	
Generating (34 sec(s))	Sep ...	admin	admin	None	

Estimated 34 seconds until the report is generated

Next Run Time	Last Modified	Owner	Author	Generated Reports	Formats
Inactive	Sep ...	admin	admin	None	
Inactive	Sep ...	admin	admin	Jul 31, 2013 4:49 PM	

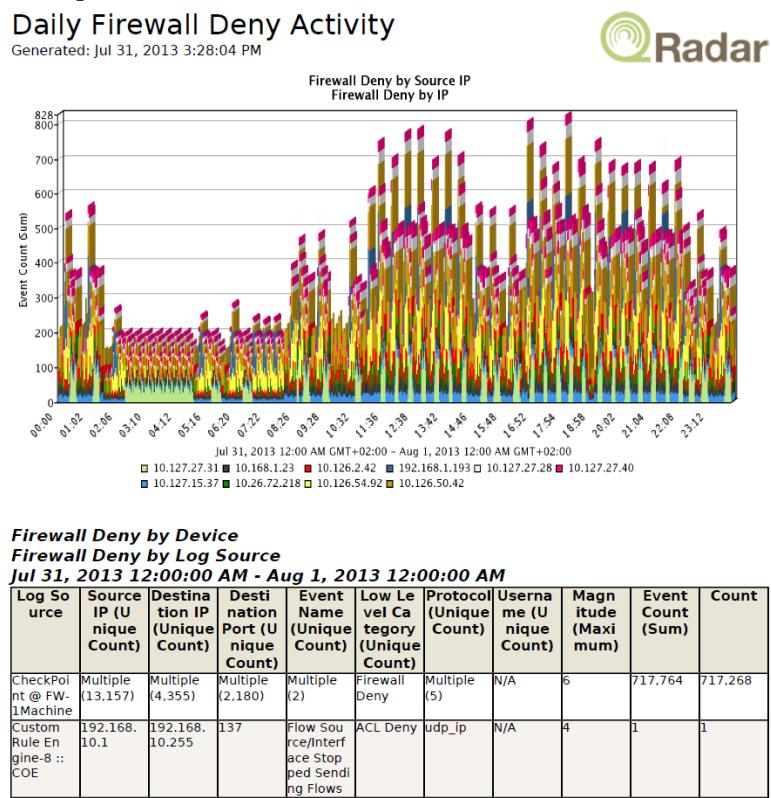
Select a generated report from the list and click the format icon to view it

© Copyright IBM Corporation 2015

Selecting the generated report

QRadar SIEM generates reports one at a time. When you generate a report while another one report is generating, your report displays **Queued** in the Next Run Time column.

Viewing a report



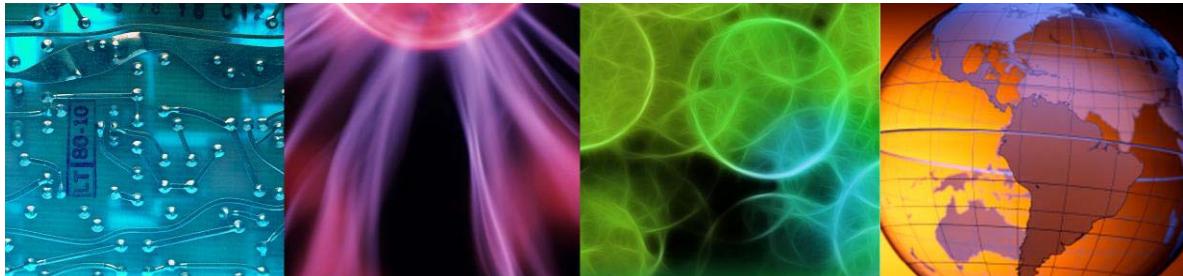
© Copyright IBM Corporation 2015

Viewing a report

Lesson 2 Creating a report template



Lesson: Creating a report template



© Copyright IBM Corporation 2015

If the default QRadar SIEM report templates do not meet your specific needs, you can create and save a customized report template. In this lesson, you learn how to use the Report Wizard to create a new report template and generate the report.

Reference: *QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>

Reporting demonstration

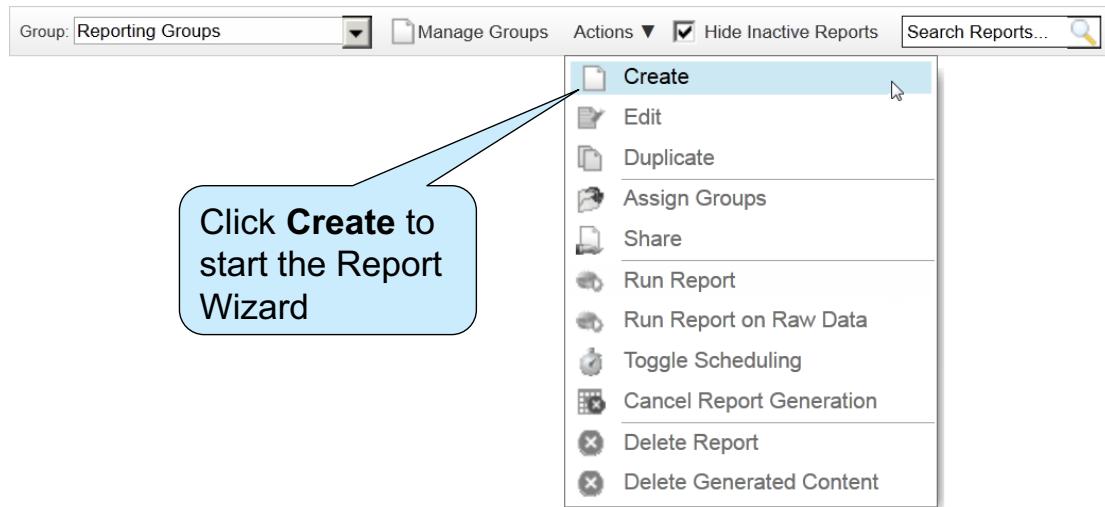


© Copyright IBM Corporation 2015

Reporting demonstration

Creating a new report template

To watch specific firewall activity in a daily report, create a custom report template

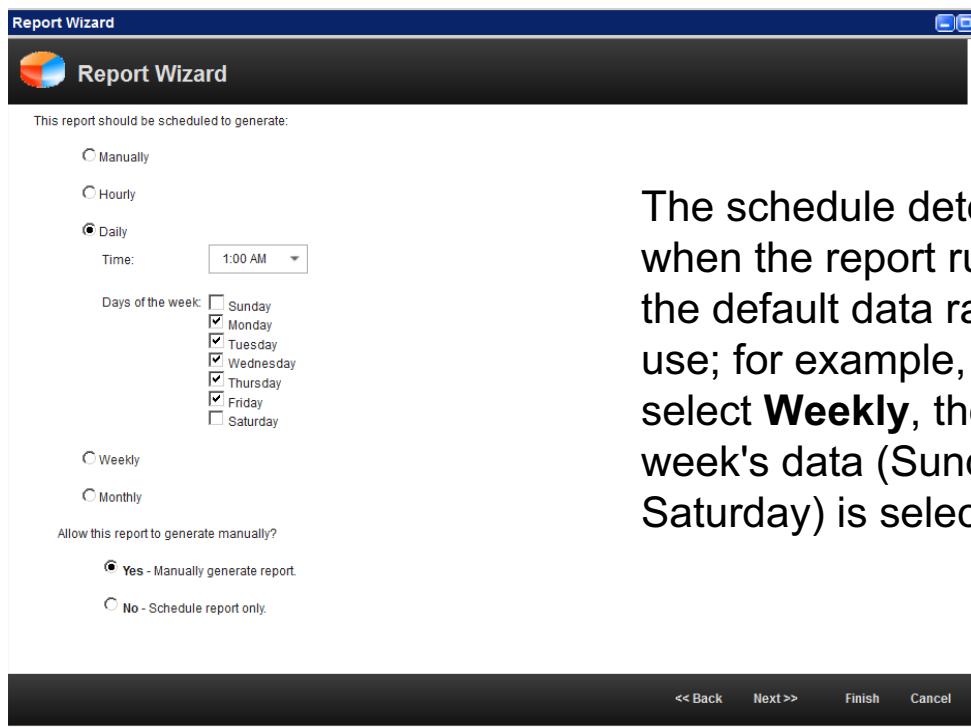


© Copyright IBM Corporation 2015

Creating a new report template

Click **Create** or **Edit** to open the Report Wizard.

Choosing a schedule



The schedule determines when the report runs and the default data range to use; for example, when you select **Weekly**, the previous week's data (Sunday-Saturday) is selected

Choosing a schedule

Use the following options to schedule the report:

- **Manually:** QRadar SIEM generates the report only when a user initiates.
- **Hourly:** Schedules the report to generate at the end of each hour using the data from the previous hour.
- **Daily:** Schedules the report to generate daily using the data from the previous day.
- **Weekly:** Schedules the report to generate weekly using the data from the previous week.
- **Monthly:** Schedules the report to generate monthly using the data from the previous month.

Choosing a layout

QRadar SIEM uses containers to segregate report pages so that different data sets can show on the same report page

Report Wizard

Report Wizard

Choose a Layout

Each divided section holds one chart. Click the layout that represents the size and number of charts required.

Orientation:

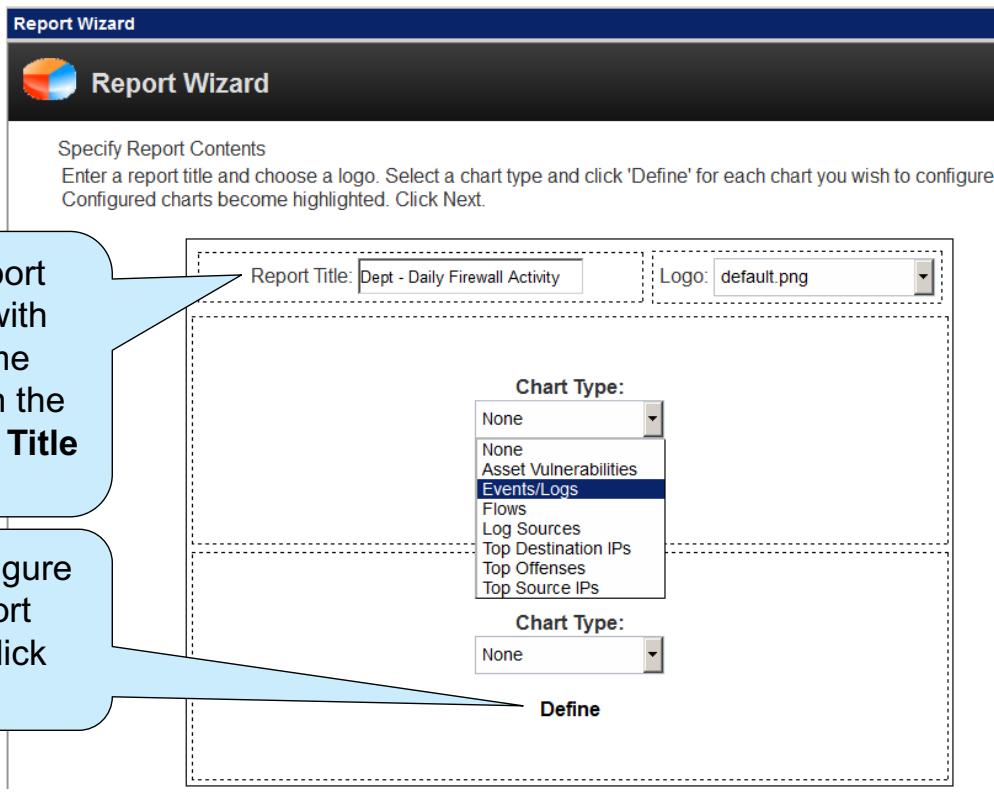
© Copyright IBM Corporation 2015

Choosing a layout



Hint: When you select the layout of a report, consider the type of report you want to create. For example, do not choose a small chart container for graph content that displays a large number of objects. Each graph includes a legend and a list of networks from which the content is derived. Choose a container large enough to hold the data.

Defining report contents



© Copyright IBM Corporation 2015

Defining report contents

On the **Reports** tab under **Branding**, QRadar SIEM administrators can upload logos. All uploaded logos are available from the **Logo** list.

Some of the chart types include the following charts:

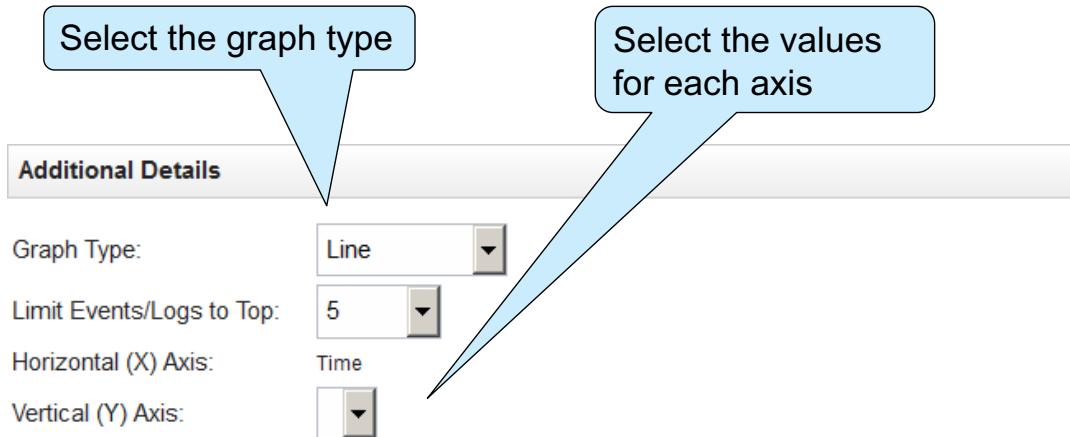
- **Asset Vulnerabilities:** Displays vulnerability data for defined assets in your deployment
- **Top Destination IPs:** Displays the top targeted IP addresses
- **Top Offenses:** Displays the top threat types to the managed network
- **Top Source IPs:** Displays the top IP addresses that attack any defined network or asset

Configuring the upper chart

The screenshot shows the 'Report Wizard' interface for creating a report titled 'Container Details - Events/Logs'. The report displays collected event/log data. The 'Chart Title' is set to 'FW Activity 10.127.15.137 by High Level Category' and the 'Chart Sub-Title' is checked as 'Automatically Specified'. Under 'Hourly Scheduling', the schedule is set to 'All data from previous hour' and the timezone is 'GMT+02:00 Europe/Amsterdam (Central European Summer Time)'. In the 'Graph Content' section, there is a 'Saved Searches' field with a dropdown menu 'Select a group...' and a search bar 'Type Saved Search or Select from List' containing 'Type to filter'. Below this, a list of available saved searches includes 'Default Firewall Gateway', 'Warnings', and 'Dept - 10.127.15.37'. A callout bubble on the left side of the interface contains the text: 'Select the previously saved search to report firewall activity of the suspicious scanning system'.

Configuring the upper chart

Configuring the upper chart (continued)



© Copyright IBM Corporation 2015

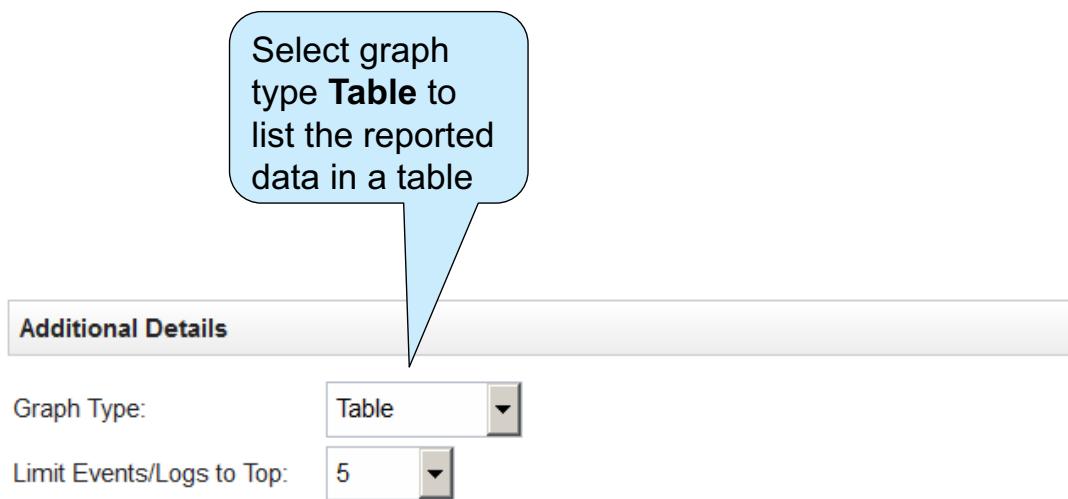
Configuring the upper chart (continued)

Configuring the lower chart

The screenshot shows the 'Report Wizard' interface. A callout box on the left says 'Define a chart for firewall activity'. The main window has sections for 'Container Details - Events/Logs' (described as displaying collected event/log data), 'Chart Title' (set to 'FW Watch'), 'Chart Sub-Title' (checkbox checked for 'Automatically Specified'), 'Hourly Scheduling' (schedule set to 'All data from previous hour', timezone to 'GMT+02:00 Europe/Amsterdam (Central European Summer Time)'), and 'Graph Content'. In the 'Graph Content' section, a callout box says 'Select a predefined search to report the top services and port numbers of traffic through firewalls'. The 'Saved Searches' dropdown is set to 'Select a group...', and the 'Type Saved Search or Select from List' input field contains 'Type to filter'. Below it, a scrollable list of 'Available Saved Searches' includes: Top Services Denied through Firewalls, Top Services/Ports Through Firewalls (which is highlighted in blue), Top Systems Attacked (IDS/IDP/IPS), Top Systems Sourcing Attacks (IDS/IDP/IPS), and Top User by Mail Service Login Failure.

Configuring the lower chart

Configuring the lower chart (continued)



© Copyright IBM Corporation 2015

Configuring the lower chart (continued)

Verifying the layout preview

The screenshot shows the 'Report Wizard' interface with a 'Layout Preview' section. The preview displays a report titled 'Dept - Daily Firewall Activity 10.127.15.37' generated on Aug 1, 2013. It includes a chart titled 'FW Activity 10.127.15.37 by High Level Category' and a table titled 'FW Watch Top Services/Ports Through Firewalls'. A callout bubble points to the preview area with the text: 'The Layout Preview provides only the layout of the report; it does not show the actual data'.

The Layout Preview provides only the layout of the report; it does not show the actual data

Dept - Daily Firewall Activity 10.127.15.37
Generated: Aug 1, 2013

FW Activity 10.127.15.37 by High Level Category
Dept - 10.127.15.37

FW Watch
Top Services/Ports Through Firewalls

© Copyright IBM Corporation 2015

Verifying the layout preview



Note: Reports can take a long time to generate. Therefore, the preview helps you configure the layout correctly before running a potentially large amount of real data for a long time.

Choosing a format

You can select any or all of the available formats for reports

Report Wizard

 Report Wizard

Choose the report format

PDF
An easily printable and transferable document

HTML
Useful displaying reports on the web in your browser

RTF
Report data in Rich Text Format

The following formats are available for single table templates only

XML
Extensible Markup Language

XLS
Excel

© Copyright IBM Corporation 2015

Choosing a format

You will most likely use the PDF format for most of your reports, but you can also generate reports in HTML and RTF format. XML and RTF facilitate further processing and the extraction of report data.

Distributing the report

Report Wizard

Report Wizard

Choose the report distribution channels

Report Console
The latest report will be sent to your report console

Select the users that should be able to view the output generated by this report.

kjell
lynette

Select All Users

Email
Enter the report destination email address(es):
 Include Report as attachment (non-HTML only) Include link to Report Console

© Copyright IBM Corporation 2015

Distributing the report



Note: You can distribute the report to multiple email addresses. Use commas to separate email addresses listed in the **Enter the report destination email address(es)** field.

Adding a description and assigning the group

- You can organize reports by groups much like rules and log sources
- You can use reporting groups to sort report templates by purpose, such as a specific regulatory or executive requirement

Report Wizard

 Report Wizard

Finishing Up
You're almost finished creating your report.

Report Description:
Daily firewall activity, specifically 10.127.15.37

Please select any groups you would like this report to be a member of:

Authentication, Identity and User Activity

Compliance

COBIT

FISMA

GLBA

GPG13

GSX-Memo22

Section D

24

25

© Copyright IBM Corporation 2015

Adding a description and assigning the group

Verifying the report summary

Report Wizard

Report Wizard

Report Summary

Review this report summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.

Note that your report has not yet been saved or scheduled. It will be saved when you select 'Finished' and only be scheduled if you chose to do so on the scheduling screen.

Template Details Container 1 Container 2

Report Title	Dept - Daily Firewall Activity 10.127.15.37
Scheduling	This report will run daily on Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday at 1:00 AM.
Logo	default.png
Formats	PDF
Template Description	Daily firewall activity, specifically 10.127.15.37
Run Now	Yes

Review the report settings

© Copyright IBM Corporation 2015

Verifying the report summary

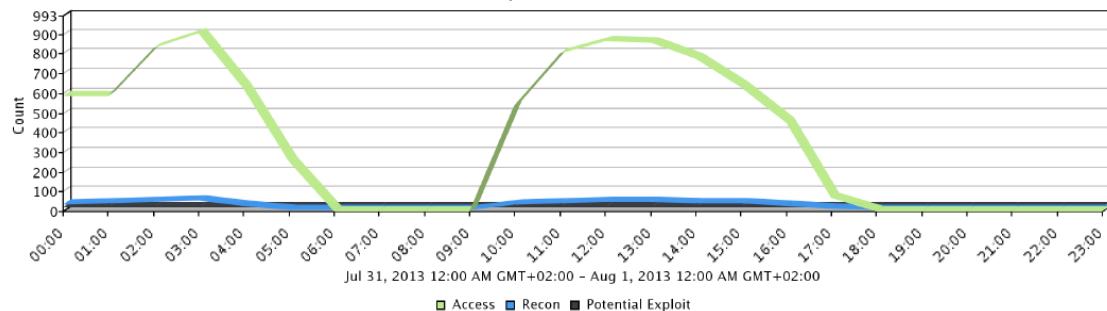
Viewing the generated report

Dept - Daily Firewall Activity 10.127.15.37

Generated: Aug 1, 2013 1:02:44 AM



FW Activity 10.127.15.37 by High Level Category
Dept - 10.127.15.37



FW Watch

Top Services/Ports Through Firewalls

Jul 31, 2013 12:00:00 AM - Aug 1, 2013 12:00:00 AM

Destination Port	Log Source	Event Name	Low Level Category	Source IP	Destination IP	Username	Event Count	Count
443	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (4,961)	Multiple (22)	N/A	409,974	407,503
0	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (4,791)	Multiple (451)	N/A	246,956	246,872
80	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (3,547)	Multiple (74)	N/A	190,056	189,528
25	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (530)	Multiple (5)	N/A	15,115	15,109
161	CheckPoint @ FW-1Machine	Firewall Permit	Firewall Permit	Multiple (4)	Multiple (57)	N/A	9,139	9,139

© Copyright IBM Corporation 2015

Viewing the generated report

The example report on the slide is useful for security analysts who investigate or watch activities. The upper chart displays firewall denies from the local system 10.127.15.37. The lower table displays firewall permits from remote sources to all local systems.

The lower table provides you with an overview of the services and ports used remotely through your firewall. The destination port is 0 for layer 3 protocol traffic such as ICMP. If you were analyzing this report, notice that the lower table displays firewall permits from remote sources to the SNMP port 161. Perhaps this is legitimate traffic from a system management provider to port 161 on some internal systems. As an analyst, this type of information is something to verify.

You can also create or activate reports for regulatory compliance and system performance.

Best practices when creating reports

- For comparison and review, present network traffic charts and event tables together
- Consider the purpose of the report and choose the least number of page containers that is necessary to communicate the data
- Do not choose a small page division for a graph that might contain a large number of objects
- Executive summary reports use one-page or two-page divisions to simplify the report focus

© Copyright IBM Corporation 2015

Best practices when creating reports



Student exercises

Use the procedures in the *Student Exercises Guide* to perform the following tasks

- View an existing report
- Create a new event report
- Create new search and report



© Copyright IBM Corporation 2015

Student exercises

Perform the exercises for this unit.

Summary

Now you should be able to perform the following tasks:

- Navigate and use the **Reports** tab
- Generate and view a report
- Use the Report Wizard to create a custom report template

© Copyright IBM Corporation 2015

Summary



10 Performing advanced filtering



Performing advanced filtering



© Copyright IBM Corporation 2015
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

QRadar SIEM provides several filters that you can apply to identify suspicious or non-standard behavior. Bar, pie, table, and time-series charts visualize security data. This unit teaches you how to use charts and apply advanced filters to examine specific activities in your environment.

Reference: *QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>

This unit has no student exercises.

Objectives

In this unit, you learn to perform the following tasks:

- Apply advanced filters that locate specific events and flows
- Use advanced search capabilities of the Ariel Query Language
- Use time series and other charts to view data

© Copyright IBM Corporation 2015

Objectives

Lesson 1 Filtering scenarios



Lesson: Filtering scenarios



© Copyright IBM Corporation 2015

The events and flows collected by QRadar SIEM provide a great deal of information about the activities in your environment. In this lesson, you learn how to apply advanced filters to look for specific activities.

Reference: *QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>

Filtering demonstration



This demonstration illustrates the scenarios described in this lesson

© Copyright IBM Corporation 2015

Filtering demonstration

Flows to external destinations

- Flows originate in the local network and connect to an external network
- Filters
 - **Source Network is not other**
 - **Destination Network is other**

Current Filters:

Destination Network is other ([Clear Filter](#)), Source Network is not other ([Clear Filter](#))

▶ Current Statistics

(Show Charts)

	Flow Type	First Packet Time ▾	Source IP	Source Port	Destination IP	Destination Port	Protocol
	□	7/31/13 10:25:37 AM	10.20.0.80	51781	🇺🇸 72.14.204.101	80	tcp_ip
	□	7/31/13 10:25:37 AM	10.20.0.80	51953	🇮🇩 94.98.224.26	55778	tcp_ip
	□	7/31/13 10:25:37 AM	10.20.0.80	51952	🇮🇳 112.135.77.198	40507	tcp_ip
	□	7/31/13 10:25:37 AM	10.20.0.80	51951	🇨🇹 190.59.102.214	60213	tcp_ip
	□	7/31/13 10:25:35 AM	10.20.0.80	51950	🇮🇩 202.65.129.229	16450	tcp_ip

© Copyright IBM Corporation 2015

Flows to external destinations



Note: You get the same results by using the **L2R** Flow Direction filter.

Remote to Remote flows

- Flows originate in the local network and connect to an external network
- Filter

Flow Direction is R2R

Current Filters:

Flow Direction is R2R ([Clear Filter](#))

▶ Current Statistics

Flow Type	First Packet Time	Storage Time ▾	Source IP	Source Port	Destination IP	Destination Port
□	7/31/13 10:31:46 AM	7/31/13 10:32:46 AM	0.220.10.10	20686	20.0.80.0	13235
□	7/31/13 10:20:05 AM	7/31/13 10:21:05 AM	74.56.208.10	21501	20.0.80.201	42753

Note: In a properly configured network, you do not see R2R flows

© Copyright IBM Corporation 2015

Remote to Remote flows

Scanning activity

- Filtering rules help locate inappropriate traffic such as scanning activity
- Filter

Custom Rule is any of:

BB:Category Definition: Recon Events, or

BB:Category Definition: Recon Flows, or

BB:Category Definition: Recon Event Categories

Current Filters:										
Custom Rule is any of [BB:CategoryDefinition: Recon Events or BB:CategoryDefinition: Recon Flows or BB:CategoryDefinition: Recon Event Categories] (Clear Filter)										
» Current Statistics										
(Show Charts)										
Destination IP	Source IP (Unique Count)	Source Network (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Application (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)
Multiple Dest.	10.10.10.101	Net_10_0_0_0	80	Net_10_0_0_0	Web.Misc	26,674,240	0	26,674,240	416,785	0

© Copyright IBM Corporation 2015

Scanning activity

Applications not running on the correct port

- Filters can identify applications running on nonstandard ports
- Filters
 - Application is Web
 - Destination Port is not any of 80, 443

Current Filters:

Application is Web ([Clear Filter](#)), Destination Port is not any of [80 or 443] ([Clear Filter](#))

▶ Current Statistics

[\(Show Charts\)](#)

	Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Application
	□	7/31/13 10:21:48 AM	10.20.0.80	64935	87.6.225.217	444	Web.SecureWeb

Note: Use a similar filter to identify nonweb flows, such as botnet traffic, on port 80

© Copyright IBM Corporation 2015

Applications not running on the correct port

Data loss

- Filters can identify large amounts of data leaving the network
- Filters
 - **Flow Direction is L2R**
 - **Source Bytes greater than <threshold>**

Current Filters:

Flow Direction is L2R ([Clear Filter](#)), Source Bytes is greater than 10,000 ([Clear Filter](#))

► **Current Statistics**

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destina Port	Application	Source Bytes ▼
<input type="checkbox"/>	7/31/13 10:22:32 AM	10.20.0.80	49328	114.17.182.241	18945	other	27,108
<input type="checkbox"/>	7/31/13 10:21:21 AM	10.20.0.80	49279	78.237.66.116	61682	other	19,570 (C)
<input type="checkbox"/>	7/31/13 10:24:48 AM	10.20.0.80	51920	117.200.131.241	28599	P2P.BitTorrent	18,840 (C)
<input type="checkbox"/>	7/31/13 10:24:48 AM	10.20.0.80	51921	122.173.122.6	62063	other	14,910
<input type="checkbox"/>	7/31/13 10:22:30 AM	10.20.0.80	49223	203.173.242.87	9942	other	14,598 (C)
<input type="checkbox"/>	7/31/13 10:33:43 AM	10.10.0.80	50854	72.14.204.19	443	Web.SecureWeb	14,328

Note: Choose an appropriate threshold value for your environment

© Copyright IBM Corporation 2015

Data loss

Flows to suspect Internet addresses

- Filters can identify flows to suspect Internet addresses
- Filters
 - **Remote Network**
 - **Remote Service**

Current Filters:

Remote Network is Smurfs ([Clear Filter](#))

► Current Statistics

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Application
	7/31/13 10:21:50 AM	10.20.0.80	64935	80.99.231.108	10833	other

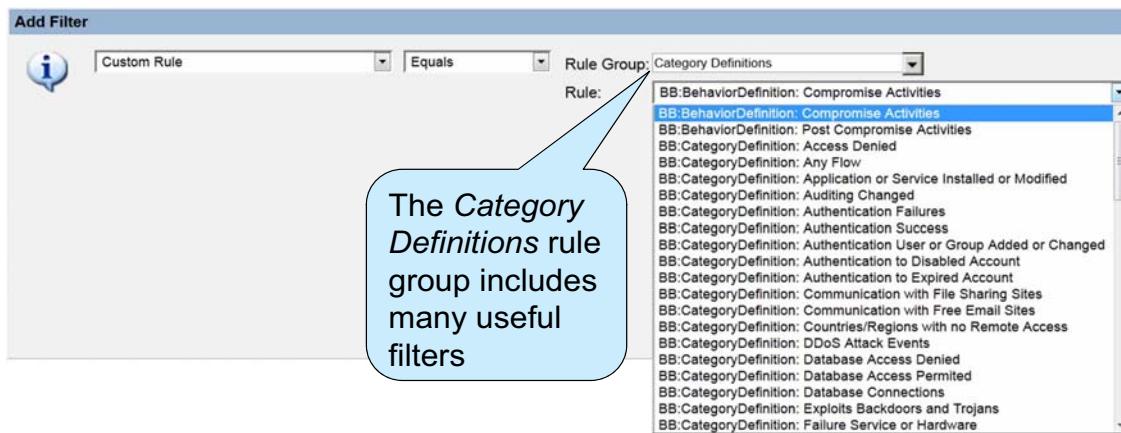
Note: Using the **Remote Networks** and **Remote Services** filters, QRadar SIEM administrators can identify customers and trusted networks and malware sources

© Copyright IBM Corporation 2015

Flows to suspect Internet addresses

Filtering on custom rules and building blocks

- When events or flows match a custom rule or building block, they are tagged with that rule
- You can filter on these tagged events and flows; such filters are useful for creating reports

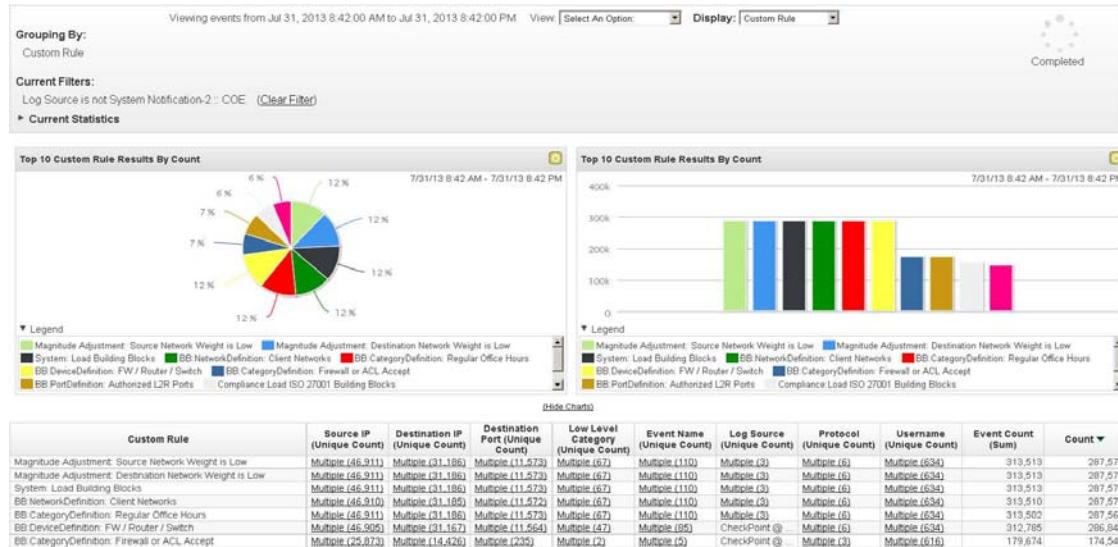


© Copyright IBM Corporation 2015

Filtering on custom rules and building blocks

Grouping by custom rules

Group events and flows by custom rules; this feature is useful when you investigate offenses



© Copyright IBM Corporation 2015

Grouping by custom rules

QRadar SIEM allows you to group events and flows by custom rules, but not by anomaly detection rules. The latter rule type is beyond the scope of this course.

Lesson 2 Using Advanced Search filters



Lesson: Using Advanced Search filters



© Copyright IBM Corporation 2015

QRadar features an advanced search facility using the Ariel Query Language (AQL). This lesson teaches you to use the AQL to construct advanced queries from one screen.

Reference: QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>

Ariel Query Language

- QRadar SIEM provides an **Advanced Search** filter option in the GUI that you can use to query the events and flows database
- The **Advanced Search** filter uses Ariel Query Language (AQL) to build SQL-like queries
- For example, the following query would look for events sharing the same source IP address over the past four hours

The screenshot shows a search interface with a dropdown menu labeled "Advanced Search". Below it is a search bar containing the AQL query: "select * from events where sourceip = '10.35.87.134' LAST 4 HOURS". To the right of the search bar is a "Search" button.

© Copyright IBM Corporation 2015

Ariel Query Language

Additional AQL examples

- AQL provides different filter types, one of which deals with using IP/CIDR filters; this query excludes a subnet

Advanced Search ▾ select * from events where not INCIDR('10.35.87.0/24', sourceIP) LAST 24 HOURS

- AQL queries can be structured to return specific fields in event or flows

Advanced Search ▾ select sourceip,logsourceName(logsourceid),qidname(qid) from events where username matches 'admin'

- AQL queries can also reference both wildcards and regular expressions; for example, this query looks for a user account name that contains the string sql

Advanced Search ▾ select sourceip,logsourceName(logsourceid) from events where username like '%sql%'

© Copyright IBM Corporation 2015

Additional AQL examples

Lesson 3 Using charts



Lesson: Using charts



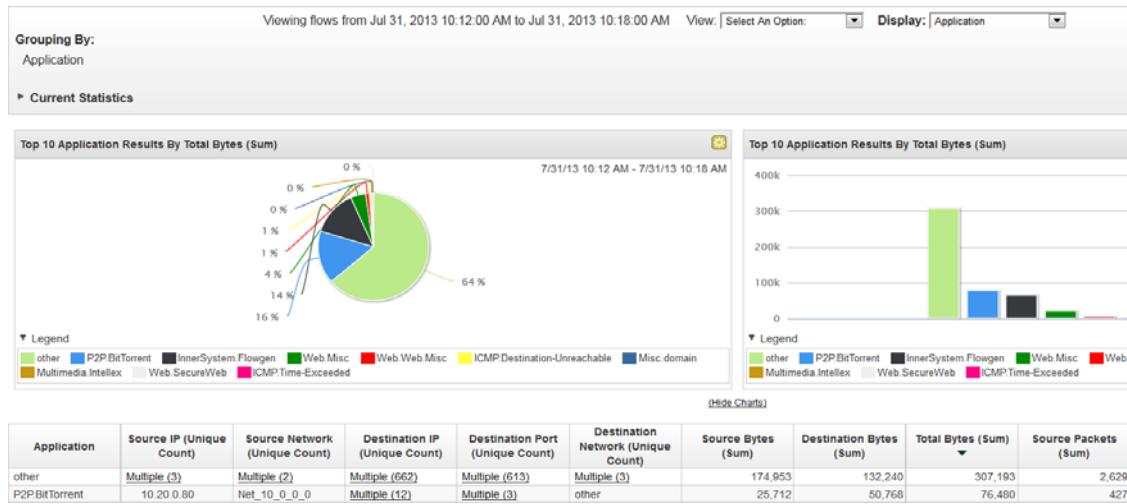
© Copyright IBM Corporation 2015

Charts graph log or network activity and are used to determine short- and long-term data trends. In this lesson, you learn how to use time-series and other charts to view log or network activity.

Reference: QRadar SIEM Users Guide <http://ibm.co/1wvpSEE>

Charts on Log and Network Activity tabs: Grouping

When you select a grouping on the **Log** tab or **Network Activity** tab, QRadar SIEM shows a pie chart and a bar chart



© Copyright IBM Corporation 2015

Charts on Log and Network Activity tabs: Grouping

After you configure a chart on the **Log Activity** or **Network Activity** tabs, the chart configurations remain when you perform one of the following activities:

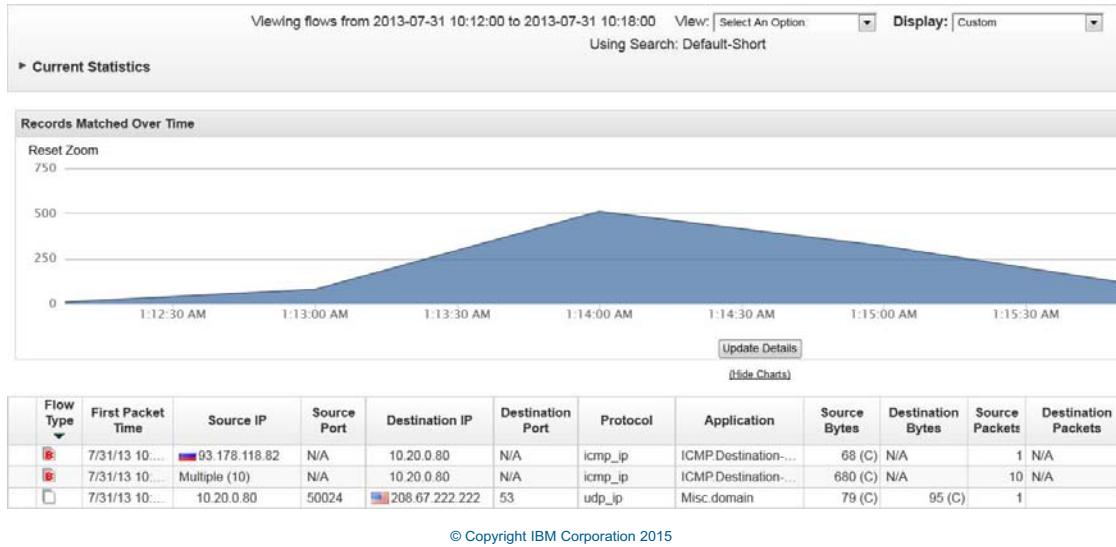
- Change the event view using the Display list
- Apply a filter
- Save the search criteria

Chart configurations do not remain when you perform one of the following activities:

- Start a new search
- Access a quick search
- View grouped results in a branch window
- Save the search results

Charts on Log and Network Activity tabs: Time range

When you select a time range other than **Real Time (streaming)**, QRadar SIEM shows a time-series chart even if it did not capture time-series data for the chart



Charts on Log and Network Activity tabs: Time range

The **Log Activity** and **Network Activity** tabs display only one time-series chart. QRadar SIEM displays this chart even if it did not capture time-series data for the chart. The data is then retrieved from the datastore. This can require considerable processing time.

The **Dashboard** tab can display many items with time-series charts. For performance reasons, QRadar SIEM displays time-series charts for ranges longer than 1 minute only if you enabled capturing of time-series data for these charts in dashboard items.

Capturing time-series data

- If you chose to capture time-series data or you scheduled a report run, QRadar SIEM counts incoming events and flows according your search criteria, grouping, and chosen value to graph
- To reduce storage needs and limit data queries, QRadar SIEM aggregates the counts into smaller accumulations
 - After each minute, the counters are aggregated into minute-by-minute accumulations
 - The minute-by-minute accumulations are aggregated into hourly accumulations
 - The hourly accumulations are aggregated into daily accumulations

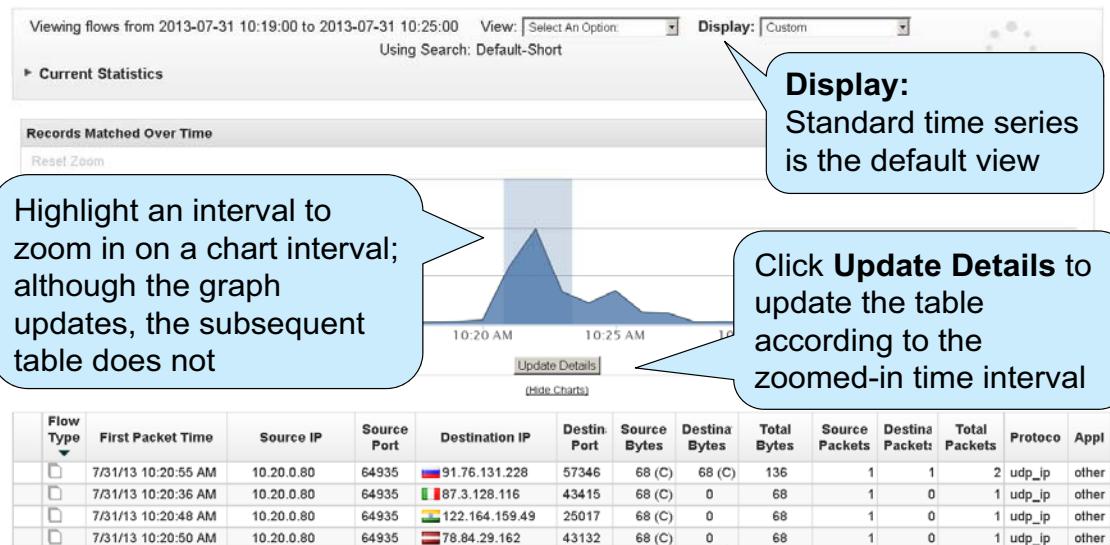
Note: Charts containing old data appear coarse-grained because QRadar SIEM deletes fine-grained accumulations earlier than the coarse-grained accumulations

© Copyright IBM Corporation 2015

Capturing time-series data

Each Event Processor runs an accumulator process. QRadar SIEM administrators can change the accumulator retention time periods.

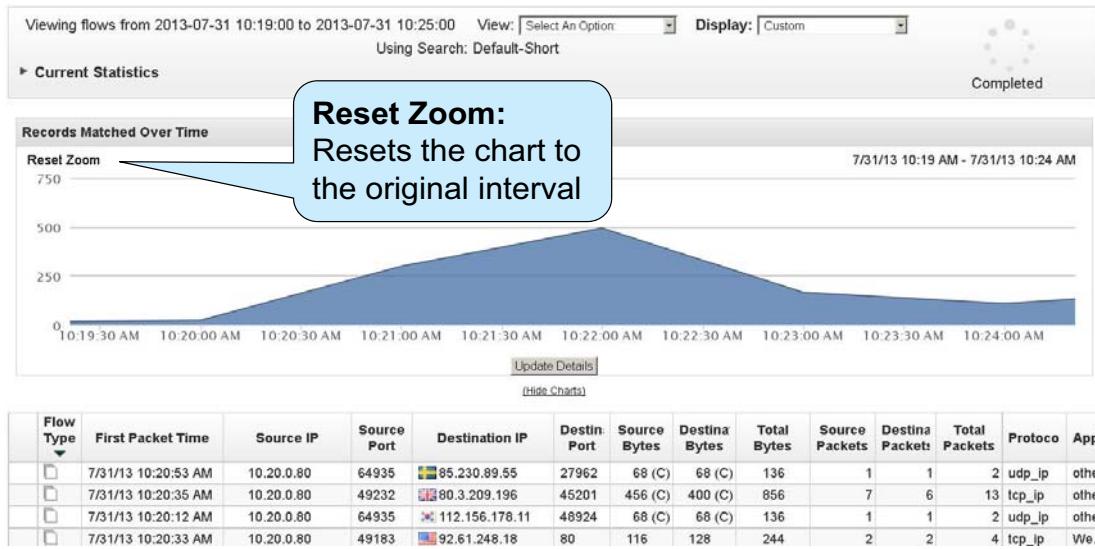
Viewing time-series charts: Zooming to focus



Viewing time series charts: Zooming to focus

Time-series charts are graphical representations of log or network activity over time. Peaks and valleys displayed in the chart depict high- and low-volume activity. Time-series charts are useful for short-term and long-term data trending. Using time-series charts, you can access, navigate, and investigate log and network activity from various views and perspectives.

Viewing time-series charts: Resetting zoom



© Copyright IBM Corporation 2015

Viewing time series charts: Resetting zooming

Plan a time-series search according to what data you want to investigate and how you want to display the data on the time-series chart. For example, consider how to group the search, what columns to display, and what filters to apply.

Summary

Now you should be able to perform the following tasks:

- Apply advanced filters that locate specific events and flows
- Use advanced search capabilities of the Ariel Query Language
- Use time series and other charts to view data

© Copyright IBM Corporation 2015

Summary

