



Section 1: Qradar Foundations

CERT PREP FOR TECHNICAL SALES FOUNDATIONS FOR IBM QRADAR FOR CLOUD (QROC) V1



SIEM Capabilities





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?

Providing context

To enable security analysts to perform investigations, QRadar SIEM correlates information

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





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



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

QRadar SIEM Console

The screenshot displays the IBM QRadar Security Intelligence console. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Forensics', 'Reports', 'Risks', 'Vulnerabilities', and 'Admin'. The main content area is divided into several panels:

- Security News:** A list of recent security news items, including 'Residents warned of computer hacking scam' and 'Using DroidJack to spy on an Android? Expect a visit from the police'.
- Security Advisories:** A list of security advisories, such as 'PHP Server Monitor - Cross-Site Request Forgery Issue' and 'PHP Server Monitor - Privilege Escalation Issue'.
- Network All:** A table showing vulnerability counts for various assets.

Vulnerability	Vulnerability Count
Information Leak - Computer Names are Visible	3
IBM with Microsoft Windows XP Professional has default administrator account	2
CVE-2002-1117 - Veritas - Backup Exec - Information Disclosure Vulnerability	2
Files are Accessible From the Network	2
CVE-2009-3103 - MS09-050 - Microsoft - Windows - Denial of Service Issue	2
CVE-1999-0504 - Microsoft - Windows - Default Credentials Issue	2
DELL XP blank password allows unauthorized	1
- Vulnerability Count / Risk:** A pie chart showing the distribution of vulnerabilities by risk level: High (65%), Medium (21%), Low (9%), Unknown (4%), and Warning (1%).
- PCI Failures:** A table showing PCI failures for various assets.

Asset	Asset Name	Vulnerability Count
172.16.60.79	JUMP	2,532
172.16.100.205	172.16.100.205	77
9.9.9.9	9.9.9.9	68
10.100.85.83	CRE Rule32 Short Server	8
- Open Services All:** A message stating 'No results were returned for this item.'
- Scans in Progress:** A section for scans currently in progress, last updated on Mon Jan 18 15:18:19 EST 2016.
- Scans Completed:** A section for scans that have been completed, including 'RC Windows Scan Again - 2015-10-26 15:23:47' and 'Windows Scan - 2015-10-22 14:32:00'.
- Impact All:** A pie chart showing the distribution of vulnerabilities by impact: Access Control Loss (14%), Downtime (14%), Reputation Loss (13%), Disclosure (13%), Information Theft (12%), Data Loss (12%), System Loss (11%), and Monitoring Failure (11%).
- Latest Published Vulnerabilities:** A section for the latest published vulnerabilities, including 'ABRT debug information installer symlink (0 Asset(s))'.

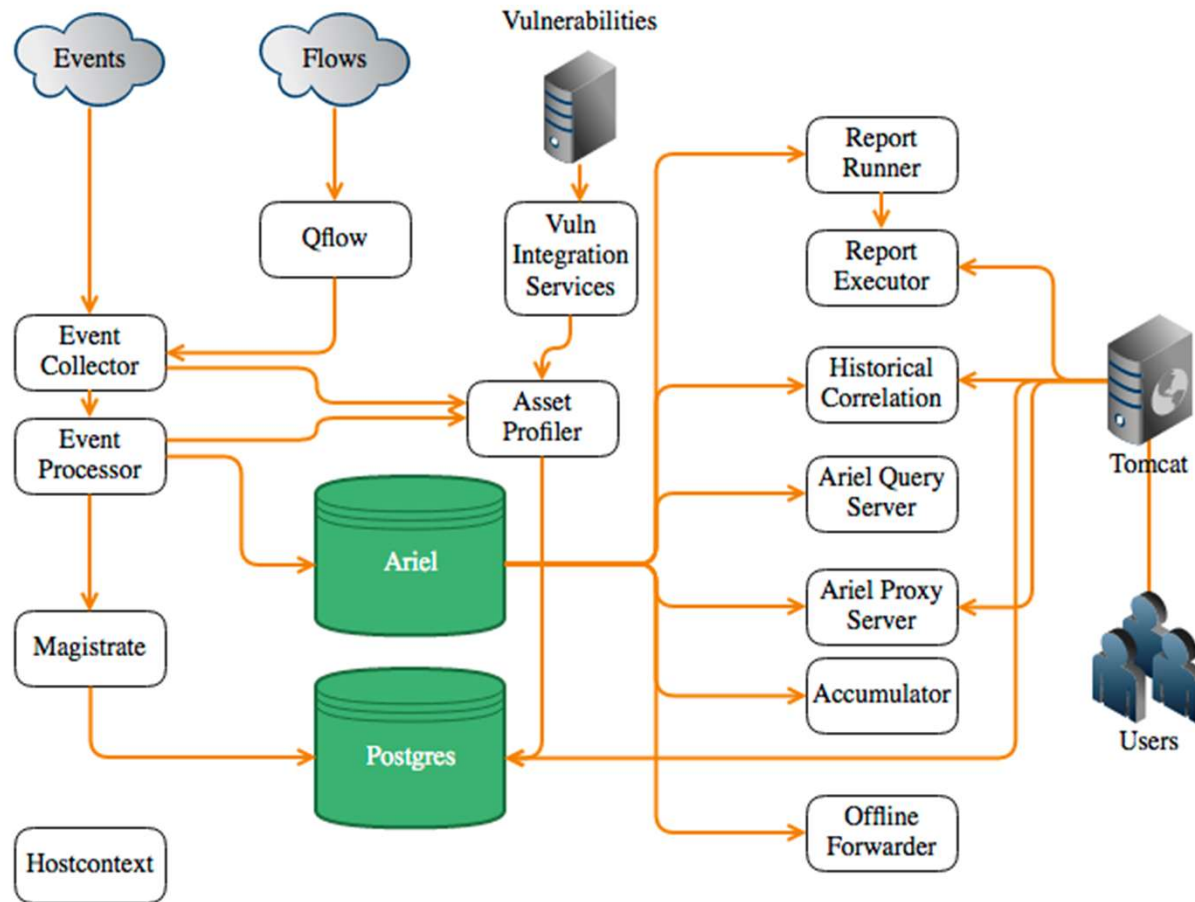
The console provides one integrated user interface for all tasks



How QRadar SIEM Collects Security Data



QRadar Data Flow - Overall





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

Flow collection and processing

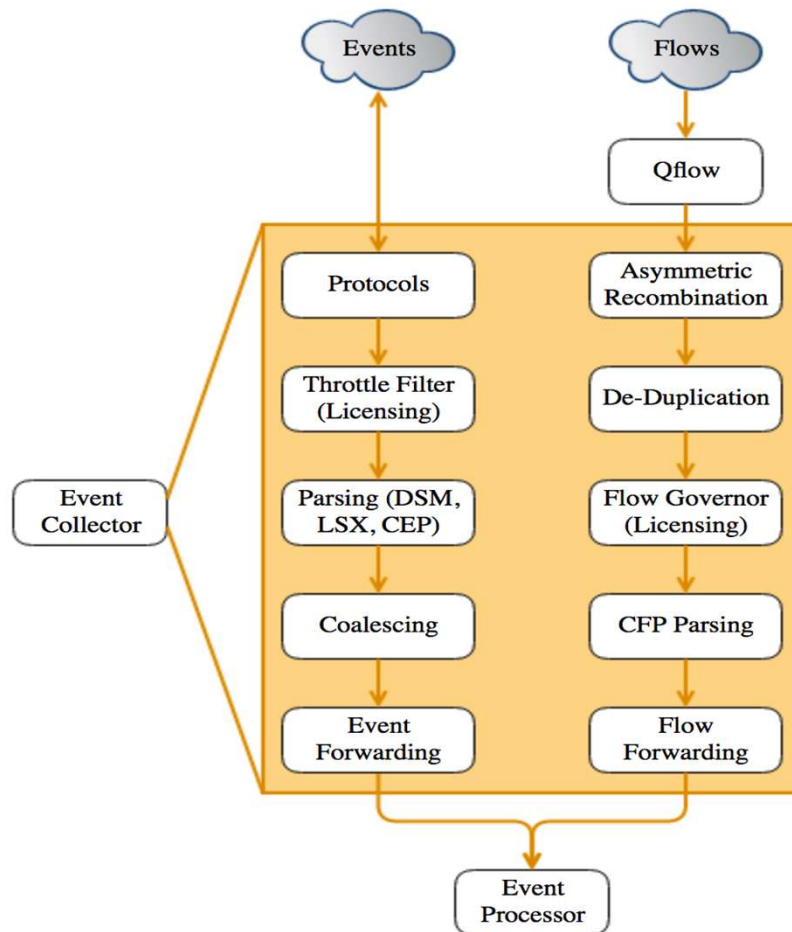


A flow is a communication session between two hosts

- 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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Oct 14, 2014, 6:59:59 AM	192.168....	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	3,816	64,432	48	52	N/A
<input type="checkbox"/>	Oct 14, 2014, 6:59:59 AM	192.168....	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	4,132	65,256	51	54	N/A
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Oct 14, 2014, 7:00:24 AM	192.168....	64348	192.168.10.10	443	tcp_ip	Web.SecureWeb	3,559	24,010	19	23	N/A
<input type="checkbox"/>	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
<input type="checkbox"/>	Oct 14, 2014, 6:59:59 AM	192.168....	61897	192.168.99.1	53	udp_ip	Misc.domain	78	0	1	0	N/A
<input type="checkbox"/>	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
<input type="checkbox"/>	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...

Event and Flow Collection





Events not counted against the EPS licences

- The list of log source types that do not incur EPS hits are as follows:
 - System Notification
 - CRE
 - SIM Audit
 - Anomaly Detection Engine
 - Asset Profiler
 - Search Results from scheduled searches
 - Health Metrics
 - Risk Manager questions, Simulations and internal logging
- For any events that are dropped from the pipeline using routing rules the dropped events will be partially credited back.
- EPS is credited back at 60% of the events dropped to a maximum of 2000 EPS.

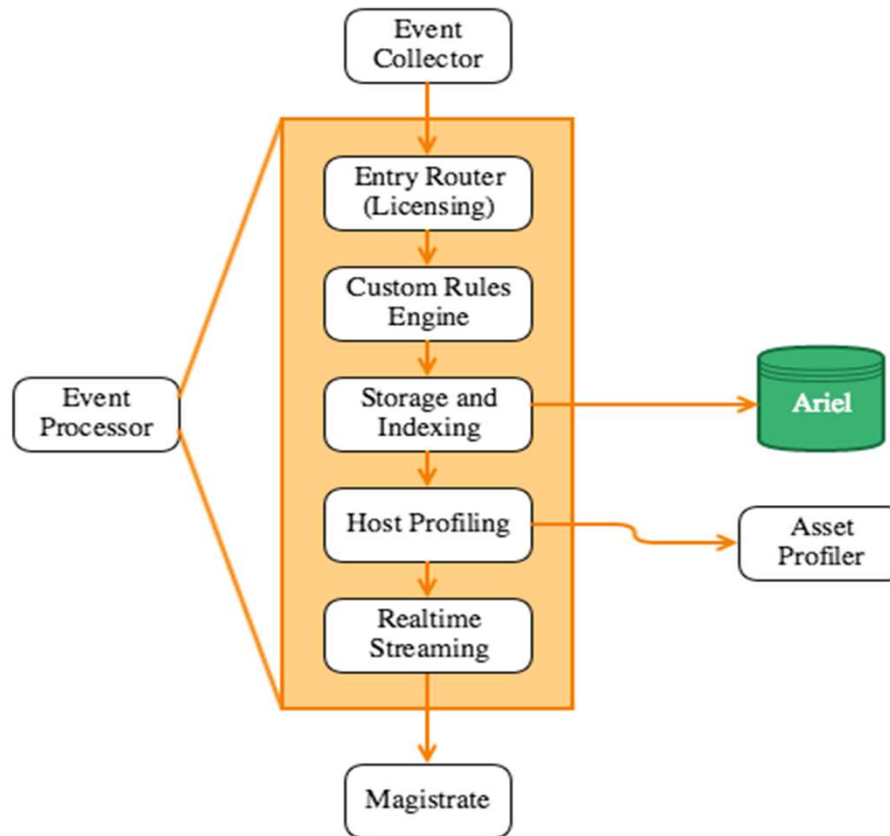
Event Coalescing



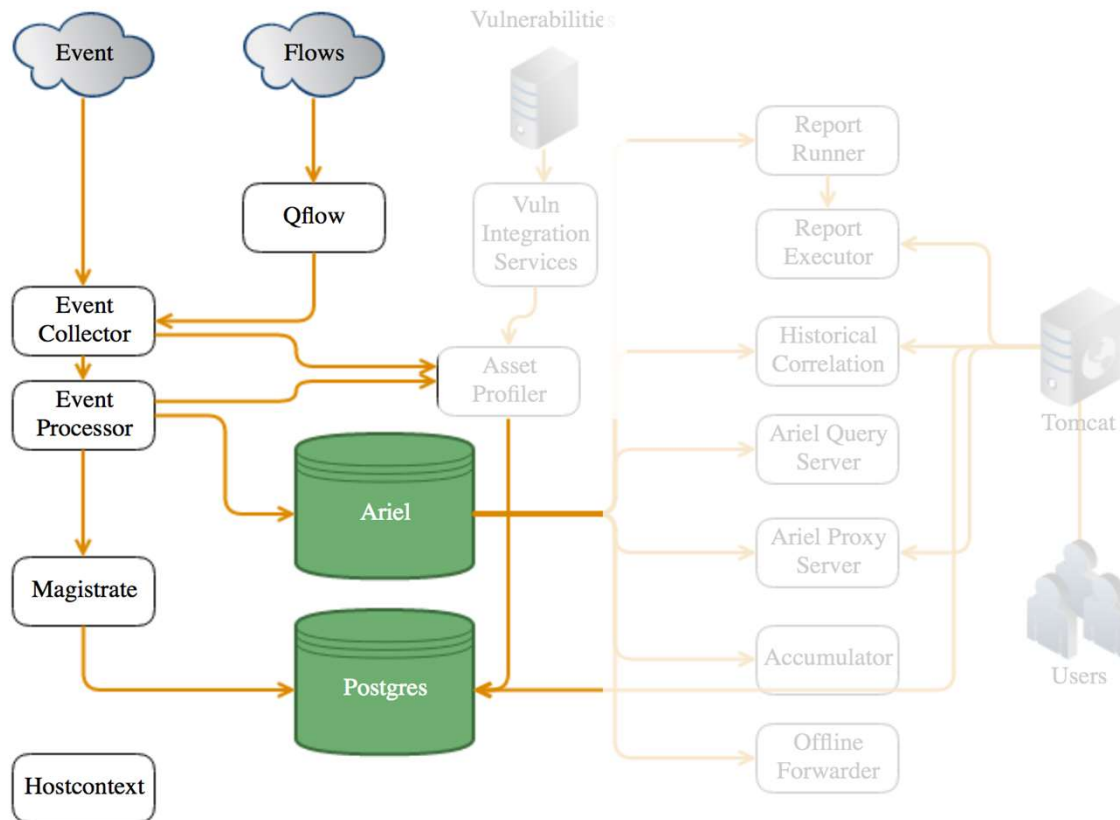
Event Coalescing is a method of reducing the data going through the pipeline.

- As data arrives in the pipeline QRadar will attempt to group like events together into a single event.
- Coalescing occurs after licensing and parsing
- Coalescing is indexed by Log Source, QID, Source IP, Destination IP, Destination Port and Username.
- If more than 4 events arrive within a 10 second window with these properties being identical any additional events beyond the 4th will be collapsed together.
- Coalesced events can be identified by looking at the Event Count column in the log viewer, if the Event Count is >1 the event has been coalesced.
- Coalescing can be turned on or off per log source or by changing the the default setting in the system setting page.

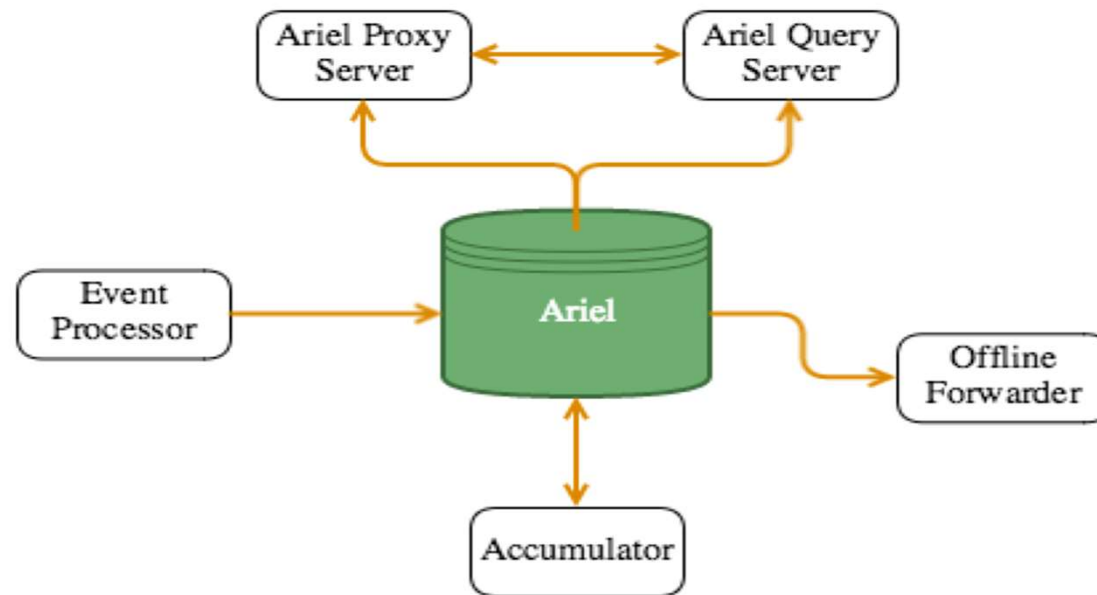
Event and Flow Correlation and Processing



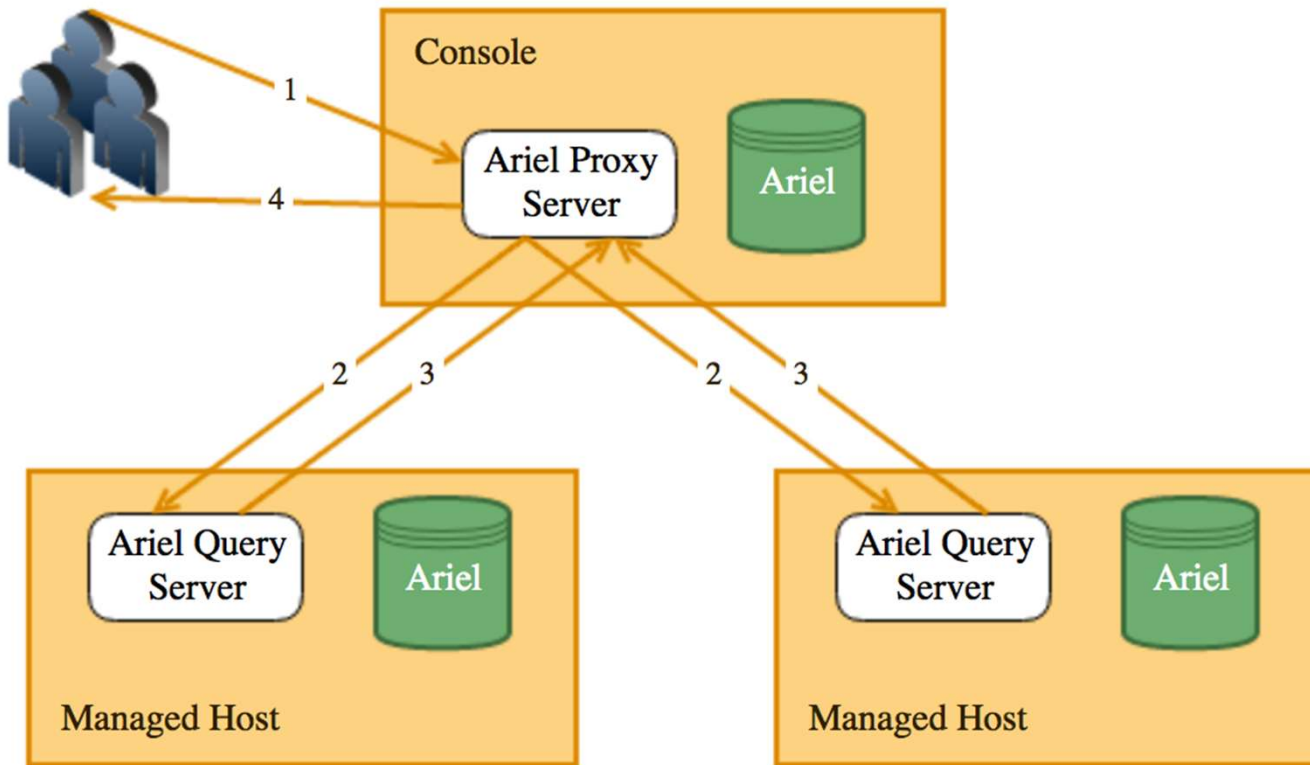
Where we are



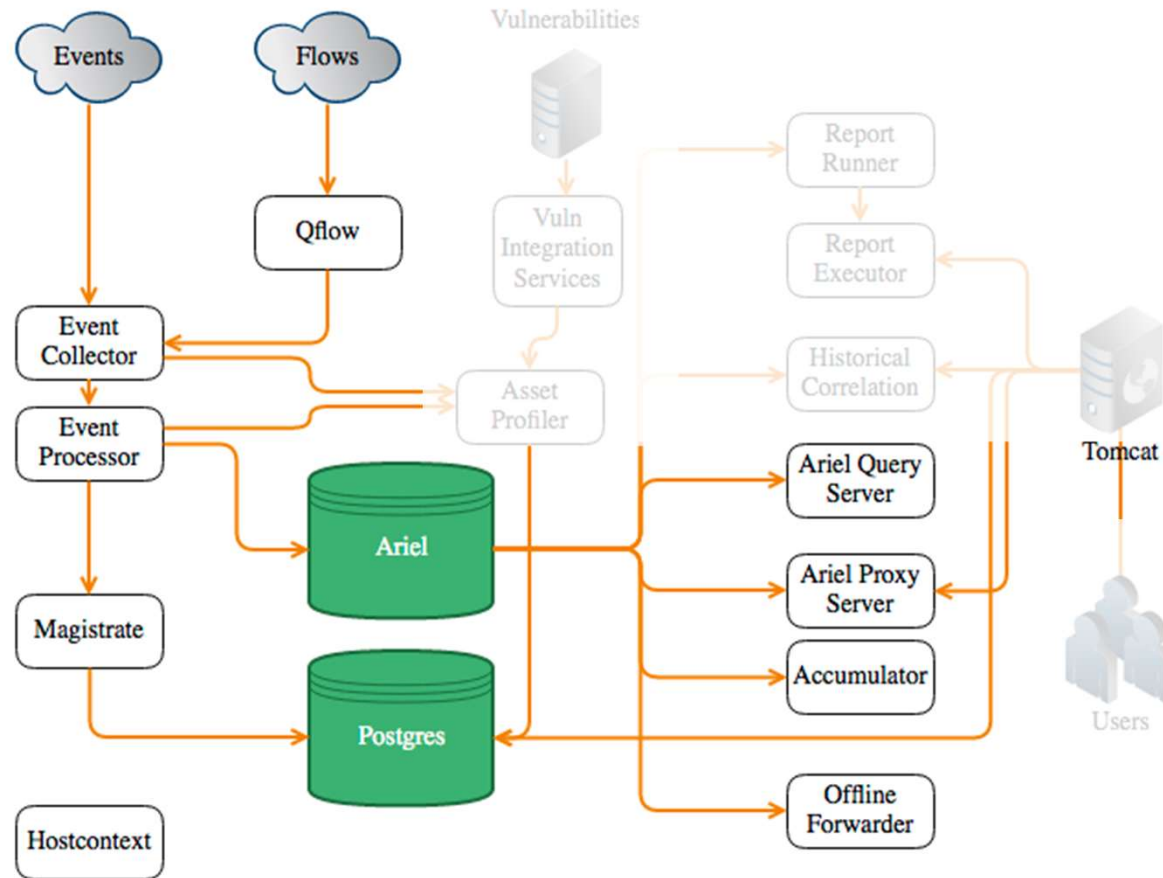
Ariel Components



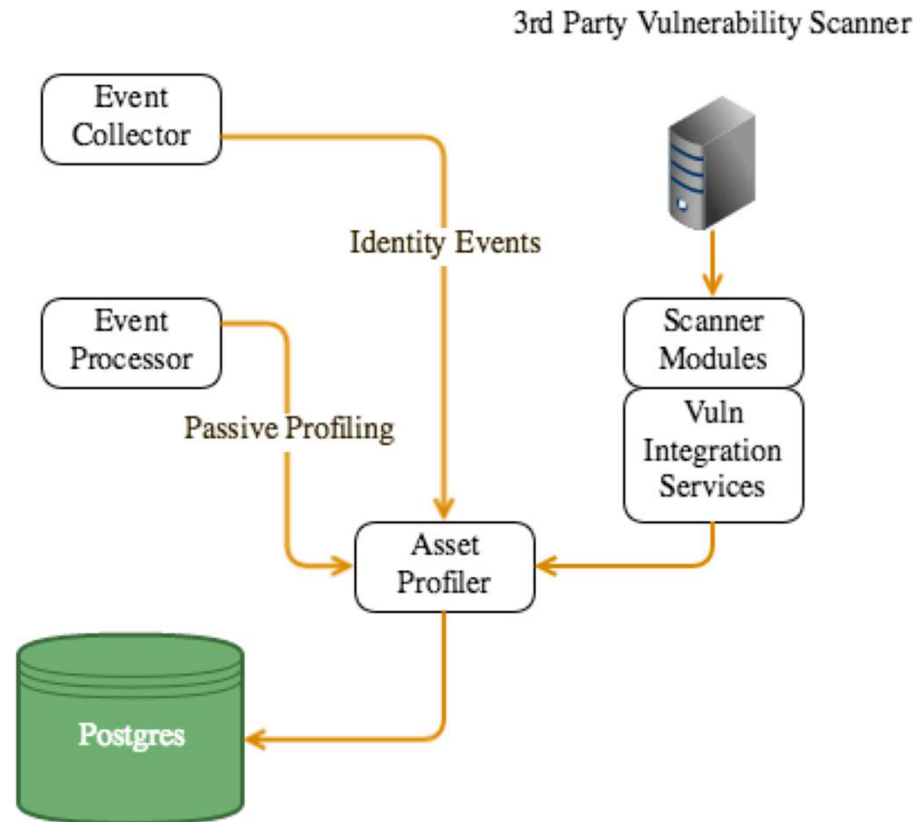
Ariel Search Flow



Where we are



Asset and Vulnerability Flow





Active scanners

For vulnerability assessment (VA) and maintaining asset profiles, QRadar SIEM can also integrate 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



Gathering asset information

Active scanners

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

Provide:

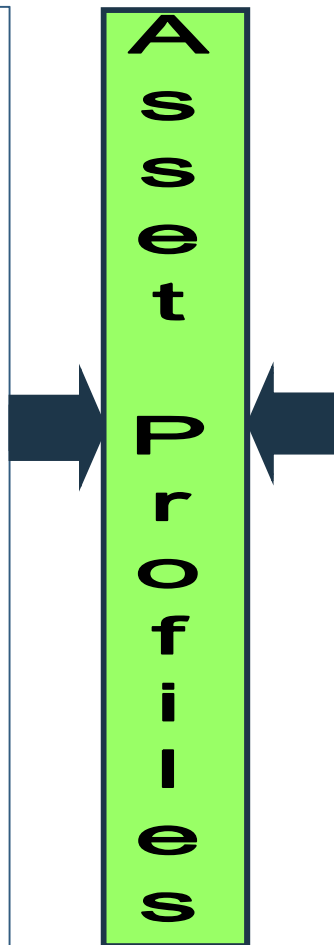
- List of hosts with risks and potential vulnerabilities
- IP and MAC addresses
- Open ports
- Services and versions
- Operating system

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



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

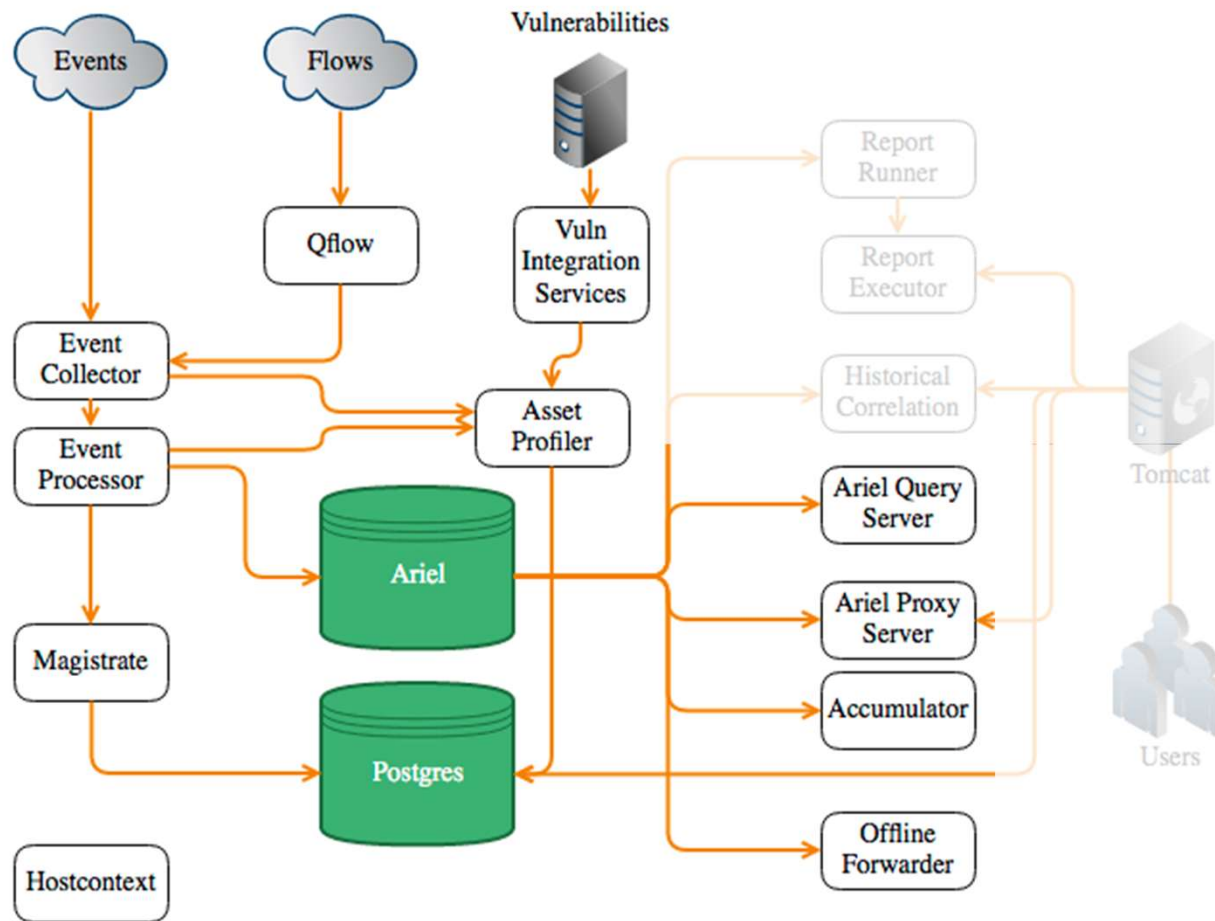
Asset profiles

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
<u>1030</u>	<u>10.111.219.138</u>	10.111.219.138	0.0	0	0
<u>1013</u>	<u>10.117.220.204</u>	10.117.220.204	0.0	0	0
<u>1014</u>	<u>10.117.220.205</u>	10.117.220.205	0.0	0	0
<u>1012</u>	<u>10.117.254.16</u>	10.117.254.16	0.0	0	0
<u>1011</u>	<u>10.117.254.36</u>	10.117.254.36	0.0	0	0
<u>1010</u>	<u>10.117.254.66</u>	10.117.254.66	0.0	0	0
<u>1009</u>	<u>10.15.20.140</u>	10.15.20.140	0.0	0	0
<u>1015</u>	<u>10.2.100.66</u>	10.2.100.66	0.0	0	0
<u>1018</u>	<u>10.20.0.80</u>	10.20.0.80	0.0	0	0
<u>1007</u>	 <u>128.245.120.152</u>	128.245.120.152	0.0	0	0
<u>1019</u>	<u>172.16.254.2</u>	chkpt1	0.0	0	0

Where we are





The Remainder

Hostcontext

“Owns” the host it is responsible for starting and stopping processes and for overall system health and backups.

Reporting Executor

A stopwatch responsible for keeping track of reports and when they should run and then instantiating the report runner

Report Runner

The process that actually generates the reports, querying postgres, Ariel, etc..

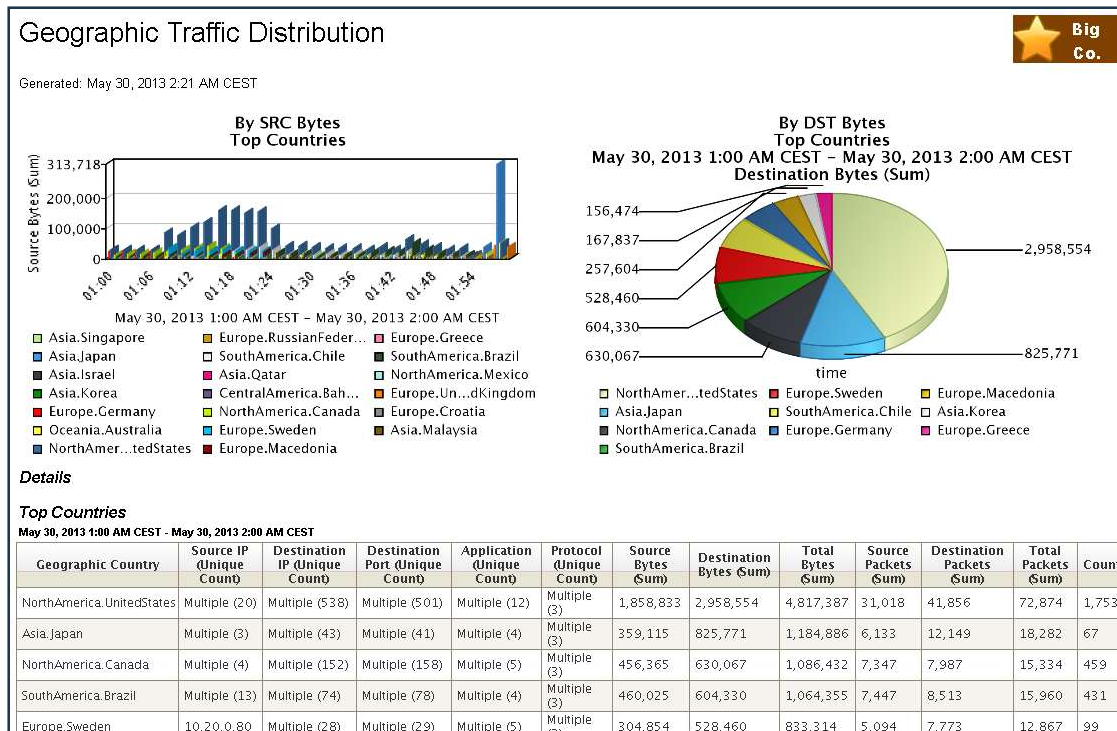
Tomcat

Process that drives our web UI and serves up web pages.

Historical Correlation
Processor

Process that is responsible for historical correlation. Runs a specified search, runs the results through CRE rules (based on QRadar time or device time) and generates offenses

Reporting








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



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



Deployment Models and Licensing



QRadar Dashboard - Fully integrated architecture and interface

One Console Security

Log Management

Security Intelligence (SIEM)

Vulnerability Management & Risk Assessment

Network and Application Visibility



Built on a Single Data Architecture

QRadar Product Portfolio

Area of Focus

Security Intelligence platform that enables security optimization through advanced threat detection, meet compliance and policy demands and eliminating data silos



Portfolio Overview

QRadar Log Manager

- Turnkey log management for SMB and Enterprises
- Upgradeable to enterprise SIEM

QRadar SIEM

- Integrated log, flow, threat, compliance mgmt
- Asset profiling and flow analytics
- Offense management and workflow

X-Force IP Reputation Feeds

Network Activity Collection & Prevention (QFlow) and Network Insights (QNI), Network analytics, behavior and anomaly detection

- Layer 7 application monitoring
- Real-time network packet analysis

QRadar Vulnerability Manager, including Risk Management

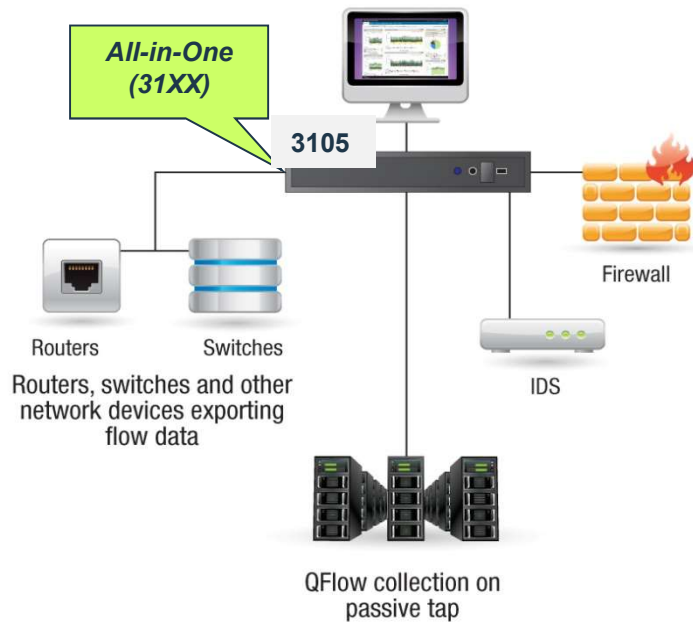
- Integrated Network Scanning & Workflow
- Risk Management to prioritize vulnerabilities
- Predictive threat modeling & simulation
- Scalable configuration monitoring and audit
- Advanced threat and impact analysis

QRadar Incident Forensics & Packet Capture

- Reconstruct raw network packets to original format
- Determine root cause of security incidents and help prevent recurrences

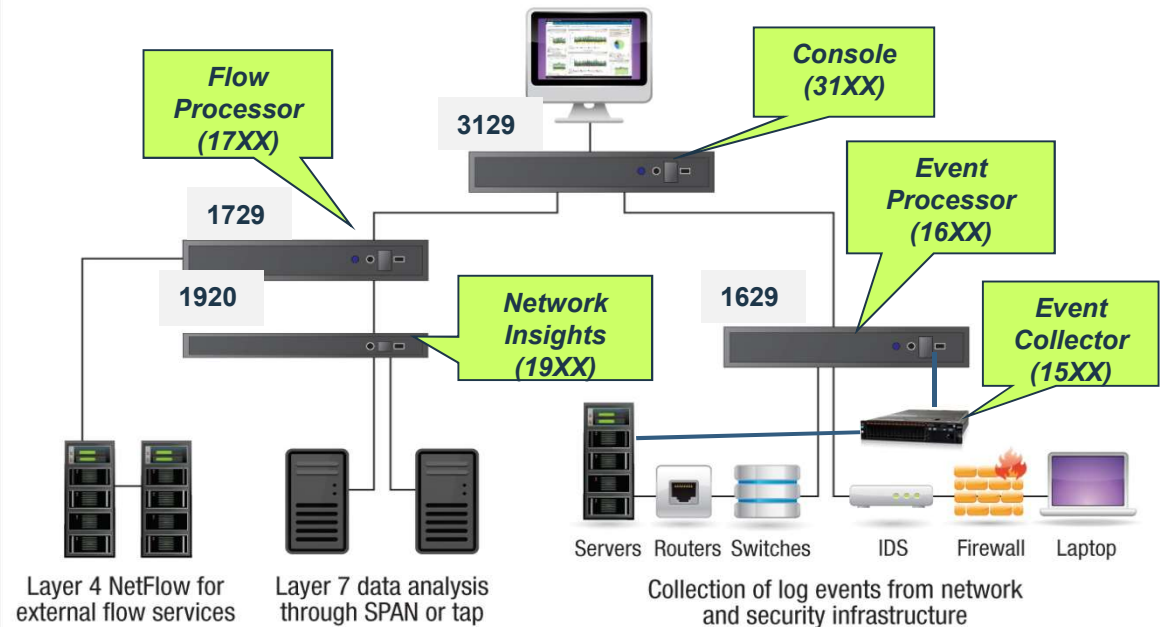
QRadar supports two deployment models: All-in-One and Distributed

Sample IBM Security QRadar SIEM 31XX
all-in-one deployment
QRadar web console



All-in-One is a single appliance used to collect both events and flow data from various security and network devices, perform data correlation and rule matching, report alerts/threats, and provide all admin functions through a Web browser.

Sample IBM Security QRadar SIEM 3129
distributed deployment
QRadar web console



A Distributed deployment consists of multiple appliances for different purposes:

- **Event Processor** to collect, process and store log events
- **Flow Processor** to collect, process and store several kinds of flow data generated from network device. Optional **QFlow Collector** is used to collect layer 7 application data.
- **Console** to correlate data from managed processors, generate alerts/reports, and provide all admin functions.

Customers can start with an All-in-One solution, and/or easily add appliances to expand their deployment

3129 All-in-One



Single XX29 Appliance

Clients can purchase a single Appliance to serve as the base for the UI and also performs all Event and Flow processing, correlation, searches, reports, etc..

3129 Console



Multiple XX29 Appliances

1629 Event Processor



1429 Data Node



1729 Flow Processor



Or, several appliances can be purchased to distribute the processing power required to perform these functions across them.

Deploying QRadar now only Requires three elements: Base License, Appliance/Node, & Capacity

- QRadar SIEM or Log Manager Base License
 - Entitles clients to the main QRadar console software.
 - Can be deployed as an All-in-One or in a distributed manner by adding managed hosts (Event Processor, Flow Processors, Data Nodes, etc.)
 - Includes base capacity of 100 EPS and 15,000 FPM
- Additional EPS and FPM Capacity purchased in bundles.
 - No specific upgrade path requirements, bundles are aggregate.
 - 'Volume-Based' pricing, the larger the bundle, the lower the cost per metric (EPS or FPM).
 - Capacity can be re-allocated among managed hosts as needed (contact q1pd@us.ibm.com).
- Flexible deployment options.
 - Can be deployed on QRadar Appliances, 3rd party appliances, in the Cloud, Virtual
 - QRadar Appliances are recommended
 - 3rd party appliances, cloud, virtual require purchase of "QRadar Node"



**Base QRadar
Software
License**



**Core
Appliance
XX05**



EPS/FPM



**All-in-1
Appliance 3105**

QRadar Architecture – How role-based licensing works

- Activation Keys – Required at first boot after installation (Pre QRadar 7.3).
 - The software prompts the user to enter an activation key for initial setup.
 - Keys are included in the appliance packaging and/or with electronically delivered Proof of Entitlement (POE)
 - Each key establishes the role the appliance will play within the deployment.
 - ✓ Enables / Disables features unique to that role.
 - ✓ Sets license value limits on some appliances to ensure optimal performance based on the hardware.
 - ✓ Hardware check to ensure adequate configuration for the role being established.
 - ✓ Includes 30 day trial license for full functionality. At the end of this period the user must apply a permanent license key.
 - ✓ Once the role is established, it cannot be changed without reinstalling the software and walking through the setup process again.



QRadar Architecture – How role-based licensing works (Cont)

- Migrating to a drop-down menu option instead of key entry, depending on product/version (QRadar 7.3 and later)
- License Keys – Required for continued operation for some roles.
 - Manually created by our licensing team (q1pd@us.ibm.com) to set capacity limits based on entitled product.
 - Currently, individual keys are required for each console, event processor, flow processor, QVM, Forensics.
 - Delivered via email and applied to the deployment via the UI.



QRadar Licensing Metrics



Events Per Second (EPS) – Controlled by the license key, this limits the number of event logs that can be collected, normalized, and correlated in real time. Any events sent to QRadar outside of the licensed limit are queued in a buffer and processed when activity slows. If the burst of events is extreme in either size or duration, events may be dropped.



Flows per Minute (FPM) – Similar to EPS, this is controlled by the license key, and limits the number of flow records QRadar can process in real time. Burst handling also similar to EPS.

Vulnerability Manager Scannable Assets – The number of assets your QRadar Vulnerability Manager license allows you to scan. The base license includes 256 scannable assets standard. To scan additional assets, license upgrades (sold in bundles in increments of 256) are required. Support for scanning more than 50K assets requires Vulnerability Manager to run on a dedicated appliance.

Risk Manager Configuration Sources – The number of devices Risk Manager can gather configuration data from. To enable this functionality, the Risk Management module needs to run on a dedicated appliance.

High Availability – Offered per instance/appliance and can be deployed to back up most QRadar managed hosts. Not yet available for Incident Forensics or Packet Capture.

Disaster Recovery / Data Redundancy – A warm/cold backup option. Licensing mirrors the primary deployment.



Capacity Upgrades expand QRadar's processing power

A new way to expand and manage license capacity.

- All upgrades are aggregate.
 - Can be sold in any combination, no more specific upgrade paths or rules.
 - Capacity managed at the console level as a total, then assigned to individual hosts as needed.
 - Can be re-allocated to other hosts without special approval to manage changing data volume requirements.
- No more distinction between Log Manager EPS and SIEM EPS. Same parts used for both products.
- Unlimited number of Log Source limits supported.

Primary Capacity Upgrades (PA Parts)
Bundle of 100 Events per Second (D1RNKLL)
Bundle of 500 Events per Second (D1RNRL)
Bundle of 1000 Events per Second (D1RNXLL)
Bundle of 2500 Events per Second (D1RP3LL)
Bundle of 10,000 Flows per Minute (D1RQALL)
Bundle of 25,000 Flows per Minute (D1RQGLL)
Bundle of 50,000 Flows per Minute (D1RQMLL)
Bundle of 100,000 Flows per Minute (D1RQTLL)



Capacity Upgrades expand QRadar's processing power

- Disaster Recovery deployments have separate upgrade parts to fit failover pricing scheme.
 - DR environment should match the primary environment from a capacity perspective.
 - Primary and DR capacity cannot be shared or combined. Both managed separately.

DR Capacity Upgrades (PA Parts)
Bundle of 100 Events per Second (D1RPFLL)
Bundle of 500 Events per Second (D1RPLLL)
Bundle of 1000 Events per Second (D1RPSLL)
Bundle of 2500 Events per Second (D1RPYLL)
Bundle of 10,000 Flows per Minute (D1RR5LL)
Bundle of 25,000 Flows per Minute (D1RRBLL)
Bundle of 50,000 Flows per Minute (D1RRHLL)
Bundle of 100,000 Flows per Minute (D1RRNLL)

X-Force IP Reputation Intelligence Feed

▪ Purpose

- To further enrich QRadar's threat detection capabilities with IBM X-Force IP reputation intelligence data on a subscription basis



▪ X-Force IP Reputation

- X-Force is IBM's security threat research team that collects and maintains comprehensive internet threat and reputation data such as spam servers, Botnet command and control servers, malware distribution points, anonymous proxies, and dynamic and dialup ranges.

▪ Integration to QRadar

- X-Force IP Reputation data is constantly updated and maintained, with updates being pushed out periodically to subscribing QRadar appliances.
- Any QRadar event/flow activity involving IP Reputation addresses is automatically flagged in offenses, rules, reports. The data can be used to identify new threats, or validate threats detected through existing QRadar means.

▪ Ordering

- **Now included in version 7.2.8 and beyond!**
- **Customers insistent on running an earlier version still need to subscribe this service.**
- Need to be purchased for console, and any event or flow processors in the deployment.
- Qflow, Event Collectors, Data Nodes, QVM, Forensics, PCAP do not require X-Force licenses.
- Also needs to be purchased for all DR appliances (no failover parts at this time, use same part numbers).



*X-Force IP
Reputation
data*



**QRadar Appliance with
X-Force IP Reputation
feed subscribed**



High Availability and Disaster Recovery

- High Availability (HA) acts as an active ‘hotspare’
 - Unique activation process enables HA functionality.
 - Heartbeat monitor constantly communicates with the primary appliance.
 - Upon failure, HA appliance will inherit license, IP address, all settings of the primary.
 - Each HA appliance must be purchased per instance. (D1RS0LL for SIEM, D1RSKLL for Log Manager)
 - License is generic, can back up any appliance type.
 - Not yet available for Risk Manager, Forensics, Packet Capture, or Network Insights
 - Network topology needs to be considered to reduce latency.
- Disaster Recovery (DR) acts as warm or cold spare.
 - Data and settings copied from the primary on a set schedule.
 - Base license and additional capacity may need to match the primary if the deployment is equal to the primary site.
- In both cases, the hardware should be identical between the primary and HA or DR appliances.

Appliance Types



QRadar Product Short-Hand Terms

The QRadar product structure is mostly identified by a 4 digit product code that can be decoded as such:

XX

Software Role/Type

- **Software Role/Type Codes:**
 - 31 = All-In-1 or Console (**Base Offering**)
 - 16 = Event Processor
 - 17 = Flow Processor
 - 18 = Combined Event/Flow Processor
 - 19 = Network Insights
 - 15 = Event Collector
 - 12 = Qflow Collector (Copper NIC)
 - 13 = Qflow Collector (Fiber NIC)
 - 14 = Data Node
 - 60 = Vulnerability Manager
 - 70 = Risk Manager

XX

Hardware Designation

- **Hardware Codes:**
 - XX05 = Based on x3550 M5 BD, 64GB RAM, 6.2TB storage
 - XX28-C* = Based on PowerEdge R730xd XL, 128GB RAM, 40TB storage
 - XX29 = Based on x3650 M5 BD, 128GB RAM, 72TB storage
 - XX48 = Based on X3650 M5 BD, 128GB RAM, 24TB storage
 - XX01/02* = 1Gbps / 3Gbps (Qflow Only)
 - XX10* = 10Gbps (Qflow Only)
 - XX20 = Network Insights
- **Legacy Codes**
 - XX01 = Dell R710 Platform
 - XX24 = Either Dell R510 or x3650 M3 Platform (Check individual specs)
 - XX28 = Based on x3650 M4 BD, 128GB memory, 40TB storage
2000 = Entry level All-in-One (Discontinued)
 - 21XX = Entry level All-in-One (Discontinued)
 - 1101 = Low-end Qflow Collector (Discontinued)

***Note: Dell versions of appliance hardware are followed by “-C”**

SIEM All-in-One 3105, 3129 and 3148 Appliances

▪ Positioning

- QRadar appliance for centralized deployment in a small/medium/large enterprise
- Contains event & flow processing capabilities

▪ Characteristics and Capacity

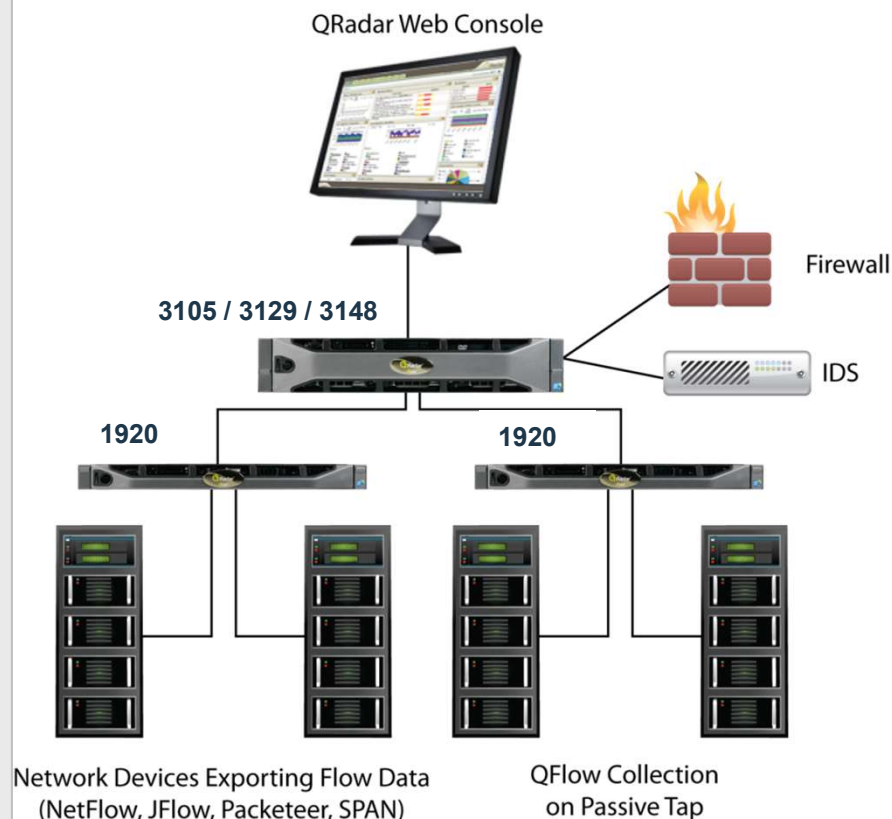
▪ Memory Capacity

- 3015 – 64 GB
- 3129/3128-C/3148 – 128 GB
- Requires **external** QFlow Collectors for layer 7 network activity monitoring
- Dedicated storage for QRadar*
 - 3105: 6.2TB of storage
 - 3129 / 3128-C: 40TB of storage
 - 3148: 22TB of storage

▪ Capacity

- 3105: Can process up to 5000 EPS & 200K FPM
- 3129/ 3128-C: Can process up to 15K EPS and 300K FPM
- 3148: Can process up to 30K EPS and 600K FPM
- Upgradable to 31XX Console for distributed deployment with events/flows transferred to new 16XX, 17XX, or 18XX appliance.

▪ HA / DR available



SIEM Console 3105, 3129, and 3148 Appliances

▪ Positioning

- Console dedicated to management of distributed deployment in a large enterprise
- Manages distributed event/flow processors

▪ Characteristics and Capacity

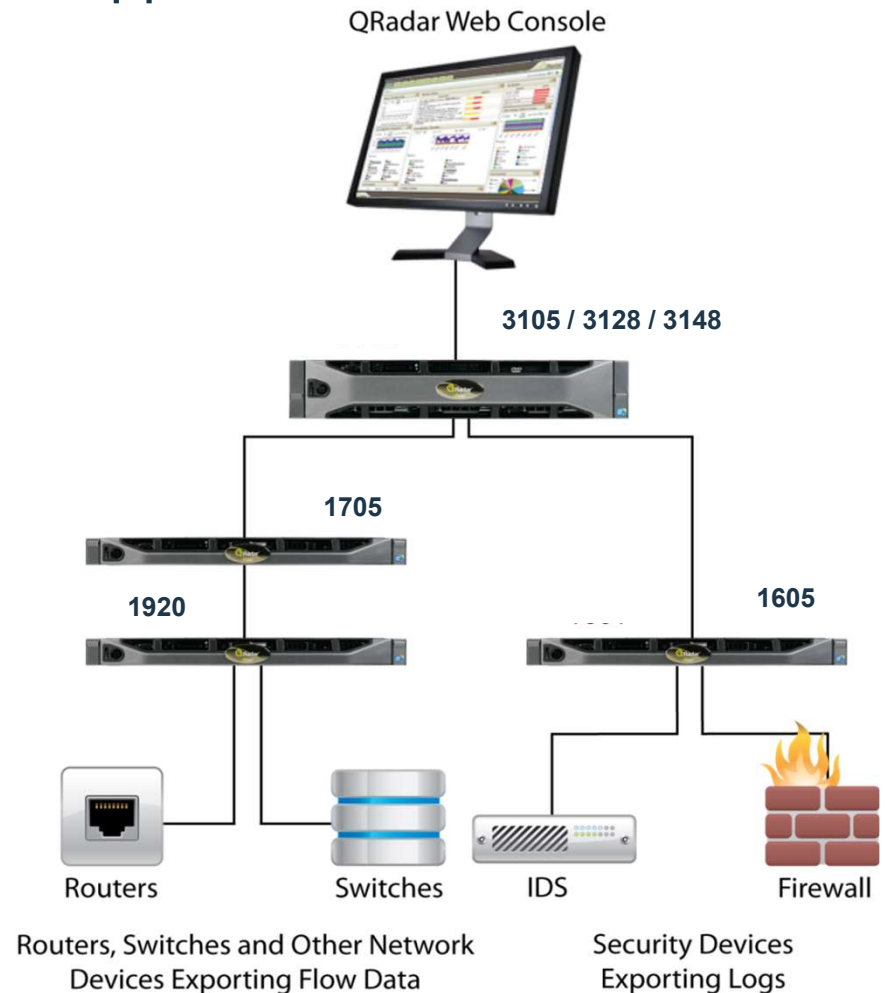
- Focuses on processing and analysis of offenses, generating views and reports
- Requires 16XX to collect log events or 17XX to collect flows (or 18XX for both)
- Requires external QFlow Collectors for layer 7 network activity monitoring
- Dedicated storage for QRadar*
 - 3105: 6.2TB of storage
 - 3129 / 3128-C: 40TB of storage
 - 3148: 22TB of Storage

▪ Capacity

- Distributed to dedicated Event and Flow Processors

▪ HA / DR available

*May vary based on configuration



SIEM Event Processor 1605, 1629, and 1648 Appliances

▪ Positioning

- High capacity and scalable event collection for distributed deployment in a large enterprise

▪ Characteristics and Capacity

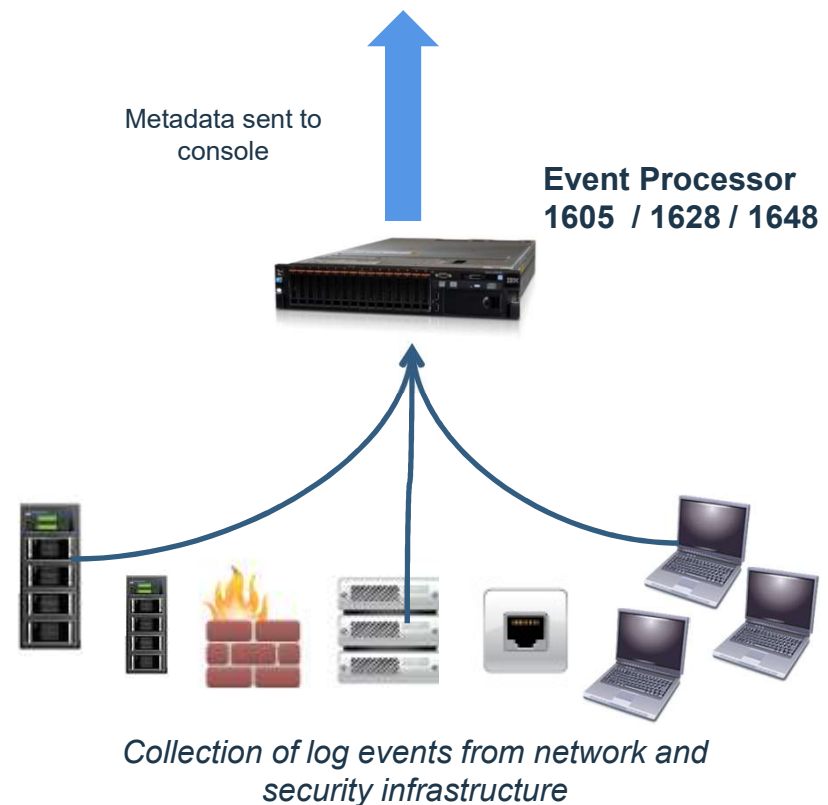
- Collect logs from network devices, security devices, operating systems and applications
- Requires Console 31XX
- Dedicated storage for QRadar*
 - 1605: 6.2TB of storage
 - 1629 / 1628-C: 40TB of storage
 - 1648: 22TB of storage

▪ Capacity

- 1605 can process up to 20,000 EPS
- 1629 / 1628-C can process up to 40,000 EPS
- 1648 can process up to 80,000 EPS

▪ HA / DR available

*May vary based on configuration



SIEM Flow Processor 1705, 1729, and 1748 Appliances

▪ Positioning

- High capacity and scalable flow collection for distributed deployment in a large enterprise

▪ Characteristics and Capacity

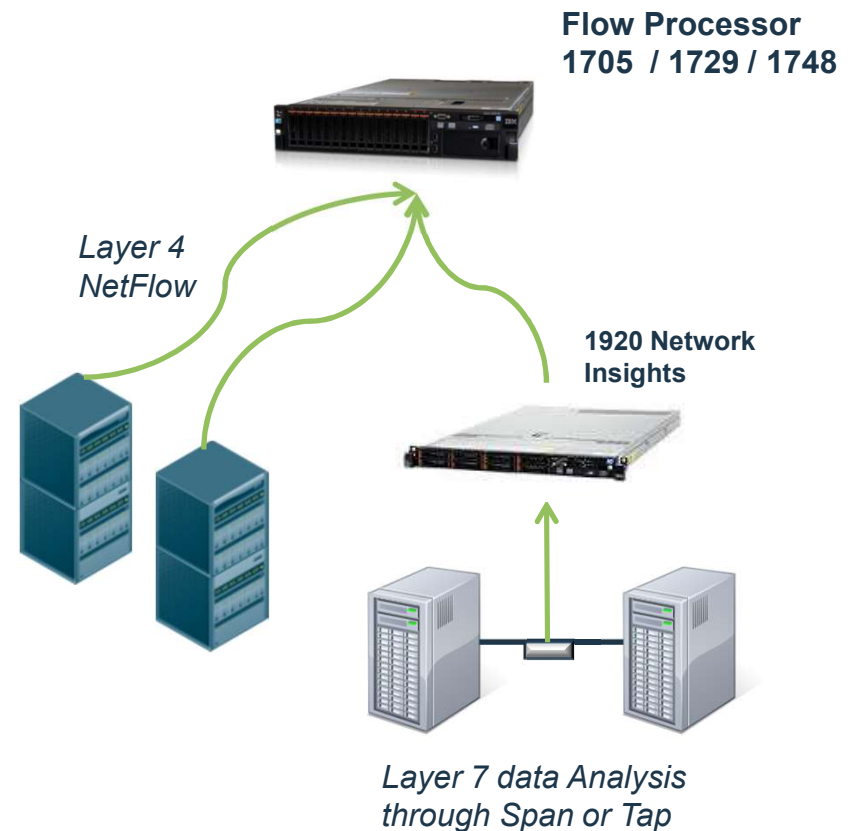
- Receives flows from external flow sources (e.g. NetFlow), Network Insights or QFlow Collectors for layer 7 network activity monitoring
- Requires Console 31XX
- Dedicated storage for QRadar*
 - 1705: 6.2TB of storage
 - 1729 / 1728-C: 40TB of storage
 - 1748: 22TB of storage

▪ Capacity

- 1705 can process up to 600K FPM
- 1729 / 1728-C can process up to 1.2M FPM
- 1748 can process up to 3.2M FPM

▪ HA / DR available

*May vary based on configuration



SIEM Combined Event/Flow Processor 1805, 1829 and 1848 Appliances

▪ Positioning

- High capacity and scalable event & flow collection for distributed deployment in a large enterprise

▪ Characteristics and Capacity

- Receives logs from network devices, security devices, operating systems and applications AND flows from external flow sources (e.g. NetFlow) or QFlow Collectors for layer 7 network activity monitoring
- Requires Console 31XX
- Dedicated storage for QRadar*

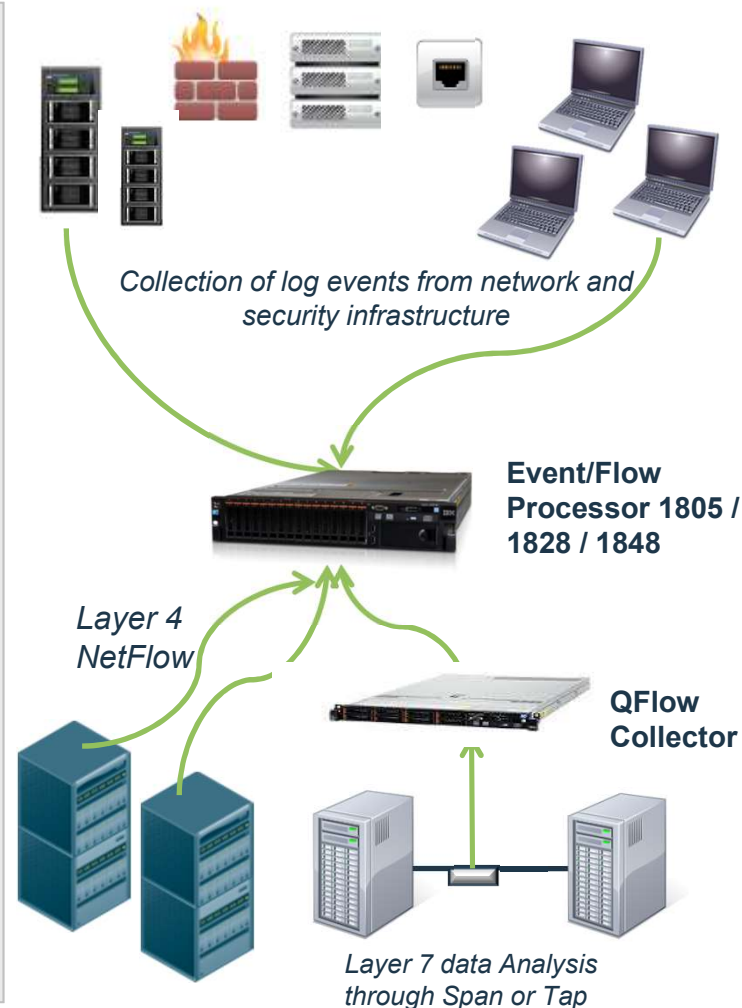
- 1805: 6.2TB of storage
- 1829 / 1828-C: 40TB of storage
- 1848: 22TB of storage

▪ Capacity

- 1805: EPS can process up to 5000 EPS & 200K FPM.
- 1829 / 1828-C: EPS can process up to 15,000 EPS & 300K FPM.
- 1848: EPS can process up to 30,000 EPS & 1M FPM.

▪ HA / DR available

*May vary based on configuration



Event Collector 1501 Appliance

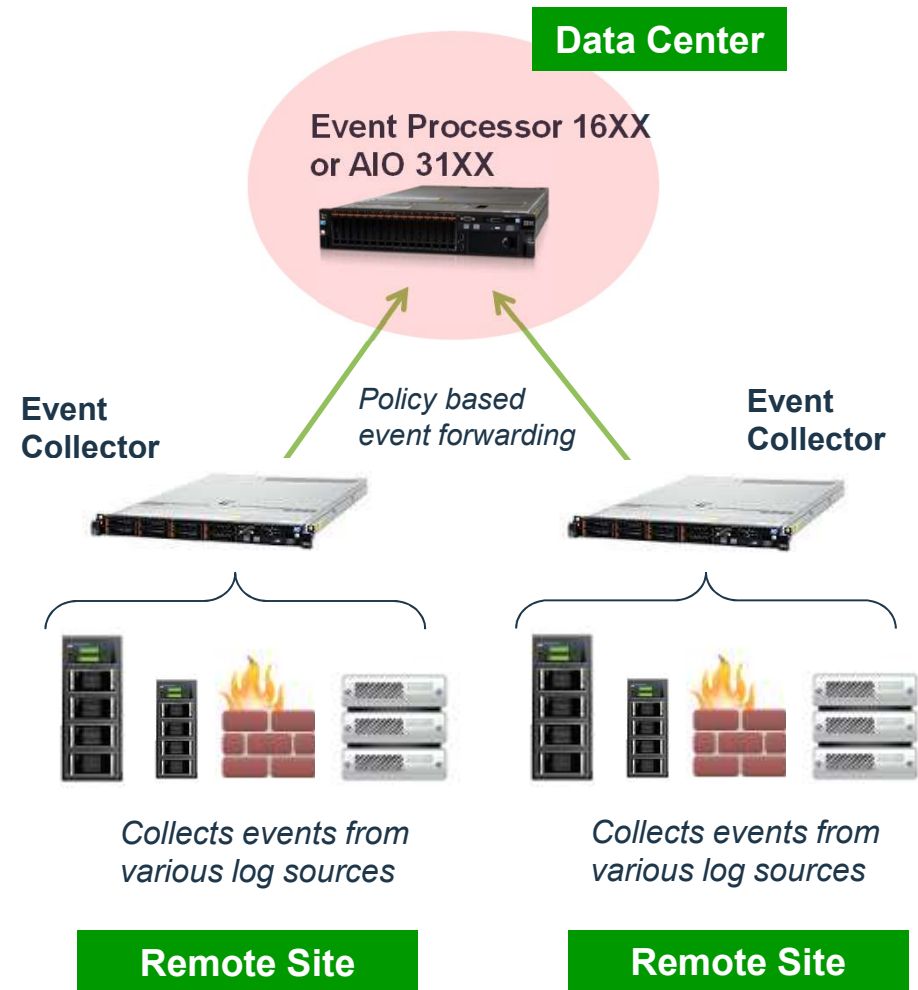
▪ Positioning

- Intended for customers with remote sites that have unreliable connectivity or constrained bandwidth, but still require reliable **event collection**, such as retail store/office, cruise ships, Naval vessels
- **Collects and parses events on a remote site, stores events temporarily, and forwards events (based on a policy) to an upstream Event Processor 16XX or All-in-1 31XX for analysis, correlation, and storage.**

▪ Characteristics and Capacity

- Software Supports up to 40K EPS but no license associated, and standard 1501 appliance should be limited to 15K EPS for best performance. EPS enforced by the license at the upstream Event Processor or AIO.

– **HA/DR NOT Available**



QFlow Collector 1201, 1202, 1301, and 1310 Appliances

▪ Positioning

- High capacity and scalable layer 7 application data collection for distributed deployment in a large/medium enterprise

▪ Characteristics and Capacity

- **Collect QFlow data through Span or Tap**
- Requires Flow Processor 17XX or All-in-One 31XX
- Performance depends on model:
 - 1201 – 1 Gbps
 - 1202 – 3 Gbps (Copper Inserts)
 - 1301 – 3 Gbps (Fiber Inserts)
 - 1310-SR – 10 Gbps (Short Range Inserts)
 - 1310-LR – 10 Gbps (Long Range Inserts)
 - 1202/1301-C – 3 Gbps (Copper & Fiber Inserts Included)
 - 1310SR/LR-C – 10 Gbps (Short and Long Range Inserts Included)

▪ Upgradability

- No upgrade available

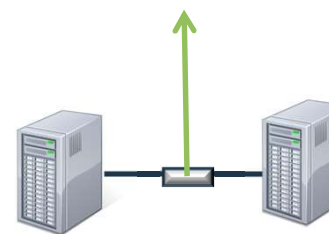
–HA/DR NOT available

QFlow Collector can send collected layer 7 application data to a Flow Processor or a Console directly.

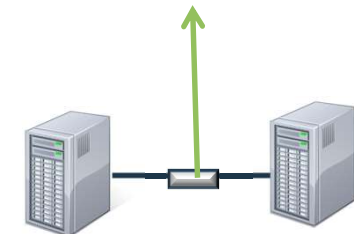
Flow Processor 17XX



All-In-One 31XX



Layer 7 data Analysis through Span or Tap



Layer 7 data Analysis through Span or Tap

Data Node 1405 and 1429 Appliances

Positioning

– Data Node is designed to be attached to a QRadar appliance to provide scalable data storage and search performance.

– Collected/processed event or flow data is distributed to the attached Data Nodes so data storage can be linearly increased. Searches from Console is also distributed to attached Data Nodes to boost performance.

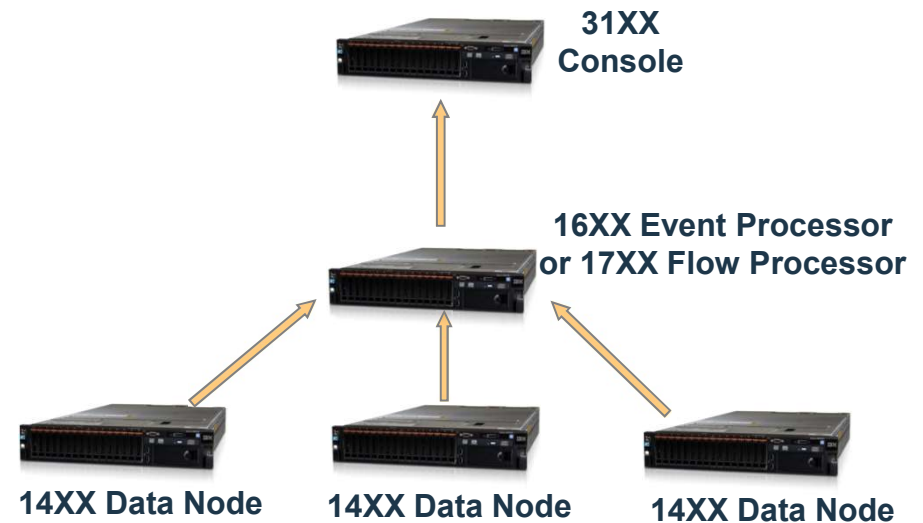
Characteristics and Capacity

- Based on QRadar Core Appliance xx05 or xx29.
- Multiple Data Modes can be attached to a single appliance EP 16XX, FP 17XX, Combo 18XX, or All-in-1 31XX
- There is no license associated with Data Node. EPS or Flow capacity is still controlled by the attached primary product.

Upgradability

- No upgrade available

HA / DR available



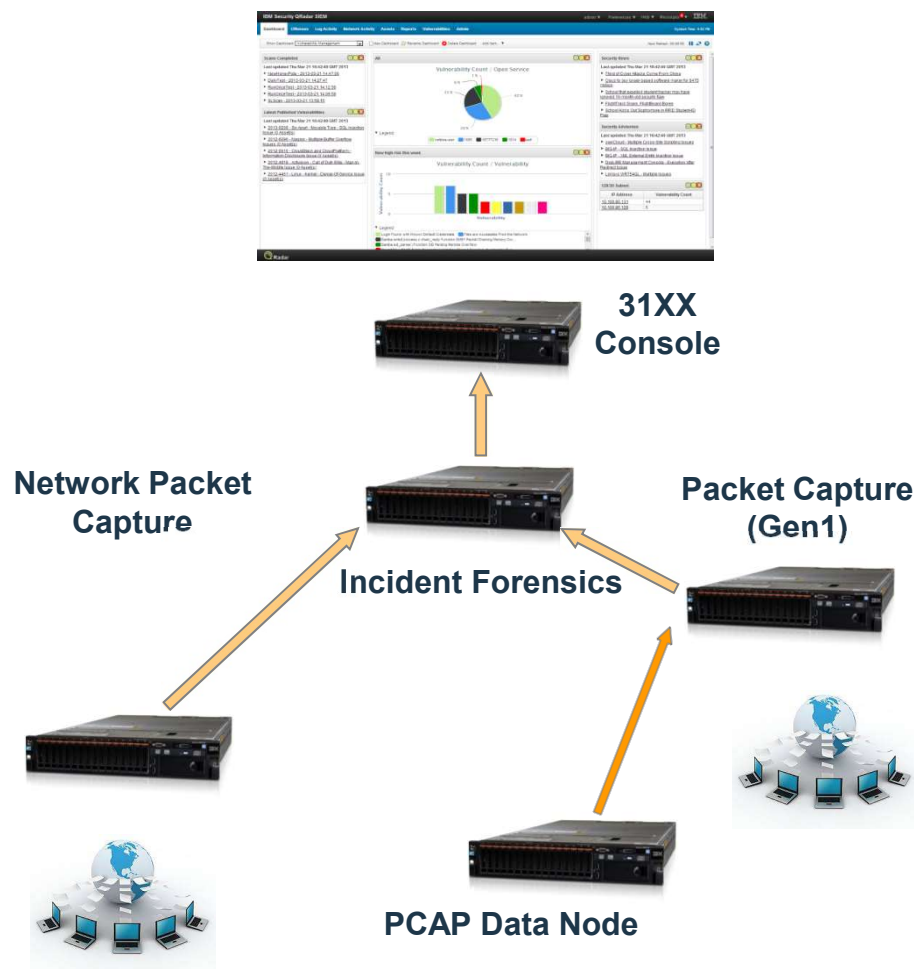
Packet Capture and Incident Forensics Appliances

Positioning

– Packet Capture appliance is to collect and store raw network packets. Incident Forensics appliance is used to reconstruct raw network packets to original format and quickly pinpoint the root cause of security incidents.

Characteristics and Capacity

- Based on the same hardware used for QRadar Core Appliances xx29 (but have different Core Appliance part numbers)
- No additional capacity license.
- Multiple Incident Forensics instances can be used in a QRadar deployment (All-in-1 or distributed)
- Multiple Packet Capture appliances can be used with a single Incident Forensics instance. Recommended maximum ratio is 5:1 but a higher ratio is possible.
- Two generations of PCAP technology currently available. Network PCAP is the preferred offering, but 1st generation can be offered with special approval.



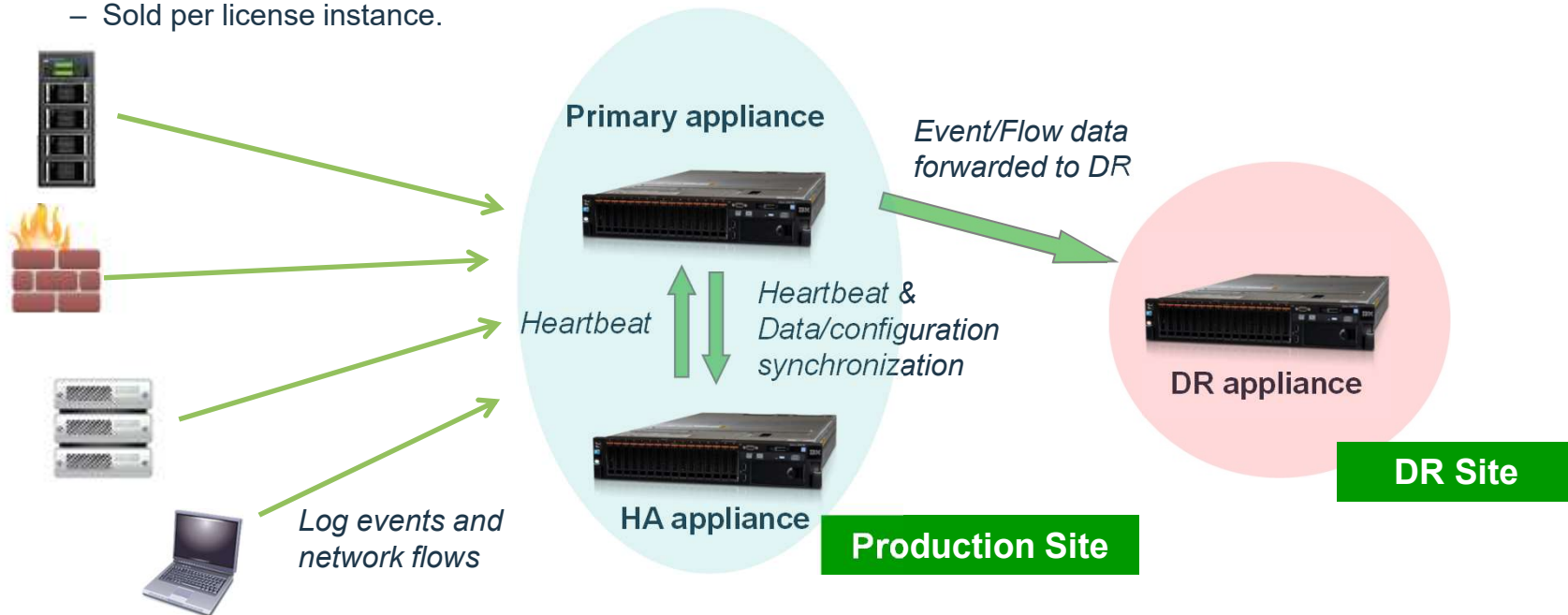
High Availability and Disaster Recovery

- High Availability

- HA appliance inherits the license from the Primary (no additional EPS/Flow increase purchase is needed).
- Data and configuration replicated from Primary appliance to HA appliance near real time.
- Failover to HA whenever Primary becomes unavailable.
- Sold per license instance.

- Disaster Recovery

- DR appliance provides redundant parallel system
- The same amount of EPS and Flows as Primary needs to be purchased for DR.
- Event and Flow Data from Primary to DR, but configuration is not copied over.





Virtual Appliances vs. Appliances (1/2)

- Appliances
 - All-in-One Appliances, Console, Event Processors, Flow Processors, Event & Flow Collectors, Risk Manager, Forensics and Packet Capture
- Virtual Appliances
 - “QRadar running on virtual hardware” = preconfigured ISO of “QRadar & OS” configured to deploy and run on VMware installed by customers themselves.
 - Tested and supported on VMware ESXi 5.0, 5.1, 5.5 and 5.6
 - Any VMware infrastructure (simple virtual machine, private cloud, public cloud) with appropriate hypervisor version is supported.
- Appliances & Virtual Appliances
 - Both delivered as an ISO (downloadable from PW)
 - Linux based, no operating system administration required.



Virtual Appliances vs. Appliances (2/2)

- Deployments can contain virtual & physical appliances in any combination
- Activation code will identify the type of system (i.e. virtual) at install time
- Storage Options (Online Data)
 - 2 options for QRadar Virtual Appliances:
 - Use local VM storage – easier, but lower performance
 - Use remote-mounted SAN/NAS
 - 2 options for QRadar Appliance:
 - Use onboard disks
 - Use SAN (fibre channel card required on Appliance)
- Virtualization Considerations
 - Majority of customer interest is in lower-end virtual deployments
 - Virtualization performance overhead for QRadar is not insignificant ~30%



Virtual/Software Appliance Specifications

- **Minimum System Specifications (Supports XX05 licensing):**
 - CPU:** 12 Core - 2.1 - 2.6 GHz
 - Memory:** 64 GB
 - Storage:** 6 to 40TB Available
 - IOPS:** 500-1,000
- **Medium System Specifications (Supports XX29 licensing):**
 - CPU:** 24 Core - 2.2 GHz
 - Memory:** 128GB-256GB
 - Storage:** Up to 96TB
 - IOPS:** 1,000-2,000
- **High Performance Unit System Specifications (Supports XX48 licensing):**
 - CPU:** 28 Core - 2.8 GHz
 - Memory:** 128GB-1TB
 - Storage:** Up to 96TB
 - IOPS:** 25,000-250,000



Virtual/Software Appliance Specifications

- **SMALL All-in-One and/or 1600 (Under 500 EPS):**

CPU: 6 core 2.6 GHz

Memory: 32 GB

Storage: 1.5TB to 6TB Available

IOPS: 250 – 500

- **Event/Flow Collectors:**

CPU: 4 core 2.6 GHz

Memory: 16 GB






Storage: 1.5TB Available

IOPS: 250-500



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



Using the Dashboard



Dashboard overview



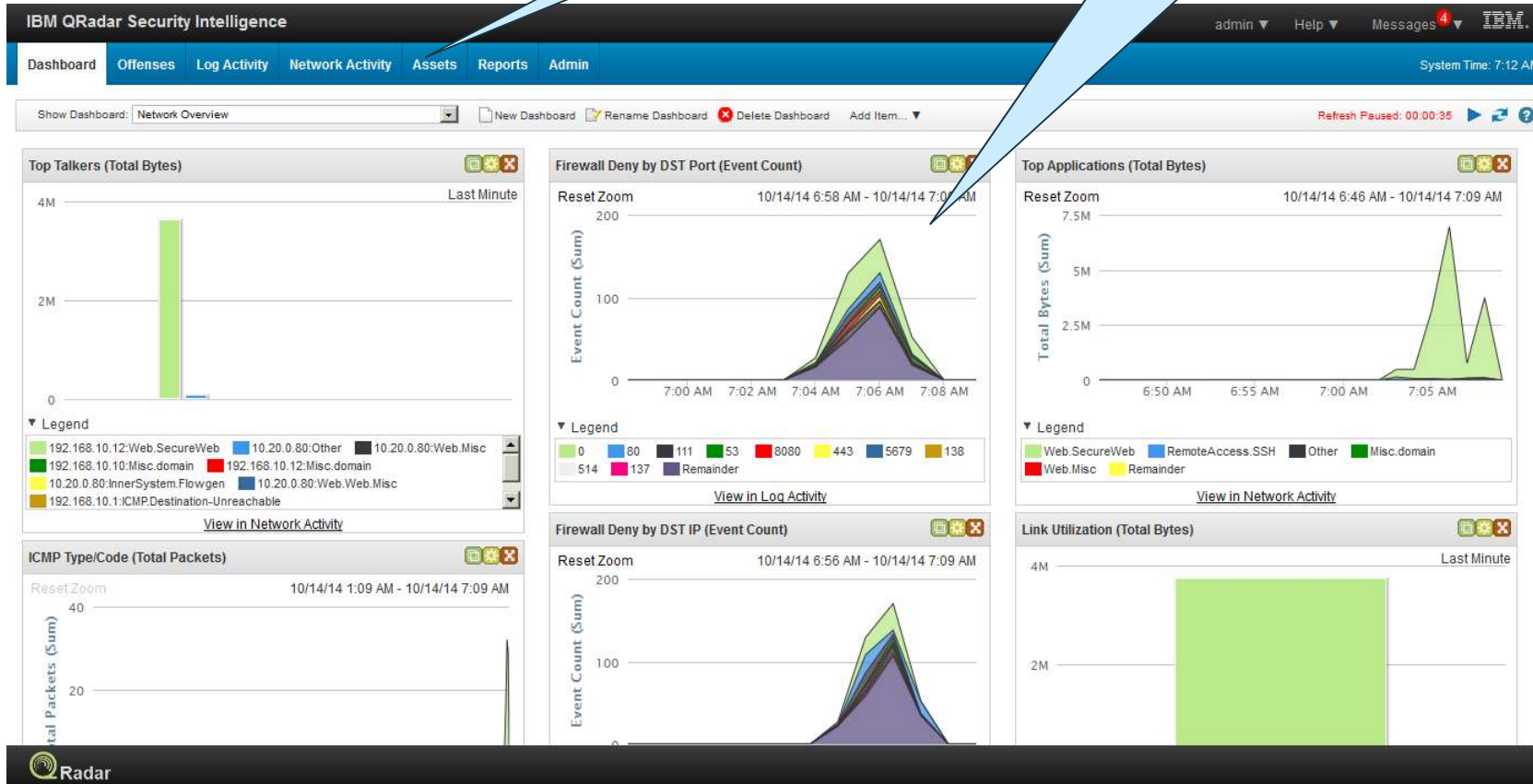
- QRadar SIEM shows the **Dashboard** tab when you log in
- Several default dashboards are available
- You can create multiple dashboards
- Each dashboard can contain items that provide summary and detailed information
- You can create custom dashboards to focus on your security or operations responsibilities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

Default dashboard

Click a tab to load it

Tabs



Tables and charts



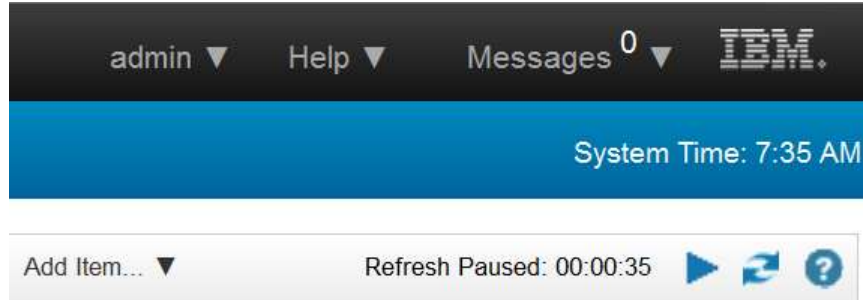
QRadar SIEM tabs



Use tabs to navigate the primary QRadar SIEM functions

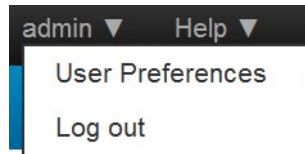
- **Dashboard:** The initial summary view
- **Offenses:** Displays offenses; list of prioritized incidents
- **Log Activity:** Query and display events 
- **Network Activity:** Query and display flows 
- **Assets:** Query and display information about systems in your network
- **Reports:** Create templates and generate reports
- **Admin:** Administrative system management
- **Other Tabs** – Vulnerability Management Risk Management, Incident Forensics (Requires Additional License), Apps installed from the App Exchange

Other menu options



The dashboard has the following additional menu options

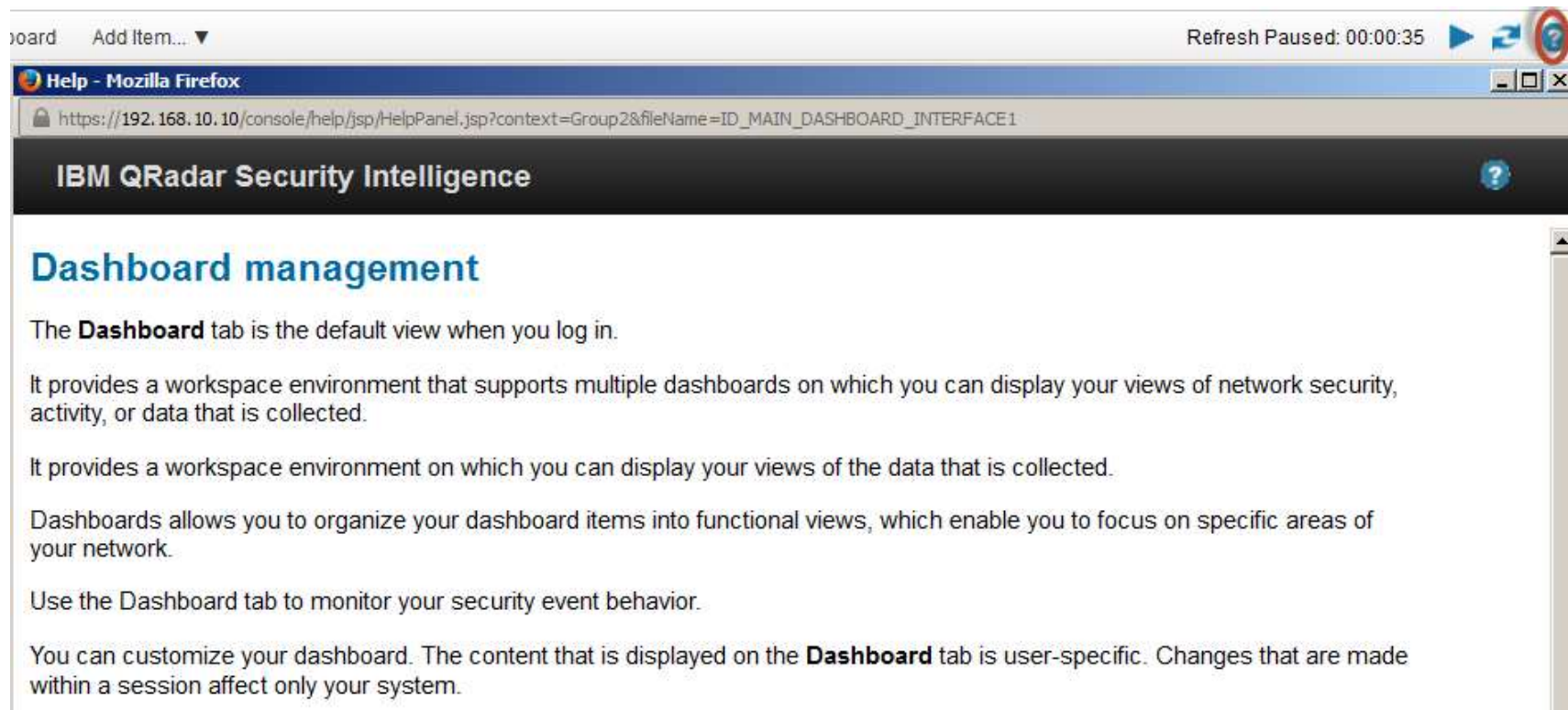
- **User Preferences**
- **Help**
- **Log out**



Name:	<input type="text" value="admin"/>
E-mail:	<input type="text" value="root@localhost"/>
Current Password:	<input type="password" value="*****"/>
New Password:	<input type="password" value="*****"/>
Confirm New Password:	<input type="password" value="*****"/>
Locale:	<input type="text" value=""/>
Enable Popup Notifications:	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

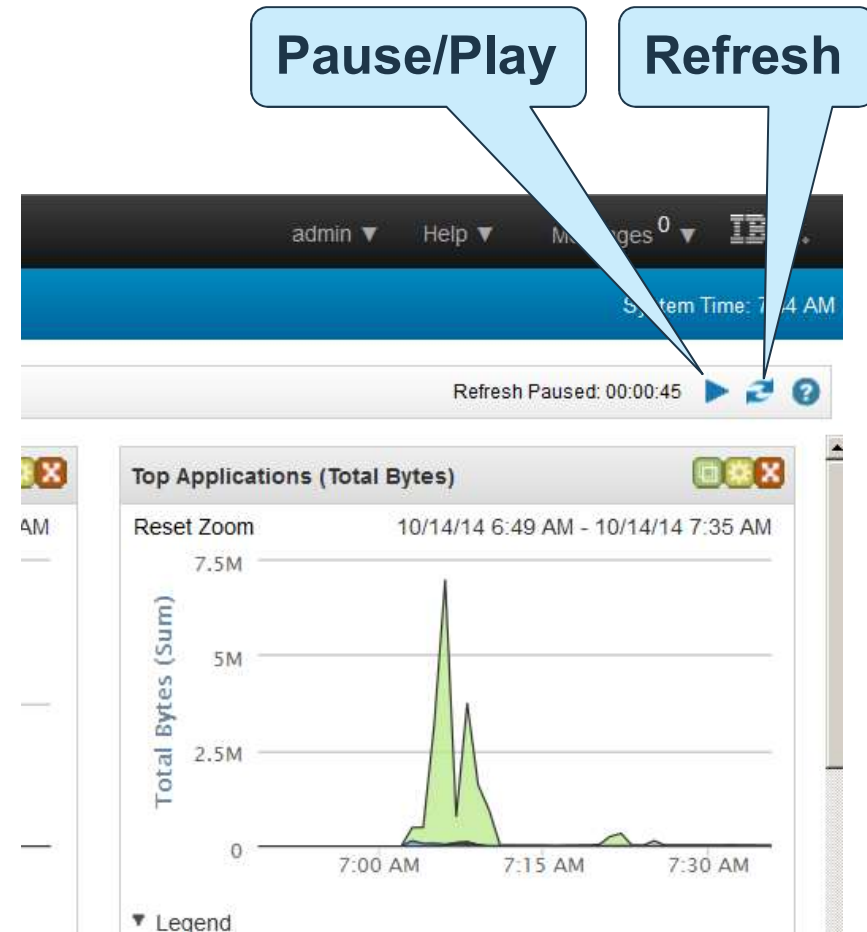
Context-sensitive help

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



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



Dashboard Types

- QRadar SIEM includes the following default dashboards
 - Application Overview
 - Compliance Overview
 - Network Overview
 - Risk Monitoring
 - System Monitoring
 - Threat and Security Monitoring
 - Virtual Cloud Infrastructure
 - Vulnerability Management
- Use multiple dashboards to better organize data

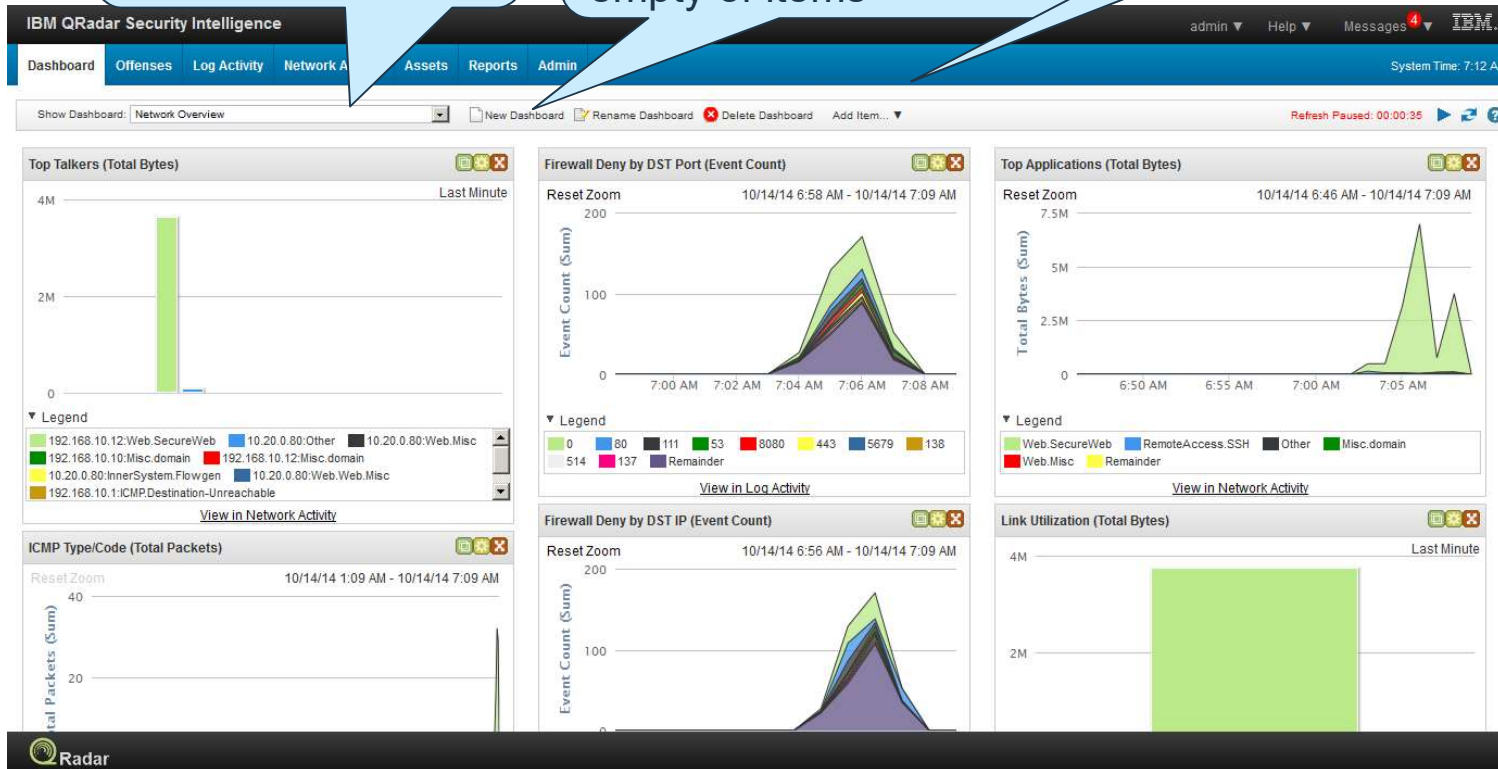


Creating a custom dashboard

Show Dashboard:
Select a dashboard to view

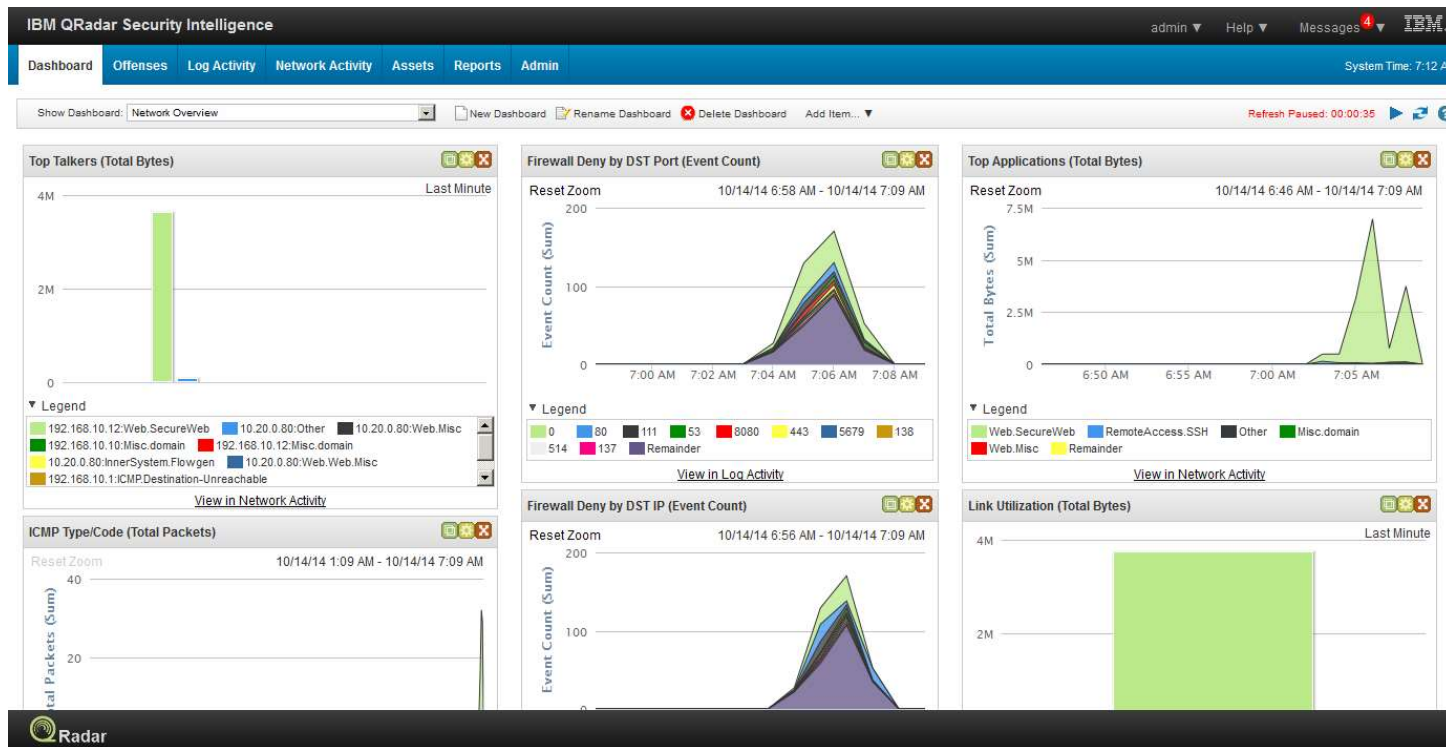
New Dashboard:
Create a new dashboard empty of items

Add item:
Add an item to dashboard



Dashboard - Items

- Include no more than 15 items on each dashboard



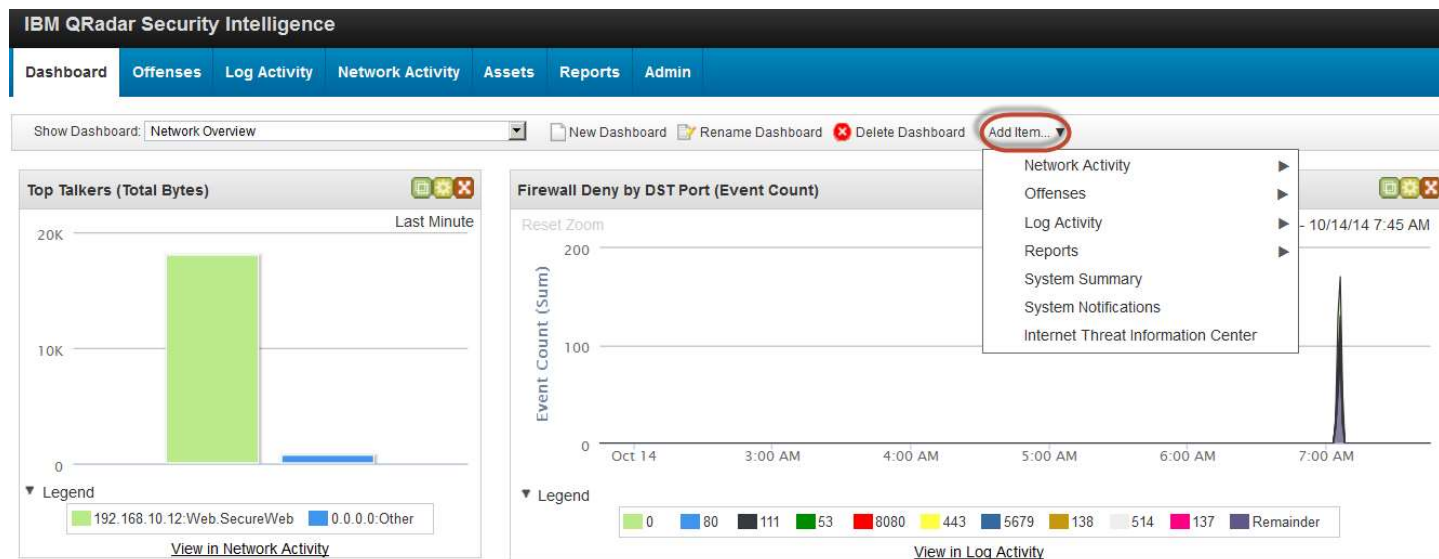
Managing dashboard items

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





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/@ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



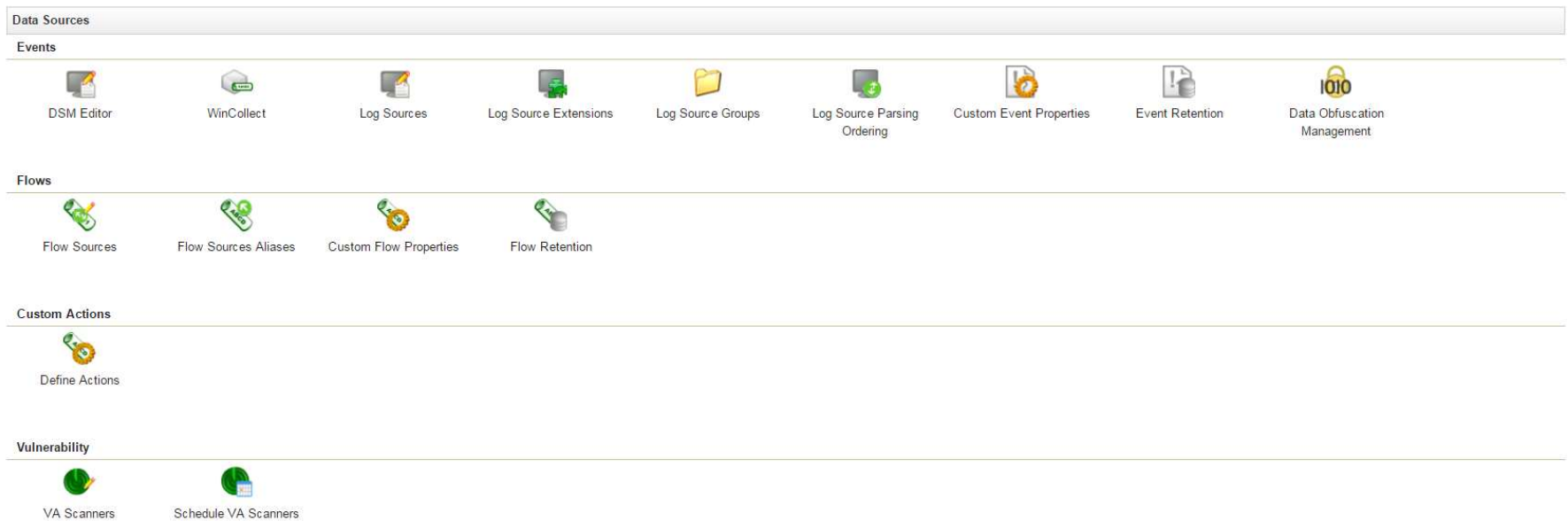


Data Sources




Collecting data: Data sources

Use the Data Sources tools to manage event, flow, and vulnerability data.



Log sources through traffic analysis

QRadar SIEM can automatically discover log sources in your deployment that send syslog-only messages to an Event Collector IP address.

 You have 32 of an allowable 750 active Log Sources as defined by your license

Name	Desc	Status ▲	Protocol	Group	Log Source Type
IBM zOS		Success	LogFileProtocol		IBM z/OS
Pers_DC		Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
Navy_DC		Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
Ref_DC		Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
WindowsAuthServer @ 9.16.1.2	WindowsAuthServer device	Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
WindowsAuthServer @ 9.168.1.4	WindowsAuthServer device	Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
OracleDbAudit @ 10.66.7.45	OracleDbAudit device	Error	Syslog		Oracle RDBMS Audit Record
Juniper JunOS Platform @ 9.168.1.8	Juniper JunOS Platform device	Error	Syslog		Juniper Junos OS Platform
FWSM @ 127.0.0.1	FWSM device	Error	Syslog		Cisco Firewall Services Module (FWSM)
Juniper JunOS Platform @ 10.69.1.1	Juniper JunOS Platform device	Error	Syslog		Juniper Junos OS Platform
WinSrv146		Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
Snort @ 10.73.1.114	Snort device	Error	Syslog		Snort Open Source IDS
OracleDbAudit @ 10.64.4.50	OracleDbAudit device	Error	Syslog		Oracle RDBMS Audit Record
OracleDbAudit @ 10.3.0.50	OracleDbAudit device	Error	Syslog		Oracle RDBMS Audit Record
WindowsAuthServer @ 9.168.1.1	WindowsAuthServer device	Error	Syslog	MSWindo...	Microsoft Windows Security Event Log

Adding log sources (1/2)



Log Sources

To add a log source:

1. In the Data Sources window, click the **Log Sources** icon.
2. Click the **Add** icon on the upper-right side of the window.
3. Select and complete the associated fields in the Add a log source pane.
4. Click **Save**.
5. Deploy the change.

Search For: Group All Log Source Groups Go Add Edit Enable/Disable

Name	Desc	Status	Protocol	Group	Log Source Type	Enabl
ASA @ 1...	ASA device	Success	Syslog		Cisco Adaptive Security Appliance (ASA)	True
CheckPo...	CheckPo...	Success	Syslog		Check Point FireWall-1	True
IBM IMS ...	IBM IMS ...	Success	Syslog		IBM IMS	True
IBMi @ 1...	IBMi device	Success	Syslog		IBM AS/400 iSeries	True

Add a log source

Log Source Name

Log Source Description

Log Source Type 3Com 8800 Series Switch

Protocol Configuration Syslog

Log Source Identifier

Enabled

Credibility 5

Target Event Collector eventcollector0 :: siemblue

Coalescing Events

Incoming Payload Encoding UTF-8

Store Event Payload

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

Save Cancel

Adding log sources (2/2)

Because it is dependent on the **Log Source Type** selected, the Add a log source pane expands to reflect the specific **Type** parameters and values used in QRadar SIEM.

Add a log source	
Log Source Name	<input type="text"/>
Log Source Description	<input type="text"/>
Log Source Type	Check Point FireWall-1
Protocol Configuration	OPSEC/LEA <input type="text"/>
Log Source Identifier	<input type="text"/>
Server IP	<input type="text"/>
Server Port	18184
Use Server IP for Log Source	<input checked="" type="checkbox"/>
Statistics Report Interval	600
Authentication Type	sslca <input type="text"/>
OPSEC Application Object SIC Attribute (SIC Name)	<input type="text"/>
Log Source SIC Attribute (Entity SIC Name)	<input type="text"/>
Specify Certificate	<input type="checkbox"/>
Certificate Authority IP	<input type="text"/>
Pull Certificate Password	<input type="text"/>
OPSEC Application	<input type="text"/>
Enabled	<input checked="" type="checkbox"/>
Credibility	5 <input type="text"/>
Target Event Collector	eventcollector0 :: siemblue <input type="text"/>
Coalescing Events	<input checked="" type="checkbox"/>
Store Event Payload	<input checked="" type="checkbox"/>

Adding log source extensions



Log Source Extensions

- Log source extensions immediately extend the parsing routines of specific devices.
- **Note:** You must use a log source extension to detect an event that has missing or incorrect fields.
- A log source extension can also parse an event when the DSM it is attached to fails to produce a result.
- You must create the extension document before you can define a log source extension within QRadar SIEM.
- If you use the DSM Editor tool, Log Source Extensions are automatically created and uploaded (recommended)

Log source parsing order

- You can configure the order that you want each Event Collector in your deployment to use to apply DSMs to log sources.
- If a log source has multiple **Log Source Types** under the same IP address or host name, you can order the importance of these incoming log source events by defining the parsing order.



Log Source
Parsing
Ordering

Log Source Host:

Filter:

10.0.120.10
10.0.82.11
10.0.82.21
10.0.82.22
10.0.82.29

Or...	Name	Log Source Type	Enabled	Configuration
1	IBMAIXServer @ 10.0.120.10	IBMAIXServer	true	Syslog :: IBMAIXServer @ 10.
2	OracleOSAudit @ 10.0.120.10	OracleOSAudit	true	Syslog :: IBMAIXServer @ 10.
3	LinuxServer @ 10.0.120.10	LinuxServer	false	None


Up

Down

Top

Bottom

Other Supported Formats

- Universal CEF
 - Accepts events from any device that produces events in the Common Event Format (CEF) from Syslog or Log File
- Universal LEEF 
 - Accept events from devices that produce events using the Log Event Extended Format (LEEF) from Syslog or Log File
 - Proprietary event format, which allows hardware manufacturers and software product manufacturers to read and map device events specifically designed for QRadar integration
 - Both Universal CEF and LEEF events must be mapped. They do not contain QID (Qradar Identifier) to categorize events

Managing flow sources



- QRadar SIEM accepts external flow data from various sources such as the following accounting technologies:
 - **NetFlow**: Protocol defined by Cisco to share accounting information from switches and routers
 - **IPFIX**: Protocol defined by IETF to share accounting information from switches and routers (NetFlow V9 resembles IPFIX)
 - **sFlow**: Advanced packet sampling technique and protocol used for network monitoring
 - **J-Flow**: Packet sampling technique and protocol developed by Juniper
 - **Packeteer**: Protocol developed by Bluecoat that is used for bandwidth management
 - **Flowlog** file: A flow log file as stored in the Ariel data structure
- QRadar SIEM accepts internal flow data from the NICs using qFlow, Napatech, and Endace.



Adding a flow source



Flow Sources

- QRadar SIEM automatically adds default flow sources for physical ports on the appliance and includes a default NetFlow flow source.
- In the Data Sources window, click the **Flow Sources** icon.

The screenshot shows the 'Add Flow source' dialog box in QRadar SIEM. The dialog has a toolbar with 'Add', 'Edit', 'Enable', and 'Delete' buttons. A callout points to the 'Add' button with the text 'Click Add.'. Below the toolbar is a table with columns 'Name', 'Flow Source Type', and a checkbox column. The table contains two rows: 'default_Netflow' with type 'Netflow v.1/v.5/v.7/v.9' and checkbox 'true', and 'Network Interface' with type 'Network Interface' and checkbox 'true'. A callout points to the 'Flow Source Type' column with the text 'Flow Source Type: Select a Flow Source Type.'. To the right of the table is the 'Flow Source Details' section. It includes a 'Flow Source Name' field, a 'Target Flow Collector' dropdown (set to 'qflow0 :: siemblue'), a 'Flow Source Type' dropdown (set to 'Flowlog File'), an 'Enable Asymmetric Flows' checkbox, and a 'Flowlog File Configuration' section with a 'Source File Path' field. A callout points to the 'Flowlog File Configuration' section with the text 'Source File Path: Enter the location of the flow file.'. At the bottom right of the dialog are 'Save' and 'Cancel' buttons. A callout points to these buttons with the text 'Click Save and then Deploy Changes.'.

Name	Flow Source Type	
default_Netflow	Netflow v.1/v.5/v.7/v.9	true
Network Interface	Network Interface	true

Flow Source Details

Flow Source Name:

Target Flow Collector: qflow0 :: siemblue

Flow Source Type: Flowlog File

Enable Asymmetric Flows

Flowlog File Configuration

Source File Path:

Save Cancel

Adding a flow source with asymmetric routing

In some networks, traffic is configured to take different paths for inbound and outbound traffic. QRadar can combine the traffic into a single flow.

Flow Source Details

Flow Source Name	COE
Target Flow Collector	qflow0 :: COE
Flow Source Type	Network Interface
<input checked="" type="checkbox"/> Enable Asymmetric Flows	

Network Interface Configuration

Flow Interface	eth0
<input type="checkbox"/> Filter String	

Save Cancel

Callouts:

- Choose a **Flow Source Type**.
- Click **Enable Asymmetric Flows**.
- Complete these fields.
- Click **Save** and then **Deploy Changes**.

Flow source aliases



Flow Source
Aliases

- You can configure a virtual name (or alias) for flow sources.
- Using the source IP address and virtual name, you can identify multiple sources being sent to the same QRadar QFlow Collector.
- QRadar QFlow Collector can use an alias to uniquely identify and process data sources being sent to the same port.

Note: Use the Deployment Actions in System and License Management to configure the QRadar QFlow Collector to automatically detect flow-source aliases.

Adding a flow source alias

To add a flow source alias:






1. Click the **Admin** tab.
2. Click the **Flow Aliases** icon.

The screenshot shows a web interface for adding a flow source alias. At the top, there is a toolbar with 'Add', 'Edit', and 'Delete' icons. Below this is a table with columns for 'IP' and 'Autodiscovered'. A callout box points to the 'Add' icon with the text 'Click **Add**.' Below the table is a form titled 'Add Flow Source Alias' with two input fields: 'IP' and 'Name'. Callout boxes provide instructions for these fields: 'IP: Type the IP address of the flow source alias.' and 'Name: Type a unique name for the flow source alias.' At the bottom right of the form are 'Save' and 'Cancel' buttons. A callout box points to these buttons with the text 'Click **Save** and then **Deploy Changes**.'



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.





Investigating event details



Navigating to the Events



- Events can be accessed from different tabs

Event Name	Log Source	Event Count	Time
SERVER-MAIL Novell GroupWise client IMG SRC buffer overflow	Snort @10.2.2.126	1	Jan 19, 2016, 4:04:57 PM

- Normalized Event data
 - Event Name, Log Source, Event Count, Time, Low Level Category,
 - Source IP, Source Port, Destination IP, Destination Port
 - Username
 - Magnitude

Navigating to the Events

In the Log Activity Tab, click pause to view a list of events.

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

Using Search: Default-Student

Current Filters:
 Event Name is not Unknown log event (Clear Filter) Event Name is not API request successful (Clear Filter) Log Source is not SIM Audit-2 :: Dooku (Clear Filter)
 Log Source is not System Notification-2 :: Dooku (Clear Filter) Log Source is not Health Metrics-2 :: janus (Clear Filter)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.44	64935	220.173.137.218	13982	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.21	54346	208.81.234.2	80	N/A
Firewall Deny	Check Point @ drop	1	Jan 18, 2017, 8:39:3...	Firewall Deny	85.246.105.142	54523	10.0.66.10	137	N/A
Firewall Deny	Check Point @ drop	1	Jan 18, 2017, 8:39:3...	Firewall Deny	61.183.15.9	12200	10.0.66.23	8080	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.18	53386	64.236.144.246	80	N/A
Firewall Deny	Check Point @ drop	1	Jan 18, 2017, 8:39:3...	Firewall Deny	85.246.105.142	54523	10.0.66.4	137	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.25	52975	68.142.110.119	80	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.9	64935	82.176.211.31	55059	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.34	64935	212.64.162.184	51394	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.21	54345	77.91.248.30	80	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.18	53385	64.236.144.246	80	N/A
Firewall Deny	Check Point @ drop	1	Jan 18, 2017, 8:39:3...	Firewall Deny	65.112.145.30	428	10.0.66.10	137	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.25	52974	207.46.148.35	80	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.34	64935	58.240.96.238	37074	N/A
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:39:3...	Firewall Permit	10.0.66.9	64935	95.133.229.49	25072	N/A

List of events

Viewing Records over time creates a time series chart



Event Name	Log Source	Even Cour	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina: Port
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:43:5...	Firewall Permit	10.0.66.25	64935	84.25.39.141	34194
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:43:5...	Firewall Permit	10.0.66.9	64935	207.6.233.111	61738
Firewall Deny	Check Point @ drop	1	Jan 18, 2017, 8:43:5...	Firewall Deny	209.204.126.162	37	10.0.66.23	137
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:43:5...	Firewall Permit	10.0.66.46	64935	71.9.133.250	33855
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:43:5...	Firewall Permit	10.0.66.21	64935	89.19.168.0	23859
Firewall Permit	Check Point @ accept	1	Jan 18, 2017, 8:43:5...	Firewall Permit	10.0.66.44	64935	93.116.73.240	46373


View event details by double-clicking a row

Event details: Base information

Event Information:
Similar offense parameters

Event Information							
Event Name	Firewall Permit						
Low Level Category	Firewall Permit						
Event Description	Firewall Permit						
Magnitude	 (3)	Relevance	6	Severity	0	Credibility	5
Username	N/A						
Start Time	Jan 18, 2017, 8:43:59 PM	Storage Time	Jan 18, 2017, 8:43:59 PM	Log Source Time	Jan 1, 2017, 11:56:01 AM		
Policy	N/A						
Domain	Default Domain						

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	10.0.66.9	Destination IP	 207.6.233.111
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	64935	Destination Port	61738
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
IPv6 Source	0:0:0:0:0:0:0:0	IPv6 Destination	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Event details: Reviewing the raw event

Each normalized event carries its raw event

Payload Information

utf hex base64

Wrap Text

```
Jan 1 11:56:01 accept COMPANYFW >eth0 inzone: Internal; outzone: External; rule: 5; rule_uid: {38A7A90D-579E-4B9D-9FE7-66E625272E74}; src: %SRCIP%; dst: 207.6.233.111; proto: udp; xlatesrc: %NATIP%; NAT_rulenum: 4; NAT_addr: 1 & FireWall-1; service: 61738; s_port: 64935; xlatesport: 44989;
```

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

Event details: Additional details

QID Determines the Name, Low level and High Level Category

Protocol: Network Protocol

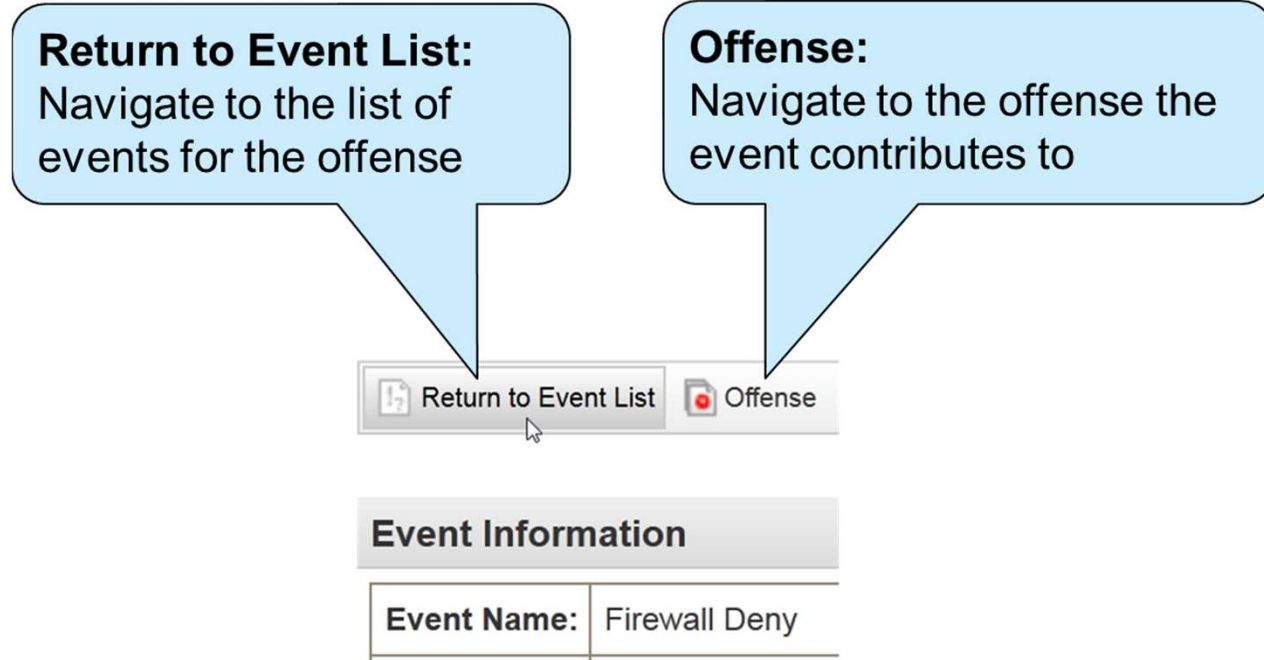
Log source that originated event

Additional Information			
Protocol	udp_ip	QID	2750008
Log Source	Check Point @ accept	Event Count	1
Custom Rules	BB:ProtocolDefinition: Windows Protocols BB:CategoryDefinition: Firewall or ACL Accept BB:DeviceDefinition: FW / Router / Switch Magnitude Adjustment: Destination Network Weight is Low Magnitude Adjustment: Context is Local to Remote Magnitude Adjustment: Source Network Weight is Low BB:Local To Remote Compliance:Load ISO 27001 Building Blocks BB:NetworkDefinition: Client Networks System: Load Building Blocks		
Custom Rules Partially Matched	System: Device Stopped Sending Events (Firewall, IPS, VPN or Switch)		
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. Relevance has been decreased by 2 because the source network weight is low.		

Rules triggered by the event

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





Building a Search to Investigate Events



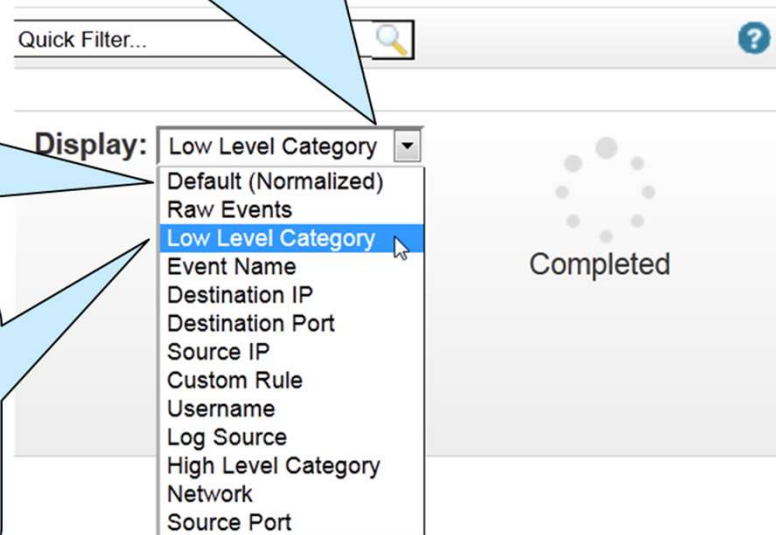
Group Events

Group search results to improve output

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

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

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



Grouping events by low-level category

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

In this example, exploring by grouping indicates a second protocol

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

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

Grouping events by protocol

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

Grouping By:
QRadar SIEM can group by Protocol

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

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

Grouping By:
Protocol

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

► **Current Statistics**

(Show Charts)

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

Removing grouping criteria

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

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

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

Viewing and changing 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

The screenshot displays a web interface for viewing events. At the top, there are navigation links: 'Save Results', 'Cancel', 'False Positive', 'Rules', and 'Actions'. A 'Next Refresh: 00:00:55' timer is visible, along with a play/pause icon and a refresh icon. A search bar is located on the right. Below the search bar, there is a 'Select An Option:' dropdown menu with the following options: 'Real Time (streaming)', 'Last Interval (auto refresh)', 'Last 5 Minutes', 'Last 15 Minutes', 'Last 30 Minutes', 'Last 45 Minutes', 'Last Hour', 'Last 3 Hours', 'Last 6 Hours', 'Last 12 Hours', 'Last 24 Hours', 'Last 3 Days', and 'Last 7 Days'. The 'Last Interval (auto refresh)' option is currently selected. To the right of the dropdown, there is a 'Display:' dropdown set to 'Default (Normalized)' and a 'Result' label. Below these, there is a 'Student view' section with a 'Duration' of '108ms' and a 'More Details' link. A 'Completed' status is shown. At the bottom, there is a table with columns: 'Time', 'Low Level Category', 'Source IP', 'Source Port', 'Destination IP', and 'Destin Port'. The table content is mostly obscured by a dark bar at the bottom of the screenshot.

Pause/Play Refresh

Monitoring the scanning host (1 of 3)

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

Clear Filter:
To monitor all traffic, remove the offense filter

Current Filters:
Offense is Local ICMP Scanner , Excessive Firewall Denies Across Multipl... (Clear Filter)

Filter:
Right-click the Source IP to filter

(Show Charts)

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

Monitoring the scanning host (2 of 3)

The image shows a user interface for monitoring a scanning host. It features two dropdown menus: 'View' and 'Display'. The 'View' menu is open, showing options from 'Select An Option:' to 'Last 7 Days', with 'Last 24 Hours' selected. The 'Display' menu is also open, showing options from 'High Level Category' to 'Source P', with 'High Level Category' selected. Two callout boxes provide context: one for the 'View' selection and one for the 'Display' selection.

View: Select An Option: [v]
Select An Option:
Real Time (streaming)
Last Interval (auto refresh)
Last 5 Minutes
Last 15 Minutes
Last 30 Minutes
Last 45 Minutes
Last Hour
Last 3 Hours
Last 6 Hours
Last 12 Hours
Last 24 Hours
Last 3 Days
Last 7 Days

Display: High Level Category [v]
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 P



View:
List events of the last 24 hours

Display:
Group by High Level Category

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

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

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

Grouping By:

High Level Category

Current Filters:

Source or Destination IP is 10.127.15.37 [\(Clear Filter\)](#)

► Current Statistics

[\(Show Charts\)](#)

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

Filtering events (1 of 3)

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

	Event Name	Log Source	Event Count
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny		1
	Firewall Deny		1
	Firewall Deny		1
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	CheckPoint @ FW-1Machine	1
	Firewall Deny	CheckPoint @ FW-1Machine	1

Filter on Event Name is Firewall Deny










Filter on Event Name is not Firewall Deny

False Positive



Filtering events (2 of 3)

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

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

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

Filtering events (3 of 3)

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

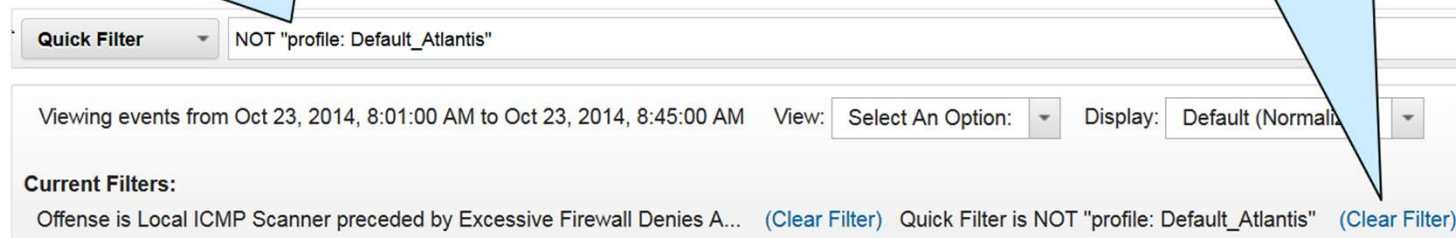
Unlike searches, filters do not query each event processor

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



The screenshot shows a security dashboard interface. At the top, there is a "Quick Filter" dropdown menu set to "NOT 'profile: Default_Atlantis'". Below this, the dashboard displays event information: "Viewing events from Oct 23, 2014, 8:01:00 AM to Oct 23, 2014, 8:45:00 AM". There are also "View:" and "Display:" dropdown menus. Under the "Current Filters:" section, two filters are listed: "Offense is Local ICMP Scanner preceded by Excessive Firewall Denies A..." and "Quick Filter is NOT 'profile: Default_Atlantis'". Each filter has a "(Clear Filter)" link next to it.

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



A screenshot of a software interface for creating filters. On the left is a list of event fields: Destination IP, Quick Filter, Source or Destination IP, Category, Destination Asset Name, Destination IP (highlighted in blue), Destination Port, Log Source, Log Source Group, Source Asset Name, Source IP, Event Name, Anomaly Alert Value, Source or Destination MAC Address, Any IP, Any Port, Associated With Offense, Credibility, Custom Rule, Custom Rule Partially Matched, and Custom Rule Partial or Full Matched. On the right, a filter configuration area shows a dropdown menu set to "Does not equal any of" with the value "200.142.144.0/24" and a plus sign. Below this, a text box contains the filter rule: "Destination IP is not 200.142.143.0/24". At the bottom of the configuration area are buttons for "Remove Selected", "Add Filter", and "Cancel".

Saving search criteria

Save the search with the criteria specified

Please enter the name of this search below.

Search Name: Dept - 10.127.15.37

Assign Search to Group(s) Manage Groups

Prepend name with department name or initials for easy identification

Assign to group

Timespan options:

Last Interval (auto refresh) Recent Specific Interval

Last 24 Hours

Start Time 7/30/2013

End Time 7/31/2013

Set as default search for the Log Activity tab

Include in my Quick Searches Set as Default

Share With Everyone Include in my Dashboard

Allows you to add the search as an item to a dashboard

OK Cancel

The screenshot shows a configuration window for saving search criteria. At the top, there is a text input field for the search name, which contains 'Dept - 10.127.15.37'. To the right, there is a section for assigning the search to a group, with a tree view showing various system components. The 'Usage Monitoring' component is selected. Below this, there are radio buttons for 'Last Interval (auto refresh)', 'Recent', and 'Specific Interval'. The 'Recent' option is selected, and a dropdown menu shows 'Last 24 Hours'. Further down, there are fields for 'Start Time' (7/30/2013) and 'End Time' (7/31/2013). At the bottom, there are several checkboxes: 'Include in my Quick Searches' (checked), 'Share With Everyone' (checked), 'Set as Default' (unchecked), and 'Include in my Dashboard' (checked). The window ends with 'OK' and 'Cancel' buttons.

Event list using the saved search

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

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**

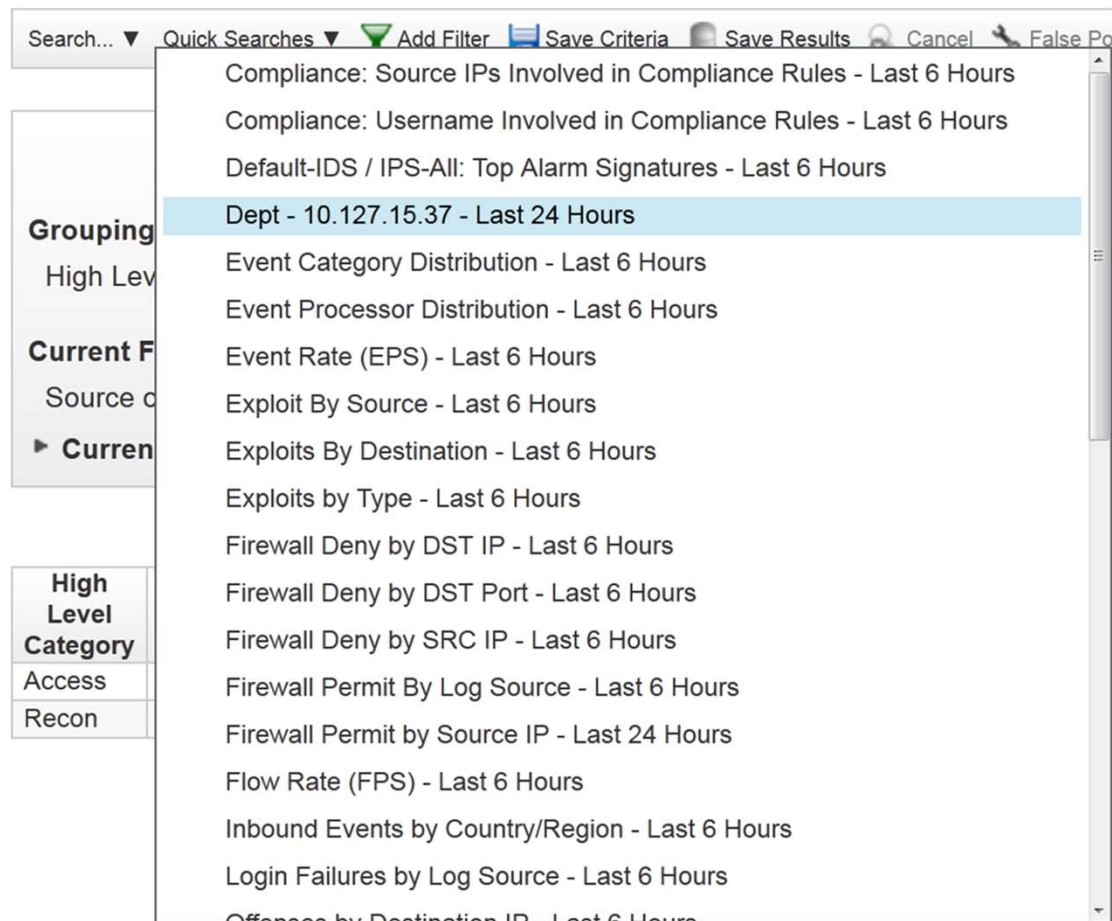
(Show Charts)

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

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

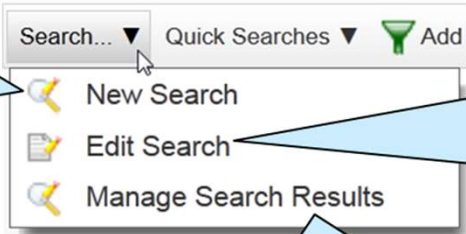
About Quick Searches

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



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



The image shows a screenshot of the 'Search' menu in the QRadar SIEM interface. The menu is open, showing three options: 'New Search', 'Edit Search', and 'Manage Search Results'. Each option is accompanied by a magnifying glass icon. The menu is located in the top right corner of the interface, next to a search bar and a 'Quick Searches' dropdown. Three callout boxes provide detailed information about each menu option.

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

Finding and loading a saved search

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

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

Saved Searches Group:

Type Saved Search or Select from List

Available Saved Searches

- Default-VPN-VPNGateway: Top Time Connected by IP
- Default-VPN-VPNGateway: Top Time Connected by User
- Default-VPN-VPNGateway: Top Users by #s of Connections
- Default-VPN-VPNGateway: Warnings
- Dept - 10.127.15.37**
- DOS Attacks by Destination IP

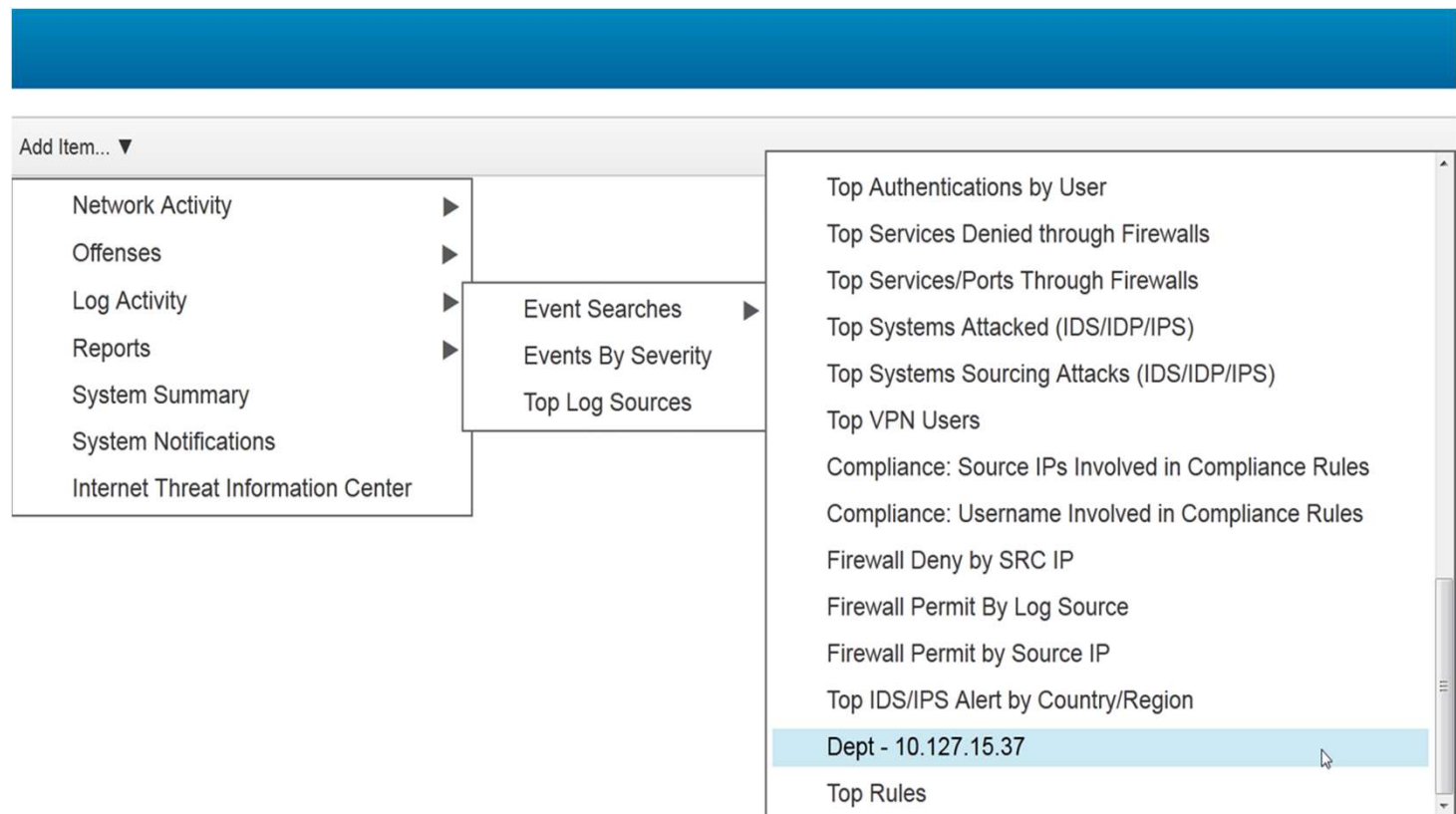
Search actions

The image shows a screenshot of a search interface with an 'Actions' dropdown menu open. The menu items are: 'Show All' (with a green checkmark icon), 'Export to XML' (with a right-pointing triangle icon), 'Export to CSV' (with a right-pointing triangle icon), 'Delete' (with a red 'X' icon), 'Notify' (with an envelope icon), and 'Print' (with a printer icon). A 'Quick Filter...' input field is visible to the right of the menu. Five callout boxes provide descriptions for the actions:

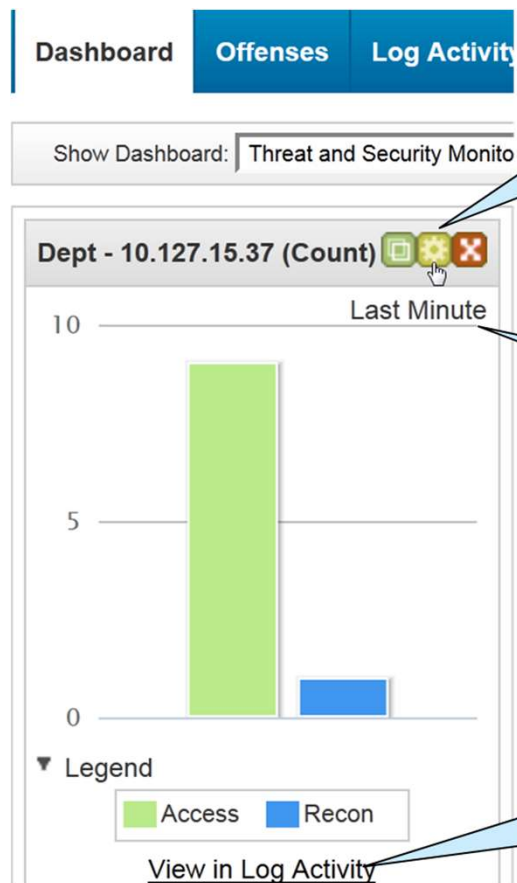
- Show All:** Clear all filters
- Delete:** Delete the result of the currently displayed search
- Export:** You can resend exported events as raw events to QRadar SIEM
- Notify:** Send an email when the search in progress finishes

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



Viewing the saved search in the Dashboard



Settings button:
Modify the settings
of an item

You can add only
grouped searches as
dashboard items

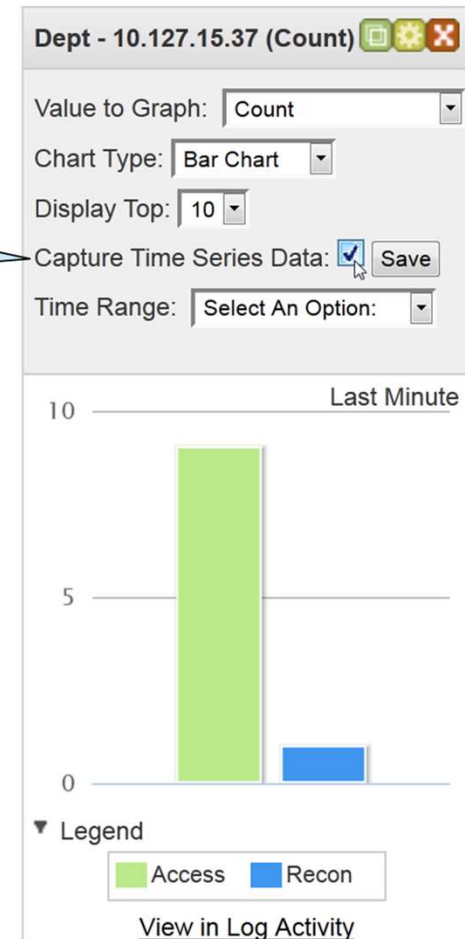
Last Minute:
Unless time-series data is captured,
the dashboard item shows only the
result of the last 1-minute interval

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

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



Selecting the time range

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

Time Range:
Select Last 24 Hours

Dept - 10.127.15.37 (Count) [Close] [Settings] [Refresh]

Value to Graph: * Count

Chart Type: Bar Chart

Display Top: 10

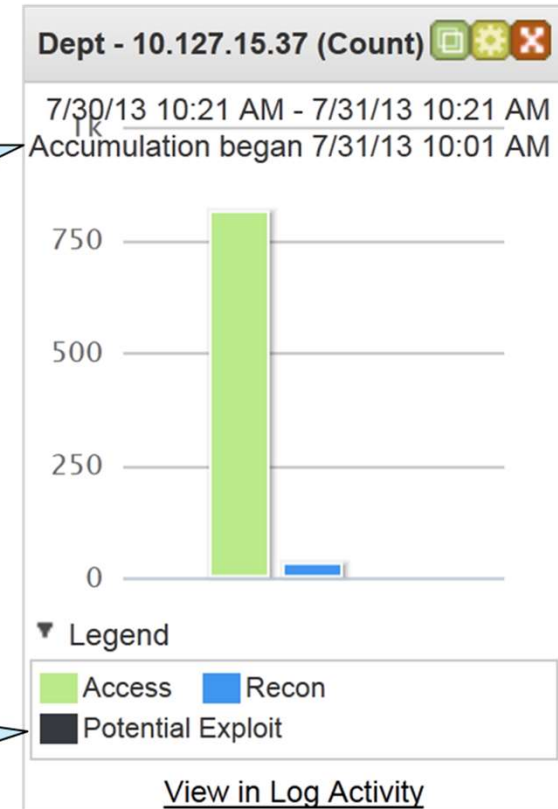
Capture Time Series Data: Save

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

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

Modifying items in the chart type table

Chart Type: Table

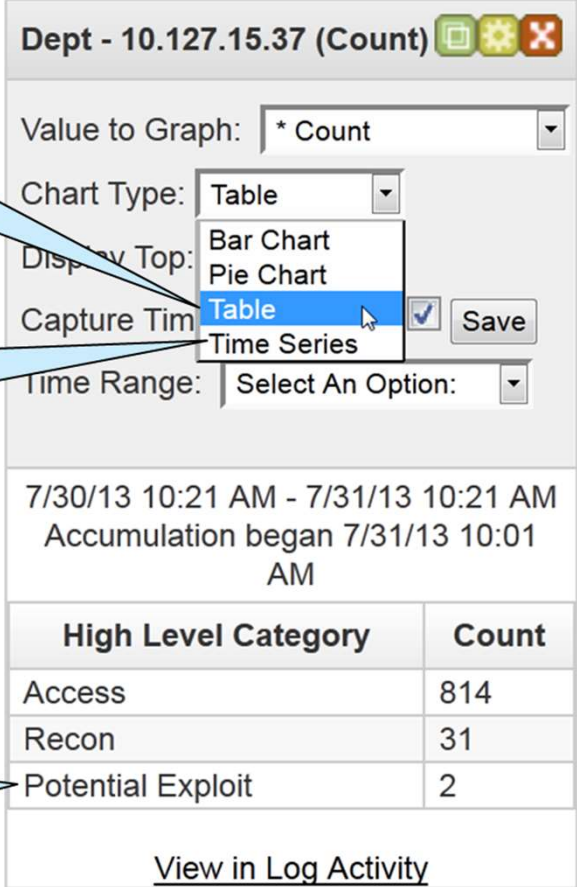
To view all high-level categories, select the chart type **Table**

Chart Type: Time Series

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

Potential Exploit:

Two events of high-level category Potential Exploit



Dept - 10.127.15.37 (Count)

Value to Graph: * Count

Chart Type: Table

Display Top: []

Capture Time: []

Time Range: Select An Option:

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

High Level Category	Count
Access	814
Recon	31
Potential Exploit	2

[View in Log Activity](#)



Ariel Query Language (AQL)



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 user interface for an "Advanced Search" feature. On the left, there is a dropdown menu labeled "Advanced Search" with a downward arrow. To its right is a text input field containing the query: `select * from events where sourceip ='10.35.87.134' LAST 4 HOURS`. The text is color-coded: `select` is blue, `*` is black, `from` is blue, `events` is black, `where` is blue, `sourceip` is black, `=` is black, `'10.35.87.134'` is orange, `LAST` is blue, `4` is black, and `HOURS` is blue. To the right of the input field is a button labeled "Search".

Additional AQL examples

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

Advanced Search Search

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

Advanced Search Search

- 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 Search



Investigating Flows





About flows

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

Network Activity tab

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

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

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

► **Current Statistics**

Application	Source IP (Unique Count)	Source (Unique Count)	Destination IP (Unique Count)
other	Multiple (18)	Multiple (18)	Multiple (16)
Multimedia.Intellex	10.20.0.80	Net_10_0_0_0	Multiple (6)
FileTransfer.NETBIOS	192.168.10.1	Net_192_168_10_1	192.168.10.255
Web.SecureWeb	Multiple (2)	Net_10_0_0_0	Multiple (10)
P2P.BitTorrent	10.20.0.80	Net_10_0_0_0	Multiple (16)
InnerSystem.Flowgen	10.20.0.80	Net_10_0_0_0	Multiple (24)
Web.Misc	Multiple (3)	Net_10_0_0_0	Multiple (15)
Misc.domain	Multiple (23)	Multiple (2)	Multiple (3)
DataTransfer.WindowsFileSharing	Multiple (3)	Multiple (3)	Multiple (3)
VoIP.Skype	10.10.0.80	Net_10_0_0_0	Multiple (17)
RemoteAccess.MSTerminalServ...	10.10.0.80	Net_10_0_0_0	10.10.0.50

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

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					

Source and destination information

QRadar SIEM provides network connection details about the flow

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

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

Additional information

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

Custom Rules:
Rules fired for this flow

Custom Rules Partially Matched:
A threshold value of these rules was not met; otherwise, the rule matched

Annotations:
Added by rules

Flow Direction



- 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

About superflows

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



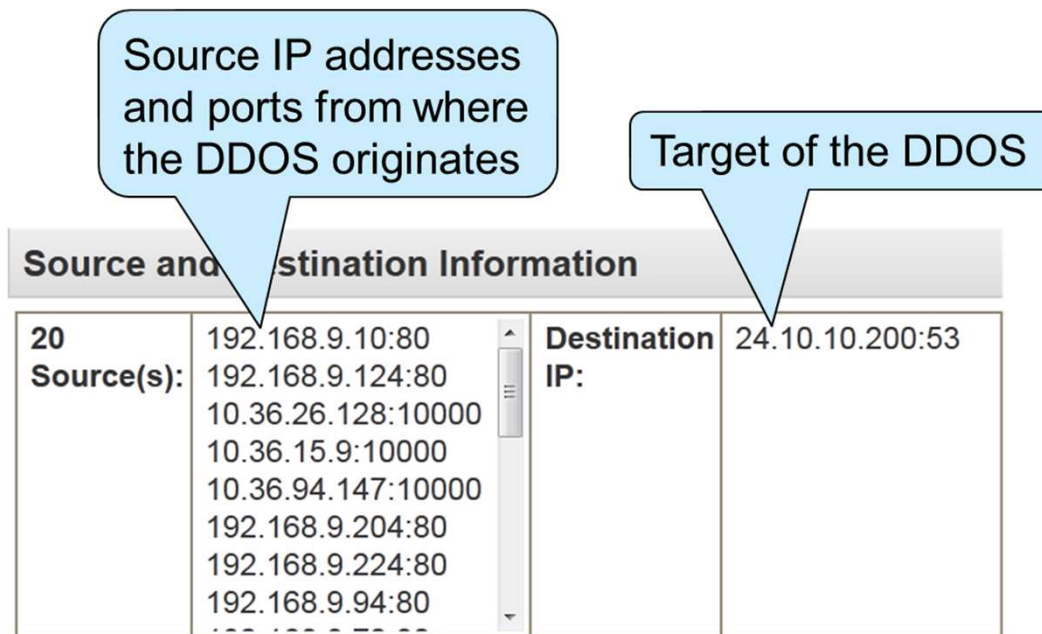
- **Type A:** Network sweep
one source IP address > many destination IP addresses
- **Type B:** Distributed denial of service (DDOS) attack
many source IP addresses > one destination IP address
- **Type C:** Portscan
one source IP address > many ports on one destination IP address

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

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 IP addresses and ports from where the DDOS originates

Target of the 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

Superflow additional information

Flow Type

Additional Information			
Flow Type:	Type B Superflow (DDOS)	Flow Source/Interface:	COE:eth0
Flow Direction:	L2R		
Custom Rules:	<u>BB:Flowshape: Outbound Only</u> <u>BB:CategoryDefinition: Suspicious Flows</u> <u>BB:CategoryDefinition: Suspicious Events</u> <u>BB:PortDefinition: DNS Ports</u> <u>BB:CategoryDefinition: Any Flow</u> <u>Botnet: Potential Botnet Connection (DNS)</u> <u>Magnitude Adjustment: Destination Network Weight is Low</u> <u>Magnitude Adjustment: Context is Local to Remote</u> <u>Magnitude Adjustment: Source Network Weight is Low</u> <u>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>		

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

Superflows Default Values

- Type A Superflows – 50
- Type B Superflows – 20
- Type C Superflows - 100

- Can be customized in “System and License Management”



Component Configuration

The following components are configurable for the selected managed host:






Flow Collector

Maximum Content Capture	64
Maximum Data Capture/Packet	256
Flow buffer size	100000
Maximum Number of Flows	0
Alias Autodetection	Yes
Remove duplicate flows	Yes
Verify NetFlow Sequence Numbers	Yes
External Flow De-duplication method	Source
Flow Carry-over Window	0
External flow record comparison mask	DBP
Create Super Flows	Yes
Type A Superflows	50
Type B Superflows	20
Type C Superflows	100
Recombine Asymmetric flows	No
Ignore Asymmetric Superflows	Yes
Use Common Destination Port	Yes



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/@ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.





Offenses Overview





Introduction to offenses

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

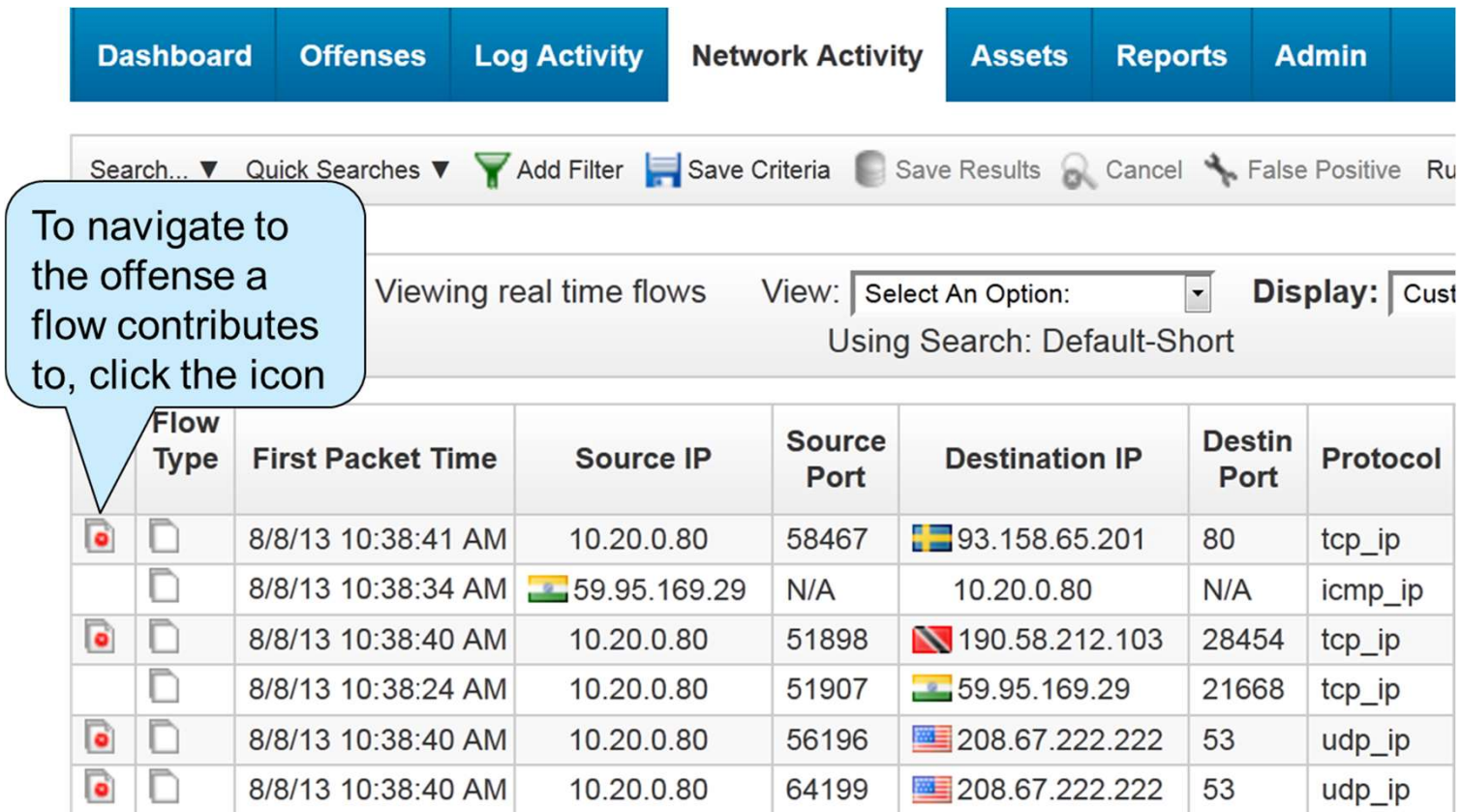


Creating and rating offenses

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

Finding an offense

A red icon indicates that a flow contributes to an offense



















Dashboard Offenses Log Activity Network Activity Assets Reports Admin

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Ru

Viewing real time flows View: Select An Option: Display: Cust

Using Search: Default-Short

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

Selecting an offense to investigate

Offenses are listed in these locations



- In Dashboard items
- In the **Offenses** tab

IBM QRadar Security Intelligence

Dashboard **Offenses** Log Activity Network Activity Assets Reports Admin

Offenses

My Offenses

All Offenses

By Category

By Source IP

By Destination IP

By Network

Rules

Search... Save Criteria Actions Print

All Offenses View Offenses: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

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

Offense Summary window

The offense summary displays information about the ICMP scanning offense

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

Offense 8

Magnitude	Local ICMP Scanner detected by Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewall Deny	Status	Offense Type	Relevance	4	Severity	7	Credibility	4
Description	Local ICMP Scanner detected by Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewall Deny	Source IP	EventFlow 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						

Offense Source Summary

IP	10.127.15.37	Location	Net-10-172-192-Net_10_0_0_0
Magnitude		Vulnerabilities	0
User	Unknown	MAC	Unknown NIC
Host Name	Unknown	Weight	0
Asset Name	Unknown	EventsFlows	410
Offenses	1		

Last 5 Notes

Notes	Username	Creation Date
No results were returned.		

Top 5 Source IPs

Source IP	Magnit...	Location	Vulne...	User	MAC	Weight	Offe...	Dest...	Last EventFlow	EventsFlows
10.127.15.37		Net-10-1...	No	Unknown	Unknown NIC	0	1	2	7h 22m 42s	410

Top 5 Destination IPs

Destination IP	Magnit...	Location	Vulne...	Chained	User	MAC	Weight	Offen...	Soor...	Last EventFlow	EventsFlows
10.26.10.5		Net-10-1...	No	No	Unknown	Unknov 0	1	1	7h 35m 51s	3	
10.26.10.110		Net-10-1...	No	No	Unknown	Unknov 0	1	1	7h 26m 24s	4	

Top 5 Log Sources

Name	Description	Group	EventsFlows	Offenses	Total EventsFlows
CheckPoint @ FW-1Machine	CheckPoint device		393	24	9181
Custom Rule Engine-8 - COE	Custom Rule Engine		17	23	513

Top 5 Users

Name	EventsFlows	Offenses	Total EventsFlows
No results were returned.			

Top 5 Categories

Name	Magnitude	Local Destination Count	EventsFlows	First EventFlow	Last EventFlow
Network Sweep		0	11	Jul 31, 2013 9:47:17 AM	Jul 31, 2013 10:22:58 AM
Firewall Deny		2	393	Jul 31, 2013 9:47:16 AM	Jul 31, 2013 10:22:52 AM
ICMP Reconnaissance		0	6	Jul 31, 2013 9:48:57 AM	Jul 31, 2013 10:20:41 AM

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

Last 10 Flows

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

Top 5 Annotations

Annotation	Time	Weight
"CRE Event": CRE Rule description: [Local ICMP Scanner] Detected a source IP address attempting recon.	Jul 31, 2013 10:08:59 AM	6
"CRE Event": CRE Rule description: [Excessive Firewall Denies Across Multiple Hosts From A Local Host]	Jul 31, 2013 10:06:29 AM	6

Offense parameters (1 of 4)


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

The screenshot shows an interface for an offense summary. At the top, there are tabs for 'Summary', 'Events', 'Flows', and 'Actions'. Below this is a table with columns for 'Magnitude', 'Status', 'Relevance', 'Severity', and 'Credibility'. The 'Magnitude' column contains a horizontal bar chart with a tooltip that reads 'Relevance 4, Severity 7, Credibility 4, Magnitude 5'. The 'Relevance' column has a value of 4, 'Severity' has a value of 7, and 'Credibility' has a value of 4. Four callout boxes provide definitions for these parameters:

- Magnitude:** Relative importance of the offense, as calculated from relevance, severity, and credibility
- Credibility:** How valid is information from that source? 20% of magnitude
- Relevance:** How important is the destination? 50% of magnitude
- Severity:** How high is the potential damage to the destination? 30% of magnitude

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	<u>410 events</u> and <u>0 flows</u> 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

Offense parameters (3 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		
Source IP(s)	<u>10.127.15.37</u>	Event Count	410 events and 0 flows in 3 categories		
Destination IP(s)	<u>Local (2) Remote (360)</u>	Start	Jul 31, 2013 9:42:44 AM		
		Duration	41m 27s		


Source IP(s):
Origin of the ICMP scanning

Start:
Date and time when the first event or flow associated with the offense was created

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

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	<u>410 events</u> and <u>0 flows</u> in 3 categories						
Source IP(s)	<u>10.127.15.37</u>	Start	Jul 31, 2013 9:42:44 AM						
Destination IP(s)	<u>Local (2) Remote (360)</u>	Duration	41m 27s						
Network(s)	<u>Multiple (2)</u>	Assigned to	<u>Unassigned</u>						

Network(s):

Local networks of the local Destination IPs that have been scanned

Assigned to:

QRadar SIEM user assigned to investigate this offense

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	<u>Net-10-172-192.Net 10 0 0 0</u>
Magnitude		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



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	<u>Net-10-172-192.Net 10 0 0 0</u>
Magnitude			
User	Unknown		

Navigate

Information

-  View By Network
-  View Source Summary
-  View Destination Summary

Offense Source Summary (3 of 4)

Offense Source Summary			
IP	10.127.15.37	Location	<u>Net-10-172-192.Net 10 0 0 0</u>
Magnitude		Vulnerabilities	0
User	Unknown		NIC
Host Name	Unknown		
Asset Name	Unknown		
Offenses	<u>1</u>		

Information


- DNS Lookup
- WHOIS Lookup
- Port Scan
- Asset Profile
- Search Events
- Search Flows

Port Scan:
Nmap scans the IP address

Search Flows:
Find flows associated with the IP address

WHOIS Lookup:
Find registered owner of 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		Vulnerabilities	0
User	Unknown	MAC	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	<u>1</u>	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

Search Results and Notes

Can View the Last search results for the Source of the Offense

Last 5 Search Results					Search Results
Magnitude	Started On	Ended On	Duration	Events/Flows	

QRadar SIEM users can add notes to offenses

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


Notes:
View all notes of the offense

Add Note:
Create new note

Last 5 Notes			Notes	Add Note
Notes	Username	Creation Date		

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

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

Top 5 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

Top 5 Categories

QRadar SIEM sorted the event and the flows into categories

Top 5 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 ...		

Last 10 Events











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

Last 10 Events Events						
Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Potential Botnet Activity		Custom Rule E...	Misc Malware	208.67.222.222	53	Aug...

Last 10 Flows

This table provides information about what happened most recently

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

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

Annotations

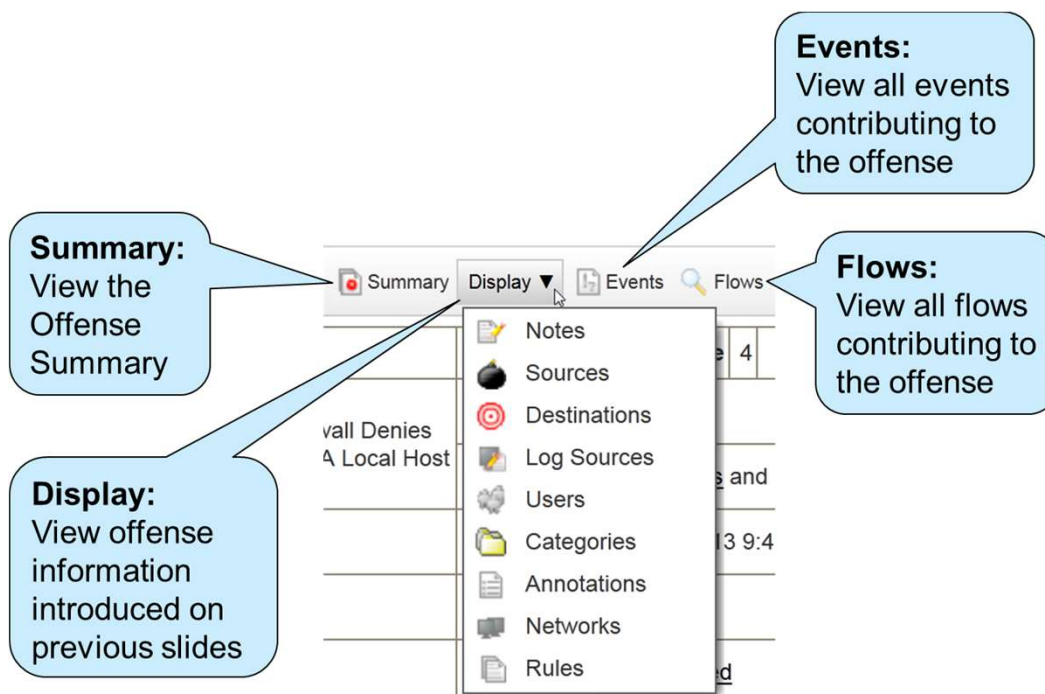
- Annotations provide insight into why QRadar SIEM considers the event or traffic threatening
- QRadar SIEM can add annotations when it adds events and flows to an offense
- Read the oldest annotation because it was added when the offense was created
- Hold the mouse over an annotation to show the entire 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.	Aug 8...	6
"CRE Event" CRE Rule description: [Potential Botnet Activity] Detected a host connecting	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.		

Offense Summary toolbar

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



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 the Actions menu open. The menu items are: Follow up (red flag icon), Hide (yellow X icon), Protect Offense (grey shield icon), Close (red X icon), Email (yellow envelope icon), Add Note (yellow notepad icon), and Assign (grey person icon). Callouts provide instructions 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

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







Offense status and flags

Status: Icon indicates








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

The actions available depend on the status of the offense

The screenshot shows a web interface for managing offenses. At the top, there are navigation tabs: 'Primary', 'Display', 'Events', 'Flows', 'Actions', and 'Print'. Below the tabs is a table with the following data:

Status	     	Relevance	4
Offense Type	Source IP		
Event/Flow count	<u>411 events</u> and		
Start	Jul 31, 2013 9		
Duration	46m 37s		
Assigned to	<u>lynette</u>		

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






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

Unprotect Offense:
Allow QRadar SIEM to delete this protected offense



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.






Introduction to Rules

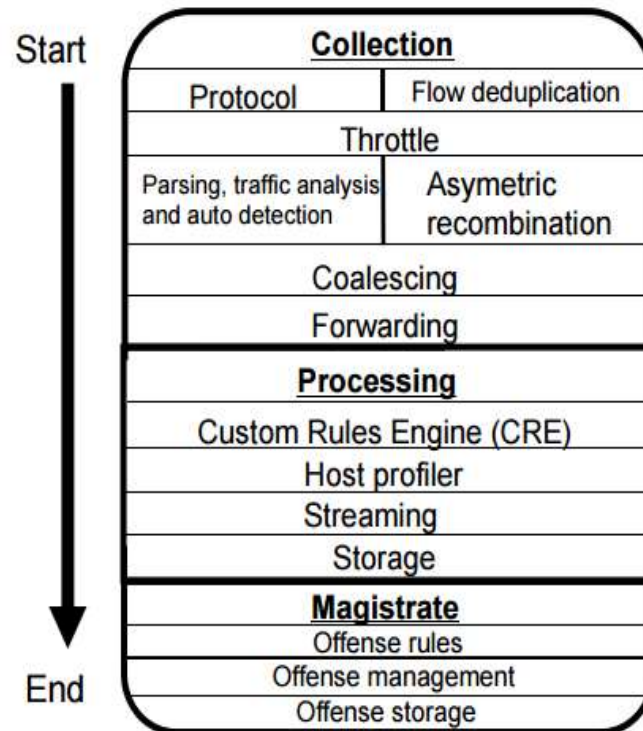


What are rules

- Rules perform tests on Events, Flows and offenses to detect unusual activity in your network.
- QRadar is capable of generating an extensive number of rule combinations to test against event data, flow data, or offenses.
- If all the conditions of a test are met, the rule may generate a response.
- Tests in each rule can reference building blocks or other rules
- A rule that is referenced by another rule cannot be disabled or deleted 
- Similar rules are grouped together by category, such as Audit, Exploit, DDoS, Recon, and more.

How rules work

- QRadar Event Collectors
 - Gather events from local and remote sources
 - Normalize these events
 - Classify them into low-level and high-level categories.
- QRadar QFlow Collectors
 - Read packets from the wire or receive flows from other devices and then converts the network data to flow records.
- Each Event/Flow Processor processes events or flow data from the QRadar Event/Flow Collectors.
- The Custom Rules Engine (CRE)
 - Processes events and compares them against defined rules to search for anomalies.
- The CRE keeps track of the systems that are involved in incidents, that contribute events to offenses




Rule Categories



- There are two categories for rules
- Custom rules
 - Custom rules perform tests on events, flows, and offenses to detect unusual activity in your network.
- Anomaly rules
 - Anomaly detection rules perform tests on the results of saved flow or event searches as means to detect when unusual traffic patterns occur in your network.
 - This search must also be grouped by a certain property (e.g: Source IP, Source Network, etc)

Rules Types

- Event Rules
 - Test against incoming log source data that is processed in real time and previously processed data (historical data) by the QRadar Event Processor.
 - Event rules can perform tests against a single event or event sequences
- Flow Rules
 - Test against incoming flow data that is processed by the QRadar Flow Processor.
 - Flow rules perform tests against a single flow or flow sequences.
- Common Rules
 - Test against event and flow data 
- Offense Rules
 - Test the parameters of an offense to trigger more responses

Rule Conditions

- Each rule might contain functions, building blocks, or tests.
- With functions, you can use building blocks and other rules to create a multi-event, multi-flow, or multi-offense function.
- You can connect rules using functions that support “AND” and “AND NOT” to include exclude tests or rules from the rule



and when the context is Local to Local
and when a flow or an event matches any of the following BB:PortDefinition: DNS Ports
and when any of these BB:CategoryDefinition: Recon Events, BB:CategoryDefinition: Suspicious Events with the same
source IP more than 5 times, across more than 59 destination IP within 10 minutes
and NOT when a flow or an event matches any of the following BB:HostDefinition: DNS Servers

Rule Responses



- If the tests of a rule match, the rule generates the configured actions and responses:
- Create an offense
- Dispatch a new Event
- Send an email.
- Generate system notifications on the Dashboard feature.
- Add or remove data to reference sets.
- Add or remove data to reference data collections.
- Generate a response to an external system.
- They can trigger a scan
- Run a custom action script in response to an event.

Rule Action

Choose the action(s) to take when an event or flow occurs that triggers this rule

Severity

Credibility

Relevance

Ensure the detected event or flow is part of an offense

Index offense based on

Annotate this offense:

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

Annotate event or flow

Drop the detected event or flow

Rule Response

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

Dispatch New Event

Email

Send to Local SysLog

Send to Forwarding Destinations

Notify

Add to a Reference Set

Add to Reference Data

Remove from a Reference Set

Remove from Reference Data

Trigger Scan

Execute Custom Action



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 ...

About Rules

- The basic components of rules are tests.
- Tests are performed on Log activity events, Network activity events, Rules and Offenses

Apply on events which are detected by the system
  and when [BB:CategoryDefinition: Authentication Success](#) match at least 1 times in 5 minutes after [Authentication: Multiple Login Failures for Single Username](#) match with the same [Username](#)



- Rule tests can be only TRUE or FALSE.
- Tests can be simple (e.g. is it a Weekday) or complex (e.g. if X followed by Y within Z timeframe)
- Tests are evaluated in the order in which they appear in a rule
- Ordering tests is important for performance
- Tests are evaluated on the EP/FP and/or Console (by the CRE)
- Rules can have Actions and Responses

A3

About building blocks



- 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 keep rules easy to read, write and understand
- 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

Slide 170

A3

I know it's too soon in the slides, but someone will eventually wonder about putting data into BB versus Reference Sets. Somewhere in the slides, do you mention which building blocks are loaded into memory (versus using reference sets which don't get loaded into memory), hence data in BB may make tests slightly more performant in real-time evaluation?

Author, 7/25/2016

About building blocks (Cont)

- 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”

Apply on events or flows which are detected by the system
and when a flow or an event matches any of the following
and when either the source or destination IP is one of the following



Building Blocks - Beware of the 'Host Definition'

- The 'BB:HostDefinition' Building Blocks are communication definitions
- Consider "BB:HostDefinition: DNS Servers"

Apply BB:HostDefinition: DNS Servers on events or flows which are detected by the Local system

and when a flow or an event matches any of the following BB:PortDefinition: DNS Ports

and when either the source or destination IP is one of the following
127.0.0.2

- The "source or destination IP" test can be updated by Server Discovery (Asset tab)

Apply BB:PortDefinition: DNS Ports on events or flows which are detected by the Local system

and when the destination port is one of the following 53

Using Building Blocks

Building Blocks are used to categorize the properties of events or flows.

For example, to create BB categories for properties you will need to know the following parameters:

- Destination IP, IPv6, MAC address or port
- Source IP, IPv6, MAC address or port
- Event name, Event category or IP protocol
- Username

Apply on events which are detected by the system

  and when the event username matches the following admin, superuser, root, toor, init, Admin, Administrator, ADMINISTRATOR, ADMIN, ROOT, SYS, SYSTEM

Combining Building Blocks to capture specific events or flows


- Example:
- Implement the **Root or Administrator account must be used to modify the audit subsystem configuration** policy rule.
- This translates into a rule that combines the following Building Block:
 - Building Block

Apply on events which are detected by the system

   and when the event username matches the following admin, superuser, root, toor, init, Admin, Administrator, ADMINISTRATOR, ADMIN, ROOT, SYS, SYSTEM

– Rule:

Apply on events which are detected by the system

   and when an event matches any of the following

   and when the event category for the event is one of the following Authentication.User Account Added

Linking tests

- Link multiple test results to a single rule or building block using the logical AND or AND NOT operators.
- Remember that tests are evaluated from the top to bottom.
- The tests terminate after the last test is executed or when one of the tests fails.
- The order of the tests can be changed
- When linking tests, put the test that applies to the smallest set of flows, events, or rules at the bottom.
- Construct logical OR by using appropriate tests on rules or Building Blocks. A4



Slide 175

A4

You might point out now or later that a test with the word "any" is the same as an OR for parameters in that test, as shown in the first and last test in the example.

Author, 7/25/2016



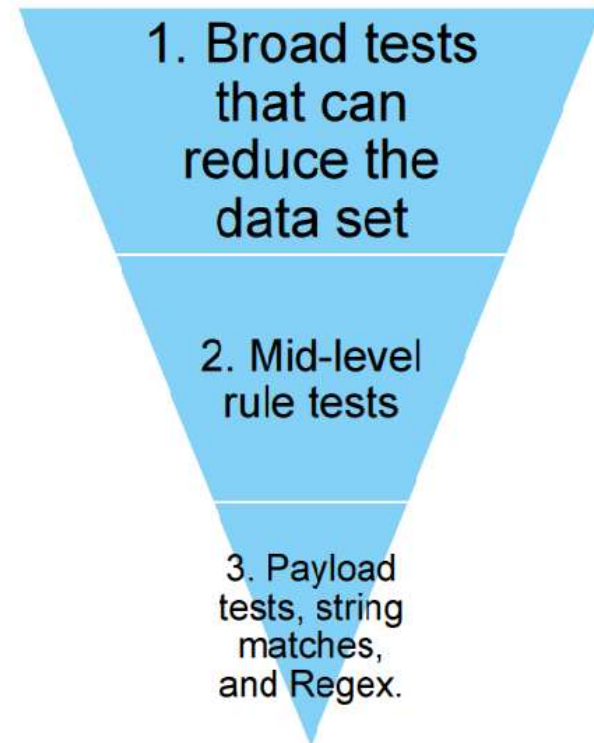
Optimizing Linking Tests (1/2)

- Tests are evaluated from the top down.
- Put the test that restricts the search results the most at the top.
- Put the test that applies to the smallest set of events or flows at the bottom.
- Example of the INEFFICIENT order:
 1. Test for clear text application usage
 2. Test payload for credit card numbers
 3. Test if logsourcegroup is PCI critical
 4. Test if network segment is PCI network

Optimizing Linking Tests (2/2)

- Example of the OPTIMIZED order:
 1. Test if network segment is PCI network
 2. Test if logsourcegroup is PCI critical
 3. Test for clear text application usage
 4. Test payload for credit card numbers

Optimizing the order of the tests will improve QRadar's Performance





Creating Custom Rules





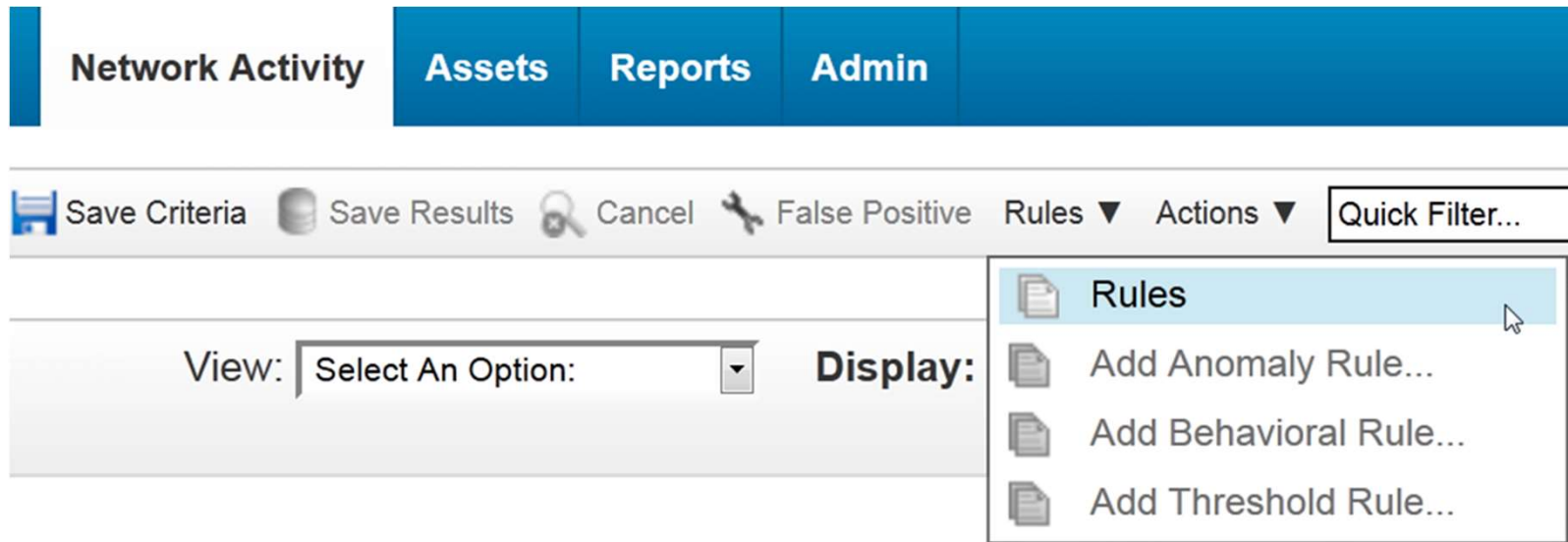
Creating a Custom Rule

- To create Rules you must have “Maintain Custom Rules” selected in your User Role
- When you define rule tests, treat rules the same way you treat searches and test against the smallest data possible
- To optimize performance, start with broad categories that narrows the data that a rule test evaluates
 - For example, start with a rule test for a specific log source type, network location, flow source or context (L2L, R2L, L2R, R2R).
- Use mid-level tests, such as IP Addresses, Port Traffic, etc
- Keep Payload and Regex tests as the last rule test
- Most rule tests evaluate a single condition

Creating a Custom Rule

Rules can be accessed from:

- Log Activity Tab
- Network Activity
- Offenses Tab



Creating a Custom Rule

- From the Offenses, Log Activity, or Network Activity tabs - click Rules.
- From the Actions list, select a rule type.
- Each rule type tests against incoming data from different sources in real time and historical data.
- For example, event rules test incoming log source data
- In the Rule pane, type a unique name that you want to assign to this rule
- From the list box, select Local or Global.
- From the Test Group list, select one or more tests that you want to add to this rule.
- The CRE evaluates rule tests line-by-line in order. The first test is evaluated and when true, the next line is evaluated until the final test is reached

The screenshot shows the 'Rule Wizard: Rule Test Stack Editor' window. At the top, it asks 'Which tests do you wish to perform on incoming events?'. Below this, there is a 'Test Group' dropdown menu set to 'All' and an 'Export as Building Block' button. A search bar labeled 'Type to filter' is present. A list of tests is displayed, each with a green checkmark icon: 'when the local network is one of the following networks', 'when the destination network is one of the following networks', 'when the IP protocol is one of the following protocols', 'when the Event Payload contains this string', 'when the source port is one of the following ports', 'when the destination port is one of the following ports', 'when the local port is one of the following ports', 'when the remote port is one of the following ports', 'when the source IP is one of the following IP addresses', 'when the destination IP is one of the following IP addresses', 'when the local IP is one of the following IP addresses', and 'when the remote IP is one of the following IP addresses'. Below the list, there is a 'Rule' field with the text '(Click on an underlined value to edit it)'. A note states 'Invalid tests are highlighted and must be fixed before rule can be saved.' At the bottom, there is an 'Apply' button, a text input field containing 'My New Rule', and a dropdown menu set to 'Local' followed by the text 'system'.

- On the Rule Responses page, configure the responses and Action that you want this rule to generate

Creating a Custom Rule

Rule Description
Shows the different tests used in the Rule

Rule Notes
Adds additional information to the Rule

Rule Actions and Responses
What do you want this rule to do

Rule Description

Apply Anomaly: Excessive Firewall Accepts Across Multiple Hosts on events which are detected by the Local system and NOT when an event matches any of the following BB:HostDefinition: Servers and when any of these BB:CategoryDefinition: Firewall or ACL Accept with the same source IP more than 100 times, across more than 100 destination IP within 5 minutes

Rule Notes

Reports excessive Firewall Accepts across multiple hosts. More than 100 events were detected across at least 100 unique destination IP addresses in 5 minutes.

Rule Actions

- Force the detected Event to create a NEW offense, select the offense using Source IP

Rule Responses

- Dispatch New Event
 - Event Name: Excessive Firewall Accepts Across Multiple Hosts
 - Event Description: Excessive Firewall Accepts were detected across multiple hosts. More than 100 events were detected across at least 100 unique destination IP addresses in 5 minutes.
 - Severity: 7 Credibility: 8 Relevance: 8
 - High-Level Category: Access
 - Low-Level Category: Firewall Permit
 - Force the dispatched event to create a NEW offense, select the offense using Source IP
 - Include detected Event from this attacker from this point forward, for 300 second(s), in the offense

This Rule will be: Disabled



Anomaly Detection Rules

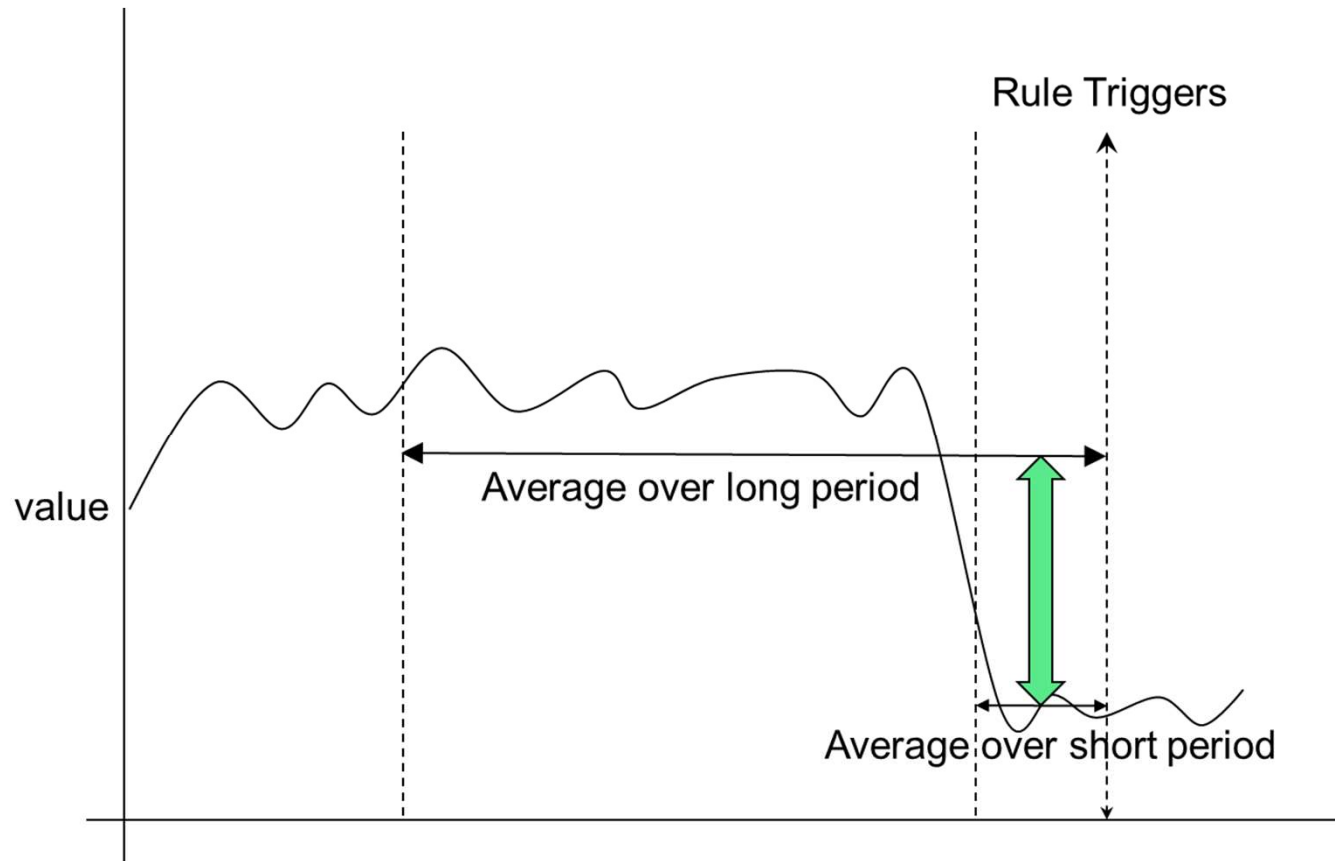




Anomaly Detection Rules

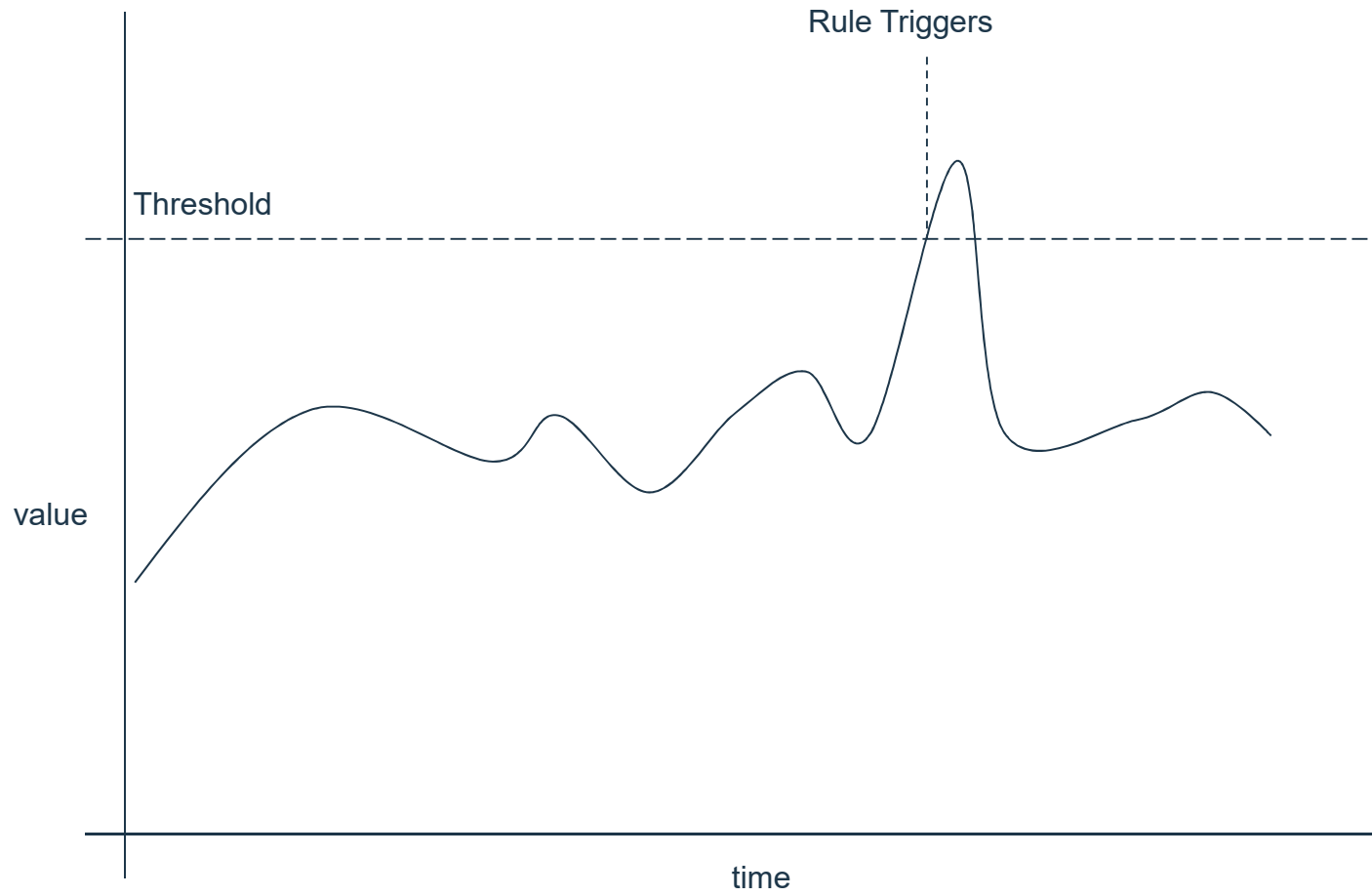
- Anomaly detection rules test the results of saved flow or events searches to detect when unusual traffic patterns occur on a network
 - Requires a saved search that is grouped around a common parameter, and a time series graph that is enabled
- **Anomaly rules**
 - Test event and flow traffic for changes in short-term events when you are comparing against a longer time frame.
- **Threshold rules**
 - Test events or flows for activity that is greater than or less than a specified range.
- **Behavioral rules**
 - Test events or flows for volume changes that occur in regular patterns to detect outliers
 - A behavior rule learns the rate or volume of a property over a pre-defined season. The season defines the baseline comparison timeline for what you are evaluating

Anomaly Rules

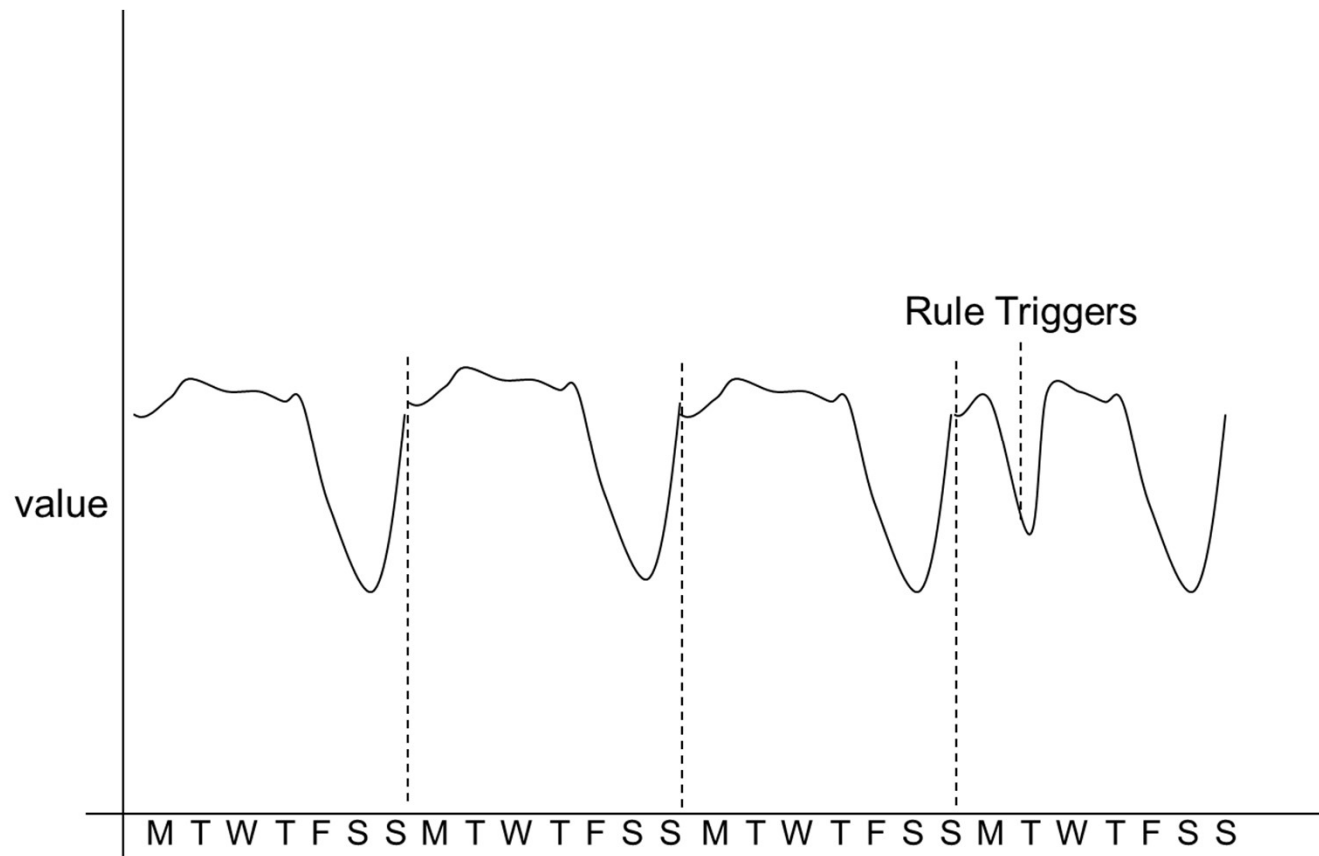




Threshold Rules








Behavioral rules





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.






Reports

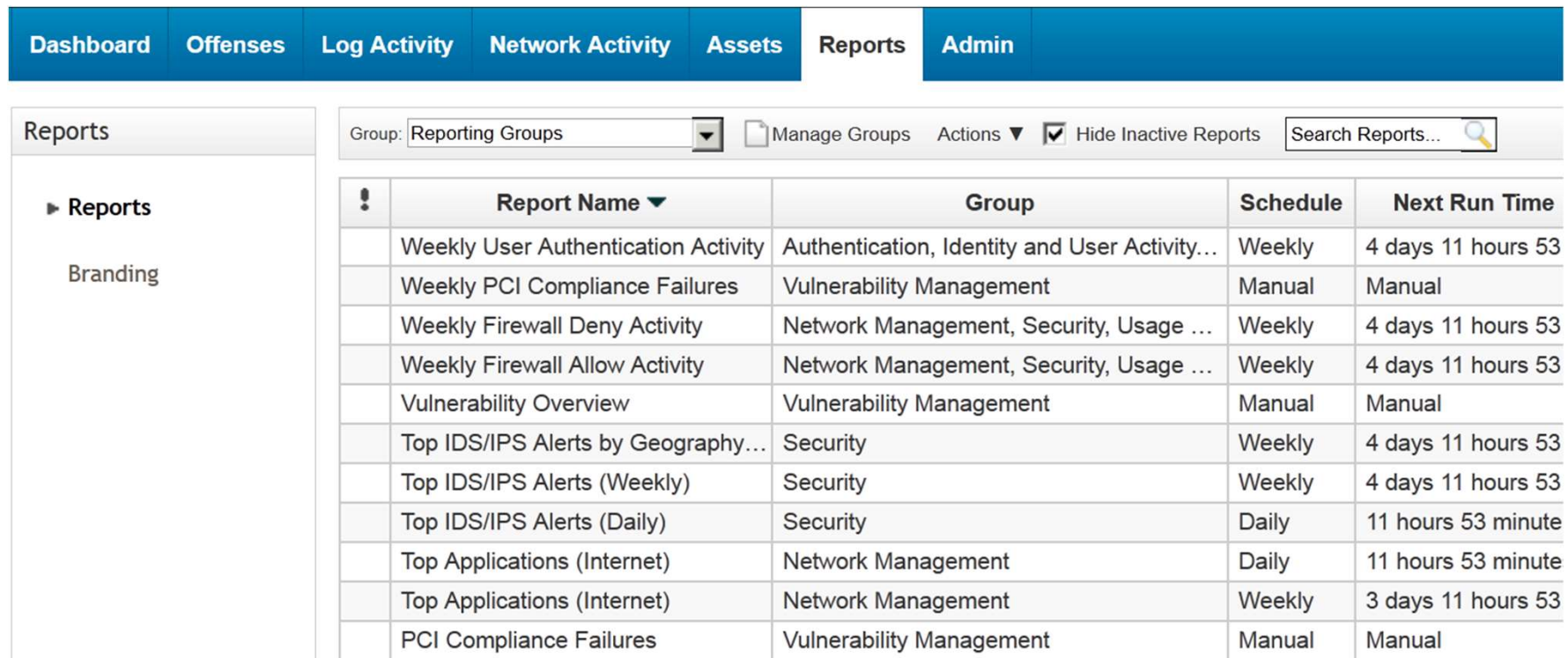


Reporting introduction

- 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

Reports tab

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



Group: Reporting Groups Actions Hide Inactive Reports Search Reports...

!	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

Finding a report

- QRadar SIEM includes more than 1500 report templates; before you create a new template, check the predefined templates
- Additional report templates can be added via the IBM Security App Exchange



The screenshot shows the QRadar Reports interface. At the top, there are navigation tabs: Activity, Network Activity, Assets, Reports, and Admin. Below the tabs, there is a search bar with the text "firewall deny" and a magnifying glass icon. To the left of the search bar, there is a "Group: Reporting Groups" dropdown menu. Below the dropdown, a tree view of reporting groups is displayed, including Contivityv2, JuniperSA, VpnConcentrator, VPNGateway, Network Management, Security, Usage Monitoring (highlighted), VoIP, Vulnerability Management, and Other. Three callout boxes provide additional information:

- Hide Inactive Reports:** Disable to view all inactive report templates
- Reporting Groups:** View report templates of a reporting group
- Search:** Display report templates whose title, description, group name, or author user name matches the search criteria

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 the QRadar SIEM interface with a table of reports and an open context menu. The table has columns for Report Name, Category, and Run Time. The context menu is open over the 'Daily Firewall Deny Activity' report, showing options like 'Run Report', 'Run Report on Raw Data', and 'Toggle Scheduling'.

Report Name	Category	Run Time
Daily Firewall Allow Activity	Network Management	Inactive
Daily Firewall Deny Activity	Network Management	Inactive
Daily Most Active Devices	Log Sources, Security	Inactive
Geographic Traffic Distribution	Network Management	8 hours 14 mi...
Large Outbound File Transfer	Network Management	Inactive
Monthly Most Active Devices	Network Management	Inactive
Network Traffic Volume	Compliance, Executive	Inactive
Network Traffic Volume	Compliance, Executive	Inactive
Top Talkers (Weekly)	Network Management	Inactive
Top URL Reports	Network Management	Inactive

- Create
- Edit
- Duplicate
- Assign Groups
- Share
- Run Report
- Run Report on Raw Data
- Toggle Scheduling
- Cancel Report Generation
- Delete Report
- Delete Generated Content

Selecting the generated report

Next Run Time	Last Modifi	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

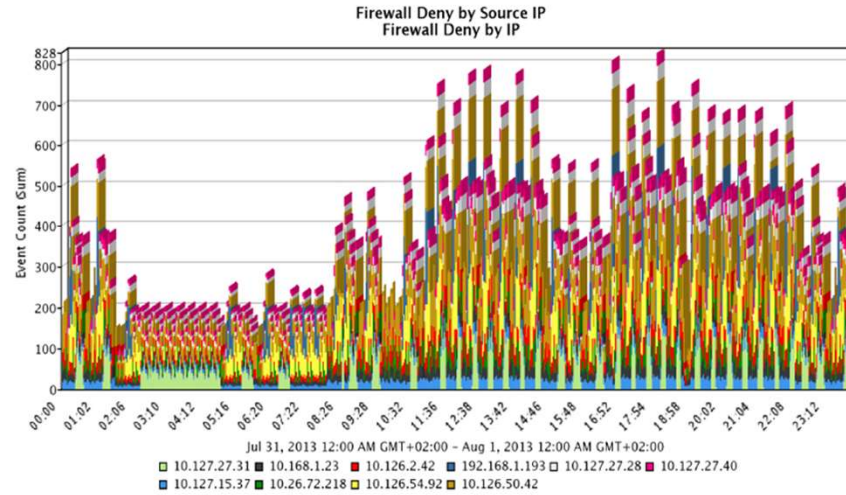
Next Run Time	Last Modifi	Owner	Author	Generated Reports	Formats
Inactive	Sep ...	admin	admin	None	
Inactive	Sep ...	admin	admin	Jul 31, 2013 4:49 PM	

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

Viewing a report

Daily Firewall Deny Activity

Generated: Jul 31, 2013 3:28:04 PM



Firewall Deny by Device

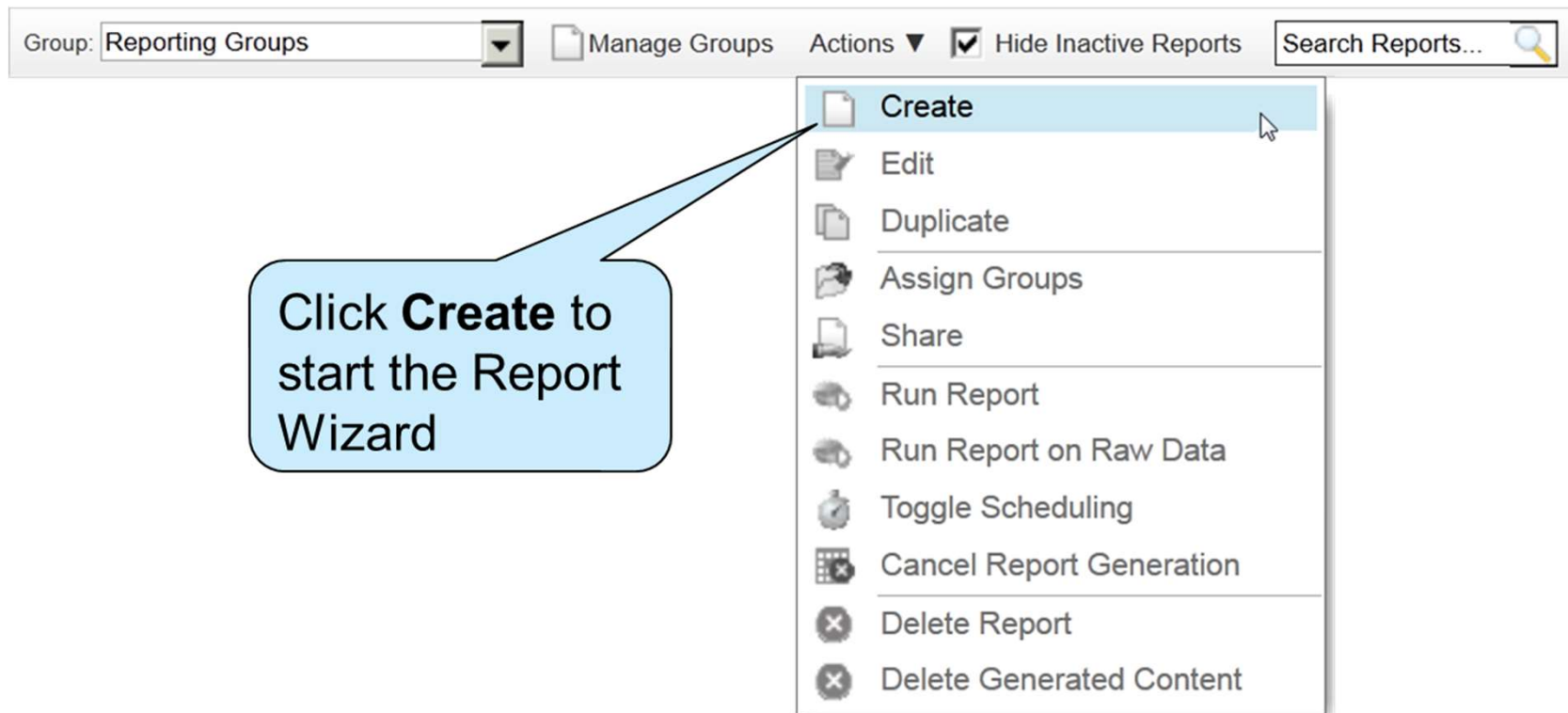
Firewall Deny by Log Source

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

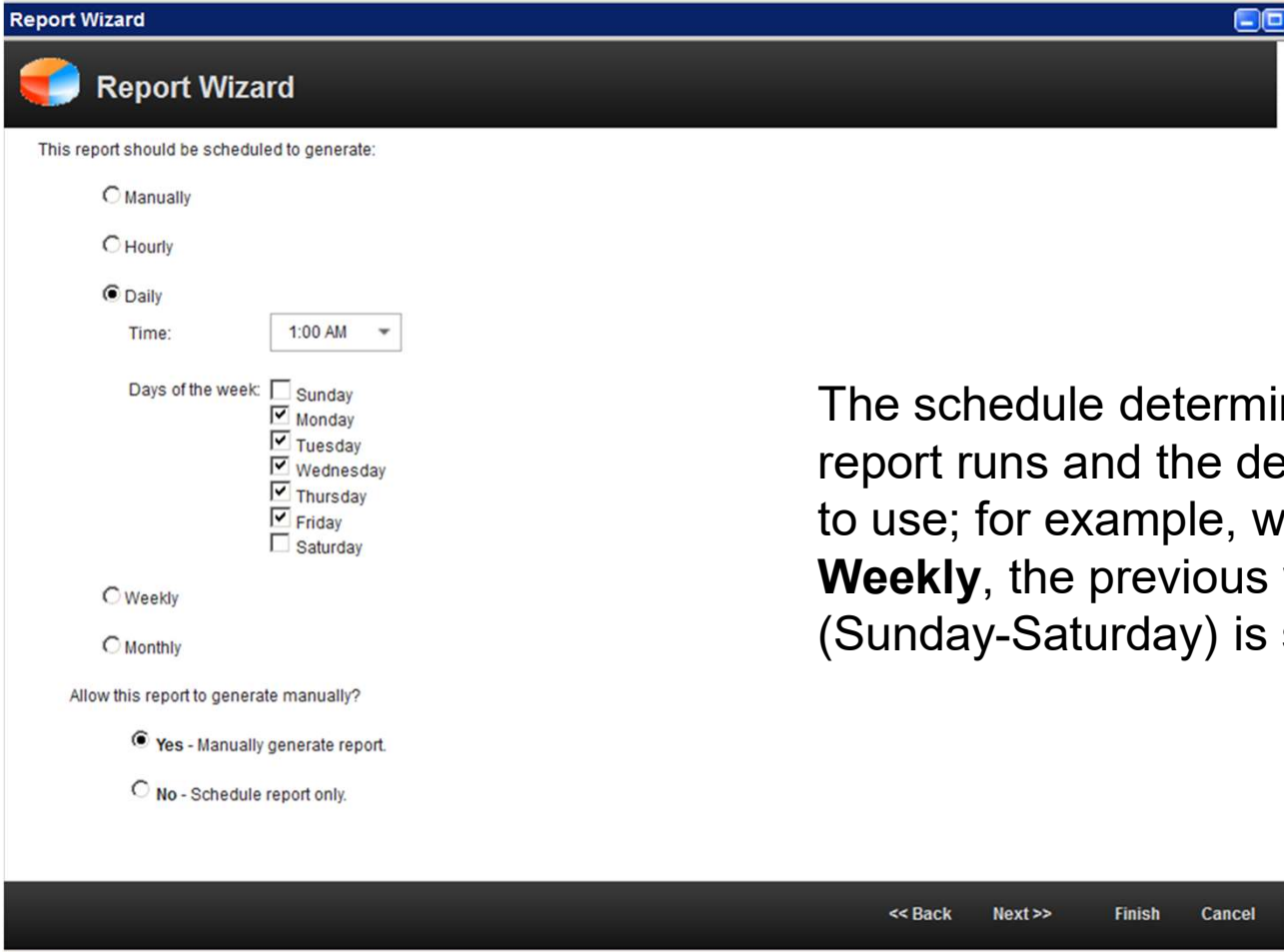
Log Source	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
Checkpoint @ FW-1Machine	Multiple (13,157)	Multiple (4,355)	Multiple (2,180)	Multiple (2)	Firewall Deny	Multiple (5)	N/A	6	717,764	717,268
Custom Rule Engine-8 :: COE	192.168.10.1	192.168.10.255	137	Flow Source/Interface Stopped Sending Flows	ACL Deny	udp_ip	N/A	4	1	1

Creating a new report template

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



Choosing a schedule



The screenshot shows the 'Report Wizard' dialog box. The title bar reads 'Report Wizard'. Below the title bar is a dark header with the IBM logo and the text 'Report Wizard'. The main content area is white and contains the following elements:

- The text 'This report should be scheduled to generate:' is followed by three radio button options: 'Manually', 'Hourly', and 'Daily'. The 'Daily' option is selected.
- Below the 'Daily' option is a 'Time:' label and a dropdown menu showing '1:00 AM'.
- Below the time is a 'Days of the week:' label followed by a list of days with checkboxes: Sunday (unchecked), Monday (checked), Tuesday (checked), Wednesday (checked), Thursday (checked), Friday (checked), and Saturday (unchecked).
- Below the days of the week are three radio button options: 'Weekly', 'Monthly', and 'Daily' (which is already selected).
- Below these options is the text 'Allow this report to generate manually?' followed by two radio button options: 'Yes - Manually generate report.' (selected) and 'No - Schedule report only.'.


At the bottom of the dialog box is a dark bar with four buttons: '<< Back', 'Next >>', 'Finish', and 'Cancel'.

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 layout

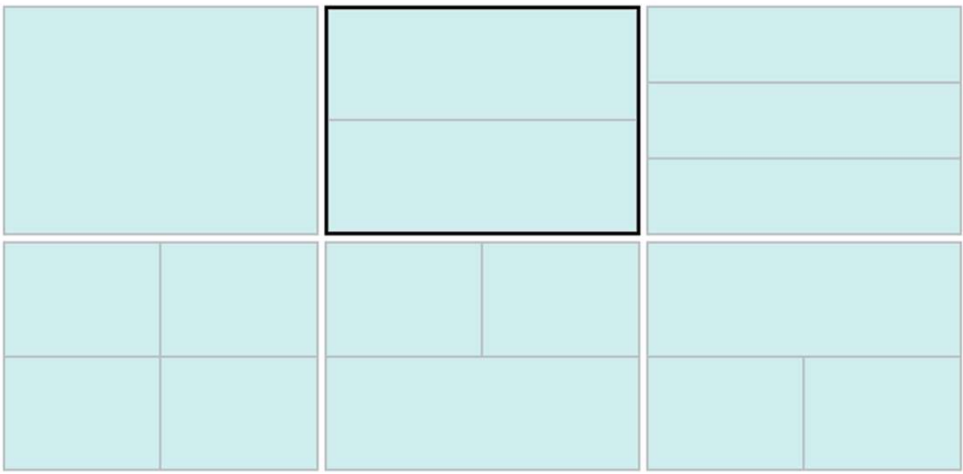
- QRadar SIEM uses containers to segregate report pages so that different data sets can show on the same report page

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:



Defining report contents

Report Wizard

Specify Report Contents
Enter a report title and choose a logo. Select a chart type and click 'Define' for each chart you wish to configure. Configured charts become highlighted. Click Next.

Report Title: Logo:

Chart Type:

- None
- None
- Asset Vulnerabilities
- Events/Logs**
- Flows
- Log Sources
- Top Destination IPs
- Top Offenses
- Top Source IPs

Chart Type:

None

Define

The report saves with the name typed in the **Report Title** field

To configure the report chart, click **Define**

Configuring the upper chart

Enter chart title

Select the previously saved search to report firewall activity of the suspicious scanning system

Report Wizard

Container Details - Events/Logs
This report displays collected event/log data.

Chart Title:

Chart Sub-Title: Automatically Specified

Hourly Scheduling

Schedule: All data from previous hour

Timezone:

Graph Content

Saved Searches Group:

Type Saved Search or Select from List

Available Saved Searches

- Default VFW VFW Gateway: warnings
- Dept - 10.127.15.37

Configuring the upper chart (continued)

Select the graph type

Select the values for each axis

Additional Details

Graph Type: Line

Limit Events/Logs to Top: 5

Horizontal (X) Axis: Time

Vertical (Y) Axis:

Configuring the lower chart

Define a chart for firewall activity

Select a predefined search to report the top services and port numbers of traffic through firewalls

Report Wizard

Container Details - Events/Logs
This report displays collected event/log data.

Chart Title:

Chart Sub-Title: Automatically Specified

Hourly Scheduling

Schedule: All data from previous hour

Timezone:

Graph Content

Data is currently being accumulated for this report.

Saved Searches Group:

Type Saved Search or Select from List

Available Saved Searches

- Top Services Denied through Firewalls
- Top Services/Ports Through Firewalls**
- Top Systems Attacked (IDS/IDP/IPS)
- Top Systems Sourcing Attacks (IDS/IDP/IPS)
- Top User by Mail Service Login Failure

Configuring the lower chart (continued)

Select graph type **Table** to list the reported data in a table

Additional Details

Graph Type:


Table ▼

Limit Events/Logs to Top:


5 ▼

Verifying the layout preview

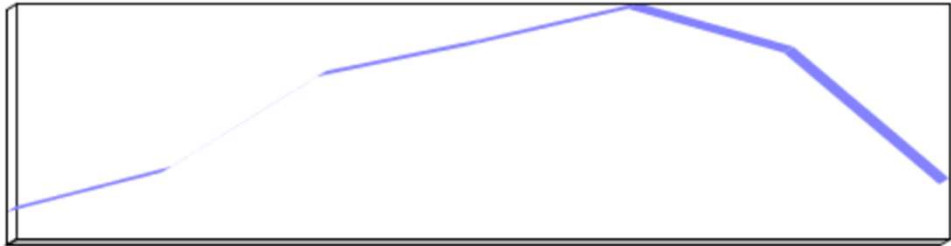
Report Wizard

 **Report Wizard**

Layout Preview
This report preview displays the report layout and chart types you have chosen. It does not reflect live 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

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

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

Distributing the report

Allow users to view the generated report

Distribute the report by email

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

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

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

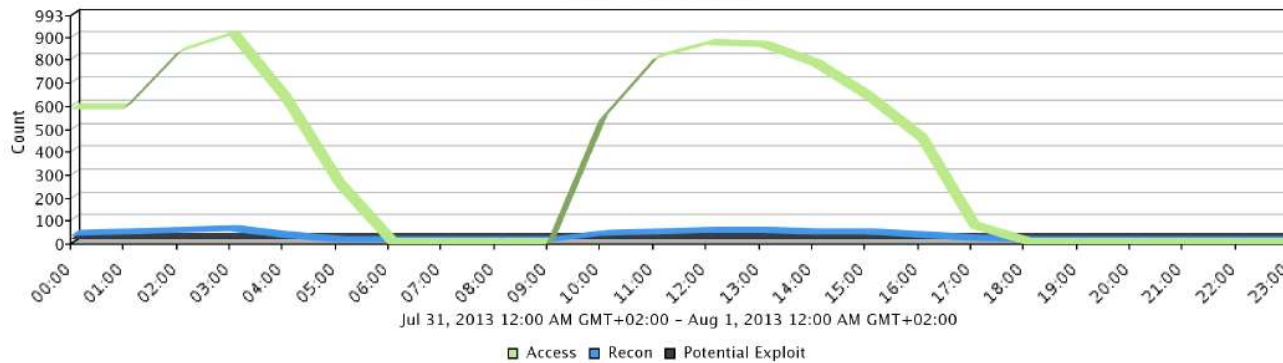
Viewing the generated report

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



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



Best practice reports for Compliancy purposes

- Usage of Service accounts
- Usage of privileged user accounts
- Account management actions: Creation, deletion, modification
- Authorized access to sensitive data
- Audit modification actions
- Log collection completion
- User authentications
- Software and machine patch management







Best practice reports for Monitoring purposes

- Behavioral change in Service account authentication or usage
- Unauthorized access to sensitive data
- Behavioral change in access to sensitive data
- Change in machine network behaviour
- Audit trail clearance
- Log collection failures
- Virus checker alerts
- Endpoint management alerts
- Critical resource patch failure



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

