IBM Security

Section 1: Qradar Foundations

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

IBM

IBM Security

SIEM Capabilities

IBM

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

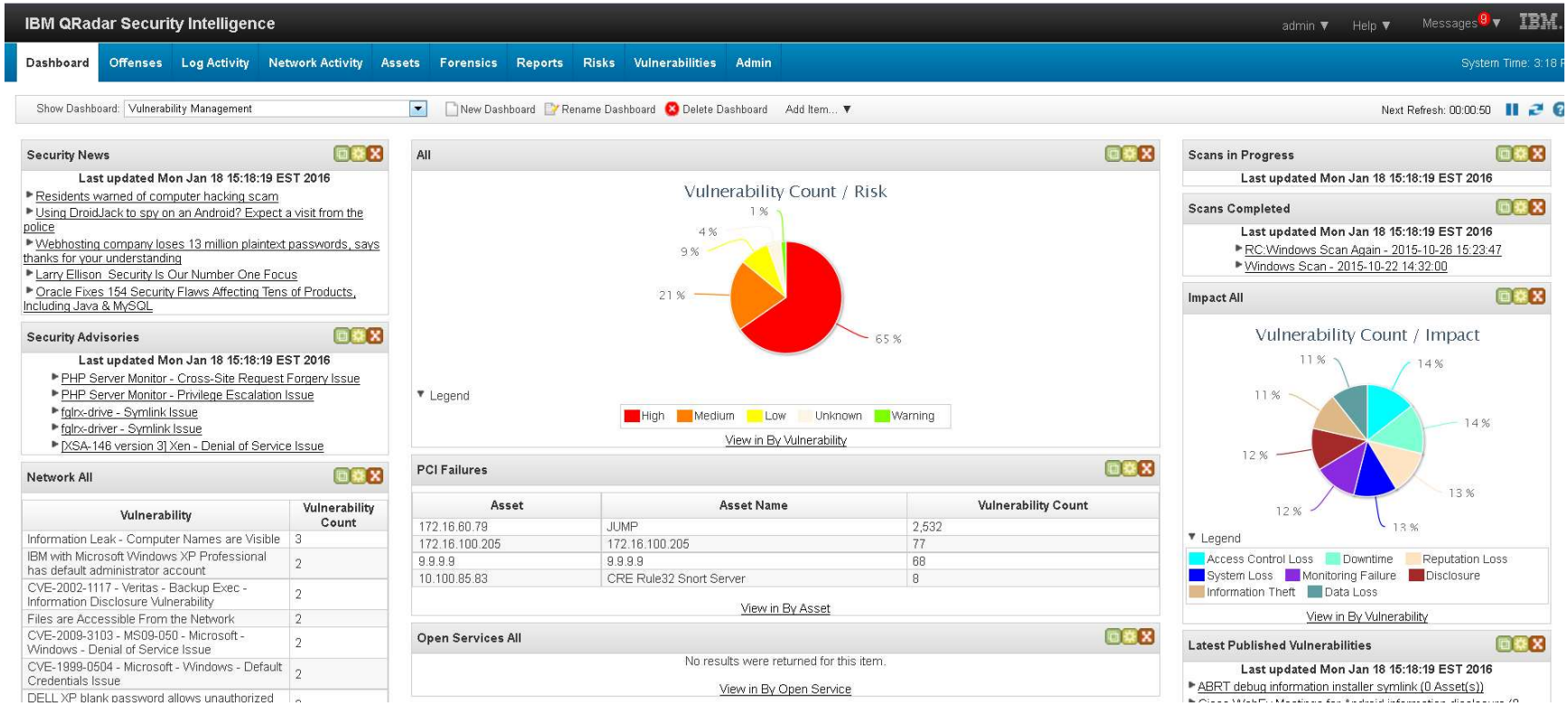
Key QRadar SIEM capabilities

- 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



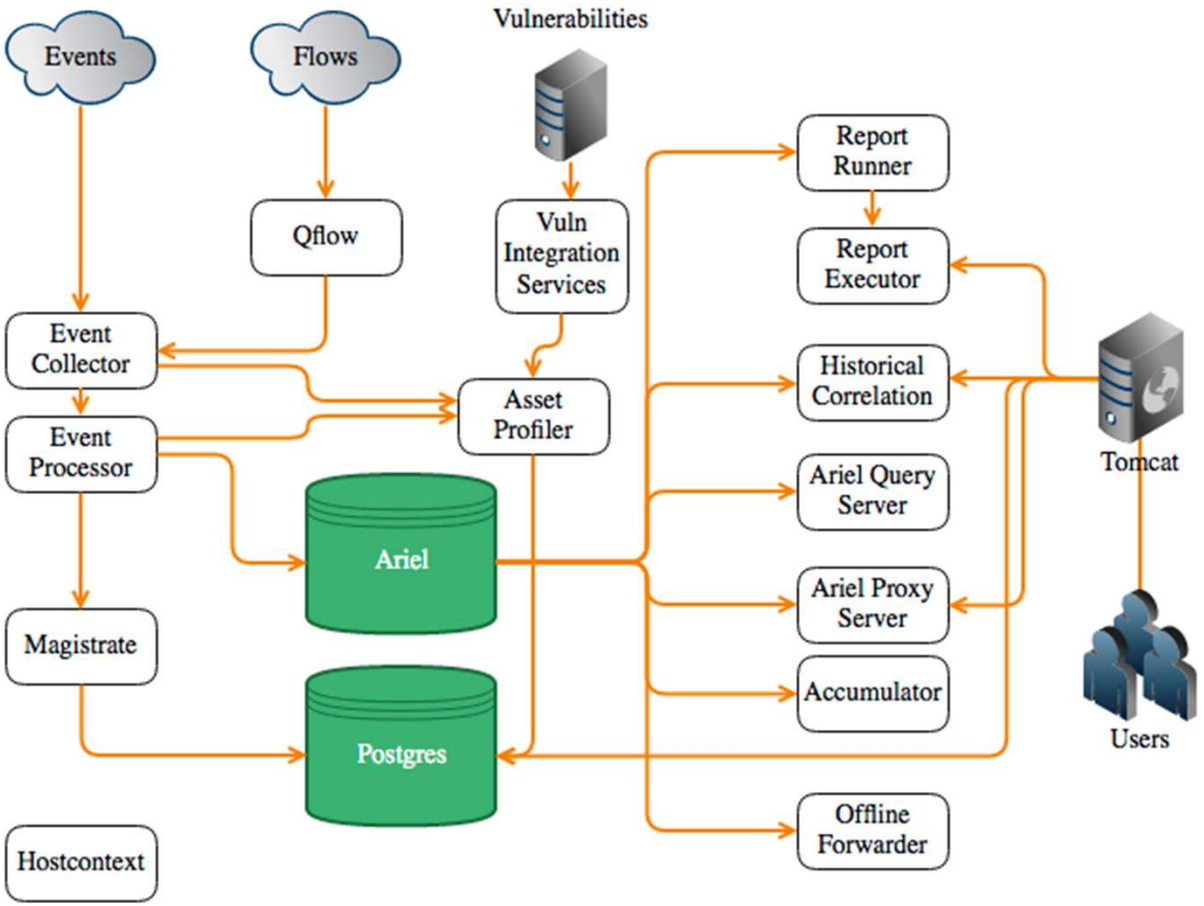
The console provides one integrated user interface for all tasks

IBM Security

How QRadar SIEM Collects Security Data

IBM

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

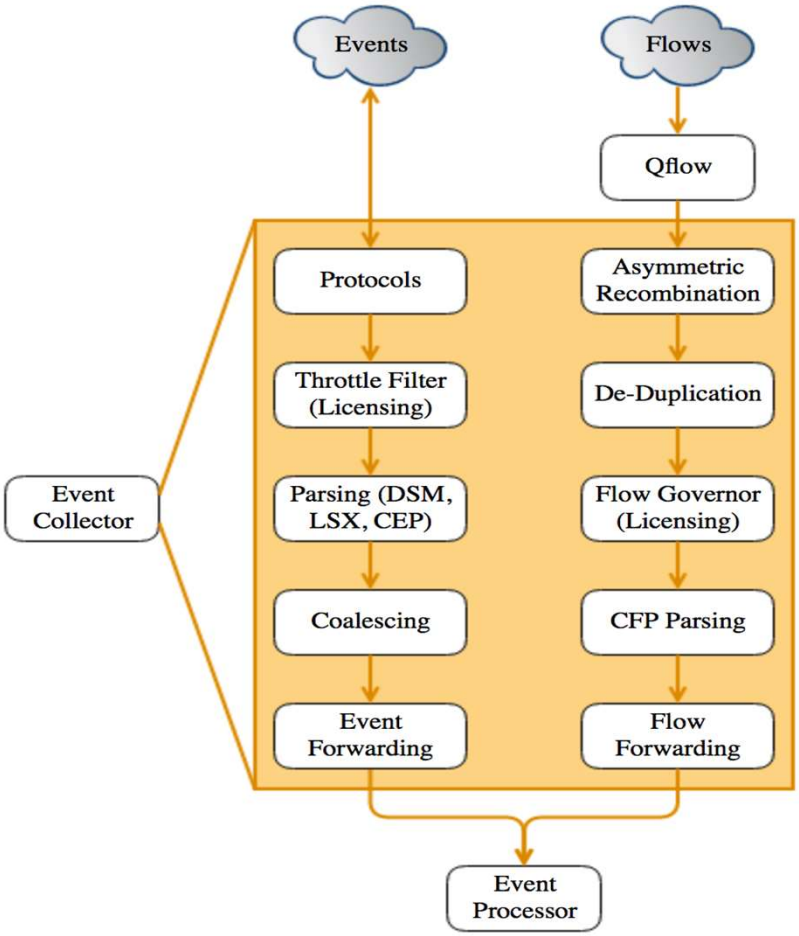
Flow collection and processing

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
	Oct 14, 2014, 7:00:13 AM	192.168....	61190	202.12.27.33	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
	Oct 14, 2014, 6:59:59 AM	192.168....	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	380 (C)	3,376 (C)	4	4	N/A
	Oct 14, 2014, 7:00:53 AM	0.0.0.0	546	0.0.0.0	547	udp_ip	Other	612 (C)	0	4	0	N/A
	Oct 14, 2014, 6:59:59 AM	192.168....	64334	192.168.10.10	22	tcp_ip	RemoteAccess.SSH	3,816	64,432	48	52	N/A
	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
	Oct 14, 2014, 7:00:09 AM	192.168....	61190	192.203.230.10	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
	Oct 14, 2014, 7:00:53 AM	0.0.0.0	546	0.0.0.0	547	udp_ip	Other	459 (C)	0	3	0	N/A
	Oct 14, 2014, 7:00:24 AM	192.168....	64348	192.168.10.10	443	tcp_ip	Web.SecureWeb	3,559	24,010	19	23	N/A
	Oct 14, 2014, 7:00:05 AM	192.168....	61709	192.168.10.1	53	udp_ip	Misc.domain	101 (C)	0	1	0	N/A
	Oct 14, 2014, 6:59:59 AM	192.168....	61897	192.168.99.1	53	udp_ip	Misc.domain	78	0	1	0	N/A
	Oct 14, 2014, 7:00:01 AM	192.168....	64335	192.168.10.10	443	tcp_ip	Web.SecureWeb	192	297	3	4	N/A
	Oct 14, 2014, 7:00:05 AM	192.168....	N/A	192.168.10.12	N/A	icmp_ip	ICMP:Destination-Unreachable	129 (C)	0	1	0	Port Unreac...

Event and Flow Collection



Events not counted agains 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

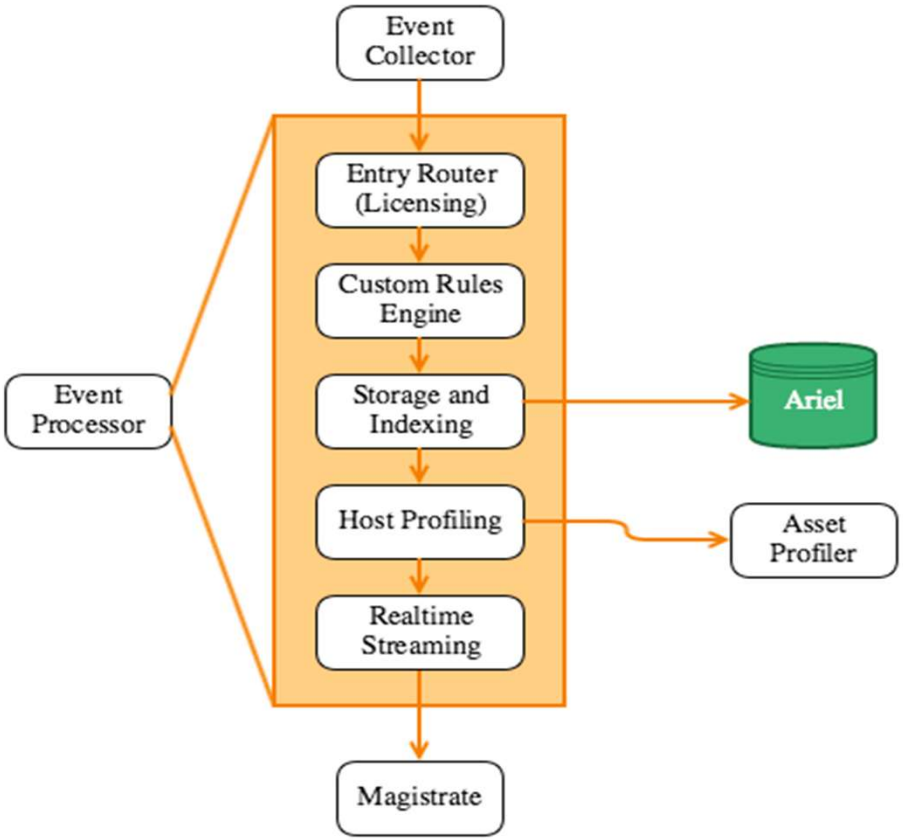
  - For any events that are dropped from the pipeline using routing rules the dropped events will be partially credited back.
  - EPS is credited back at 60% of the events dropped to a maximum of 2000 EPS.

Event Coalescing

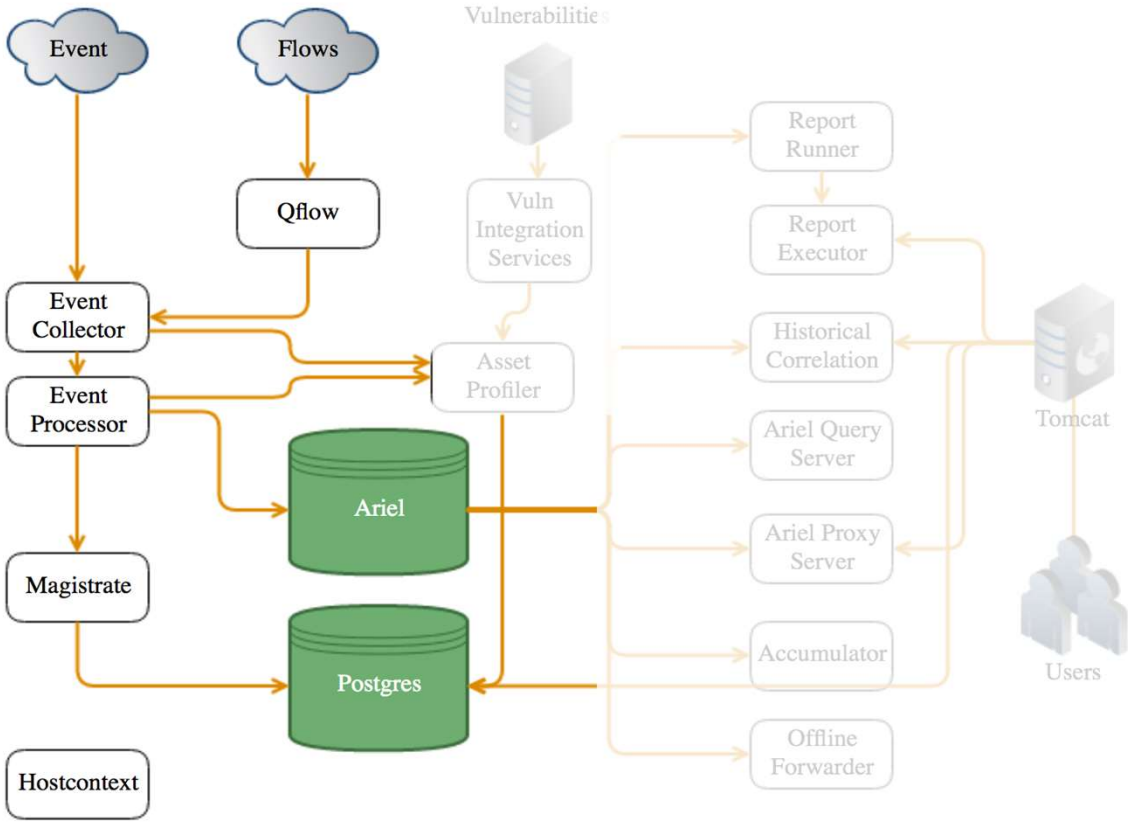
Event Coalescing is a method of reducing the data going through the pipeline.

- 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.

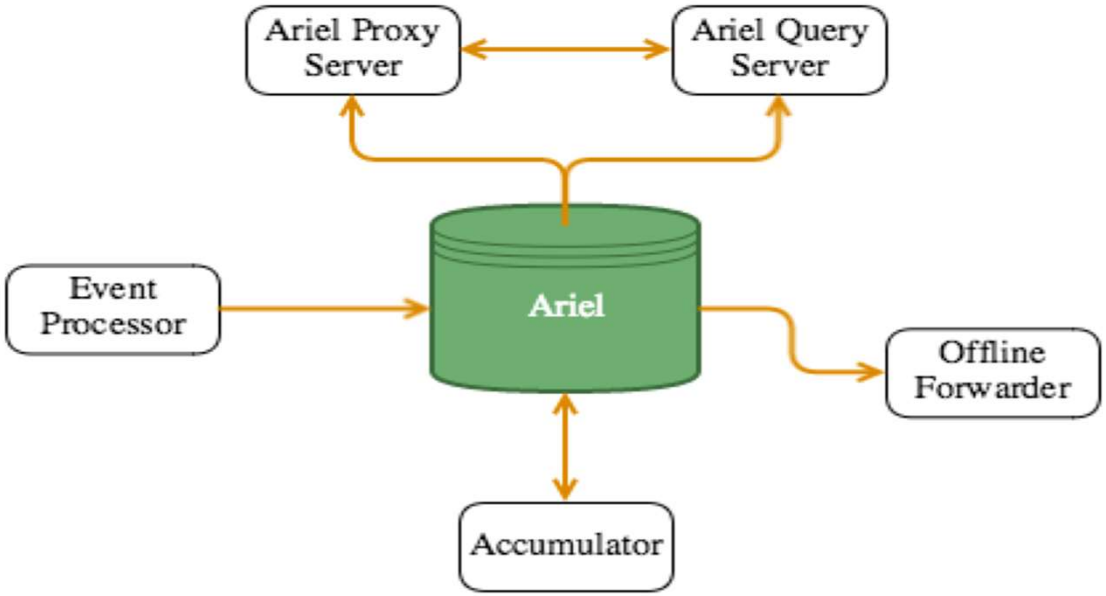
Event and Flow Correlation and Processing



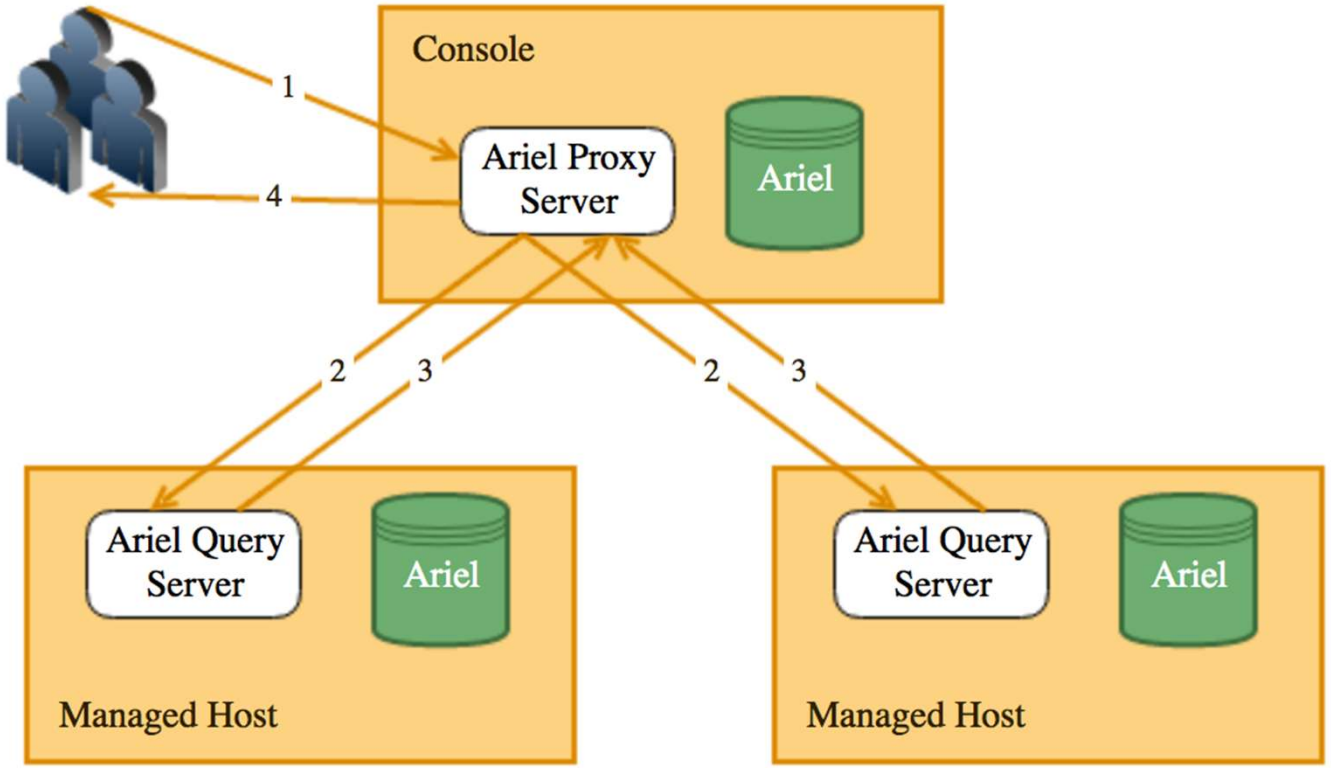
Where we are


Event
Flows
Qflow
Event Collector
Event Processor
Magistrate
Hostcontext
Ariel
Postgres
Vulnerabilitie
Vuln Integration Services
Asset Profiler
Report Runner
Report Executor
Historical Correlation
Ariel Query Server
Ariel Proxy Server
Accumulator
Offline Forwarder
Tomcat
Users

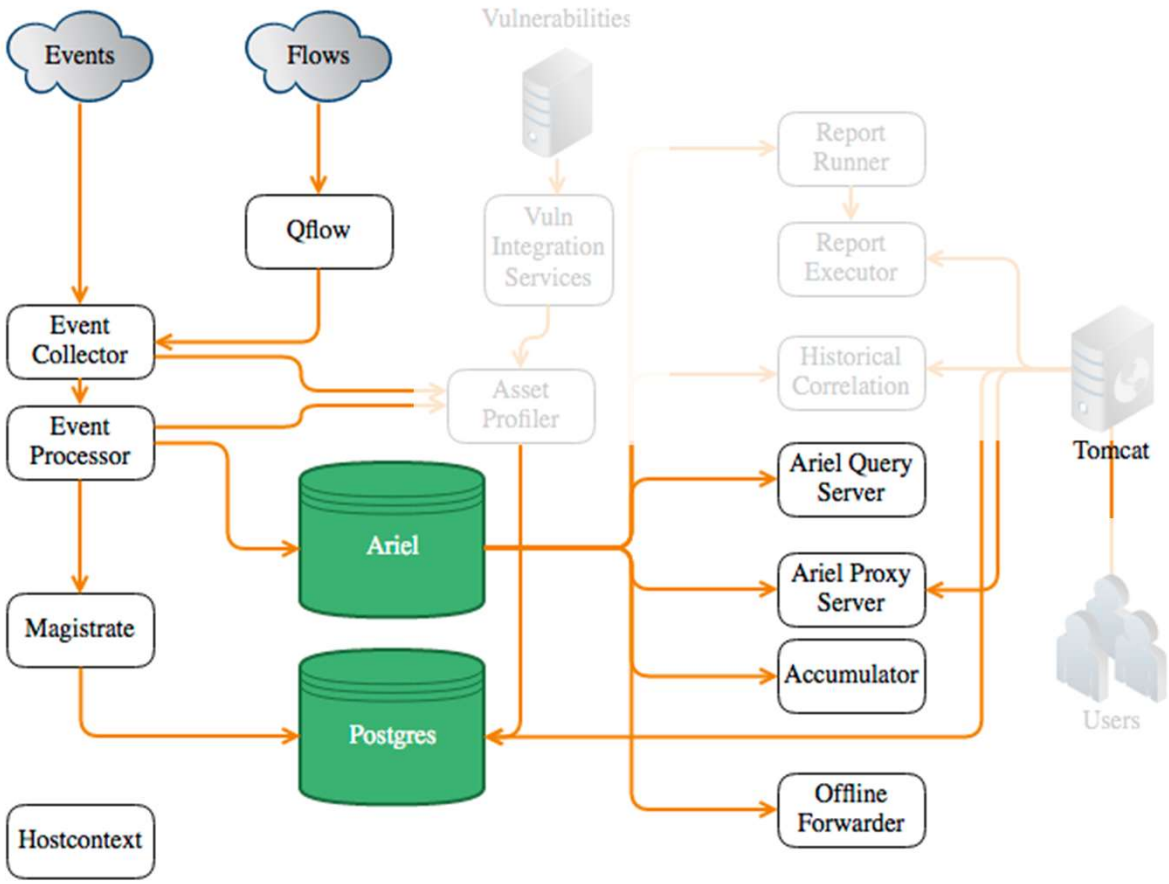
Ariel Components



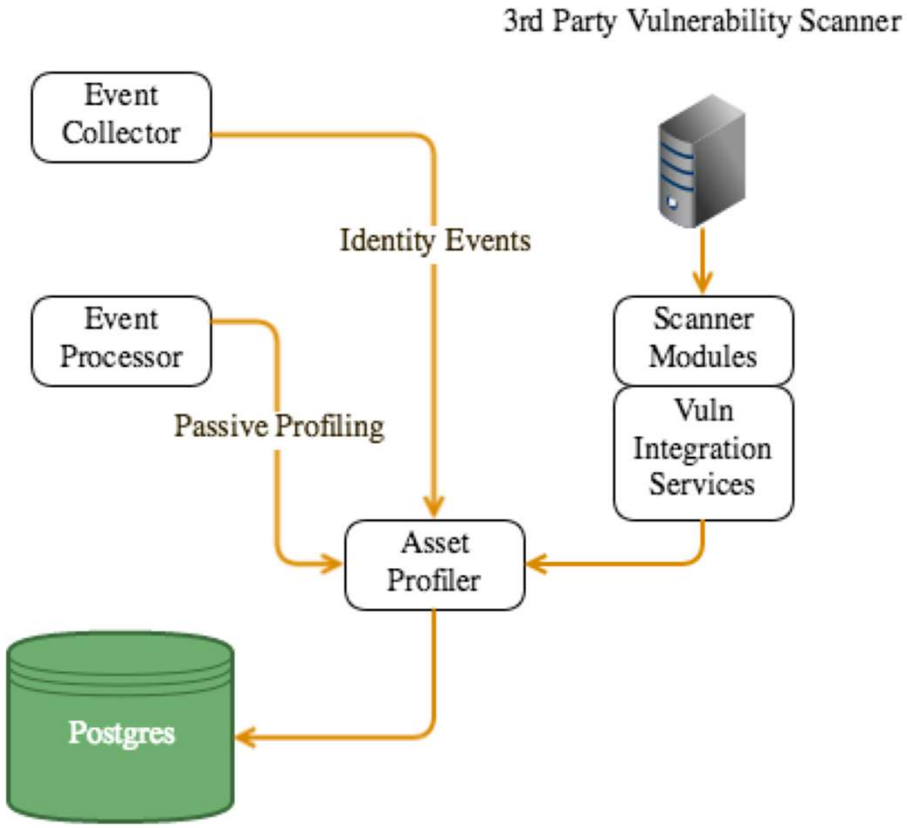
Ariel Search Flow



Where we are


Events
Flows
Vulnerabilities
Report Runner
Qflow
Vuln Integration Services
Report Executor
Event Collector
Historical Correlation
Asset Profiler
Tomcat
Event Processor
Ariel Query Server
Ariel
Ariel Proxy Server
Magistrate
Accumulator
Postgres
Users
Offline Forwarder
Hostcontext

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:

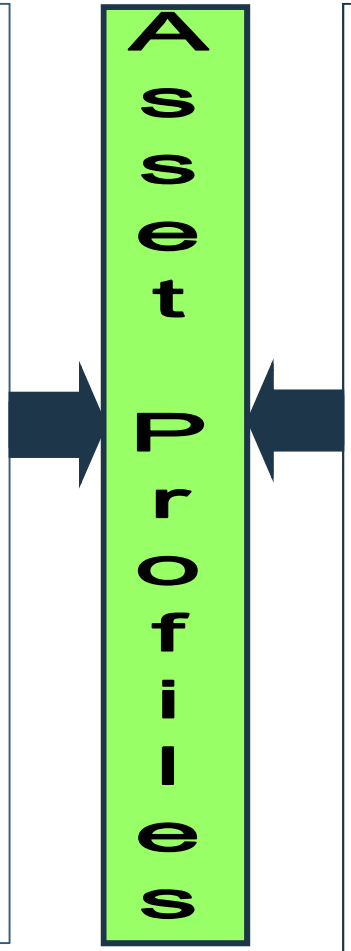
- List of hosts with risks and potential vulnerabilities
- IP and MAC addresses
- Open ports
- Services and versions
- Operating system

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

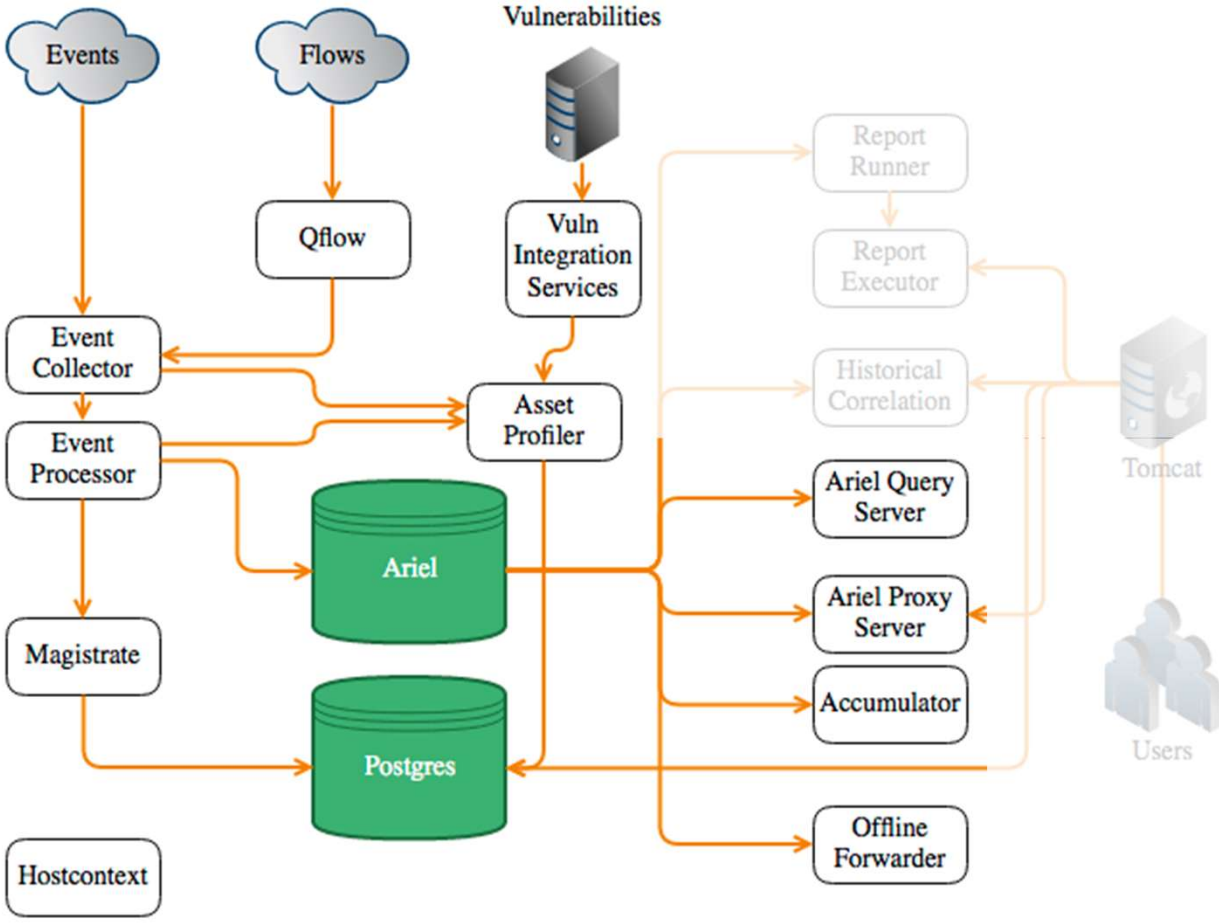
Asset profiles

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

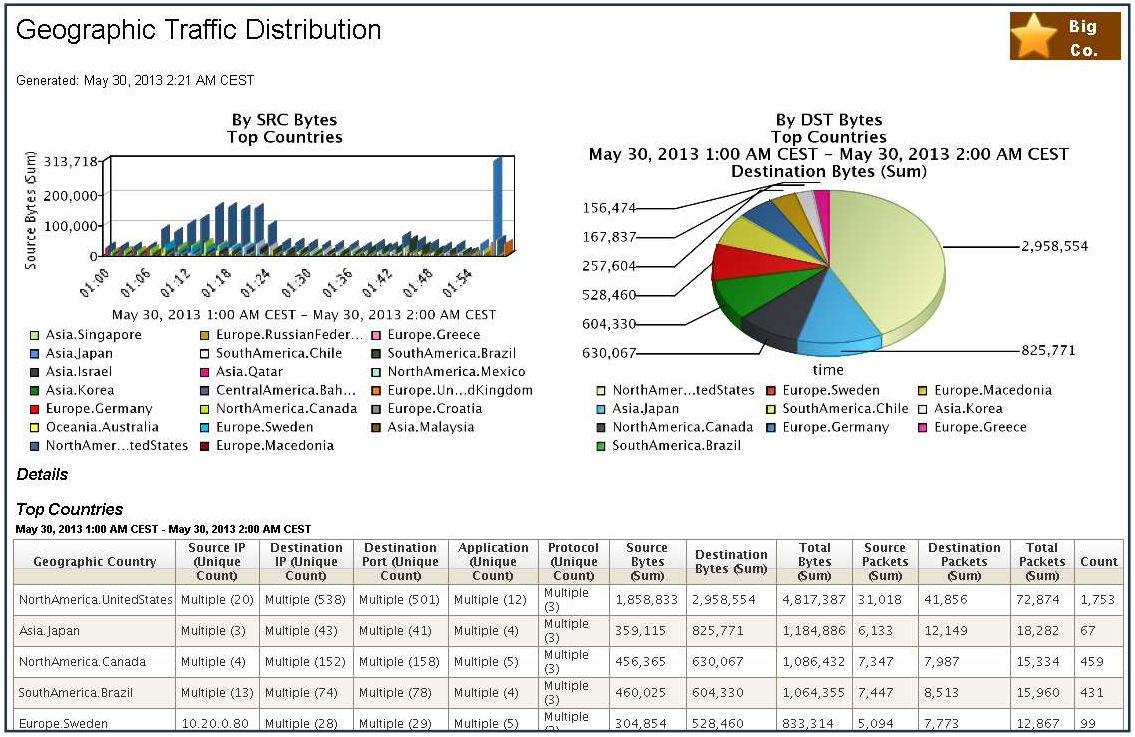
Where we are


Events
Flows
Vulnerabilities
Qflow
Vuln Integration Services
Report Runner
Report Executor
Historical Correlation
Event Collector
Asset Profiler
Event Processor
Tomcat
Ariel Query Server
Ariel
Ariel Proxy Server
Magistrate
Accumulator
Postgres
Users
Offline Forwarder
Hostcontext

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



Geographic Traffic Distribution

Big Co.

Generated: May 30, 2013 2:21 AM CEST

By SRC Bytes
Top Countries

By DST Bytes
Top Countries
May 30, 2013 1:00 AM CEST - May 30, 2013 2:00 AM CEST
Destination Bytes (Sum)

Details

Top Countries

May 30, 2013 1:00 AM CEST - May 30, 2013 2:00 AM CEST

Geographic Country	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Application (Unique Count)	Protocol (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
NorthAmerica.UnitedStates	Multiple (20)	Multiple (538)	Multiple (501)	Multiple (12)	Multiple (3)	1,858,833	2,958,554	4,817,387	31,018	41,856	72,874	1,753
Asia.Japan	Multiple (3)	Multiple (43)	Multiple (41)	Multiple (4)	Multiple (3)	359,115	825,771	1,184,886	6,133	12,149	18,282	67
NorthAmerica.Canada	Multiple (4)	Multiple (152)	Multiple (158)	Multiple (5)	Multiple (3)	456,365	630,067	1,086,432	7,347	7,987	15,334	459
SouthAmerica.Brazil	Multiple (13)	Multiple (74)	Multiple (78)	Multiple (4)	Multiple (3)	460,025	604,330	1,064,355	7,447	8,513	15,960	431
Europe.Sweden	10.20.0.80	Multiple (28)	Multiple (29)	Multiple (5)	Multiple	304,854	528,460	833,314	5,094	7,773	12,867	99

- 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

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

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.

IBM

IBM Security

Deployment Models and Licensing

IBM

QRadar Dashboard - Fully integrated architecture and interface

Log Management

Security Intelligence (SIEM)

Vulnerability Management & Risk Assessment

Network and Application Visibility

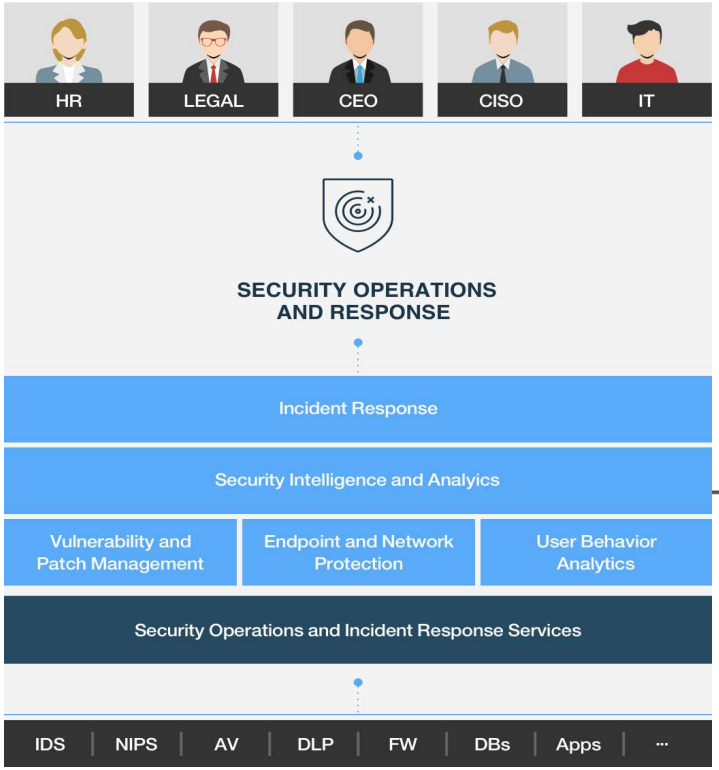
One Console Security

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

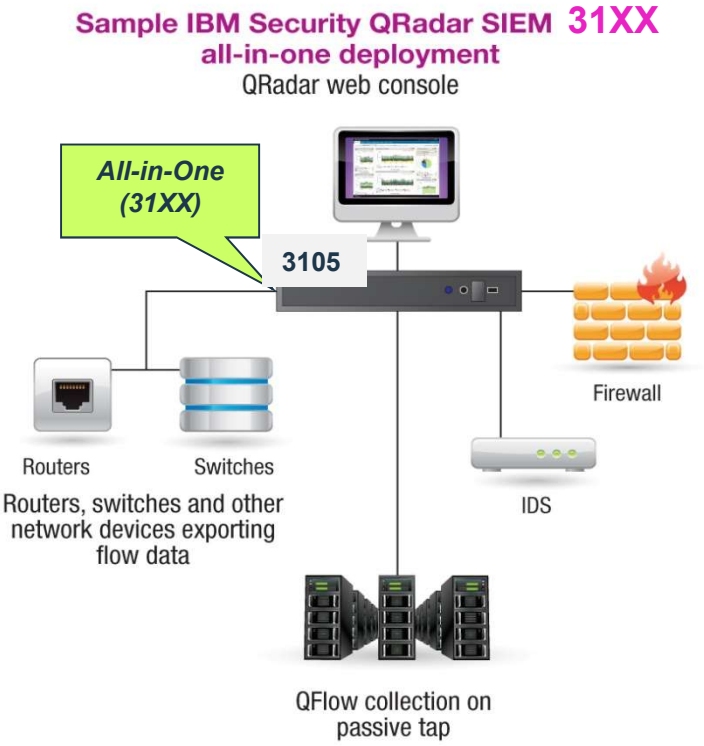
QRadar Vulnerability Manager, including Risk Management

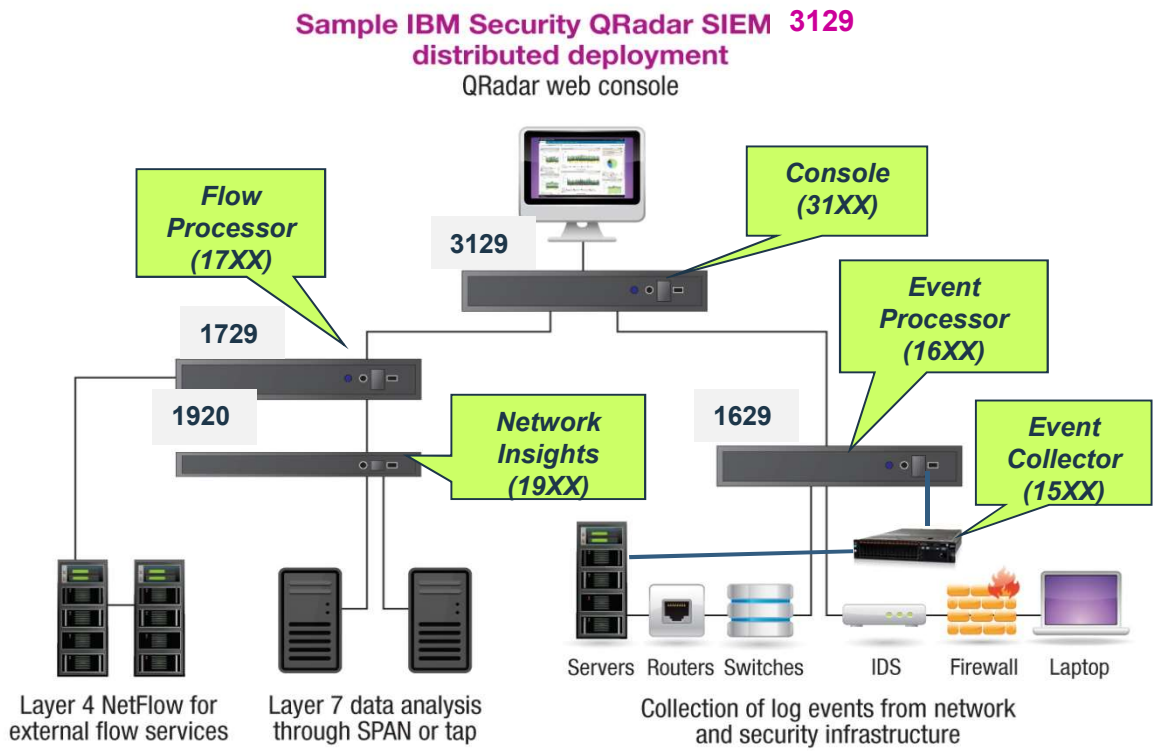
- Integrated Network Scanning & Workflow
- Risk Management to prioritize vulnerabilities
- Predictive threat modeling & simulation
- Scalable configuration monitoring and audit
- Advanced threat and impact analysis

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





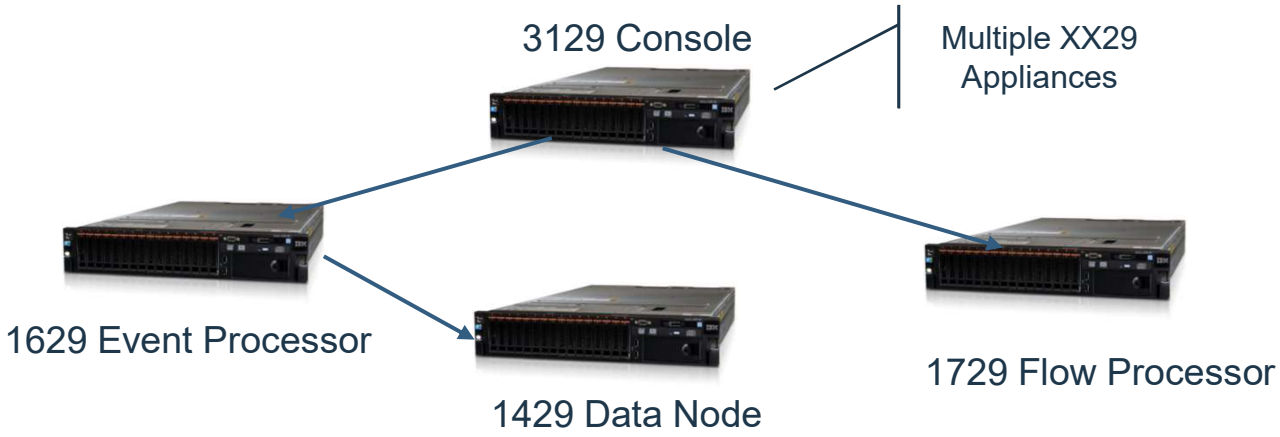
All-in-One is a single appliance used to collect both events and flow data from various security and network devices, perform data correlation and rule matching, report alerts/threats, and provide all admin functions through a Web browser.

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

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..



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 (D1RNRLL)
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.

IBM Security

Appliance Types

IBM

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 **XX**

Software Role/Type **Hardware Designation**

- **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

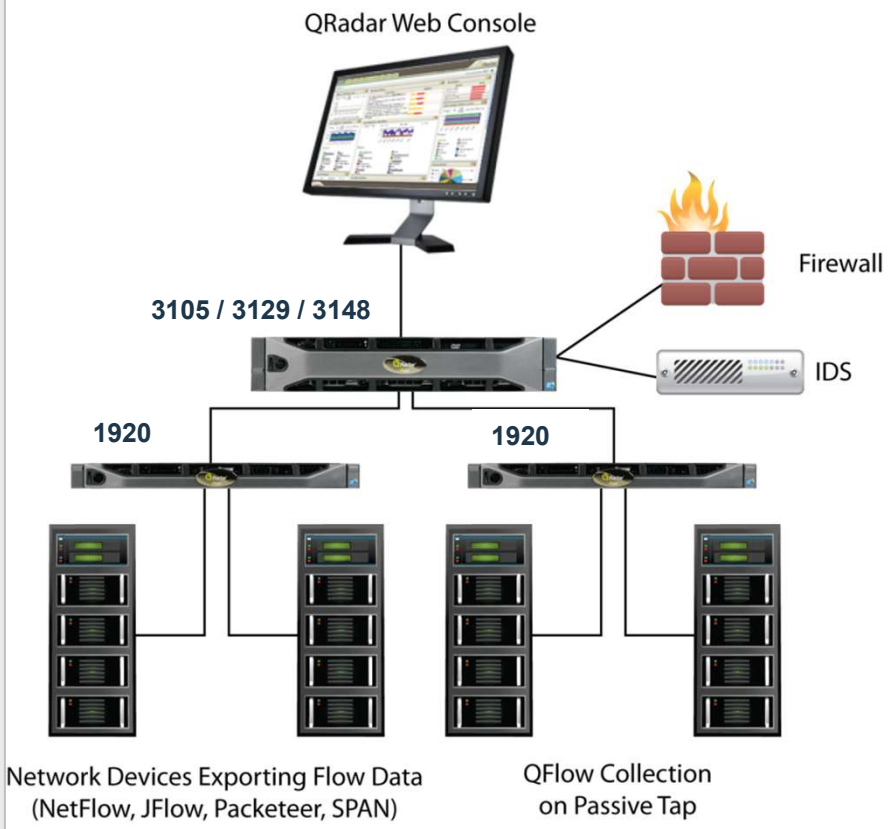
- **Hardware Codes:**
  - XX05 = Based on x3550 M5 BD, 64GB RAM, 6.2TB storage
  - XX28-C* = Based on PowerEdge R730xd XL, 128GB RAM, 40TB storage
  - XX29 = Based on x3650 M5 BD, 128GB RAM, 72TB storage
  - XX48 = Based on X3650 M5 BD, 128GB RAM, 24TB storage
  - XX01/02* = 1Gbps / 3Gbps (Qflow Only)
  - 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

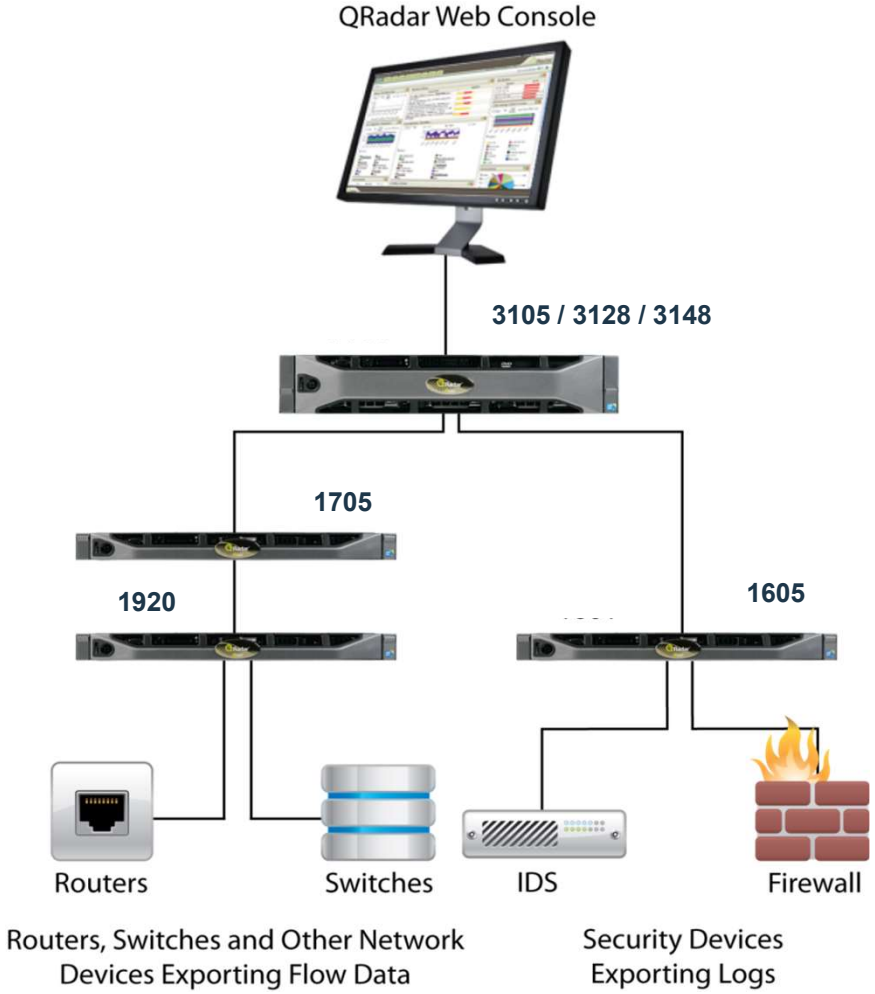
- **Positioning**
  - – QRadar appliance for centralized deployment in a small/medium/large enterprise
  - – Contains event & flow processing capabilities
- **Characteristics and Capacity**
  - **Memory Capacity**
  - 3015 – 64 GB
  - 3129/3128-C/3148 – 128 GB
  - – Requires ***external*** QFlow Collectors 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**

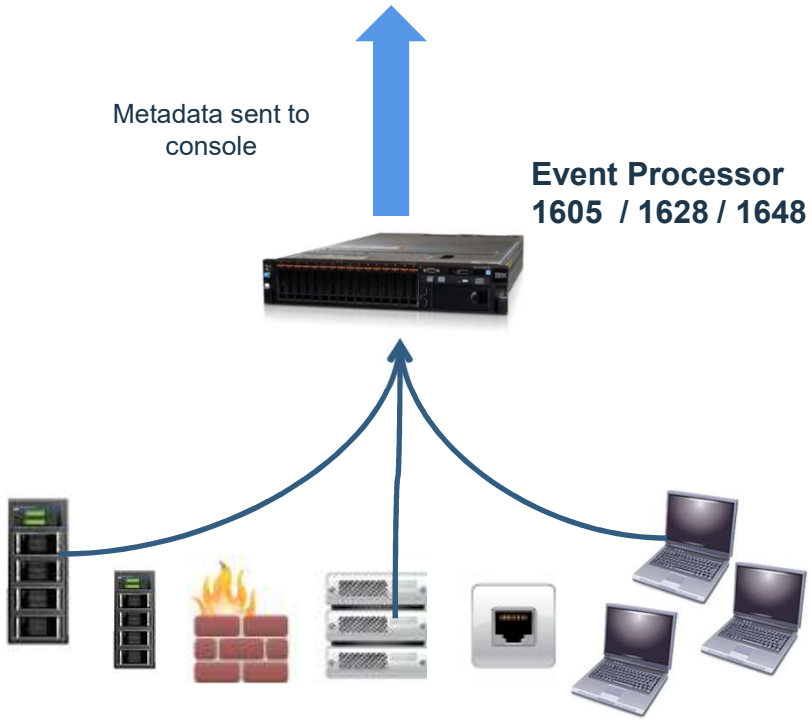
*May vary based on configuration



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

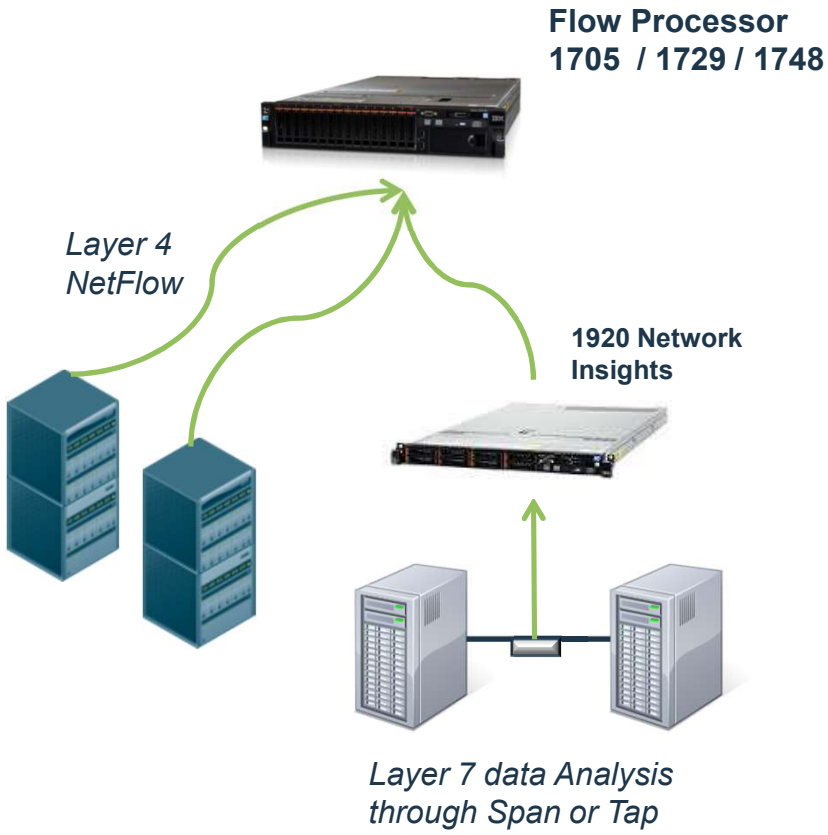


Collection of log events from network and security infrastructure

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**

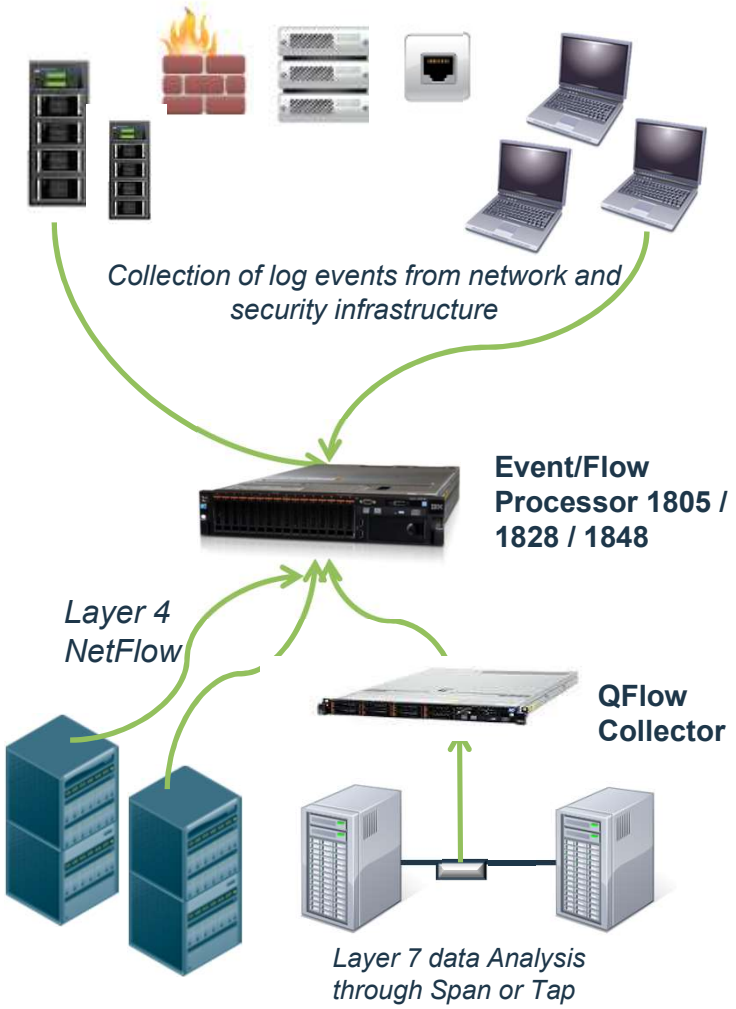
*May vary based on configuration



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**

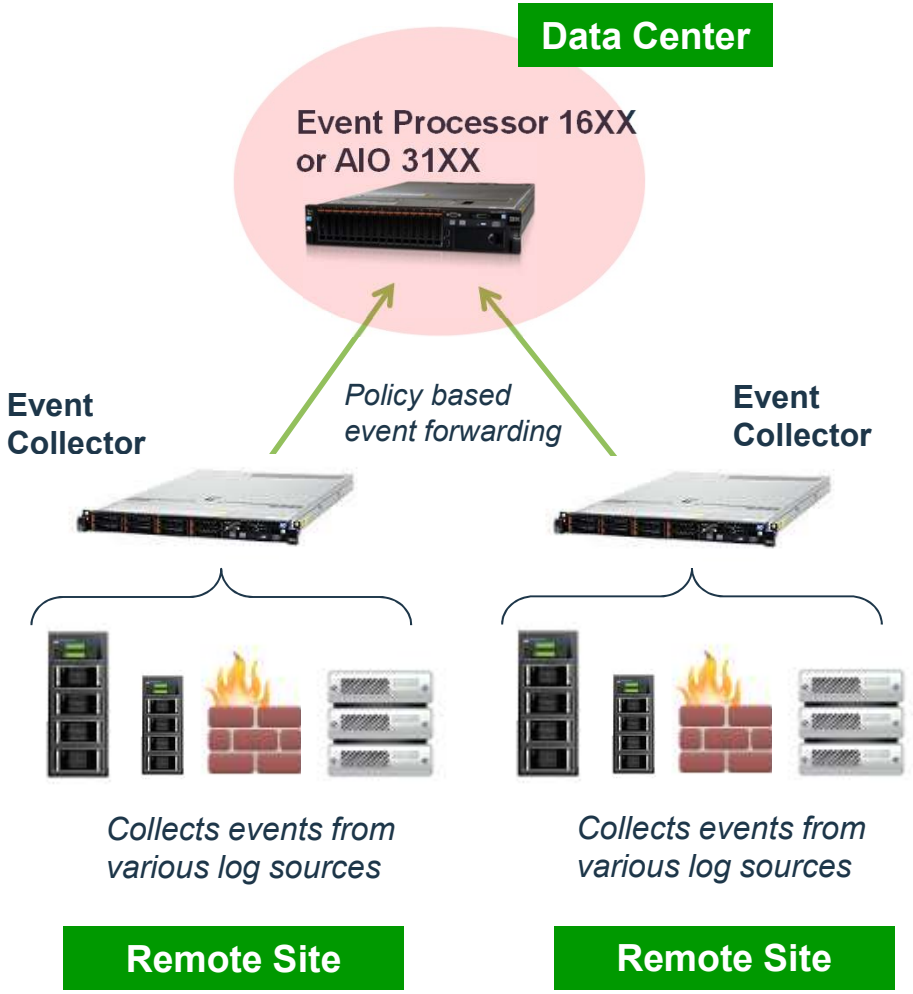
*May vary based on configuration



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**

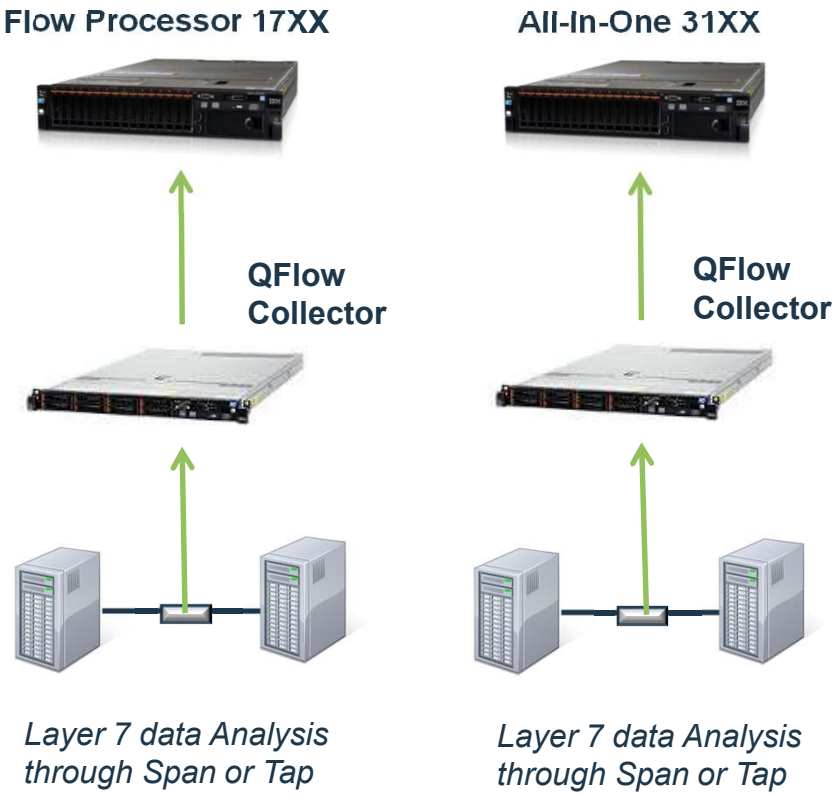


QFlow Collector 1201, 1202, 1301, and 1310 Appliances

- **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

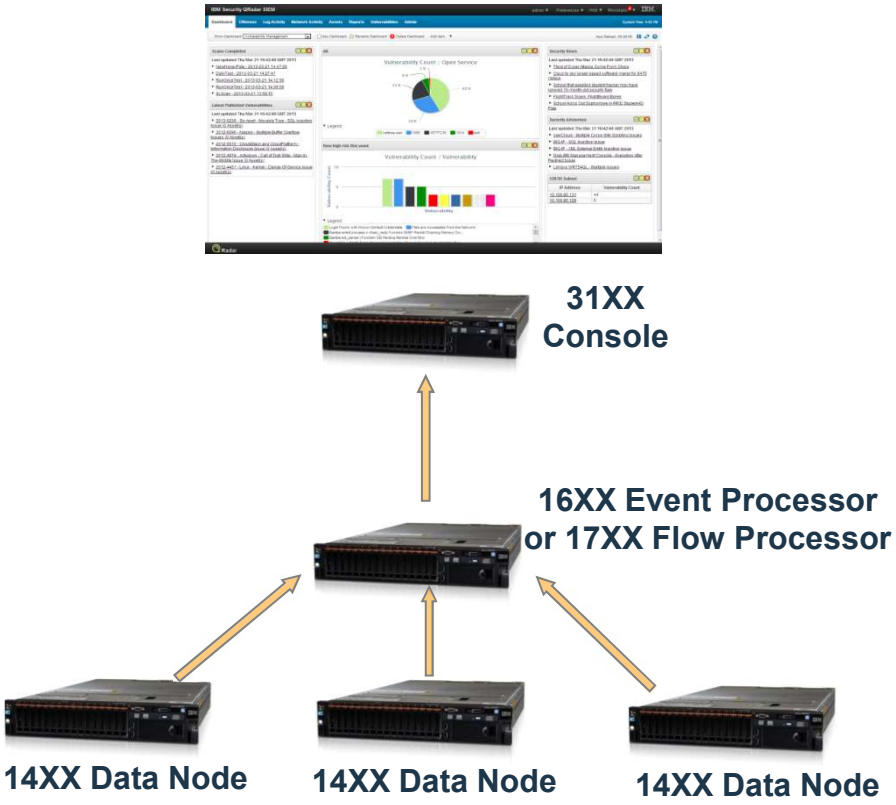
–**HA/DR NOT available**

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



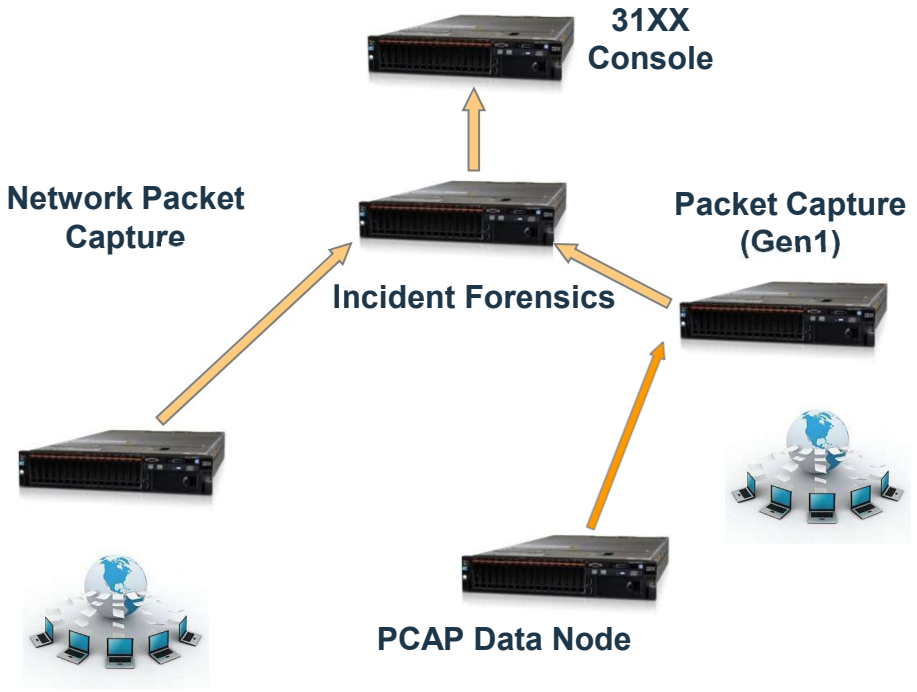
Data Node 1405 and 1429 Appliances

- **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**



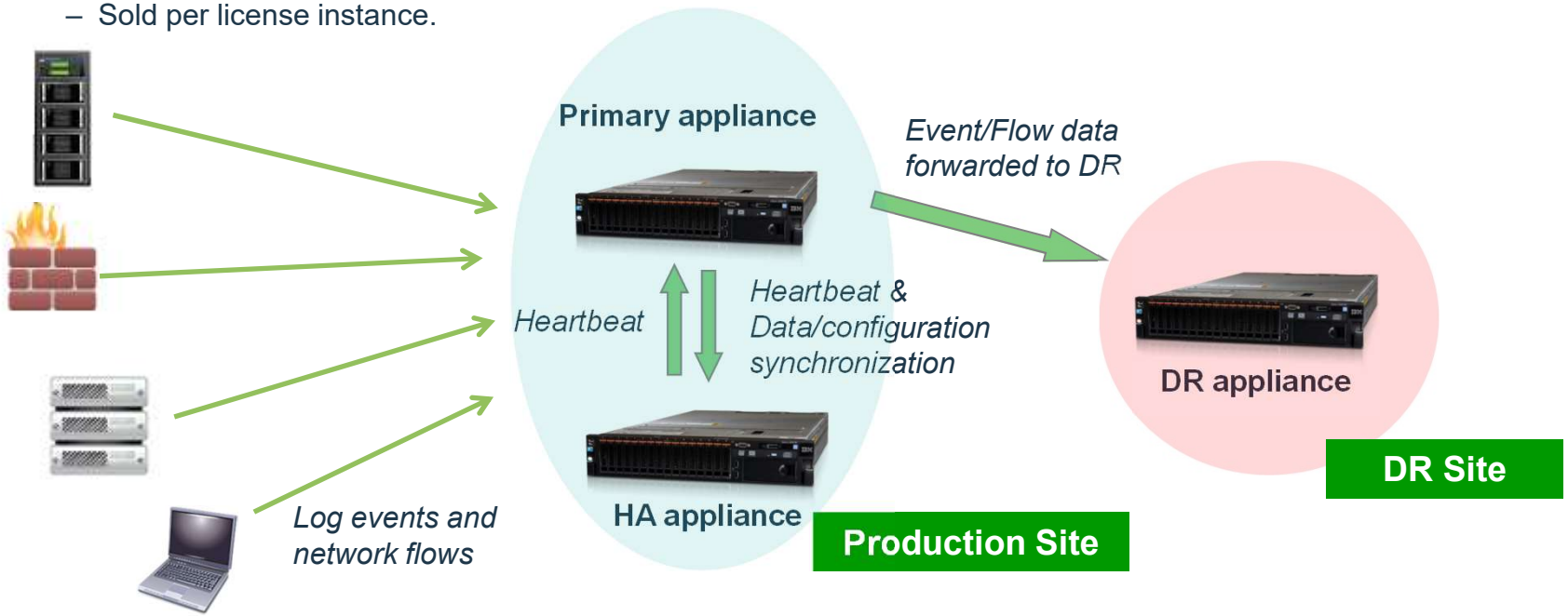
Packet Capture and Incident Forensics Appliances

- **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

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

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.

IBM

IBM Security

Using the Dashboard

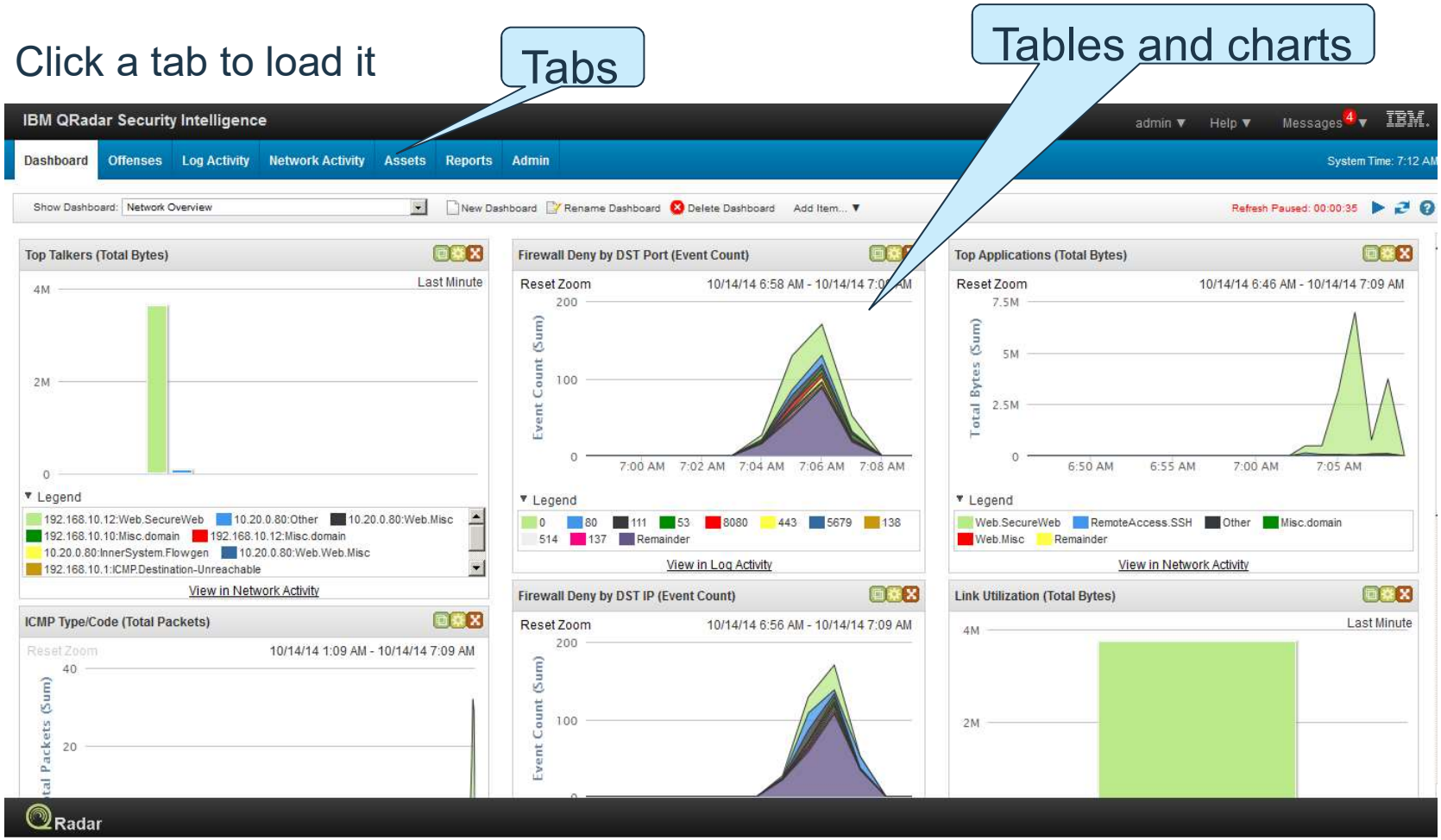
IBM

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

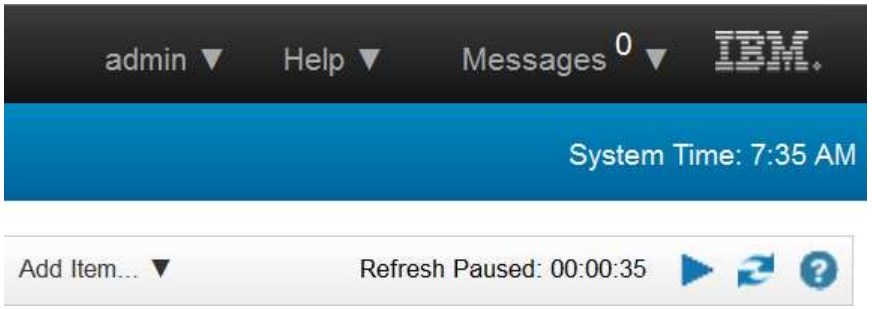


QRadar SIEM tabs

Use tabs to navigate the primary QRadar SIEM functions

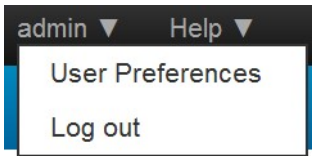
- **Dashboard**: The initial summary view
- **Offenses**: Displays offenses; list of prioritized incidents
- **Log Activity**: Query and display events
- **Network Activity**: Query and display flows
- **Assets**: Query and display information about systems in your network
- **Reports**: Create templates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

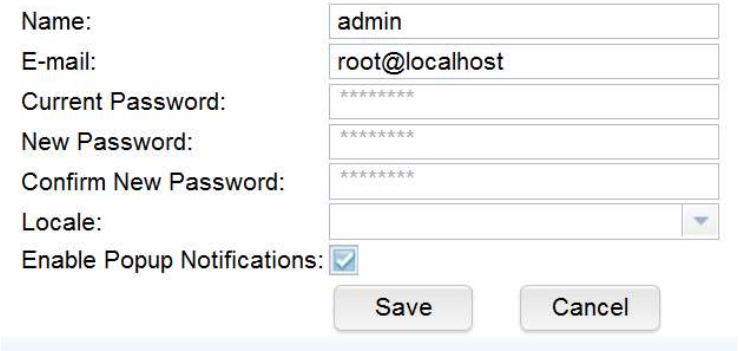
Other menu options



The dashboard has the following additional menu options

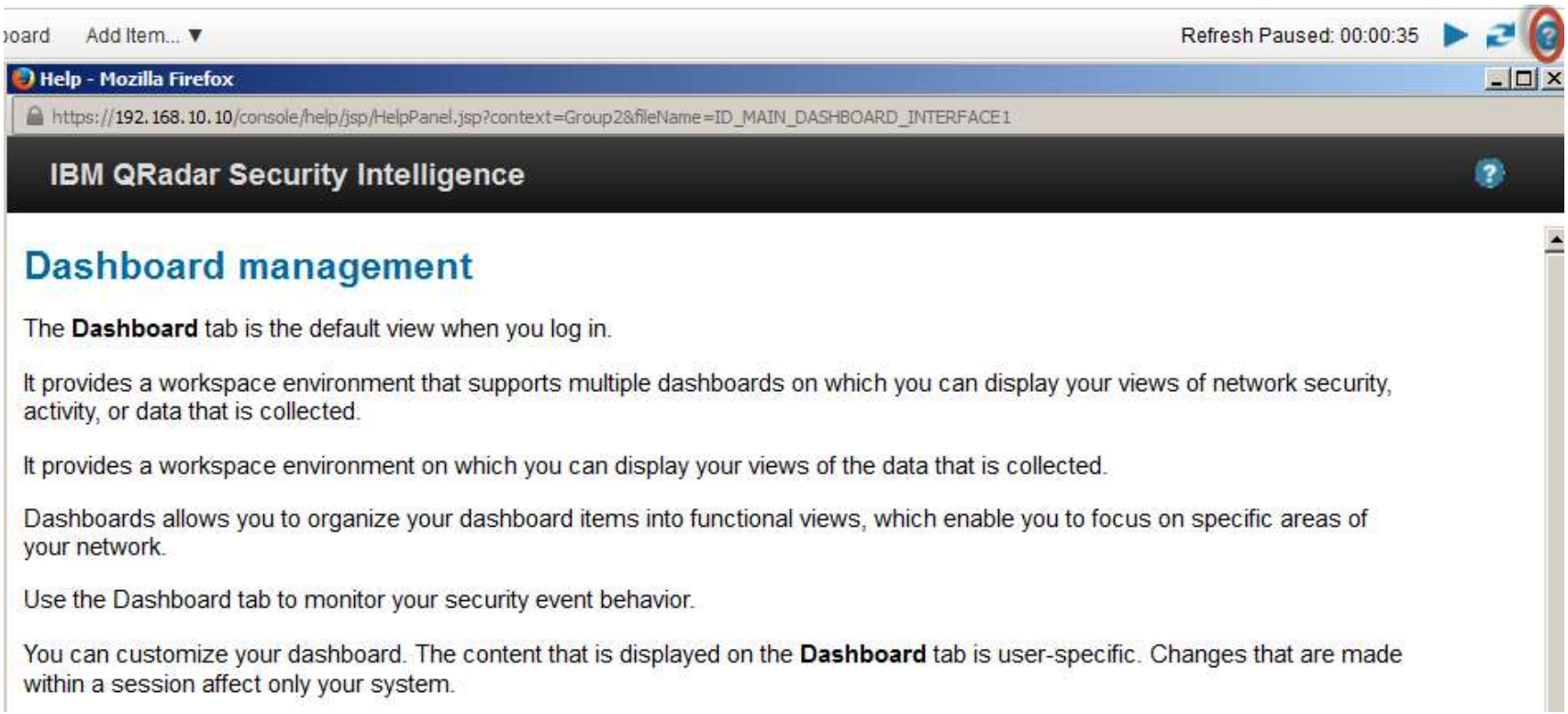
- **User Preferences**
- **Help**
- **Log out**





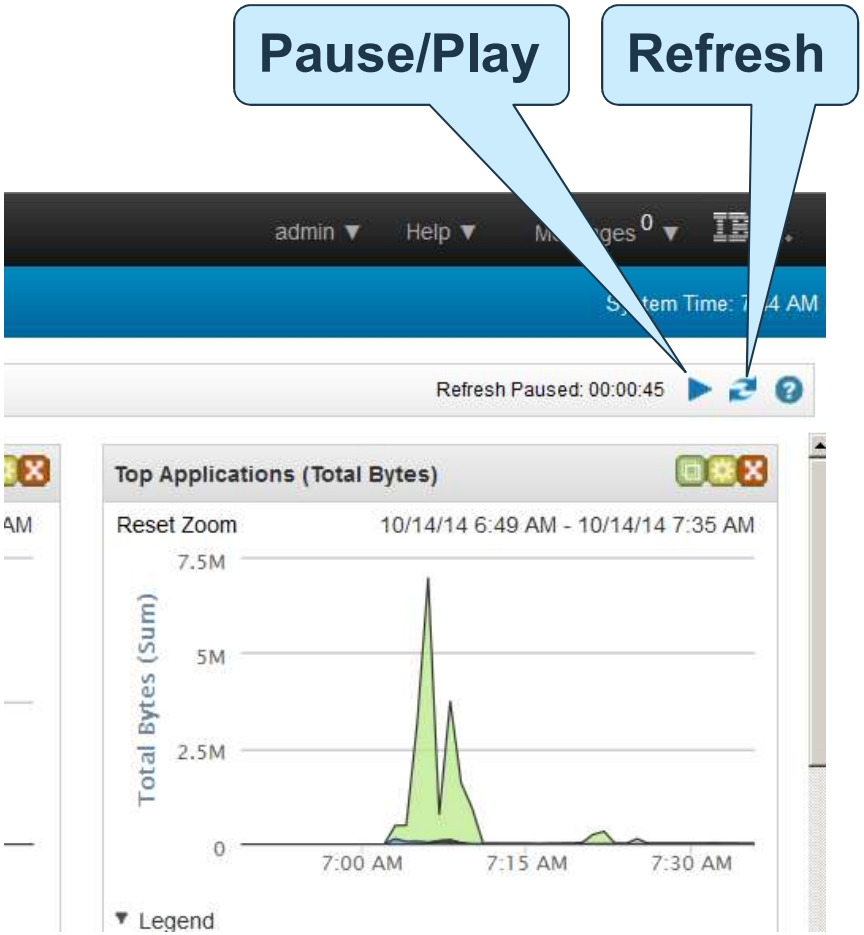
Context-sensitive help

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



Dashboard refresh

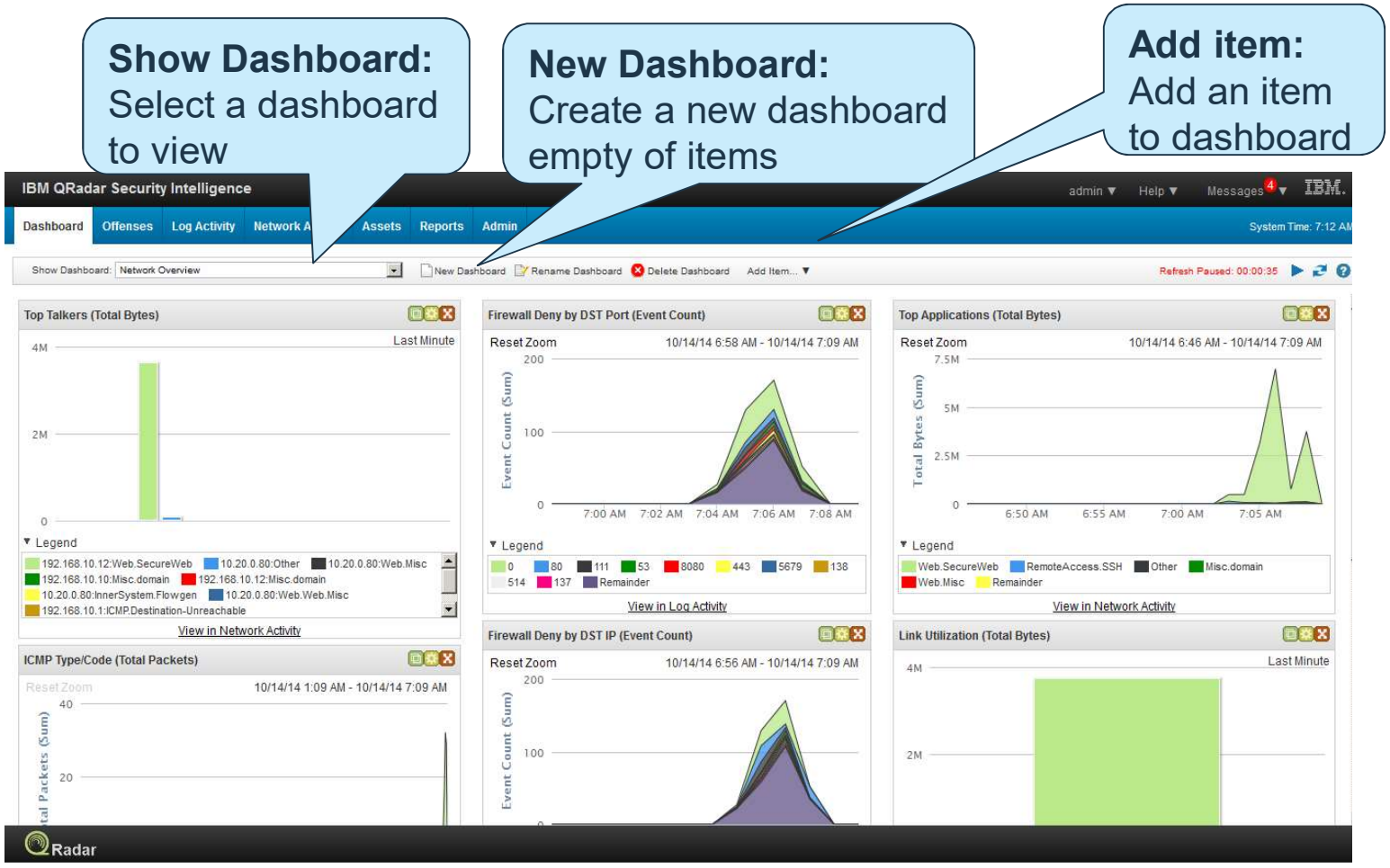
- In the displayed dashboard, events and flows refresh every minute unless you click **Pause**
- Use the **Refresh** button to manually refresh the displayed data



Dashboard Types

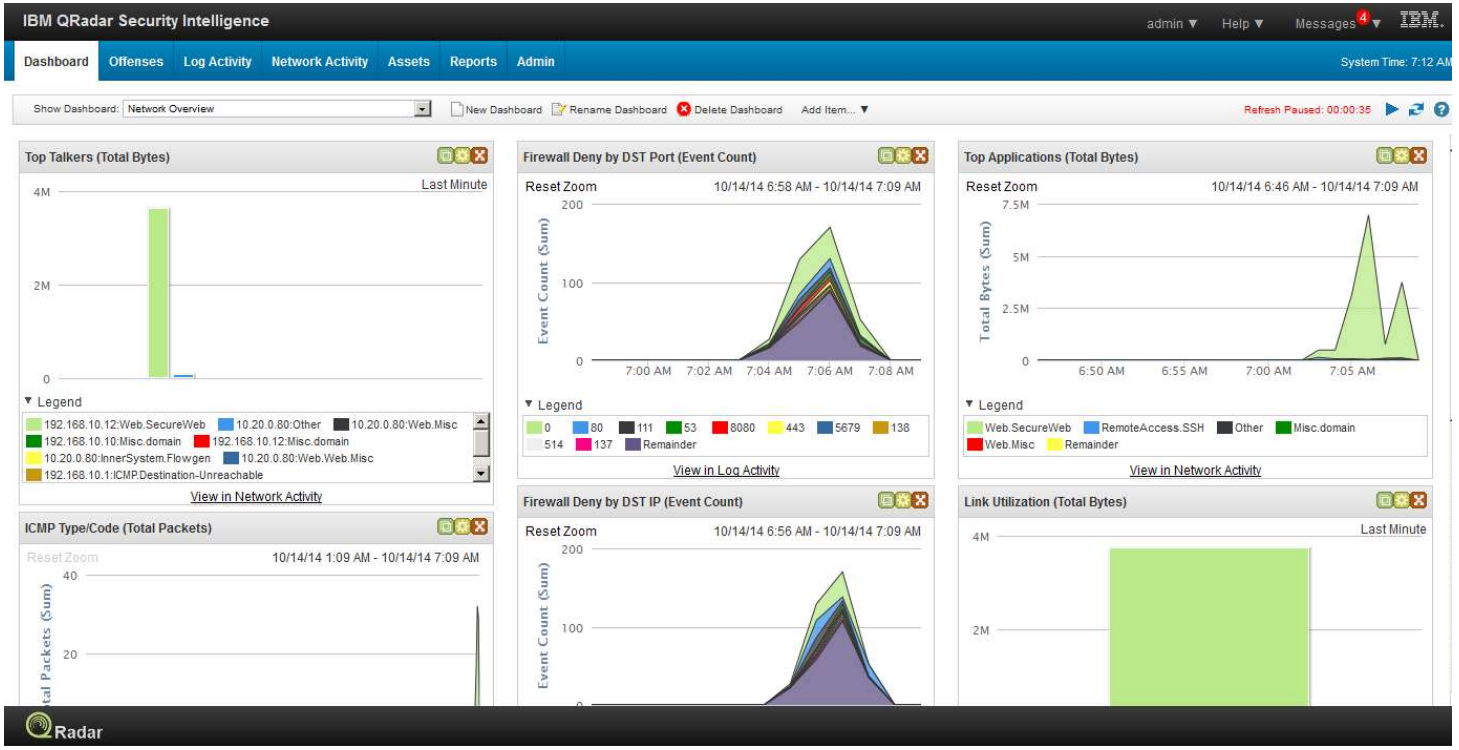
- QRadar SIEM includes the following default dashboards
  - Application Overview
  - Compliance Overview
  - Network Overview
  - Risk Monitoring
  - System Monitoring
  - Threat and Security Monitoring
  - Virtual Cloud Infrastructure
  - Vulnerability Management
- Use multiple dashboards to better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

Creating a custom dashboard



Dashboard - Items

- Include no more than 15 items on each dashboard



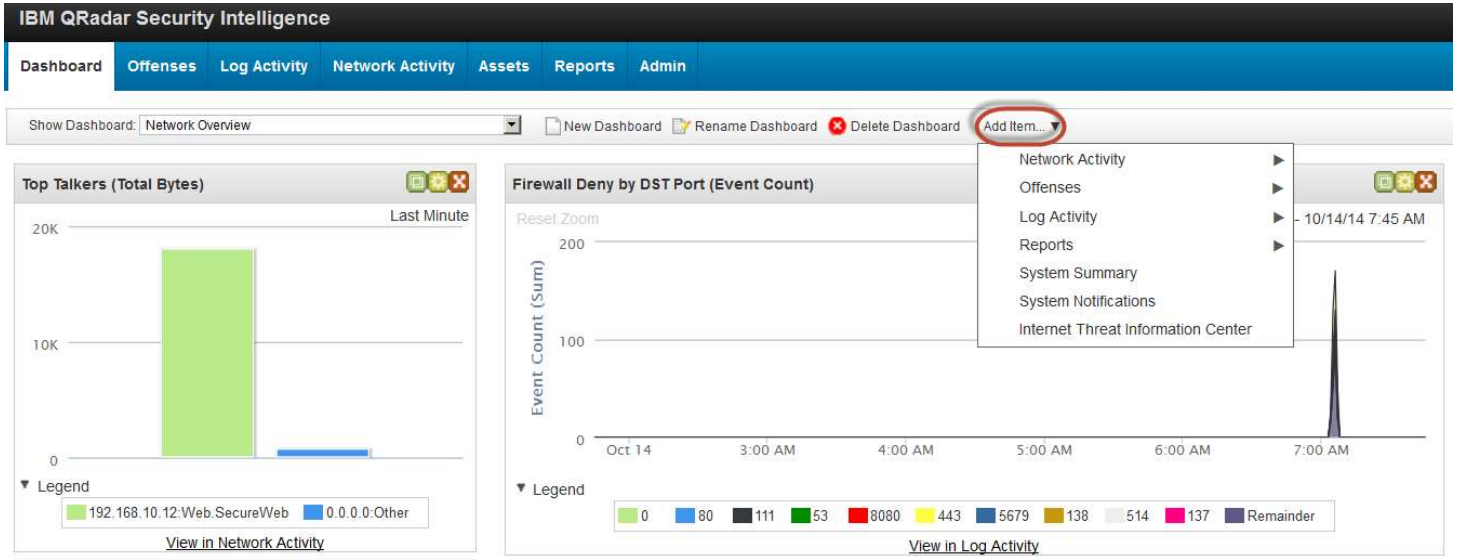
Managing dashboard items

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



IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

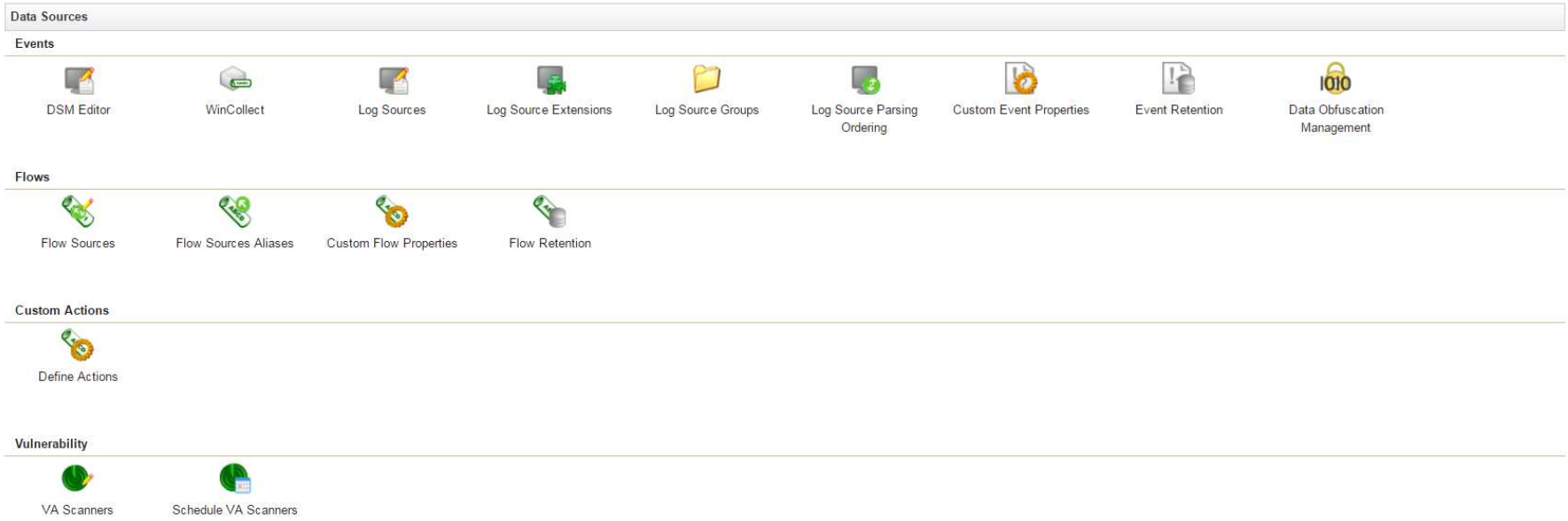
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or 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.

IBM

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

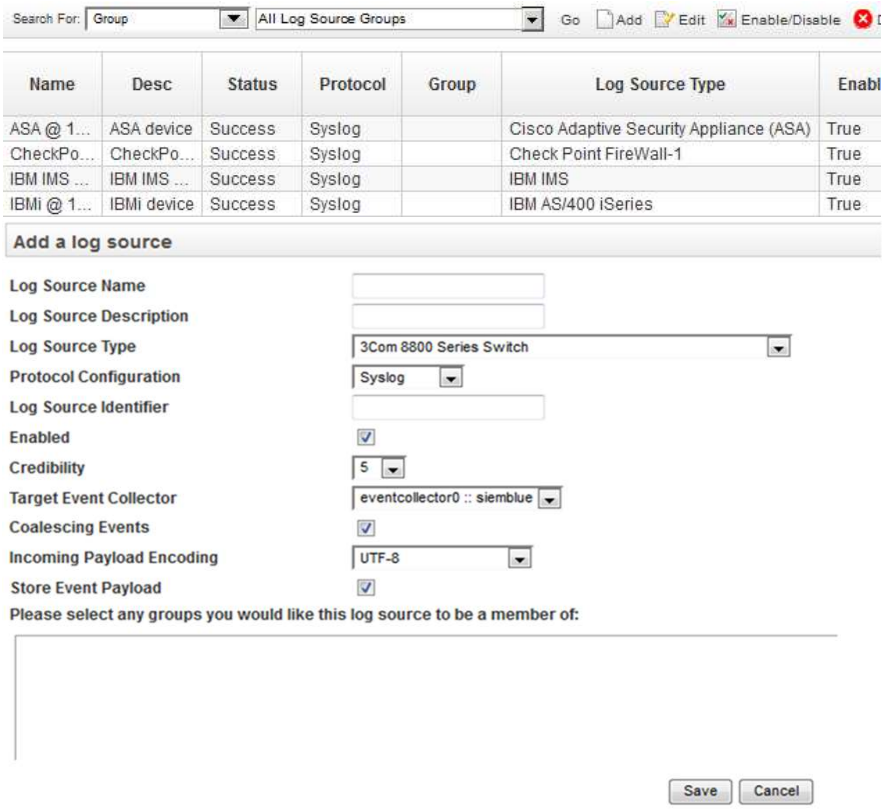
Name	Desc	Status ▲	Protocol	Group	Log Source Type
IBM zOS		Success	LogFileProtocol		IBM z/OS
Pers_DC		Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
Navy_DC		Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
Ref_DC		Error	Syslog	MSWindo...	Microsoft Windows Security Event Log
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

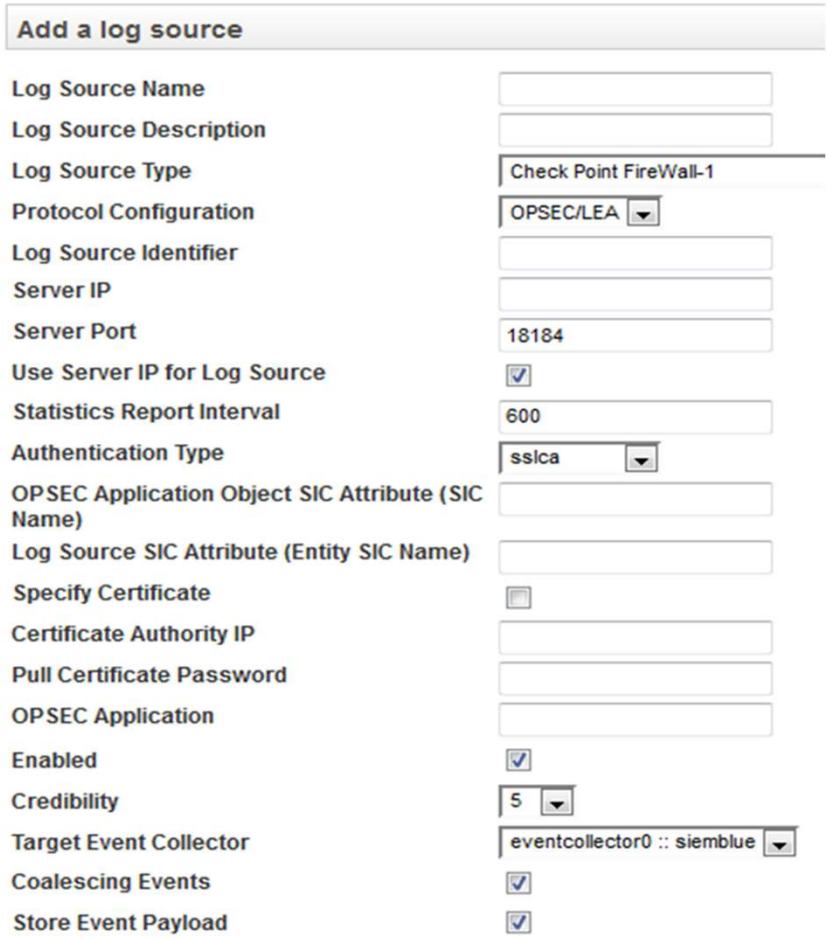
To add a log source:

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.



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.

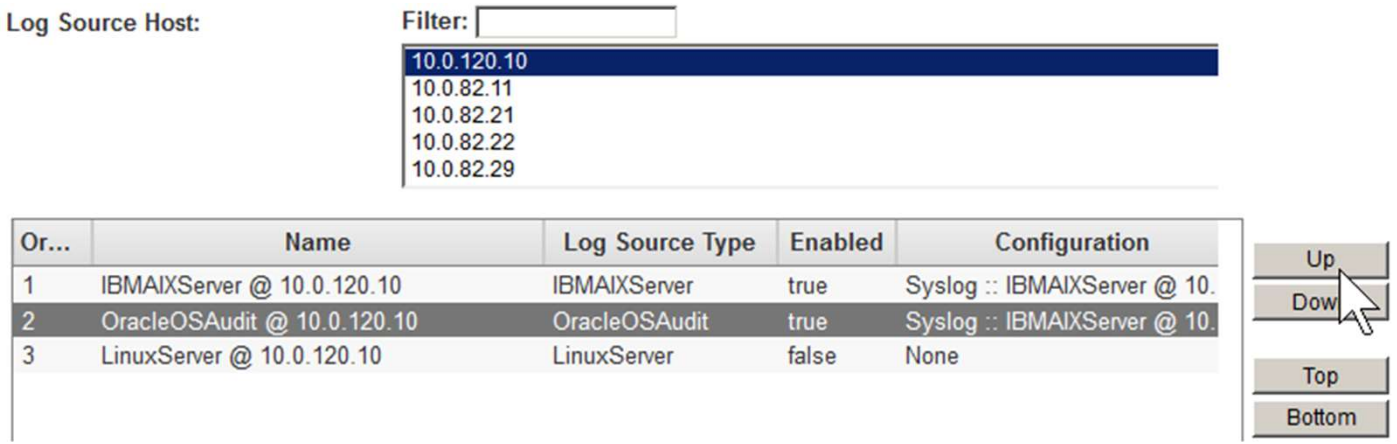


Adding log source extensions

- 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.



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

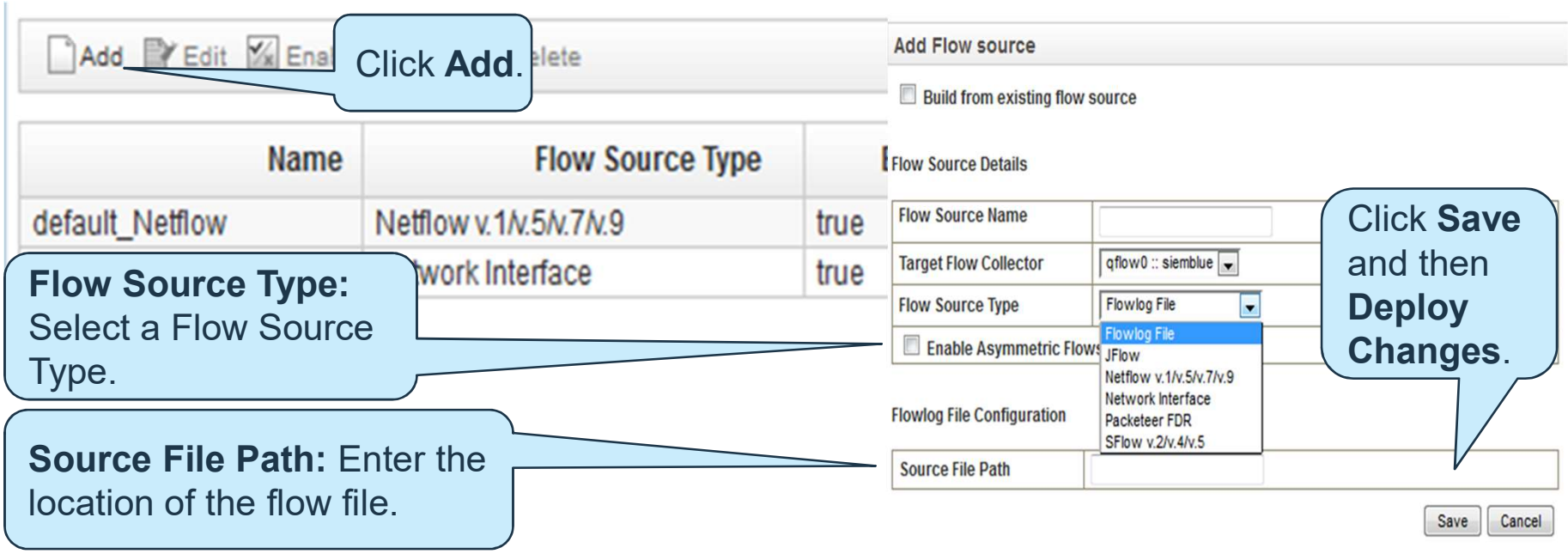
  - Accept events from devices that produce events using the Log Event Extended Format (LEEF) from Syslog of Log File
  - Proprietary event format, which allows hardware manufacturers and software product manufacturers to read and map device events specifically designed for QRadar integration
  - Both 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.

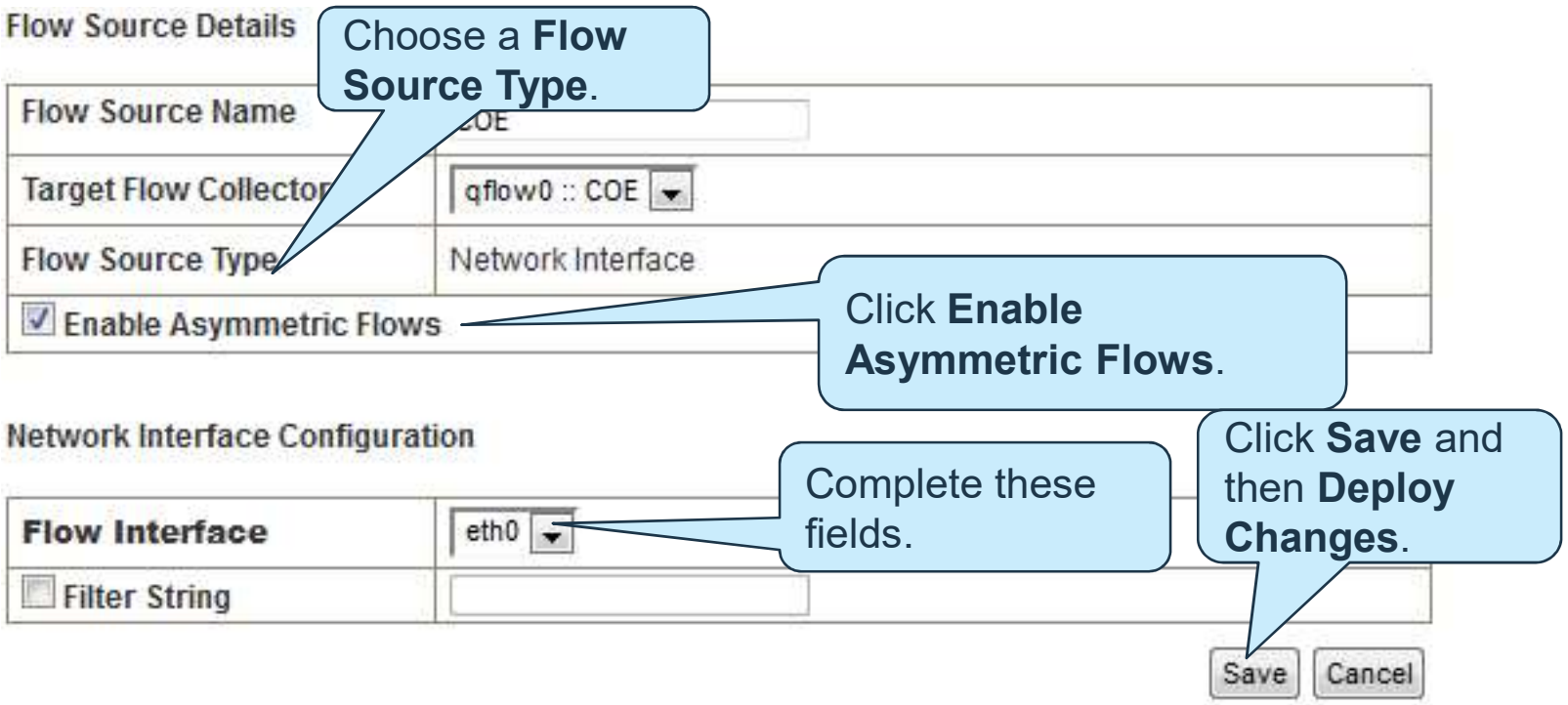
Adding a flow source

- 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.



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 aliases

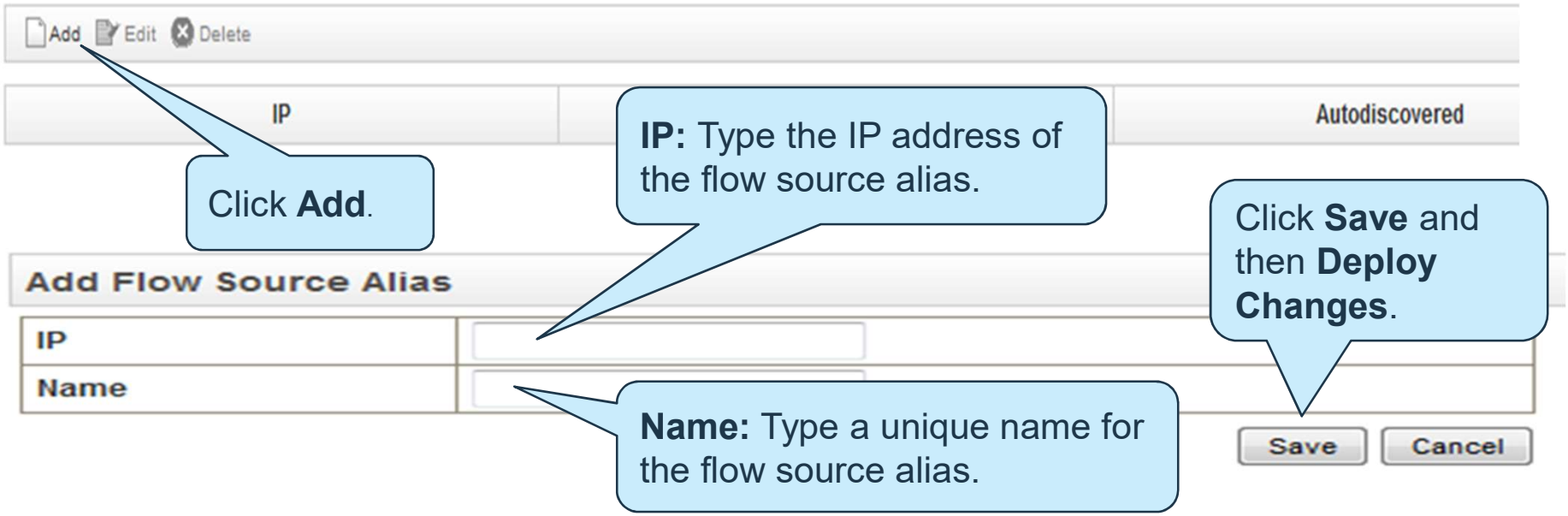
- You can configure a virtual name (or alias) for flow sources.
- Using the source IP address and virtual name, you can identify multiple sources being sent to the same QRadar QFlow Collector.
- QRadar QFlow Collector can use an alias to uniquely identify and process data sources being sent to the same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



IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

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.

IBM

Investigating event details

Navigating to the Events

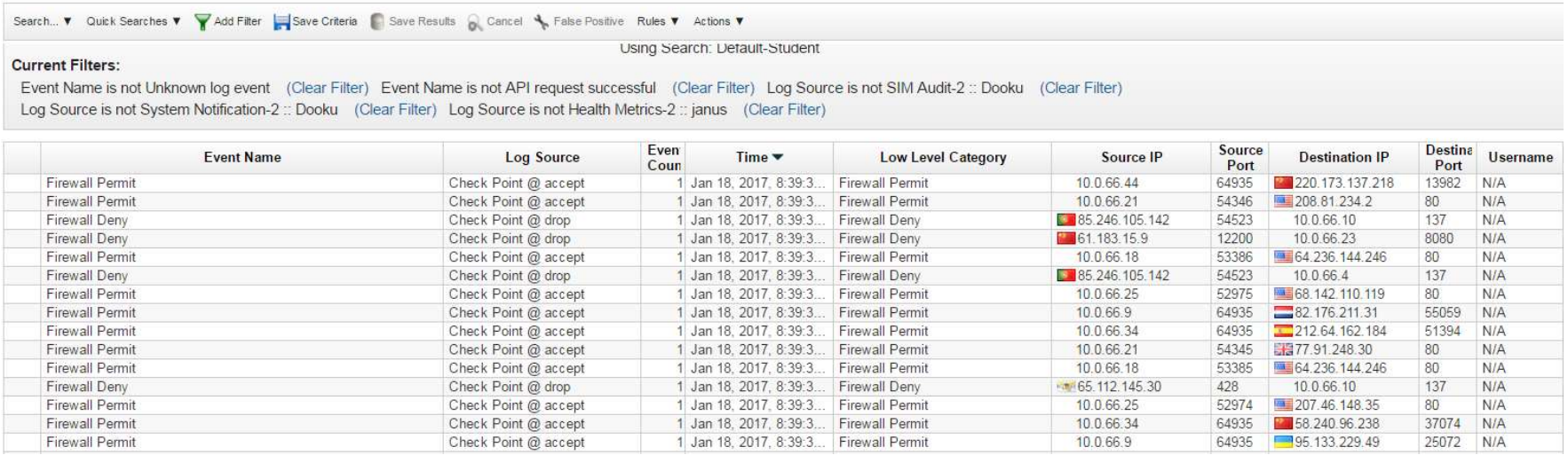
- Events can be accessed from different tabs

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

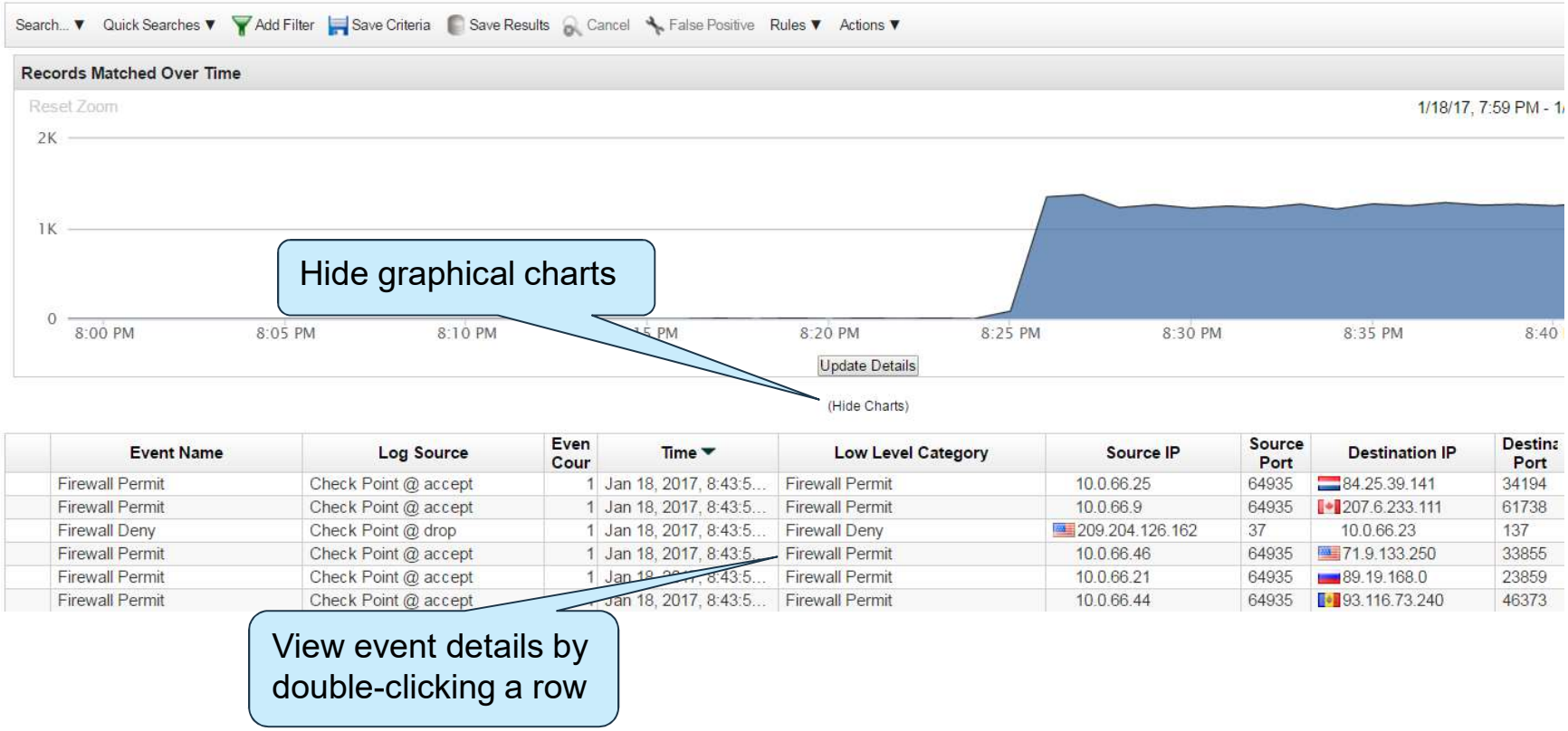
In the Log Activity Tab, click pause to view a list of events.



Event Name	Log Source	Even Coun	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destina 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 details: Base information

Event Information:
Similar offense parameters

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

Event Information

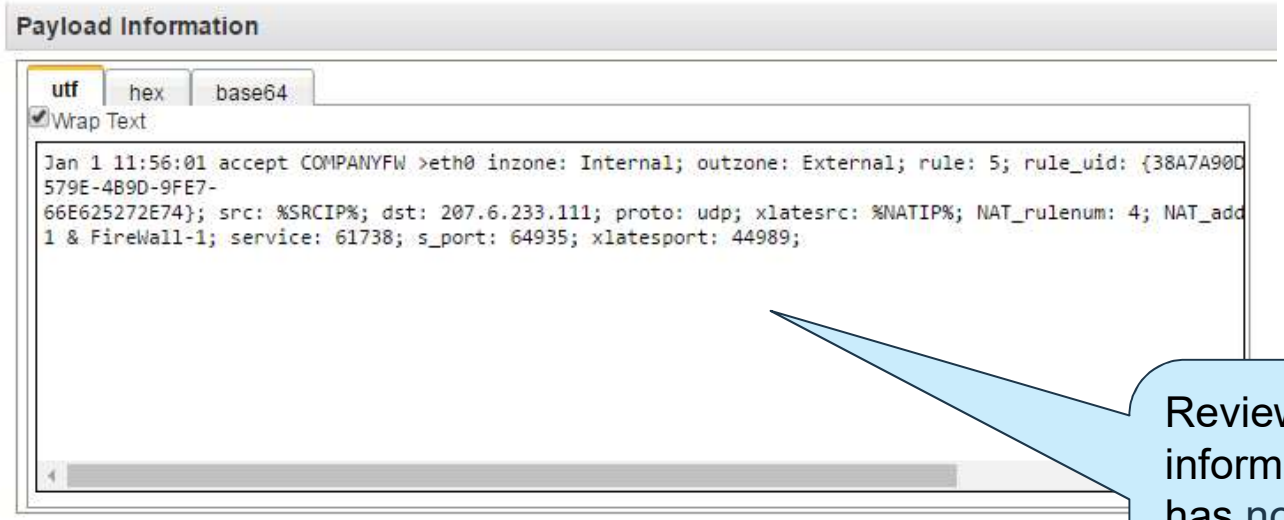
Event Name	Firewall Permit						
Low Level Category	Firewall Permit						
Event Description	Firewall Permit						
Magnitude	(3)	Relevance	6	Severity	0	Credibility	5
Username	N/A						
Start Time	Jan 18, 2017, 8:43:59 PM	Storage Time	Jan 18, 2017, 8:43:59 PM	Log Source Time	Jan 1, 2017, 11:56:01 AM		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

Source and Destination Information

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



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

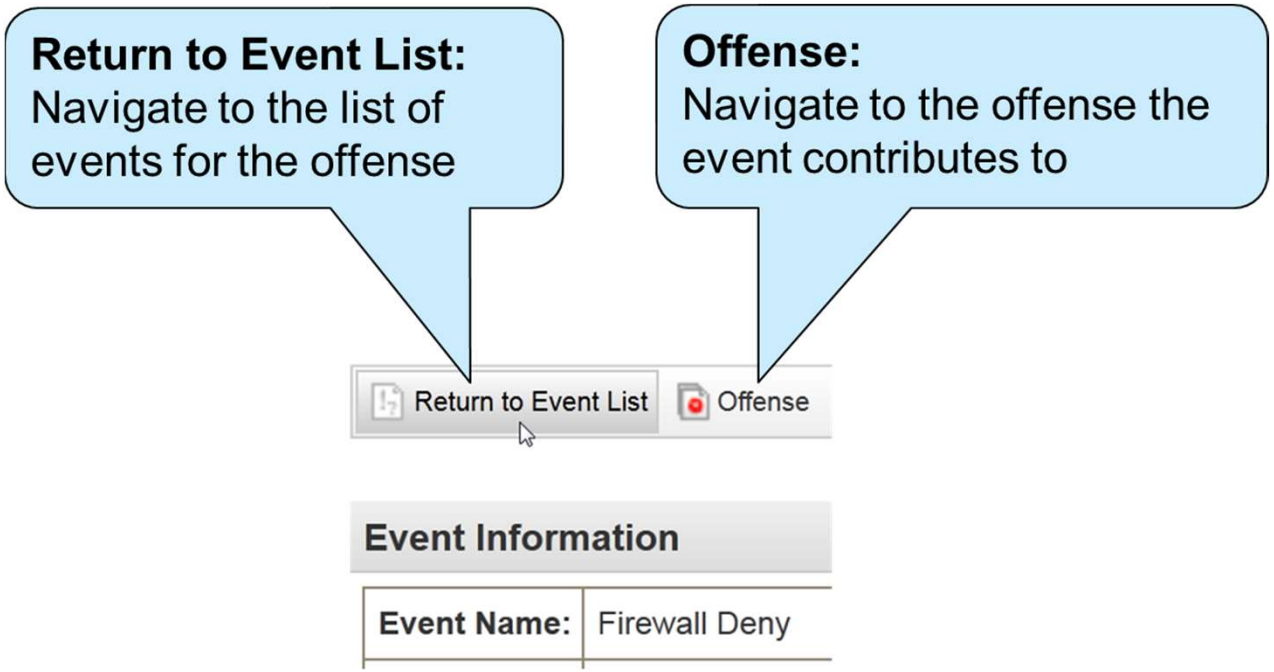
Rules triggered by the event

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.		

Returning to the list of events

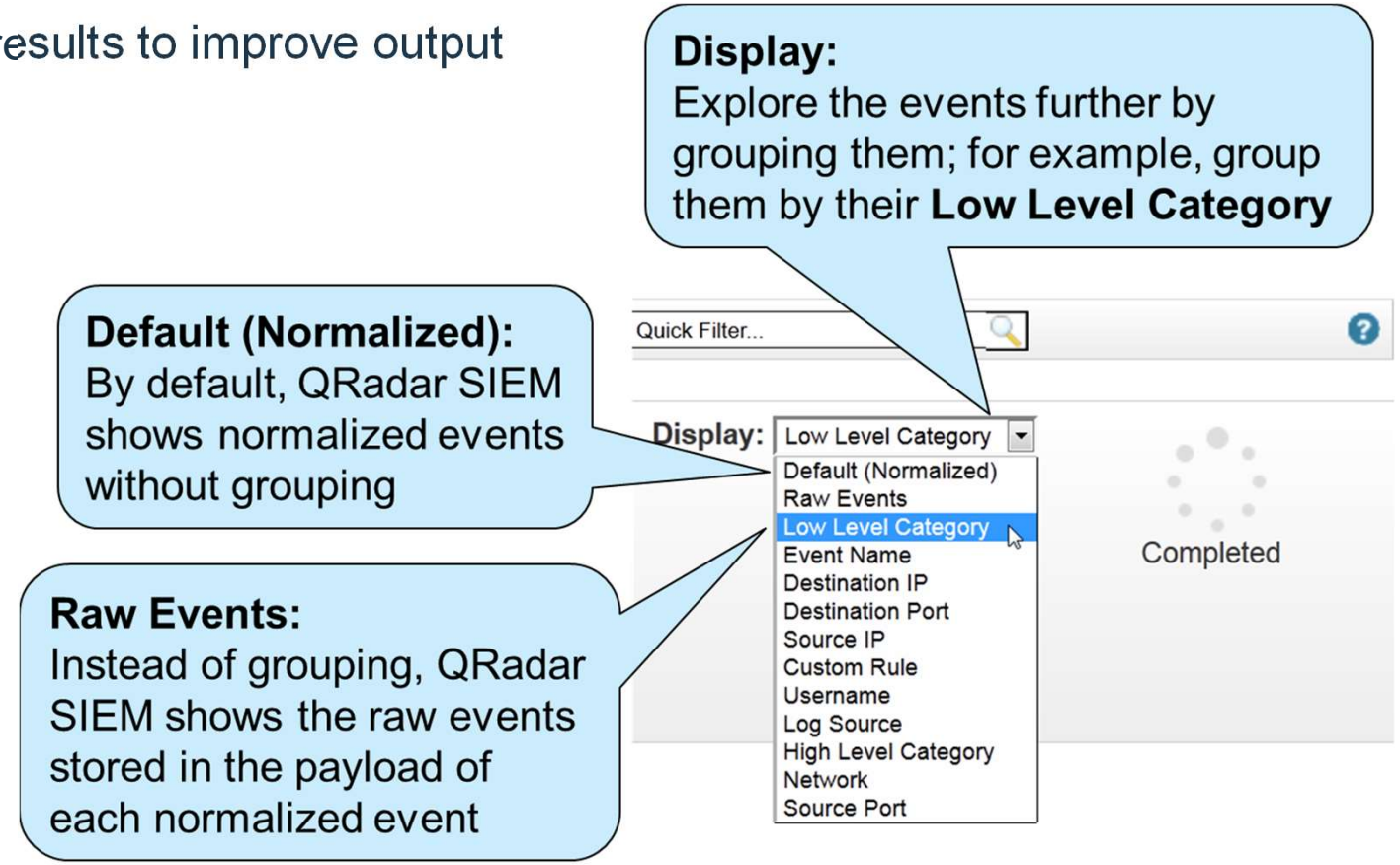
After investigating the event details, click **Return to Event List**, in the upper-left corner of the event details window, to return to the event list



Building a Search to Investigate Events

Group Events

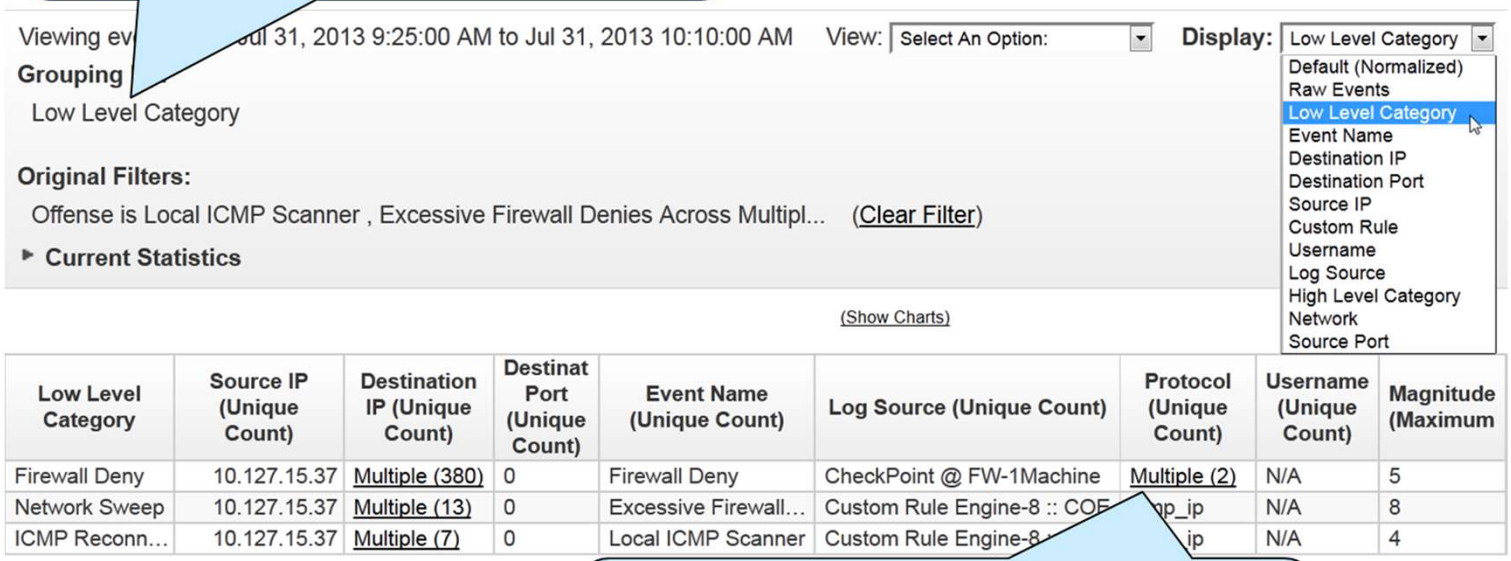
Group search results to improve output



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

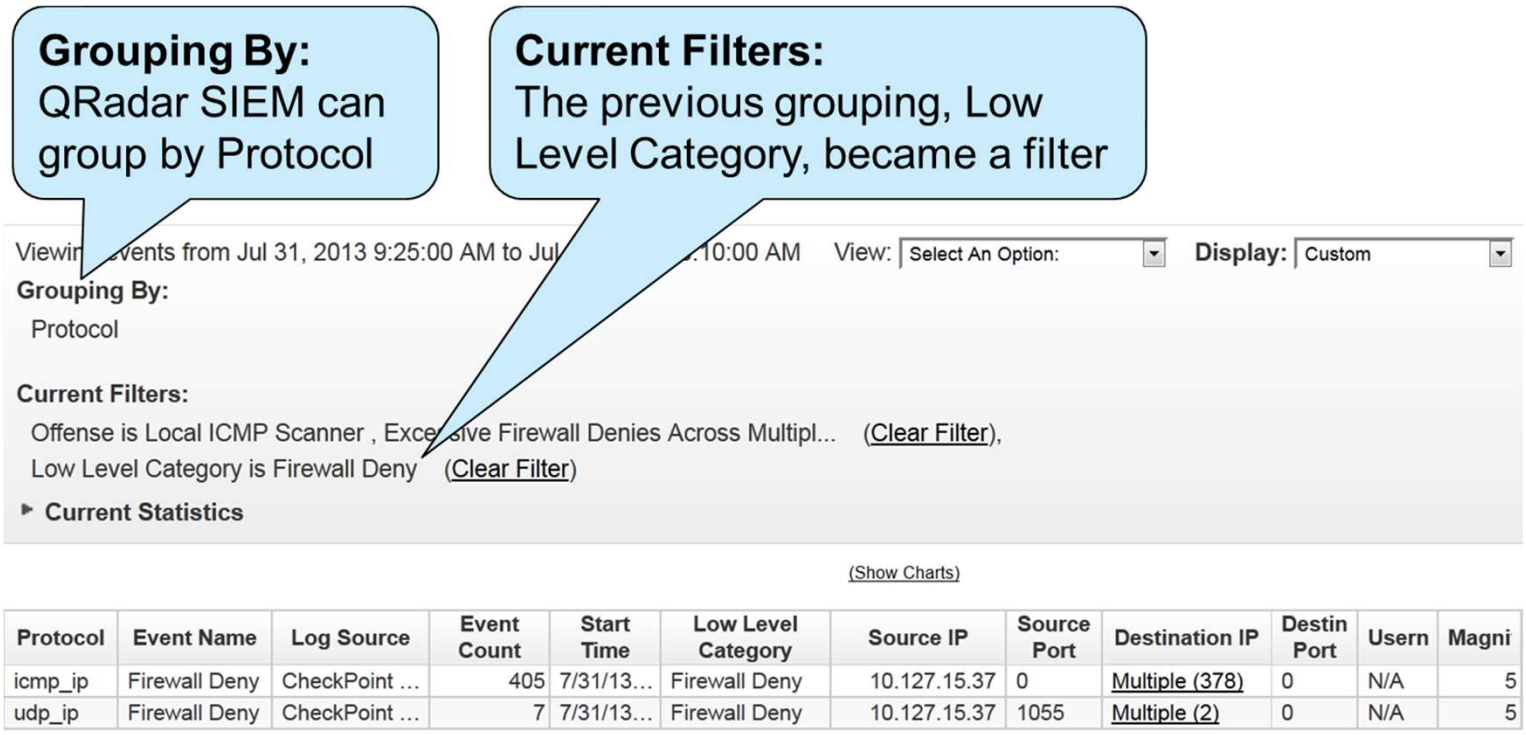


Low Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destinat Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum
Firewall Deny	10.127.15.37	Multiple (380)	0	Firewall Deny	CheckPoint @ FW-1Machine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

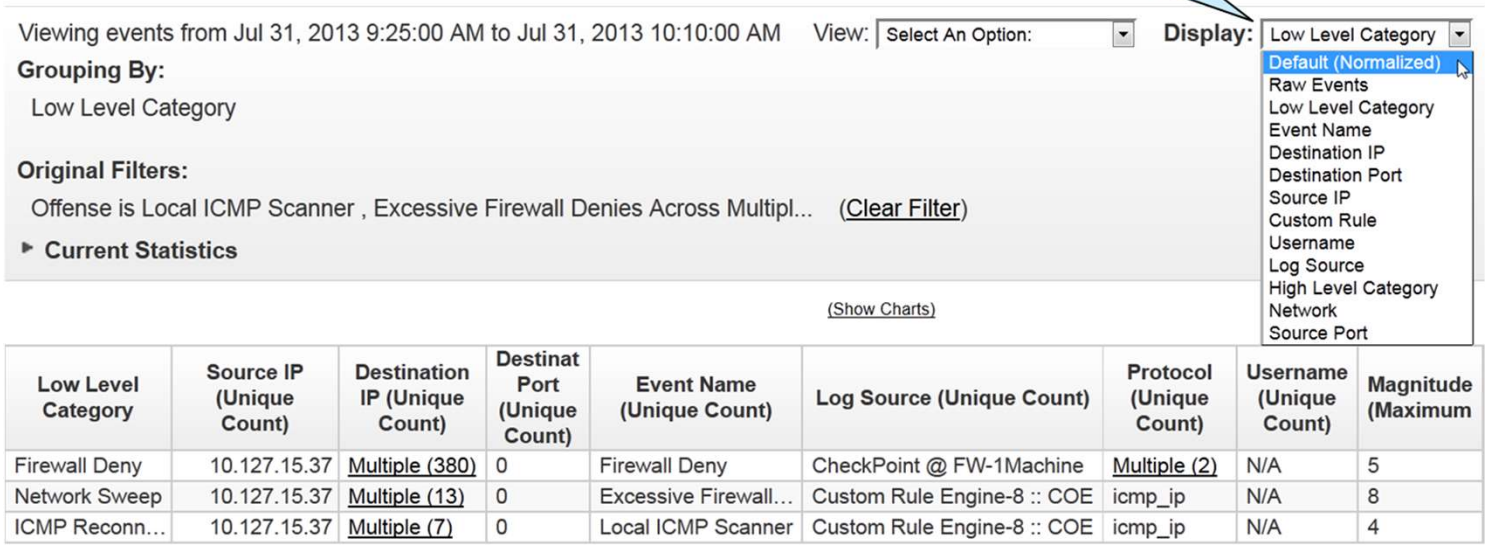
In the Protocol column, click Multiple (2) to open a window with events grouped by protocol; you learn that the firewall denied udp_ip in addition to icmp_ip



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

Removing grouping criteria

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



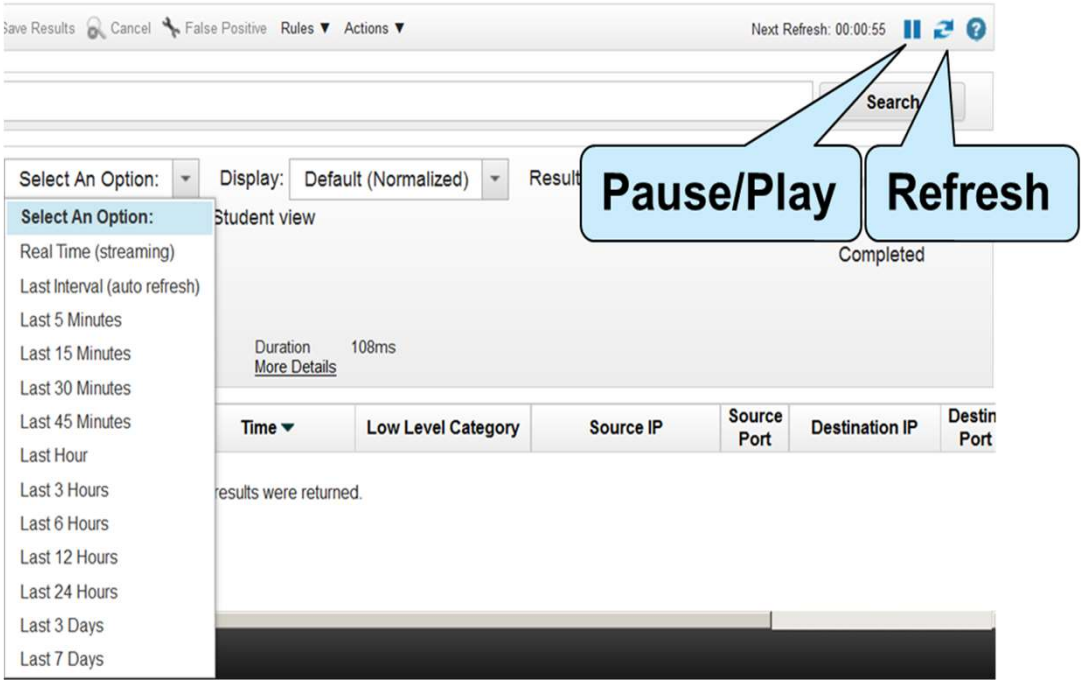
Low Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destinat Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum
Firewall Deny	10.127.15.37	Multiple (380)	0	Firewall Deny	CheckPoint @ FW-1Machine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

Viewing and changing a range of events

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

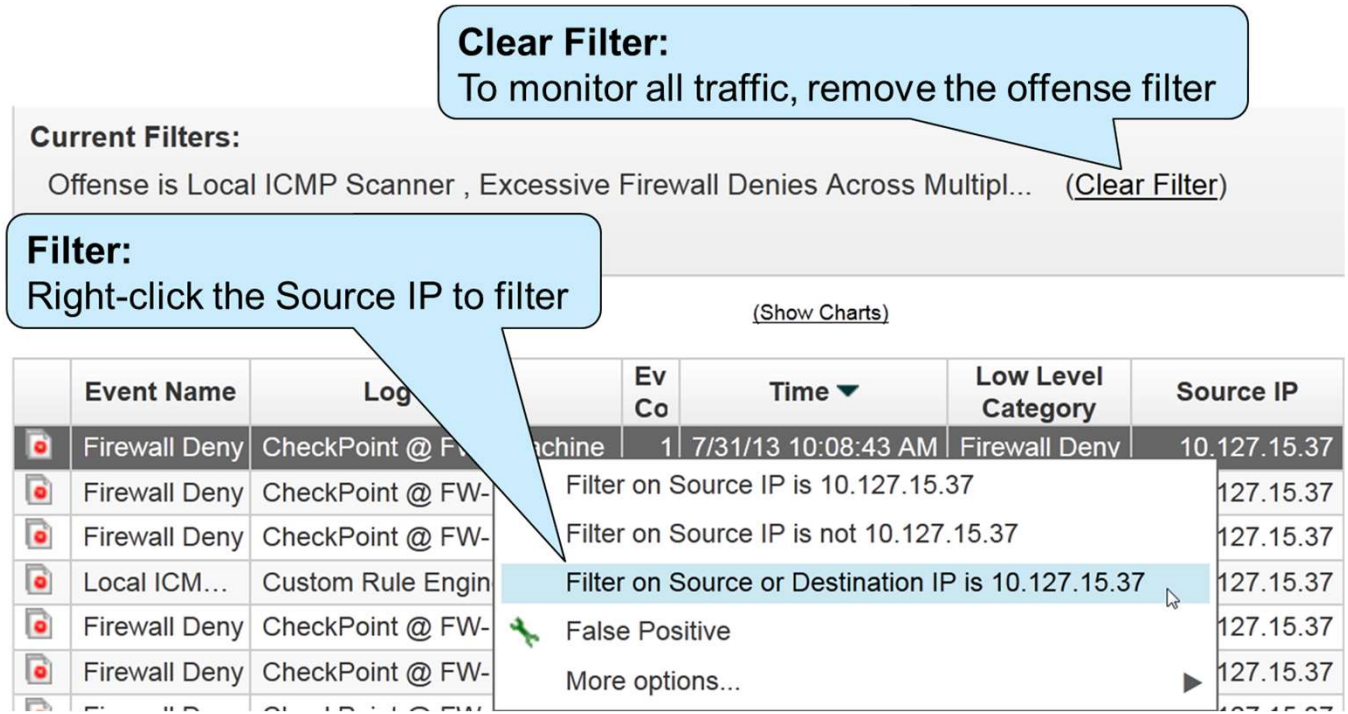
Real Time (streaming): Shows events as they arrive at the Event Processor (EP); grouping and sorting are not available

Last Interval (auto refresh): Shows the last minute of events; refreshes automatically after 1 minute

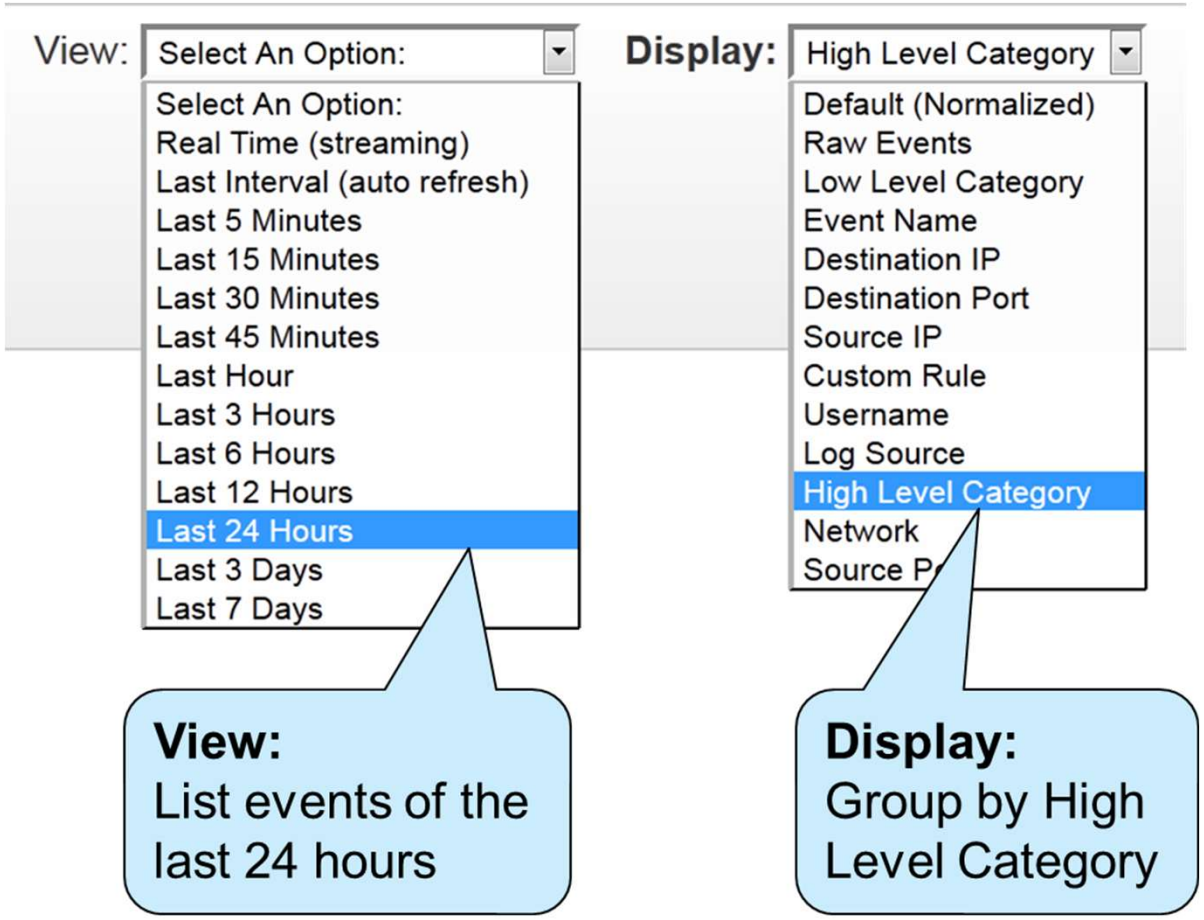


Monitoring the scanning host (1 of 3)

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



Monitoring the scanning host (2 of 3)



Monitoring the scanning host (3/3)

Save Criteria:
Save the criteria of the current search

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

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

Current Filters:

Source or Destination IP is 10.127.15.37 (Clear Filter)

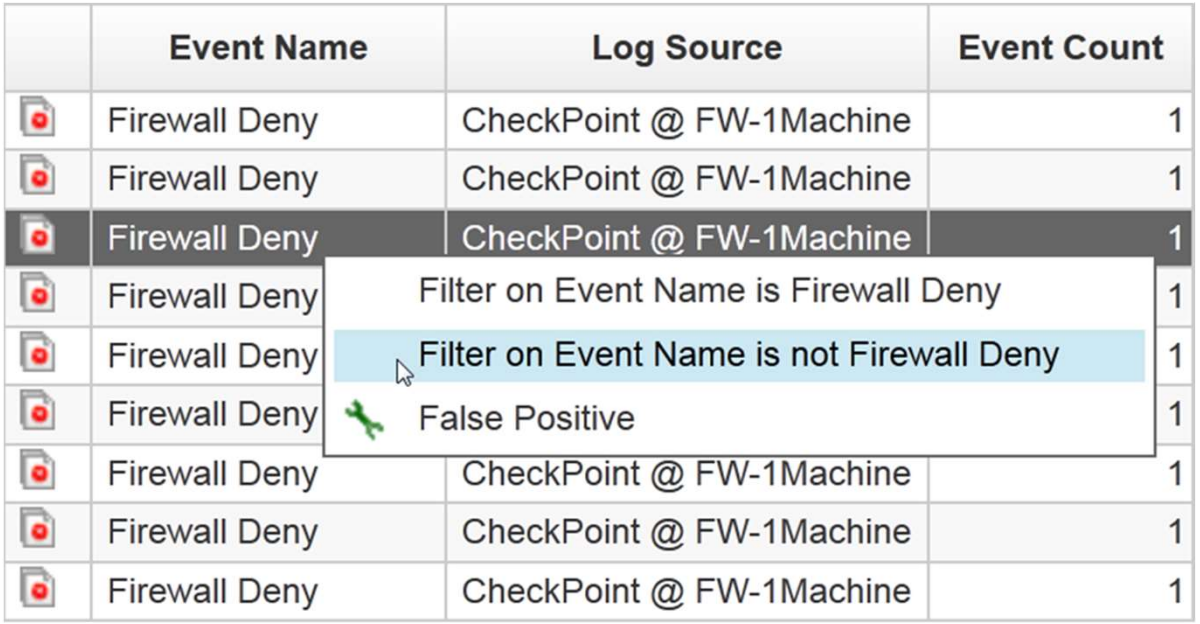
▸ **Current Statistics**

(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



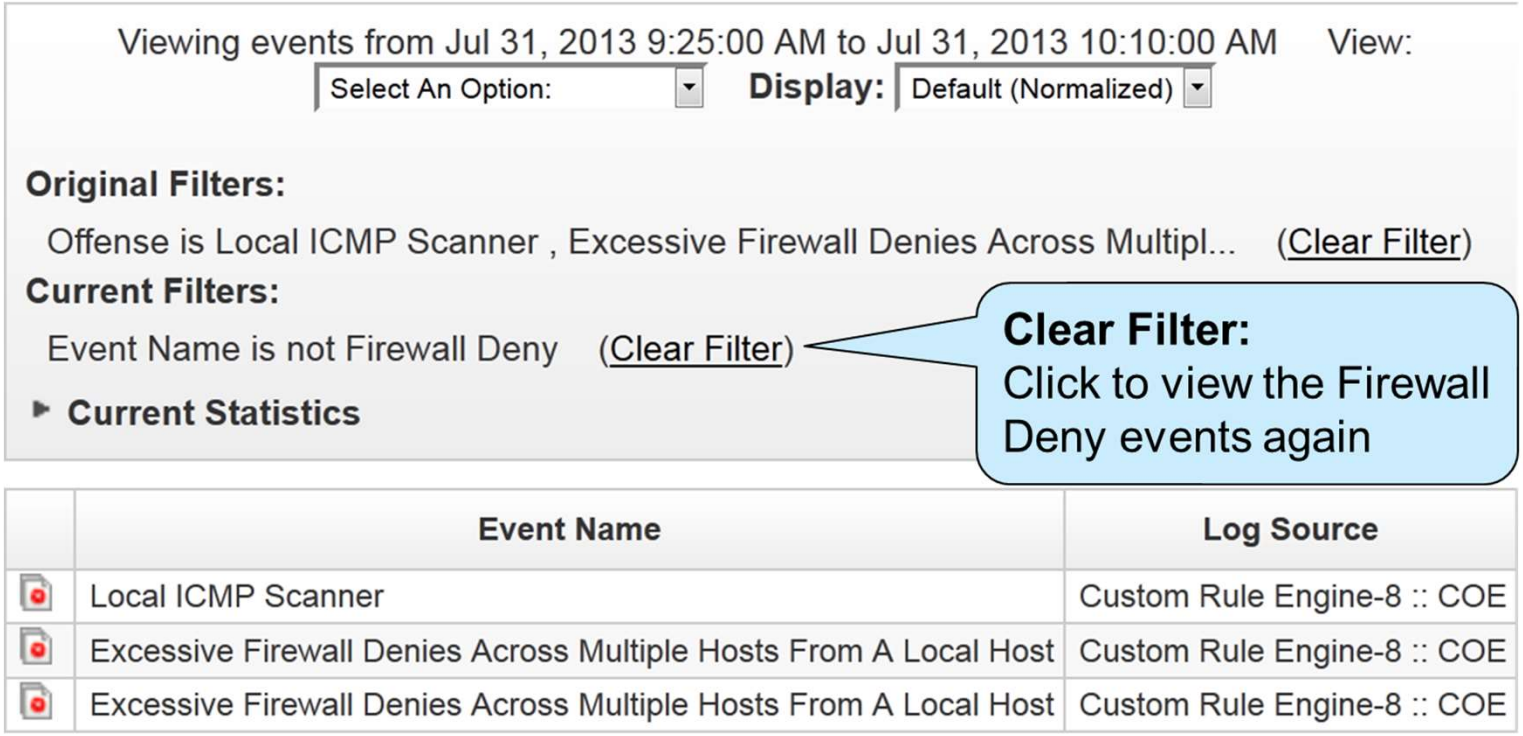
Filtering events (2 of 3)

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

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

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

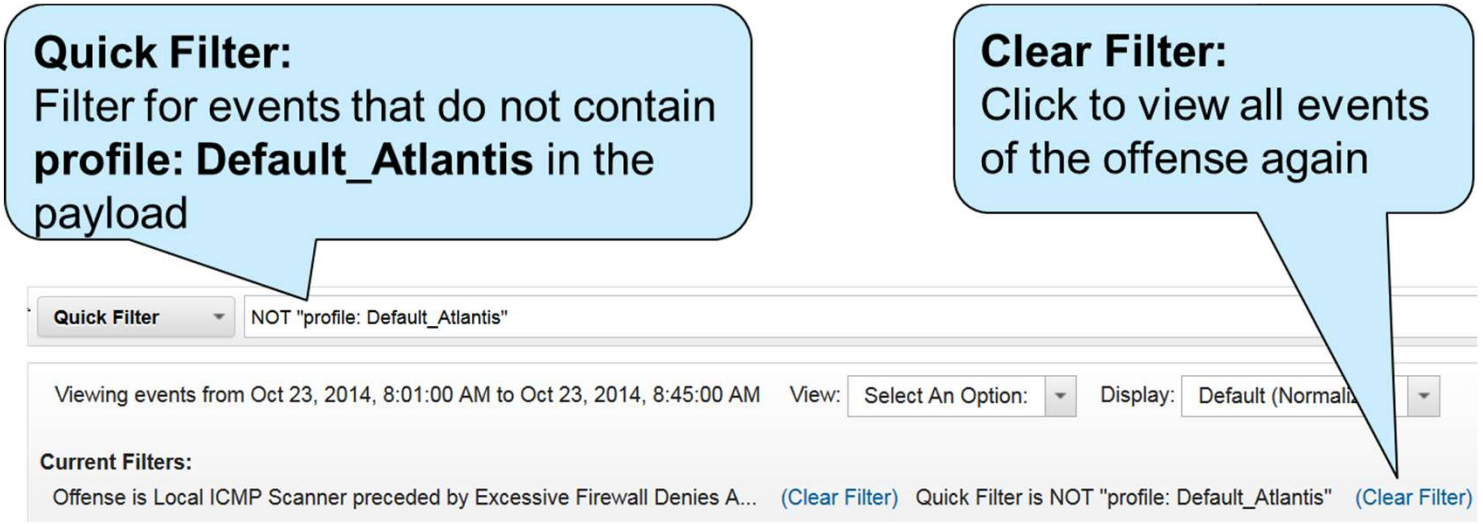
Filtering events (3 of 3)



Unlike searches, filters do not query each event processor

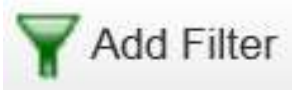
Applying a Quick Filter to the payload

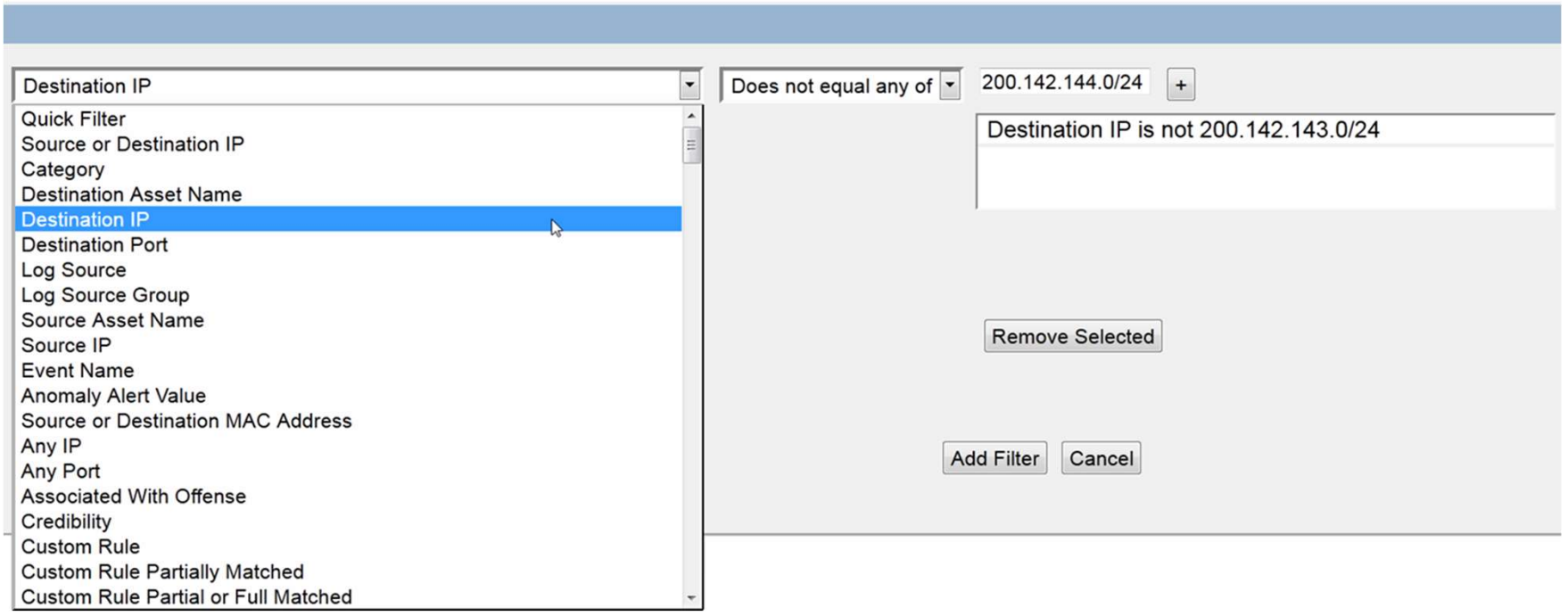
- The payload of an event contains the raw event that mentions the firewall profile that denied the connection
- To verify that the company's main profile, Atlantis, was always active, filter events without **profile: Default_Atlantis** in the payload



Using another filter option

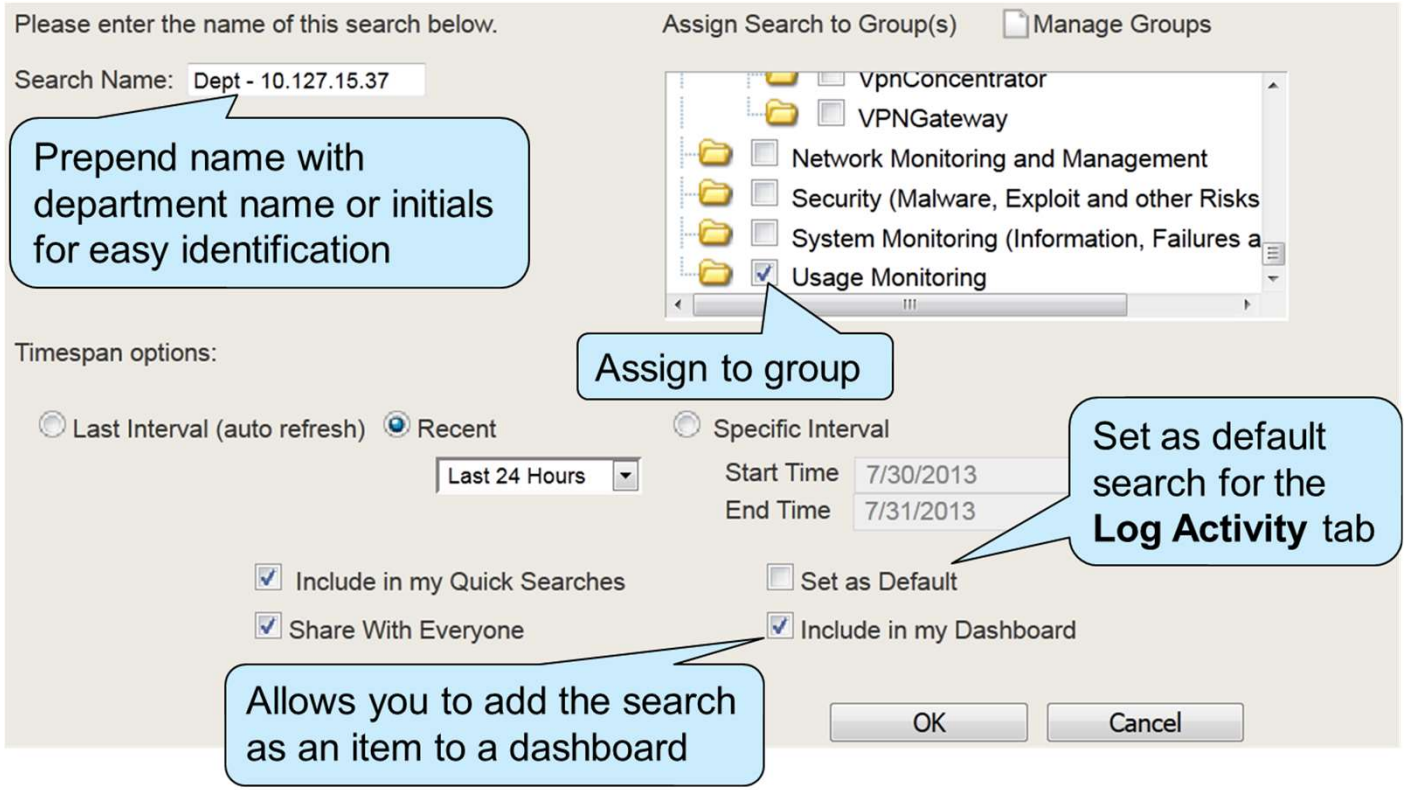
- You can use each event field as a filter
- To create a filter, in the top menu bar, click the icon



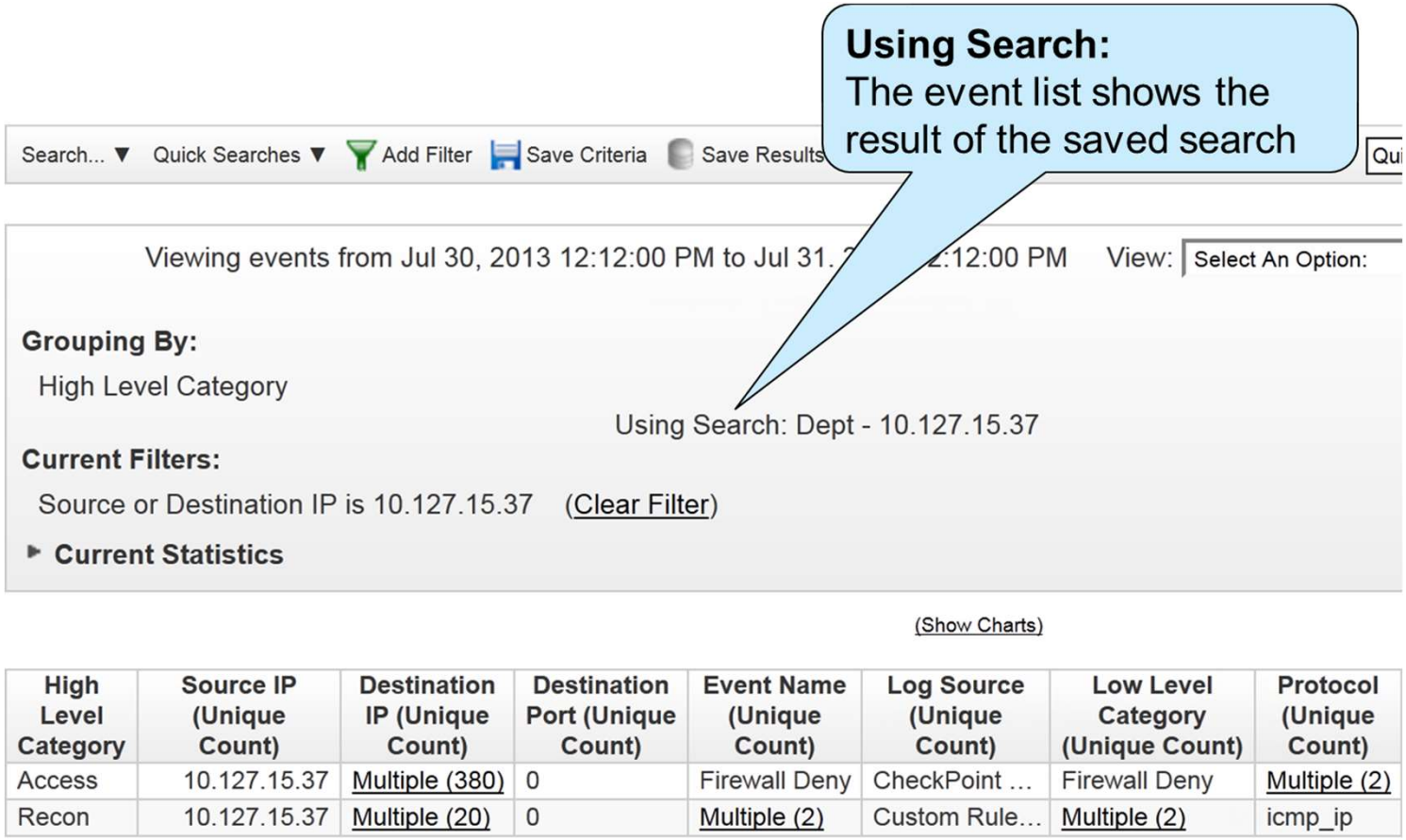


Saving search criteria

Save the search with the criteria specified



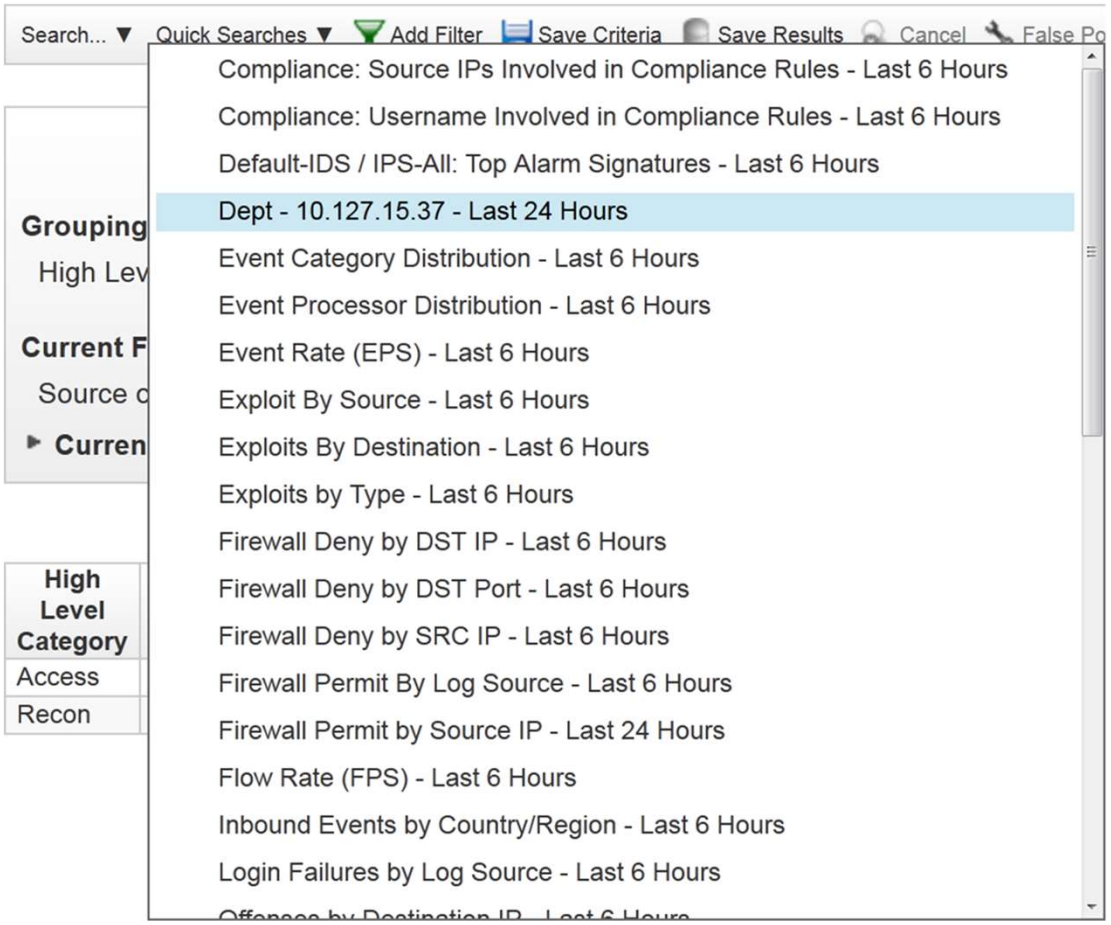
Event list using the saved search



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

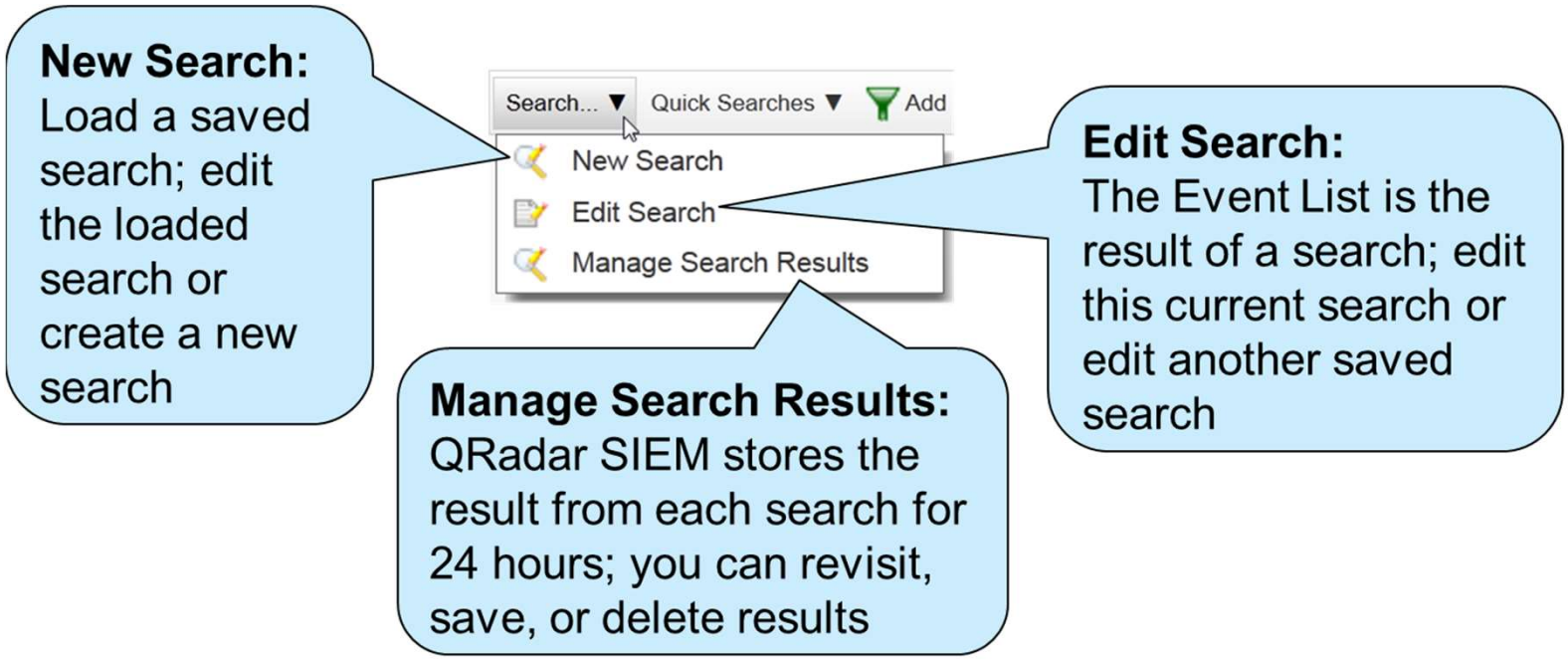
About Quick Searches

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



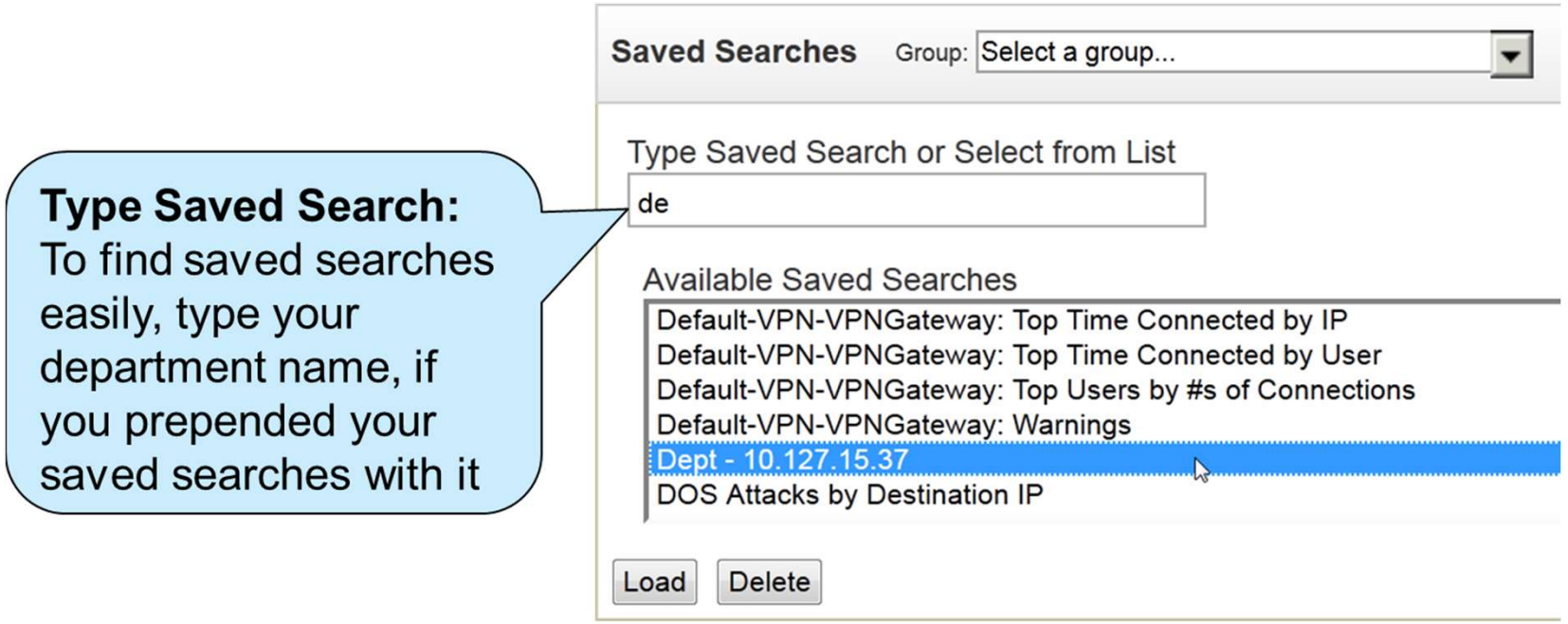
Using alternative methods to create and edit searches

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

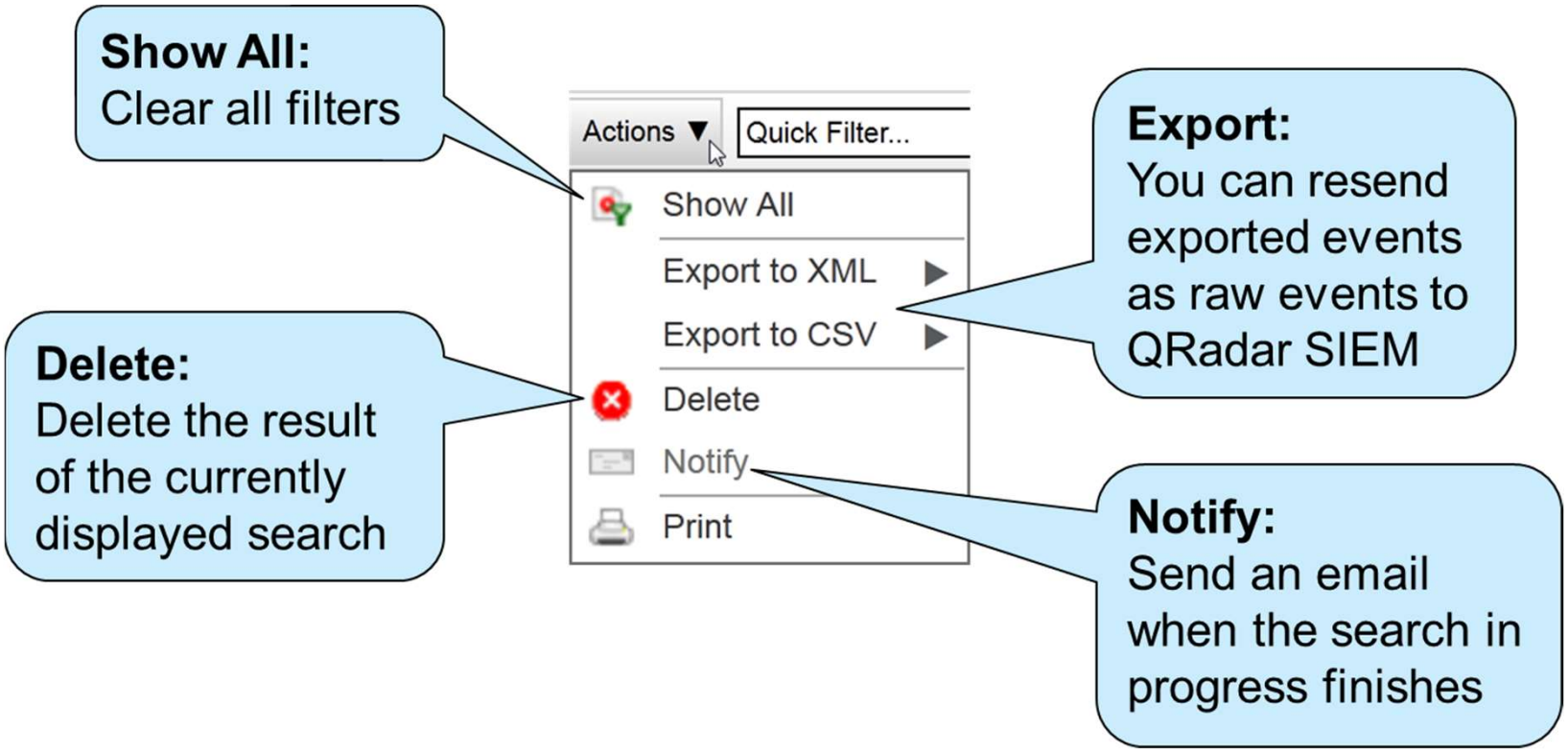


Finding and loading a saved search

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

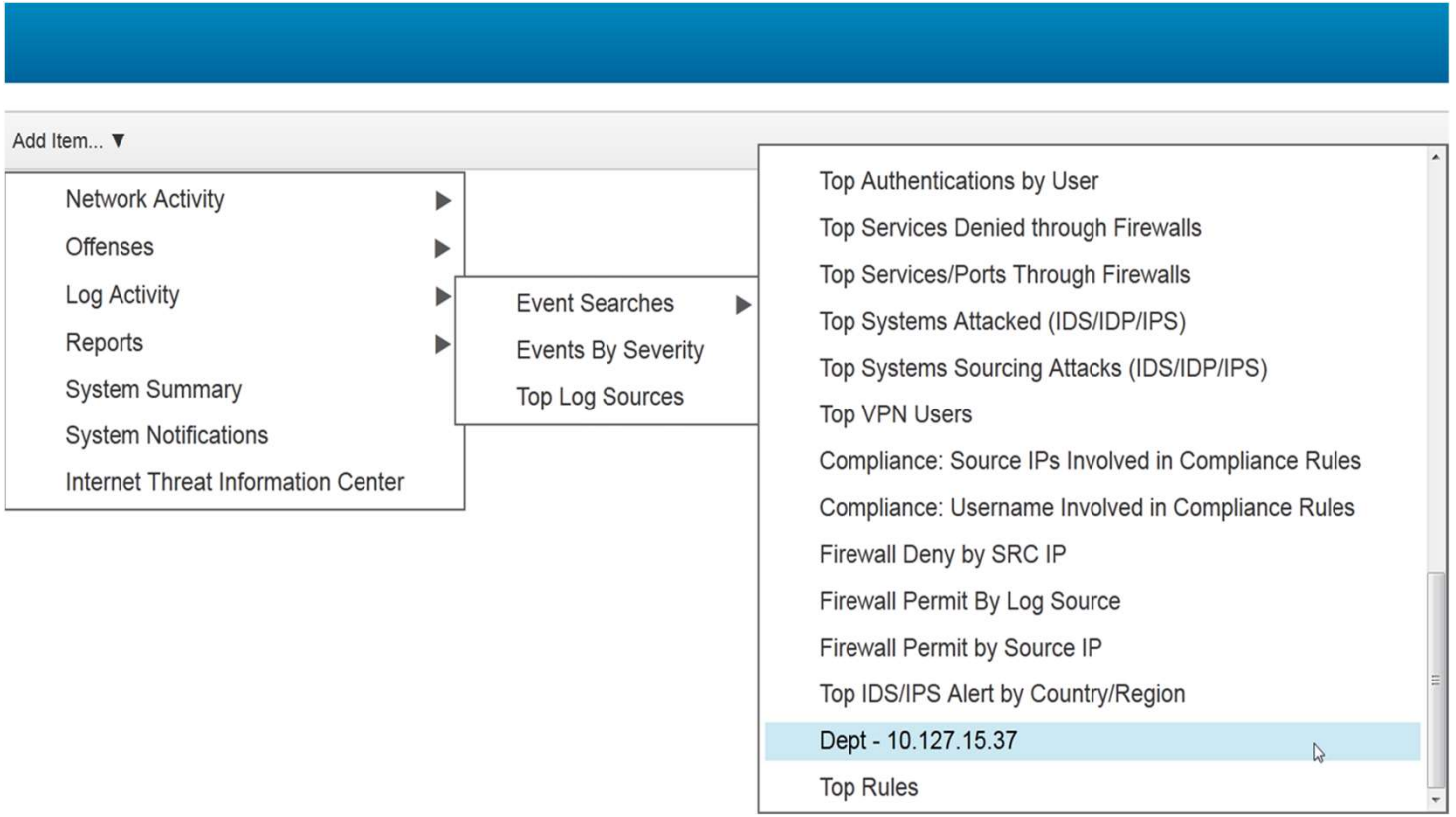


Search actions

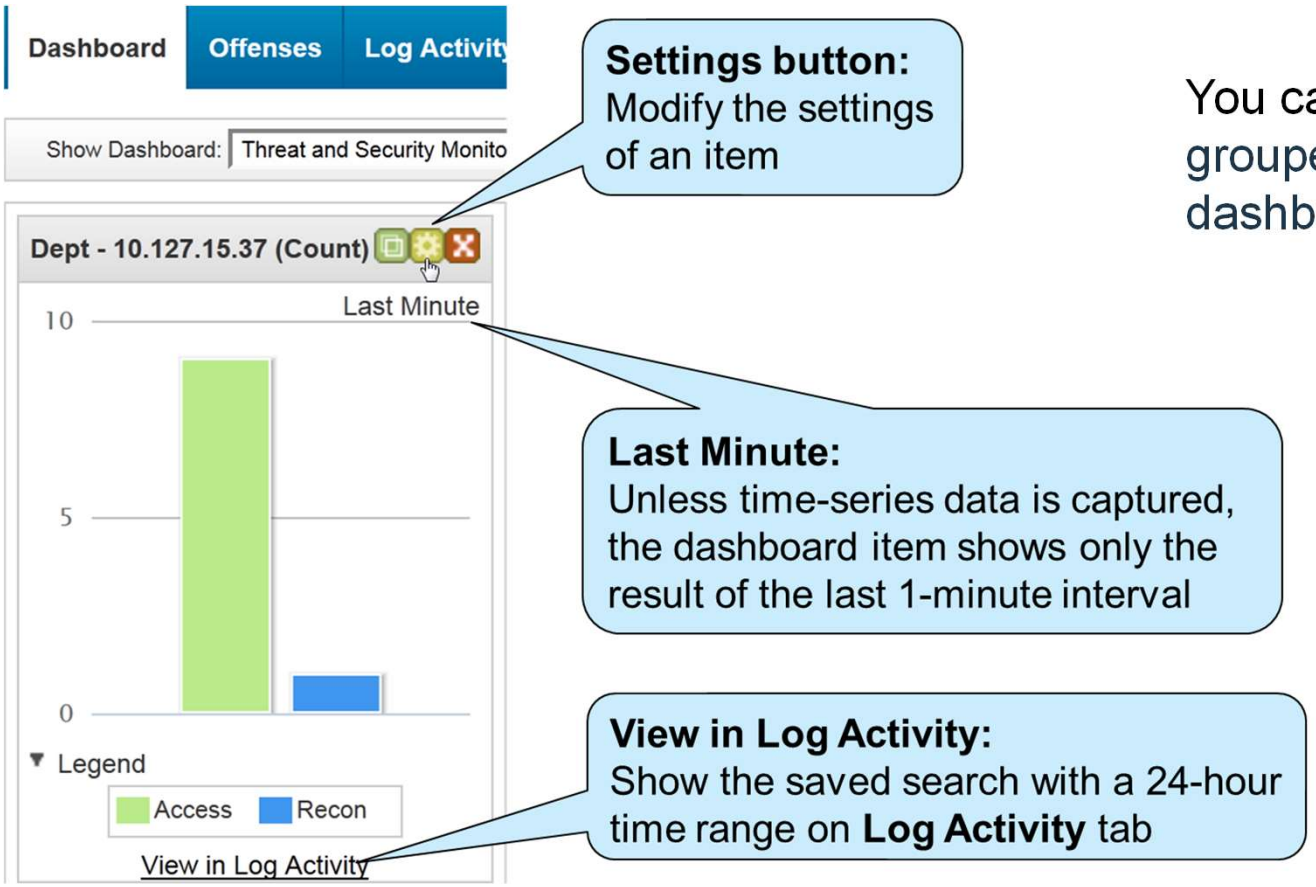


Adding a saved search as a dashboard item

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

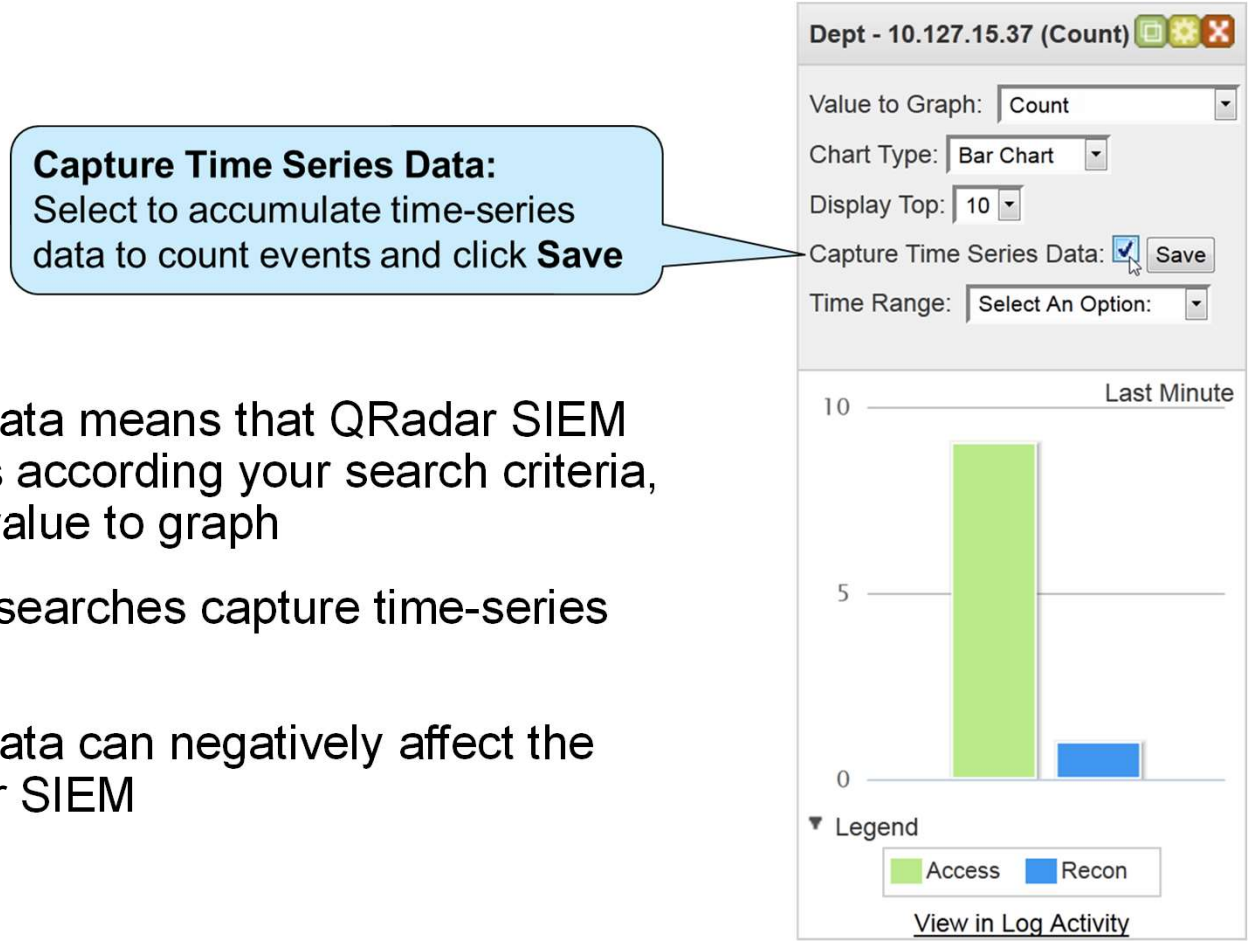


Viewing the saved search in the Dashboard



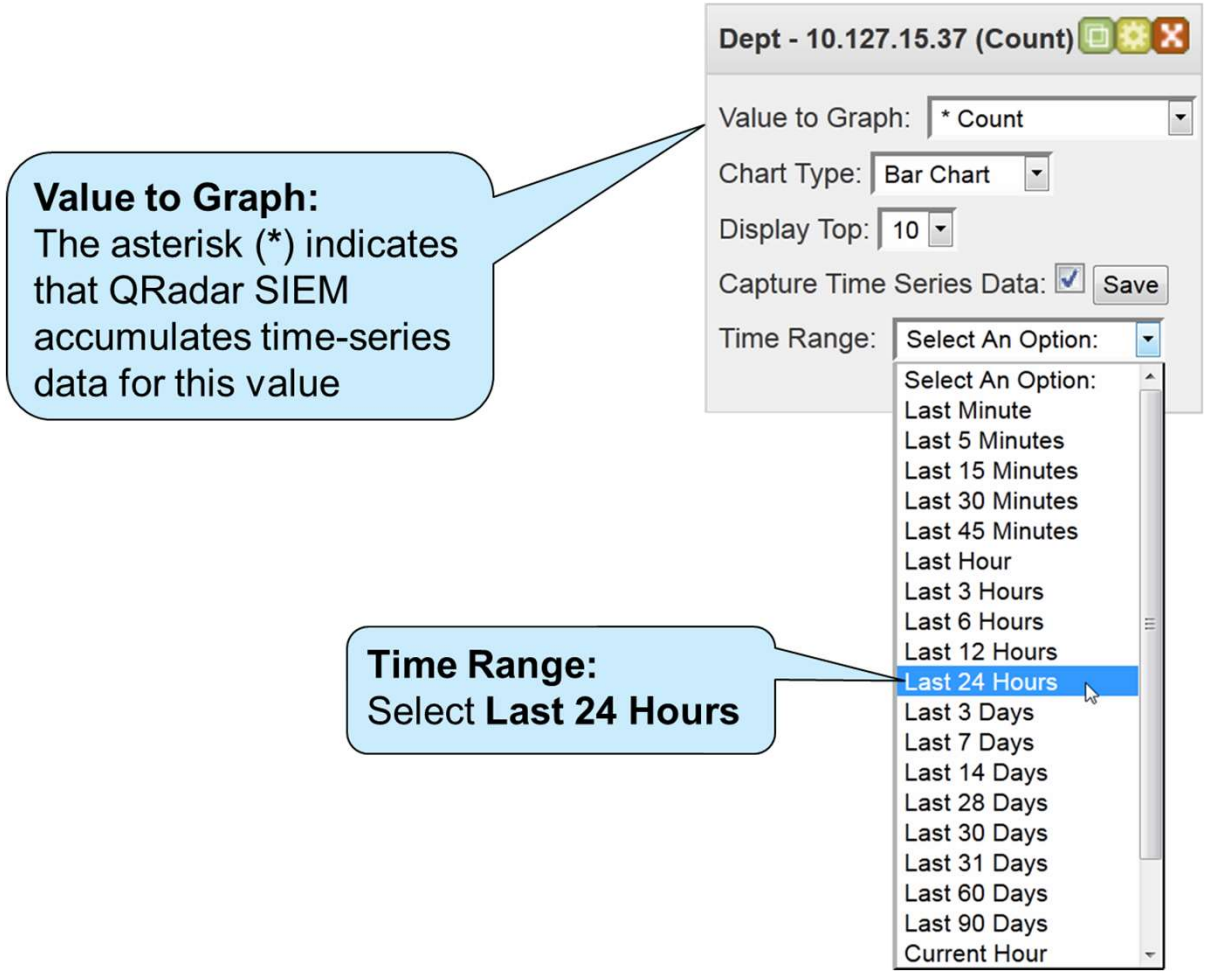
You can add only grouped searches as dashboard items

Enabling time-series data



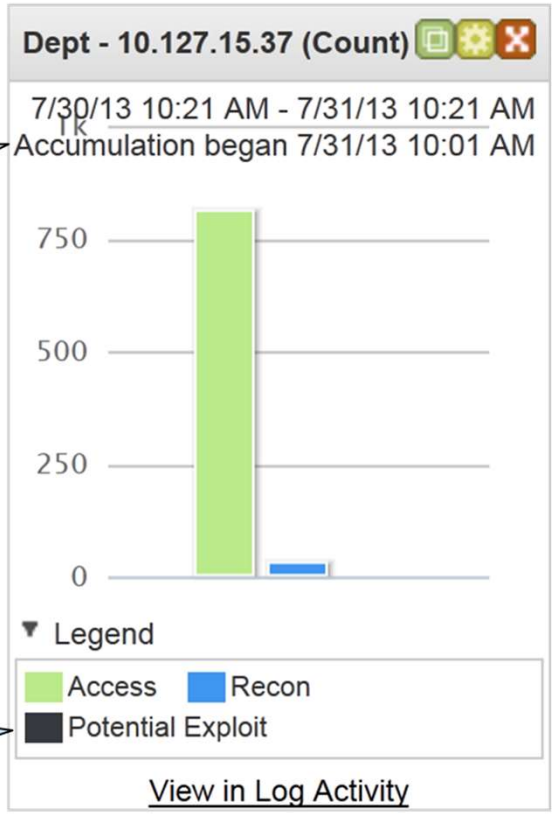
- Capturing time-series data means that QRadar SIEM counts incoming events according your search criteria, grouping, and chosen value to graph
- Most of the predefined searches capture time-series data
- Capturing time-series data can negatively affect the performance of QRadar SIEM

Selecting the time range



Displaying 24 hours in a dashboard item

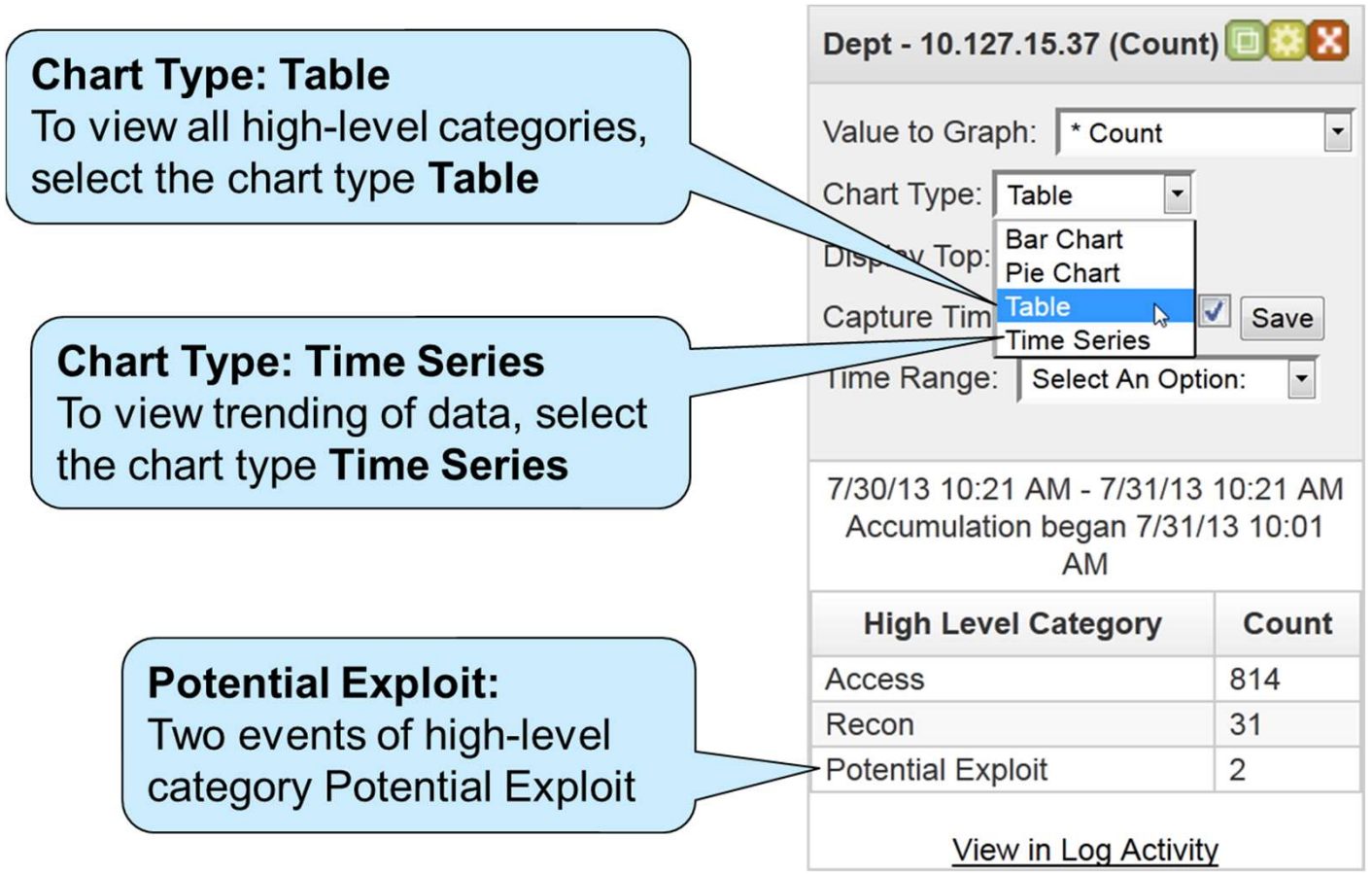
Accumulation began:
QRadar SIEM started accumulating time-series data on this date at this time



- 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



Ariel Query Language (AQL)

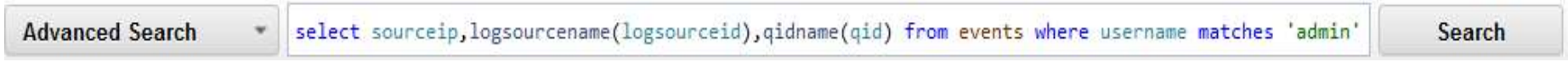
Ariel Query Language

- 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

Additional AQL examples

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

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



- 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`

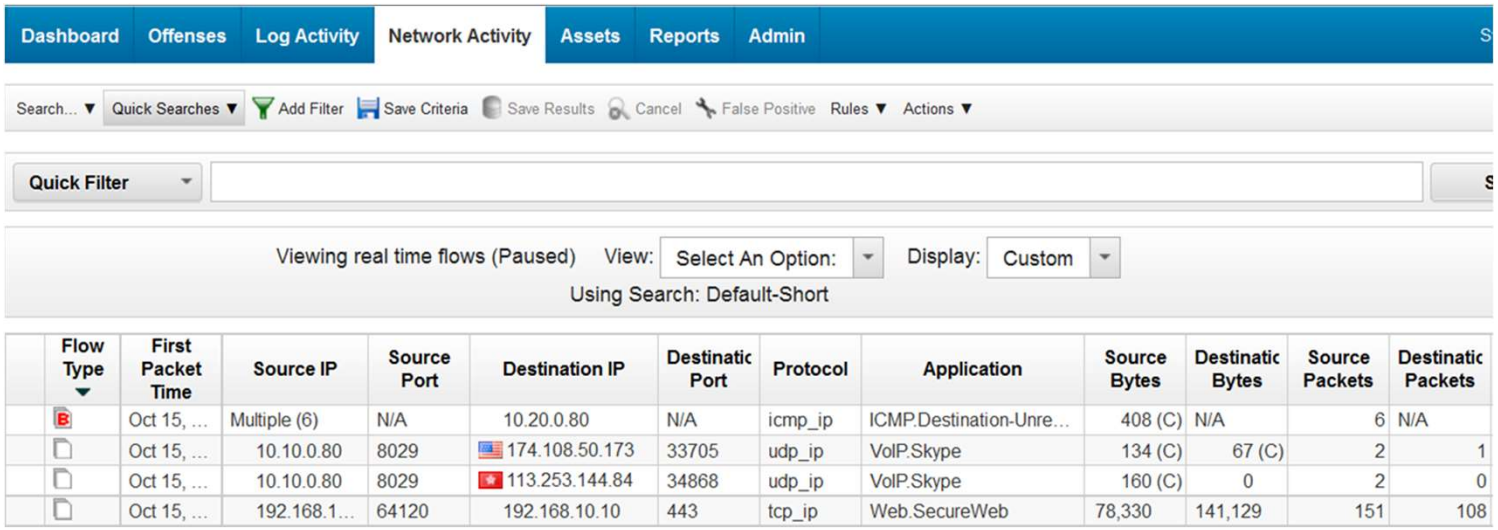
Investigating Flows

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

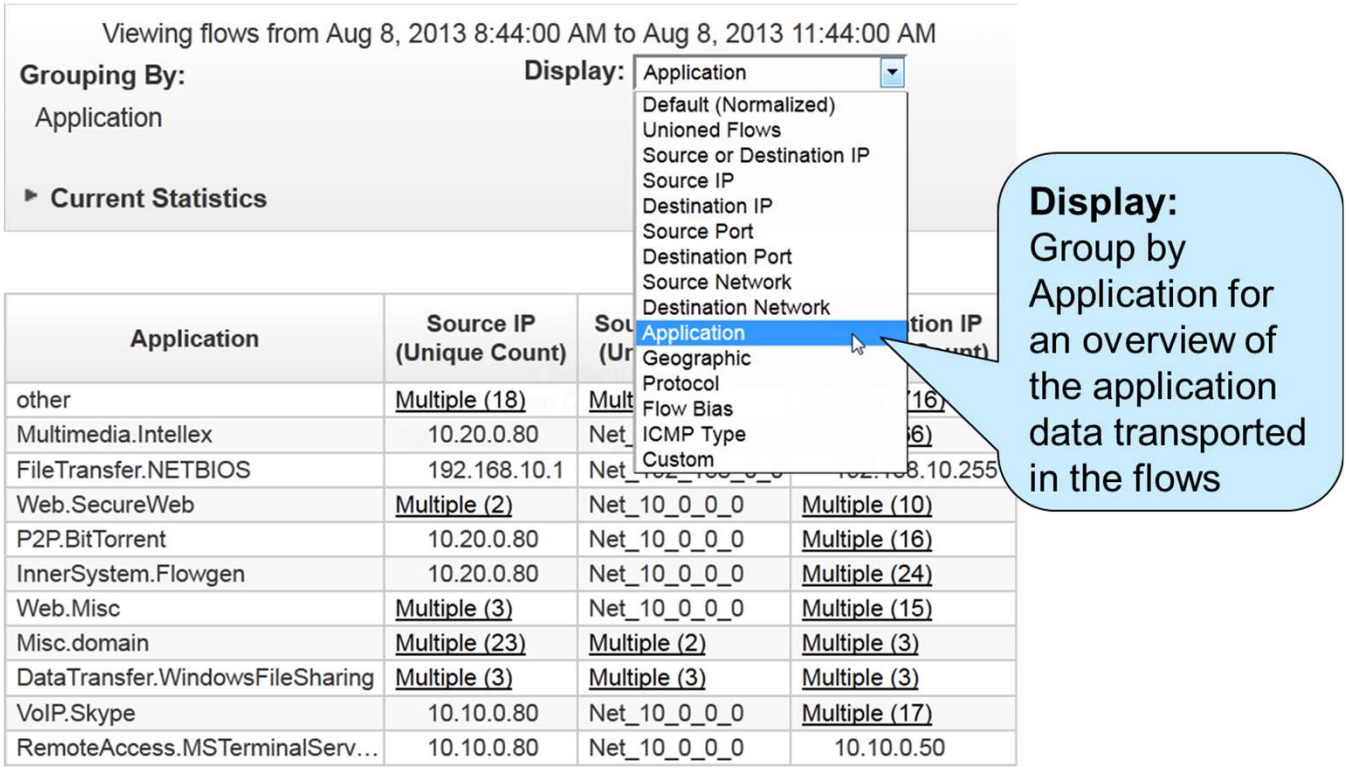
- Click the **Network Activity** tab to perform these tasks
  - Investigate flows sent to QRadar SIEM
  - Perform detailed searches
  - View network activity
- Flows on the **Network Activity** tab are shown in a similar way as events are on the **Log Activity** tab



Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destinatic Port	Protocol	Application	Source Bytes	Destinatic Bytes	Source Packets	Destinatic 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.



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

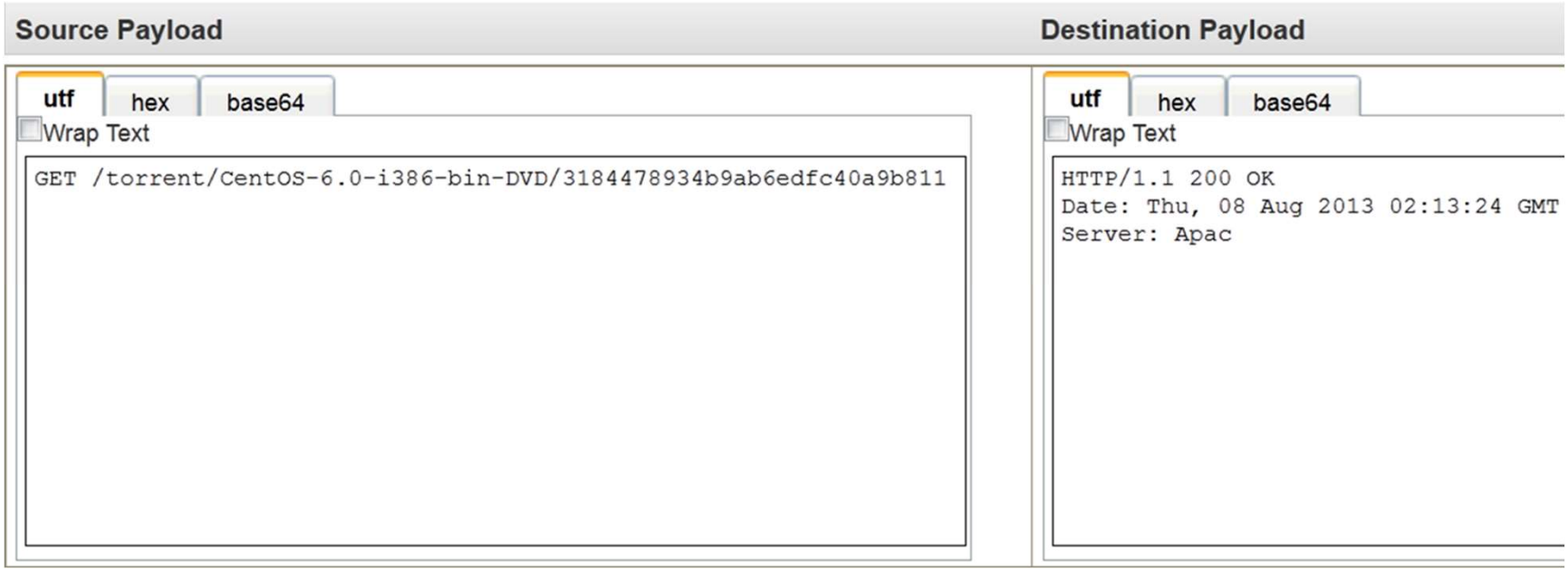
QRadar SIEM provides network connection details about the flow

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

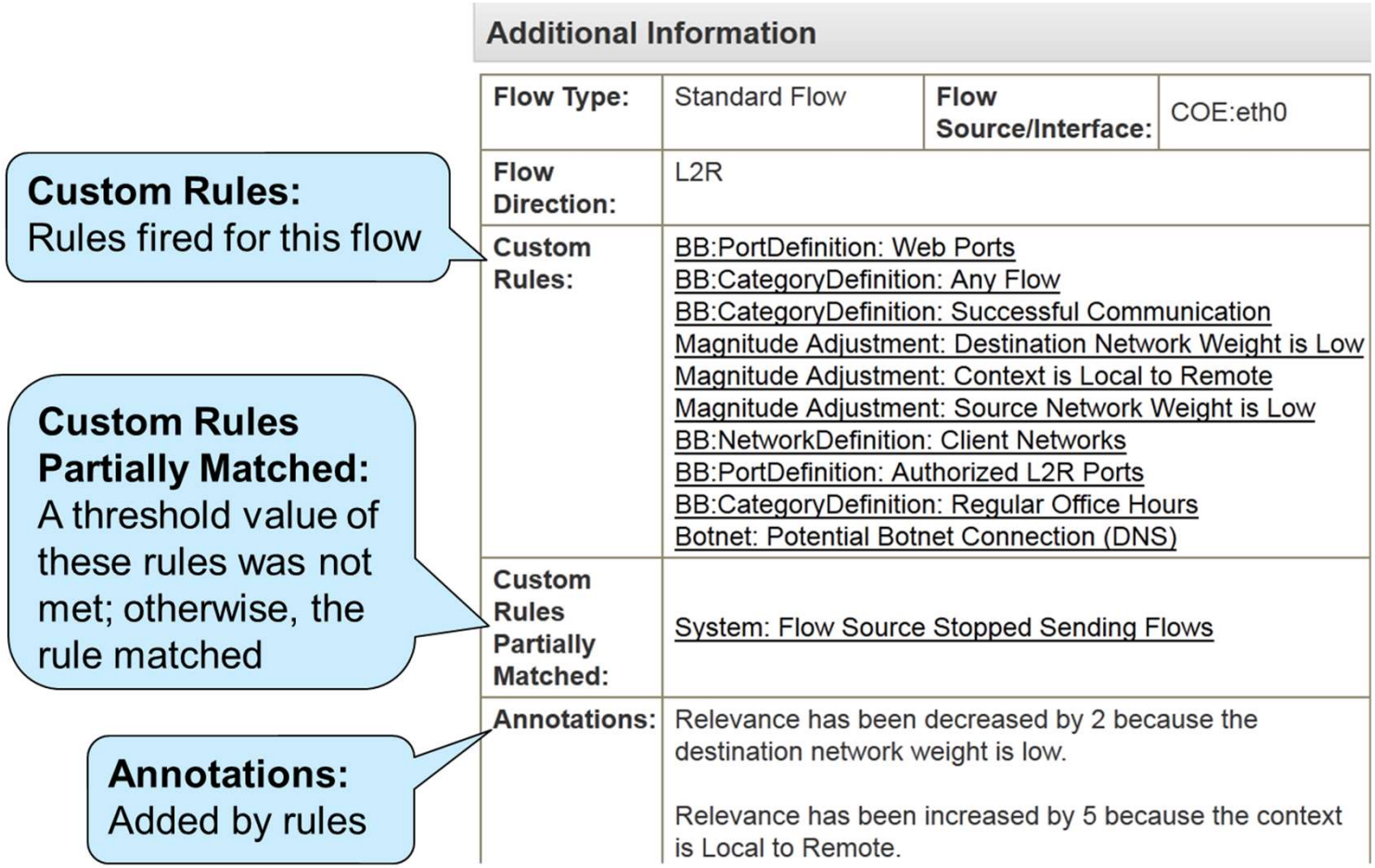
Layer 7 payload

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



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:	BB:PortDefinition: Web Ports BB:CategoryDefinition: Any Flow BB:CategoryDefinition: Successful Communication Magnitude Adjustment: Destination Network Weight is Low Magnitude Adjustment: Context is Local to Remote Magnitude Adjustment: Source Network Weight is Low BB:NetworkDefinition: Client Networks BB:PortDefinition: Authorized L2R Ports BB:CategoryDefinition: Regular Office Hours Botnet: Potential Botnet Connection (DNS)		
Custom Rules Partially Matched:	System: Flow Source Stopped Sending Flows		
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.		

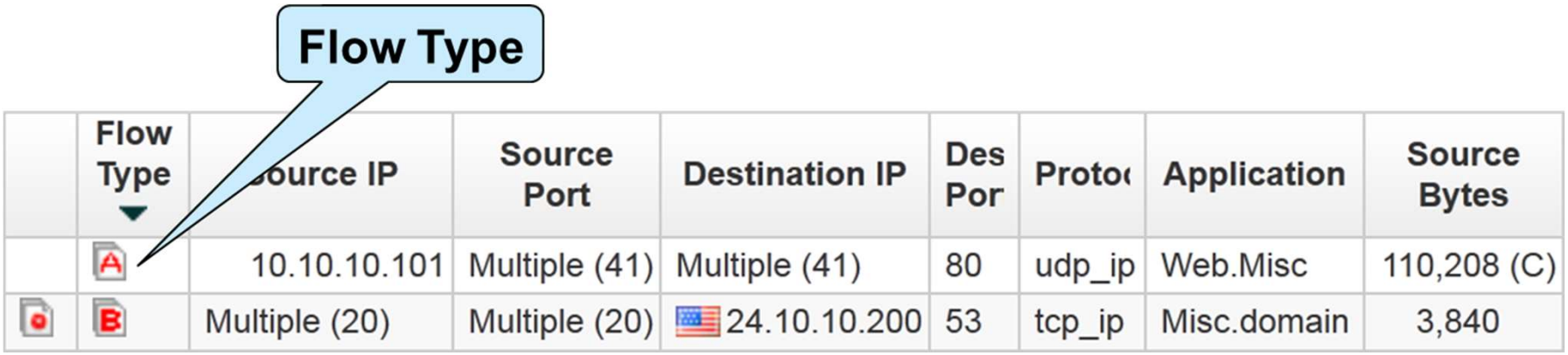
Flow Direction

- 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

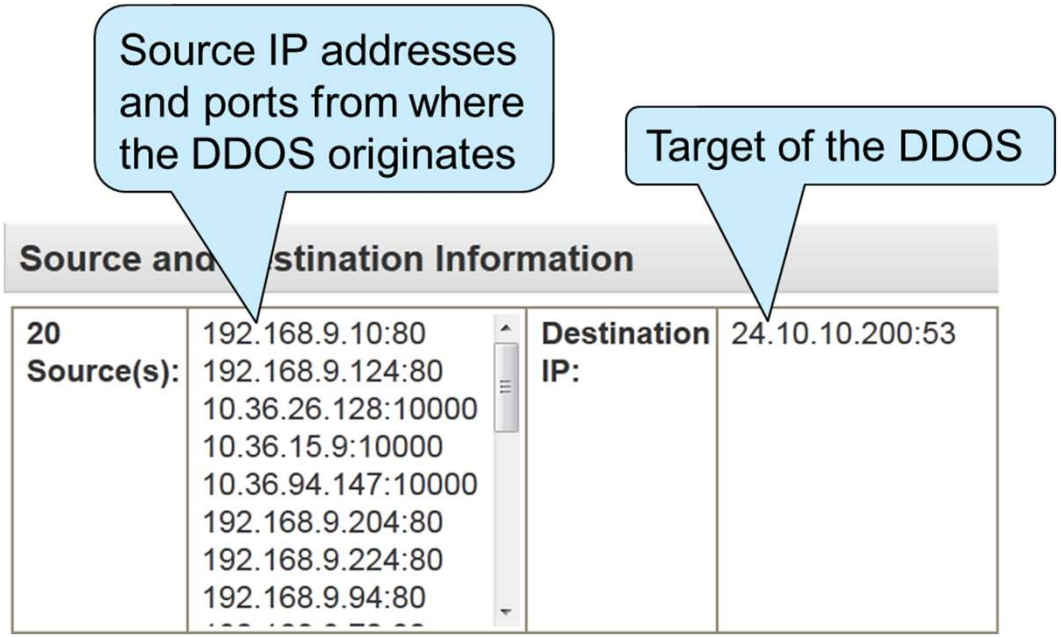
QRadar SIEM aggregates flows with common characteristics into superflows that indicate common attack types

- **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

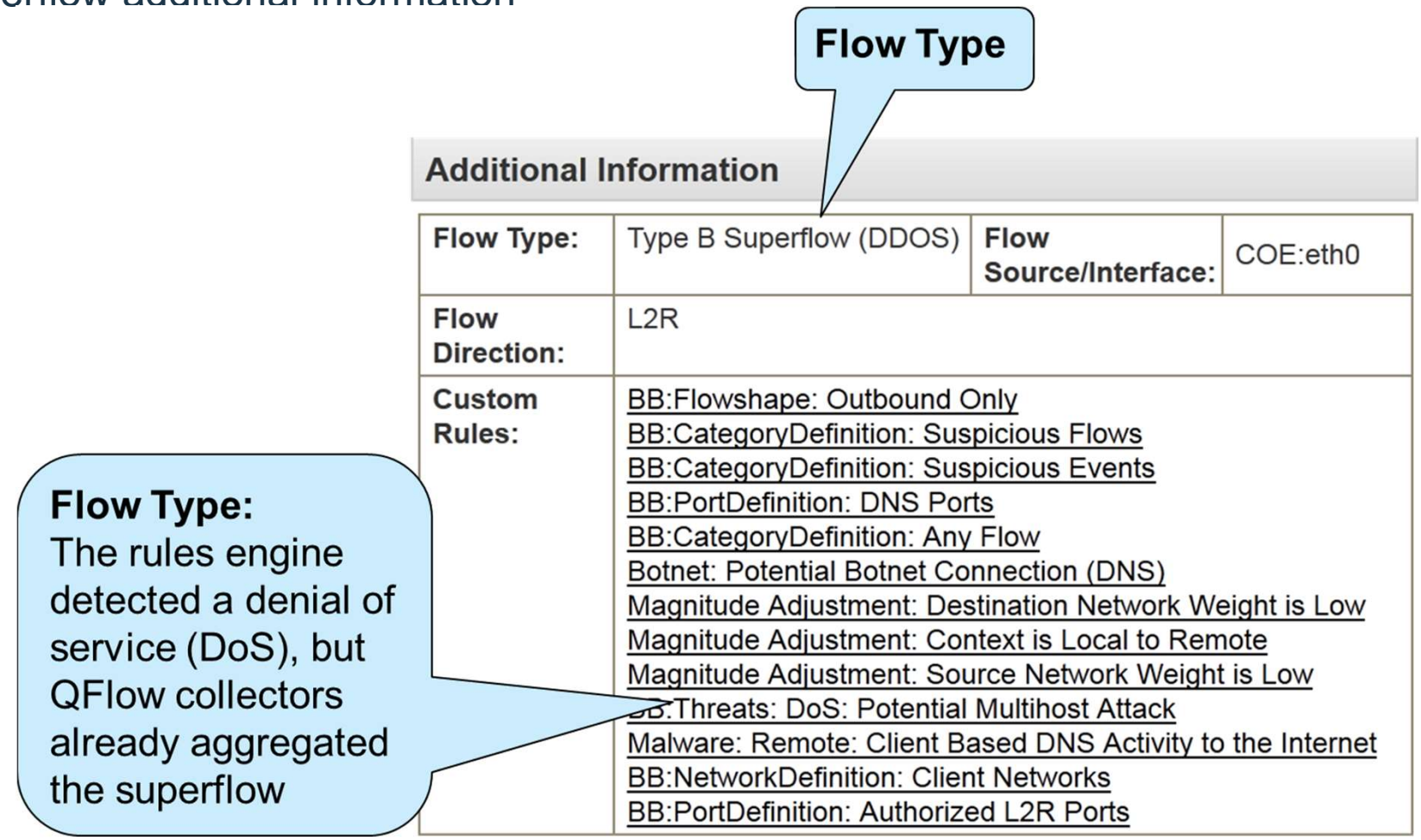


Superflow source and destination information

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



Superflow additional information



Superflows Default Values

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

- Can be customized in “System and License Management”

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

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

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.

IBM

Offenses Overview

Introduction to offenses

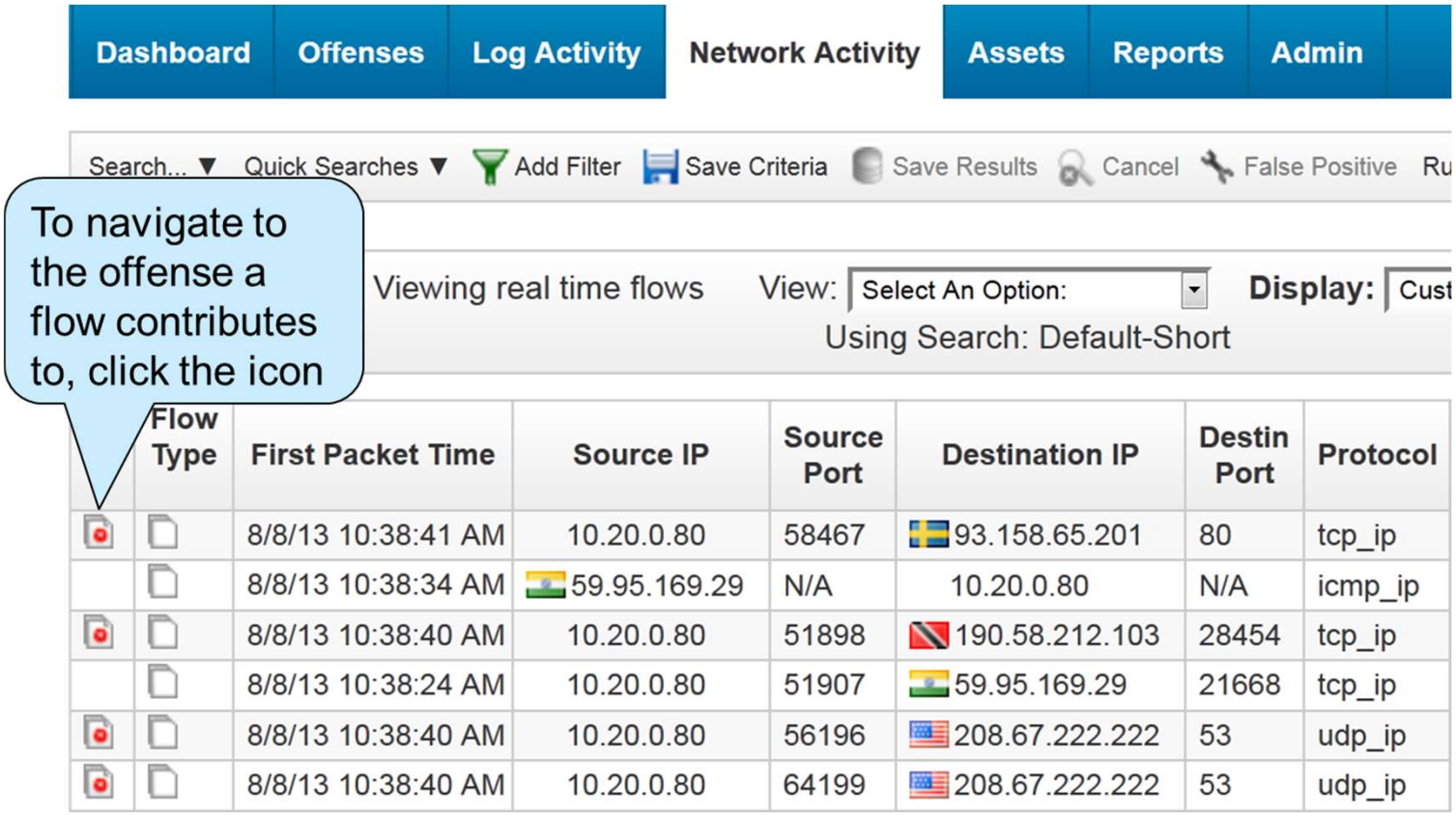
- The prime benefit of QRadar SIEM for security analysts is that it detects suspicious activities and ties them together into *offenses*
- An offense represents a suspected attack or policy breach; some common offenses include these examples
  - Multiple login failures
  - Worm infection
  - P2P traffic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

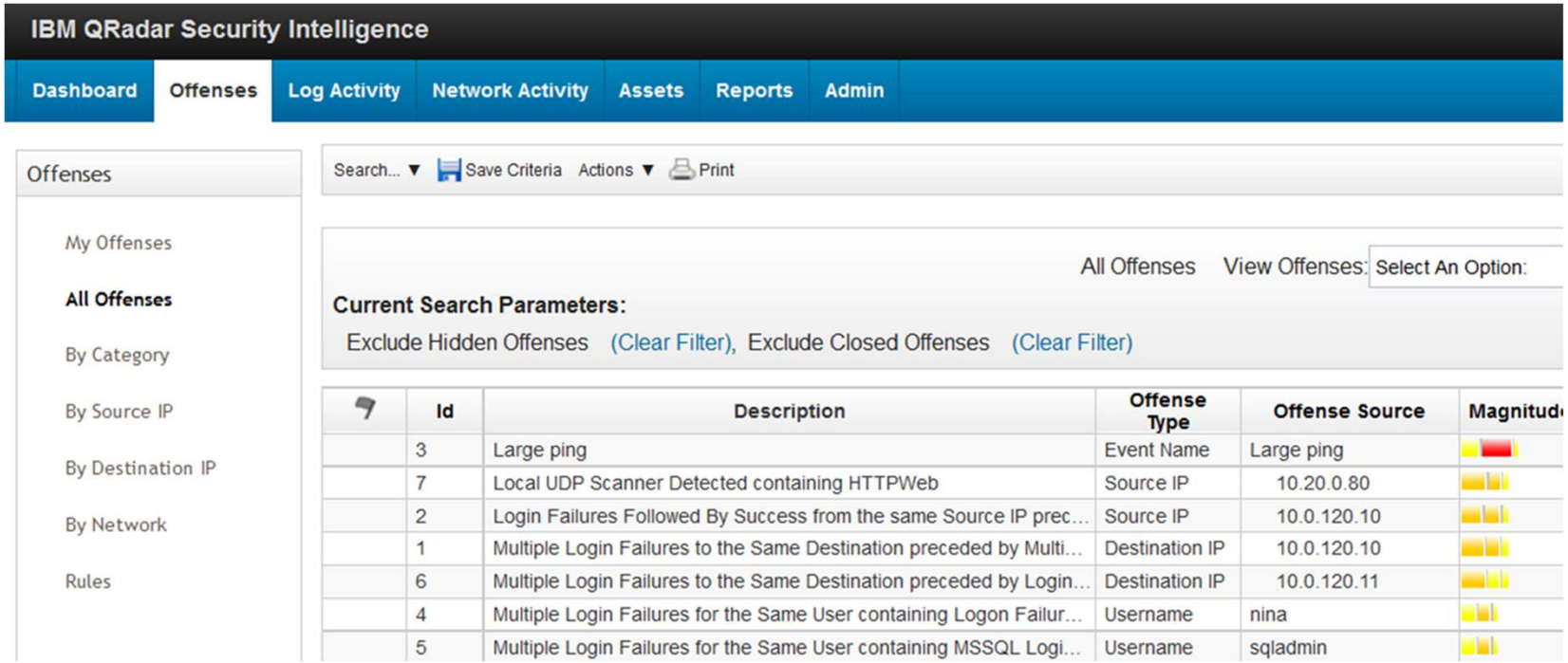
A red icon indicates that a flow contributes to an offense



Selecting an offense to investigate

Offenses are listed in these locations

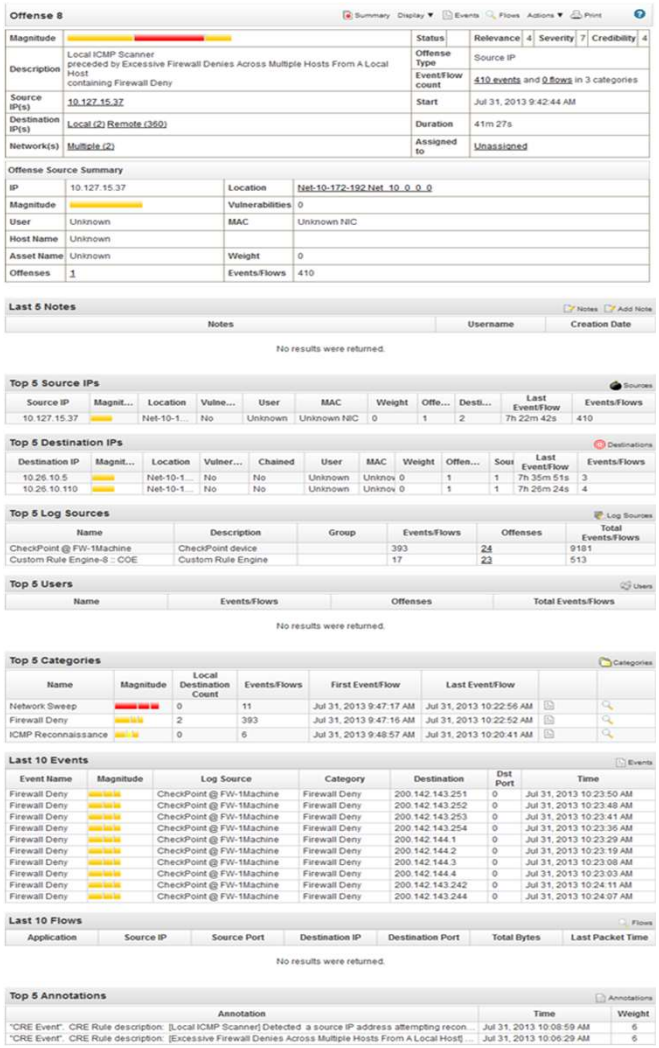
- In Dashboard items
- In the **Offenses** tab



Offense Summary window

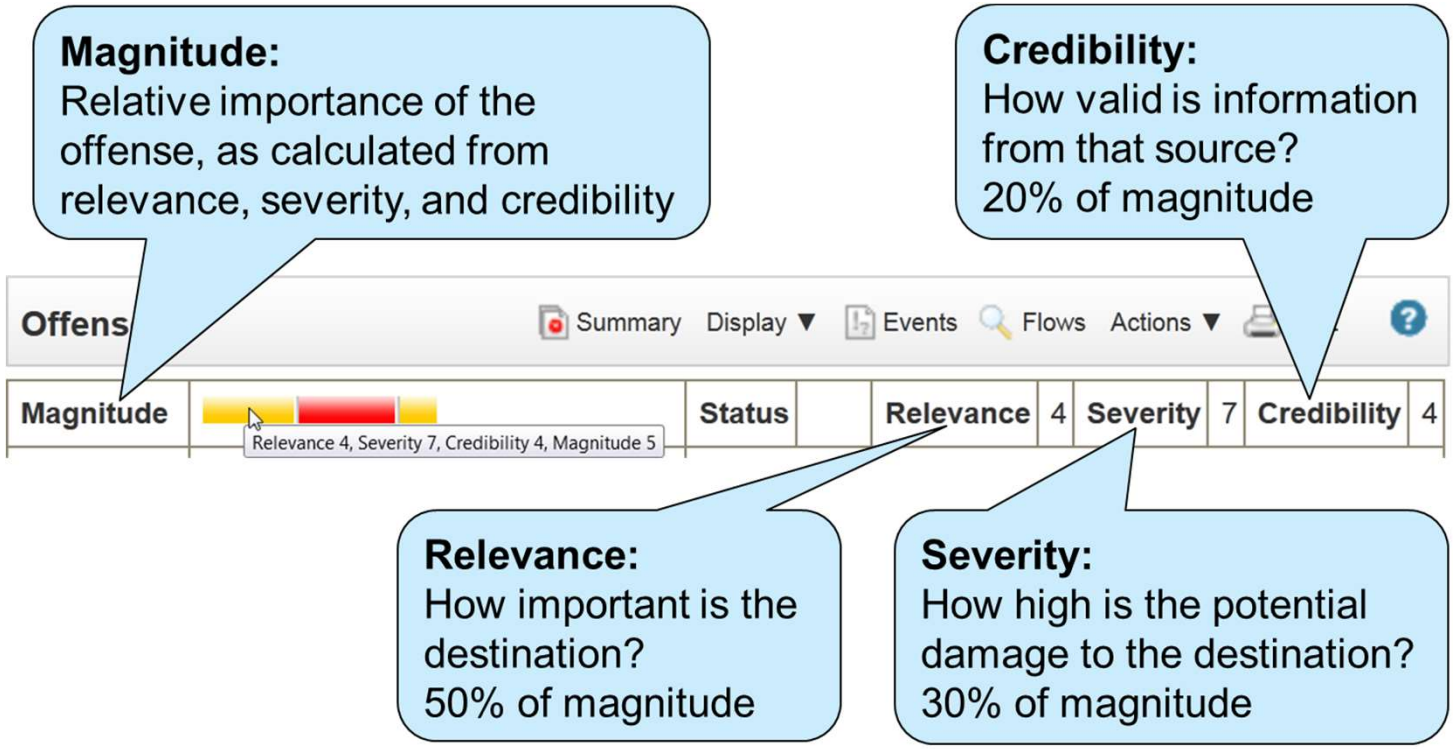
The offense summary displays information about the ICMP scanning offense

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

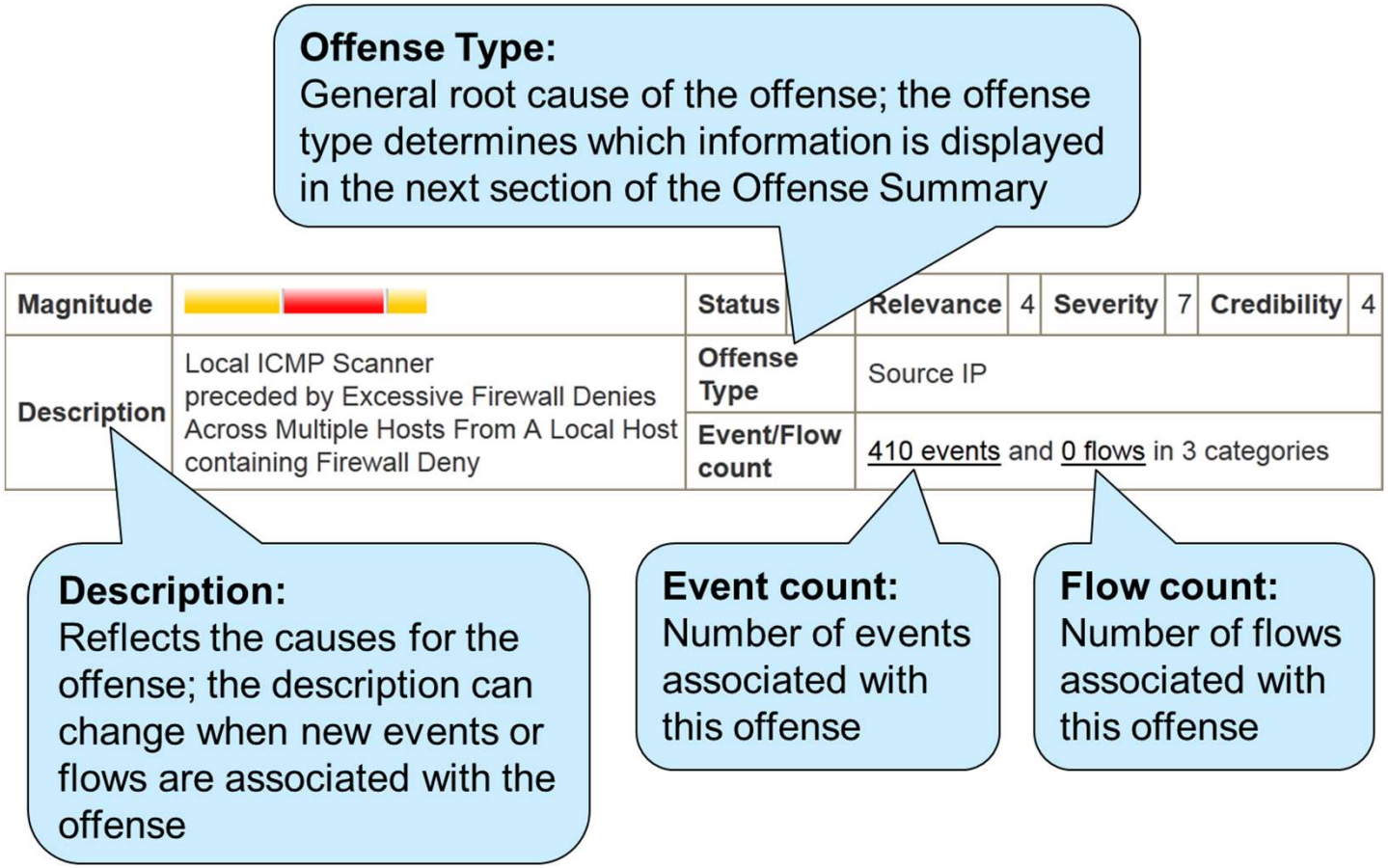


Offense parameters (1 of 4)

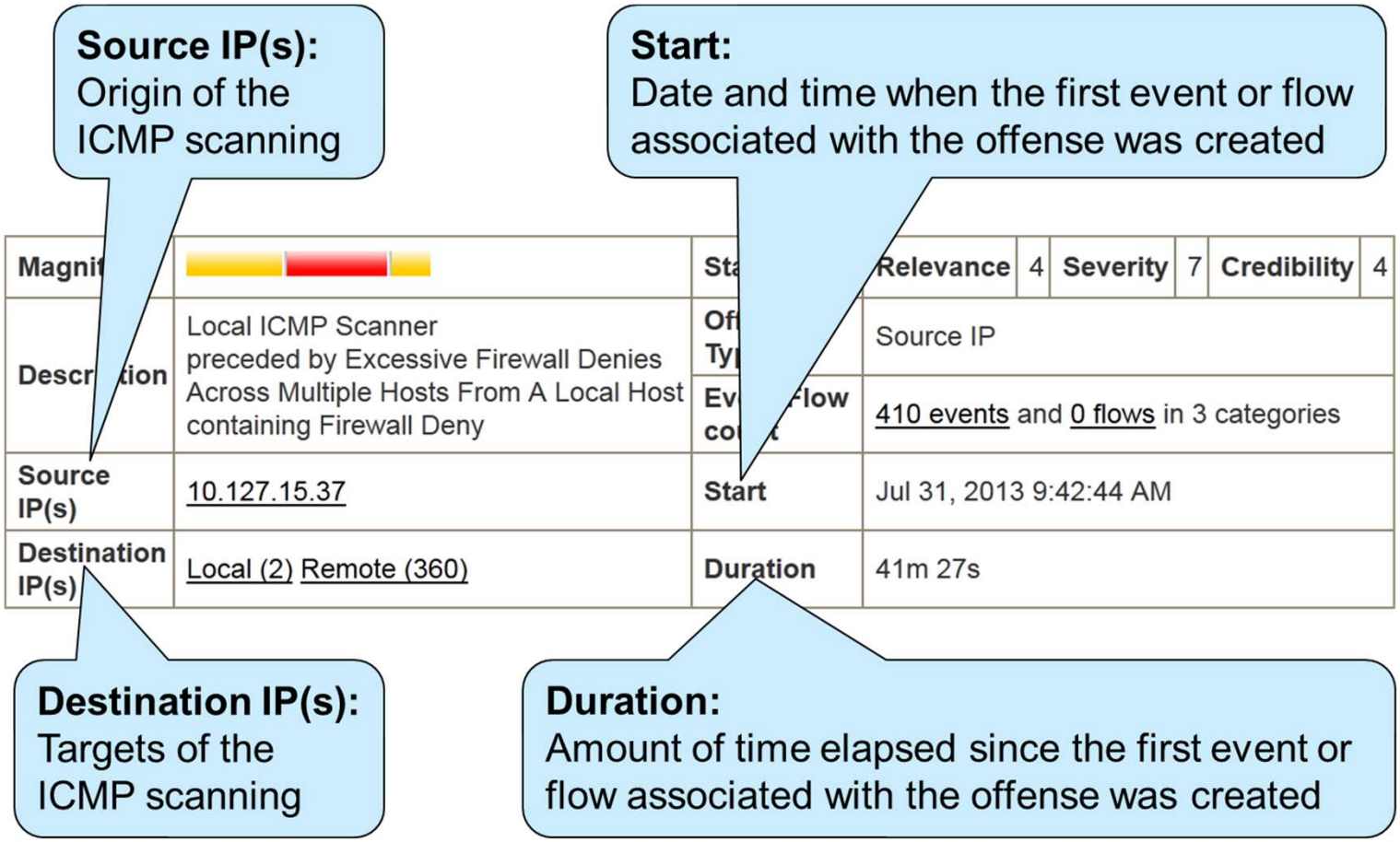
Investigating an offense begins with the parameters at the top of the offense summary window



Offense parameters (2 of 4)



Offense parameters (3 of 4)



Offense parameters (4 of 4)

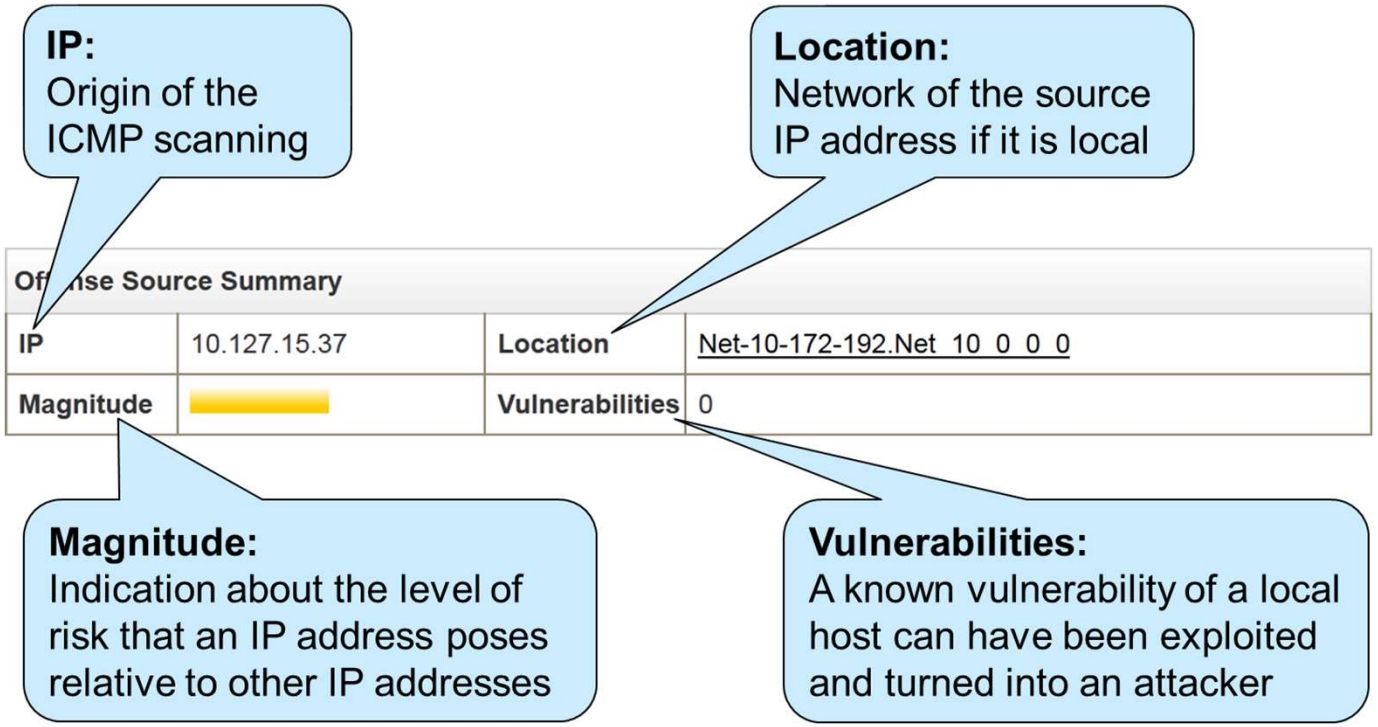
Magnitude		Status		Relevance	4	Severity	7	Credibility	4
Description	Local ICMP Scanner preceded by Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewall Deny	Offense Type	Source IP						
		Event/Flow count	410 events and 0 flows in 3 categories						
Source IP(s)	10.127.15.37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

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

Assigned to:
QRadar SIEM user assigned to investigate this offense

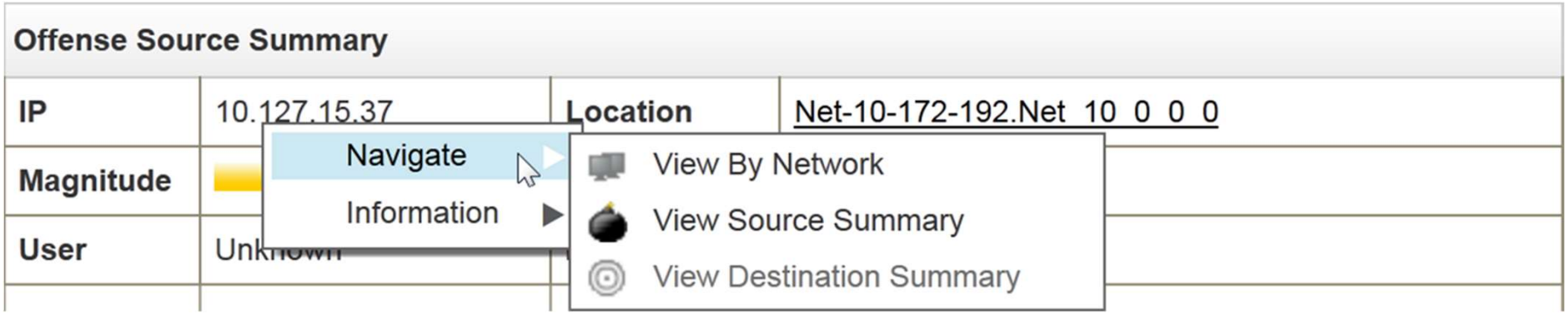
Offense Source Summary (1 of 4)

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

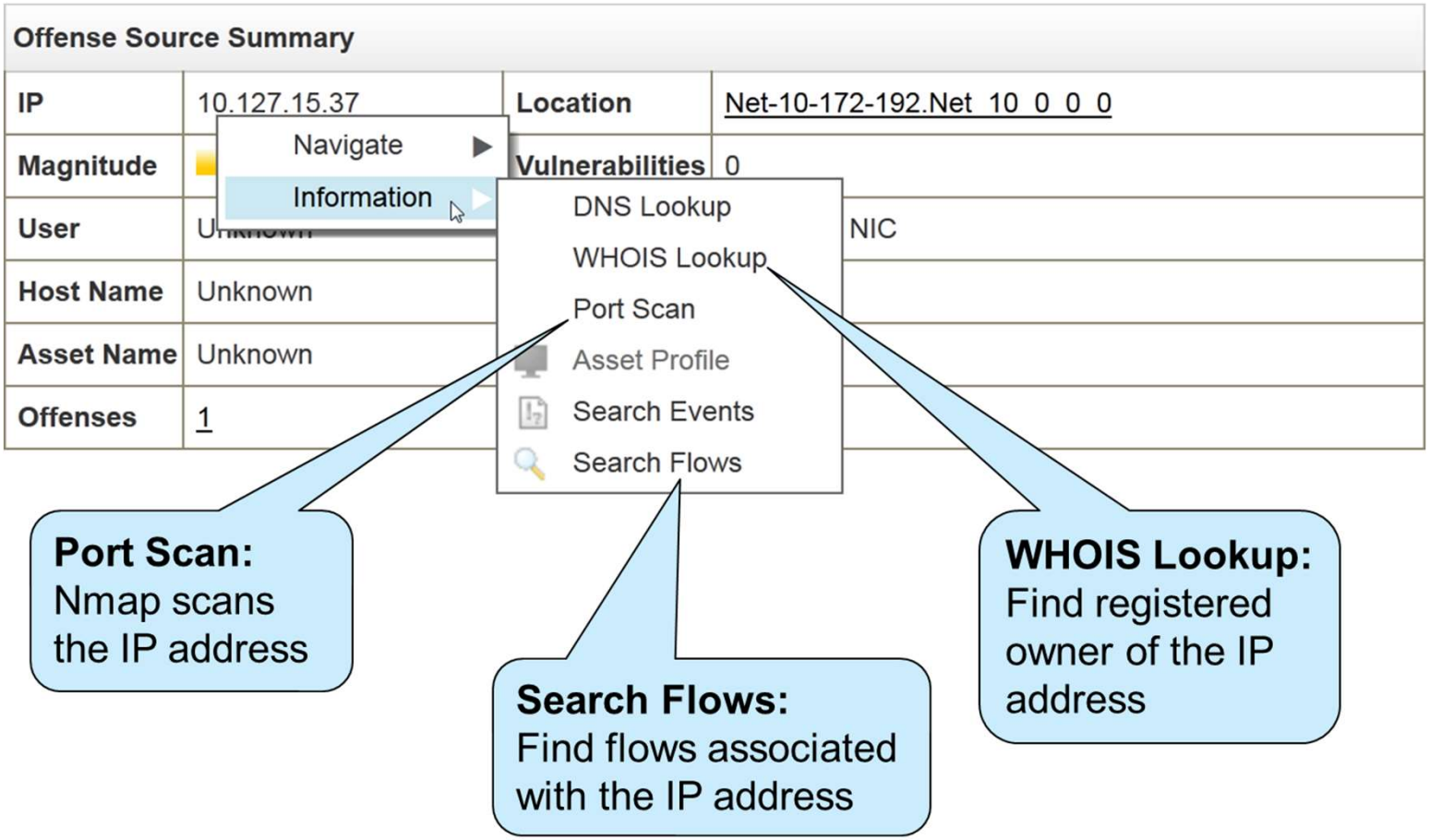


Offense Source Summary (2 of 4)

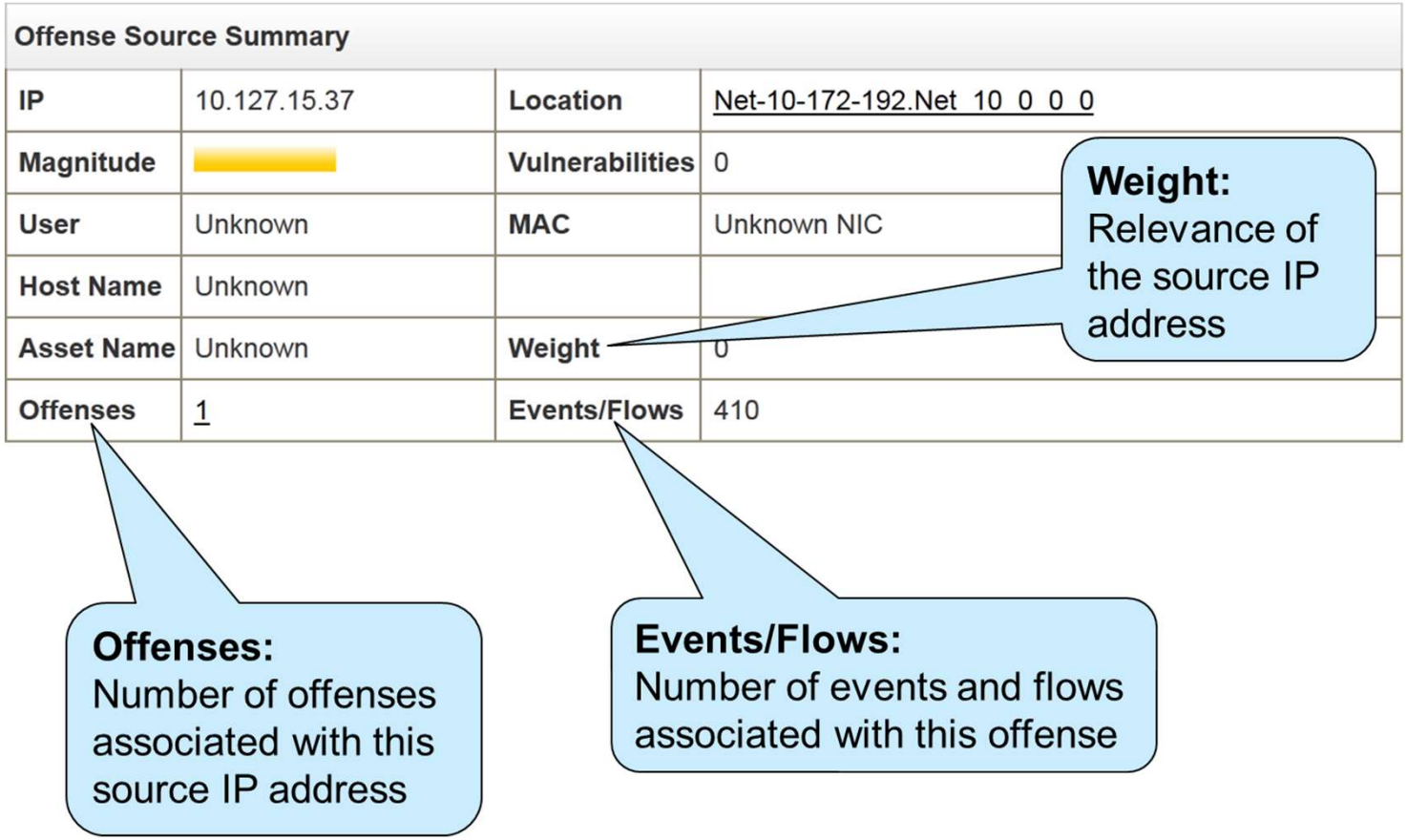
When you right-click the IP, you see navigation options for further investigation



Offense Source Summary (3 of 4)



Offense Source Summary (4 of 4)

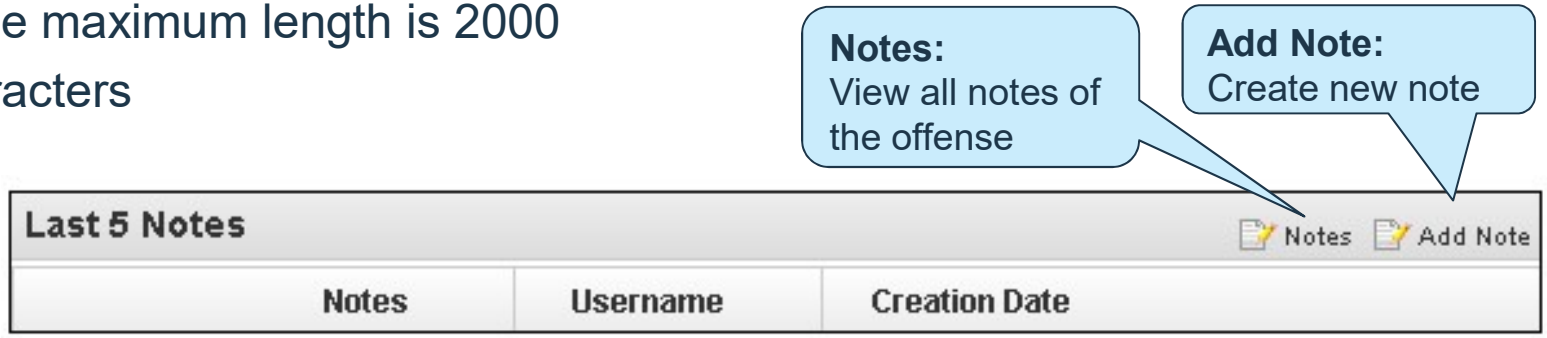


Search Results and Notes

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

QRadar SIEM users can add notes to offenses

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



Top 5 Source and Destination IPs

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

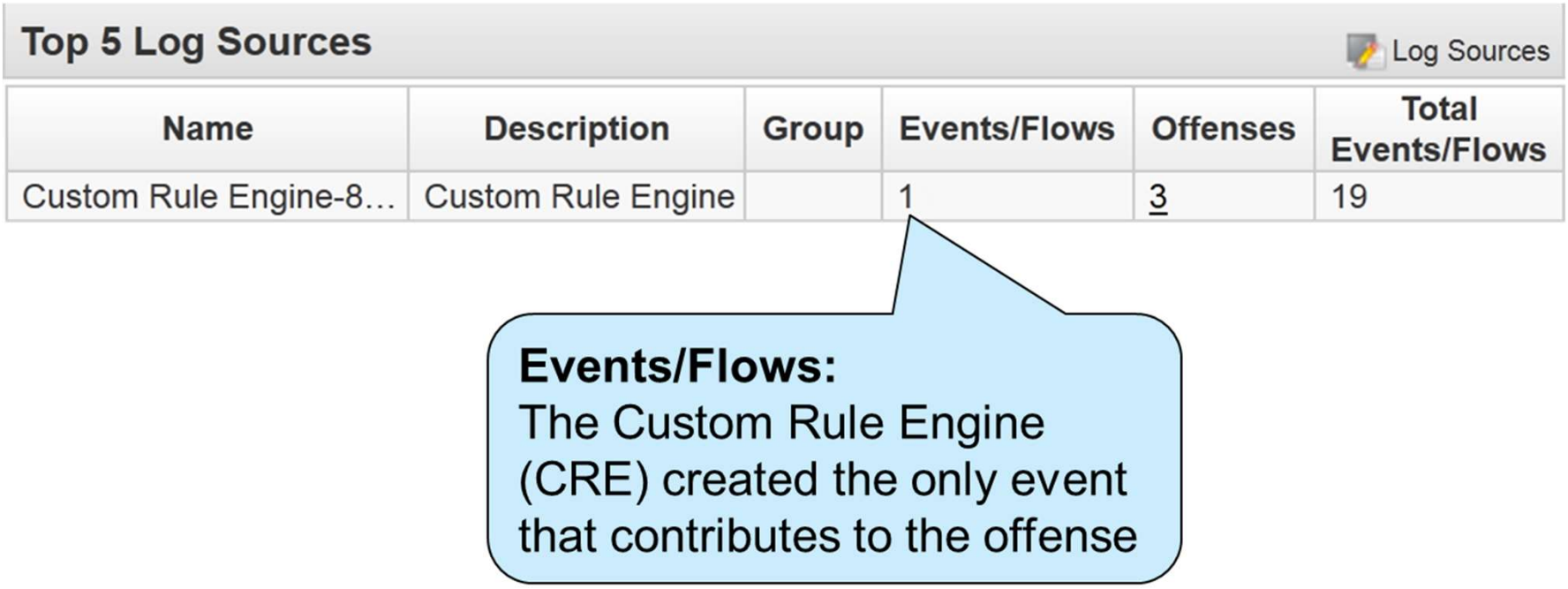
Top 5 Source IPs — Sources

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

Top 5 Destination IPs — Destinations

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

Top 5 Log Sources



Top 5 Categories

QRadar SIEM sorted the event and the flows into categories

Top 5 Categories Categories

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

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

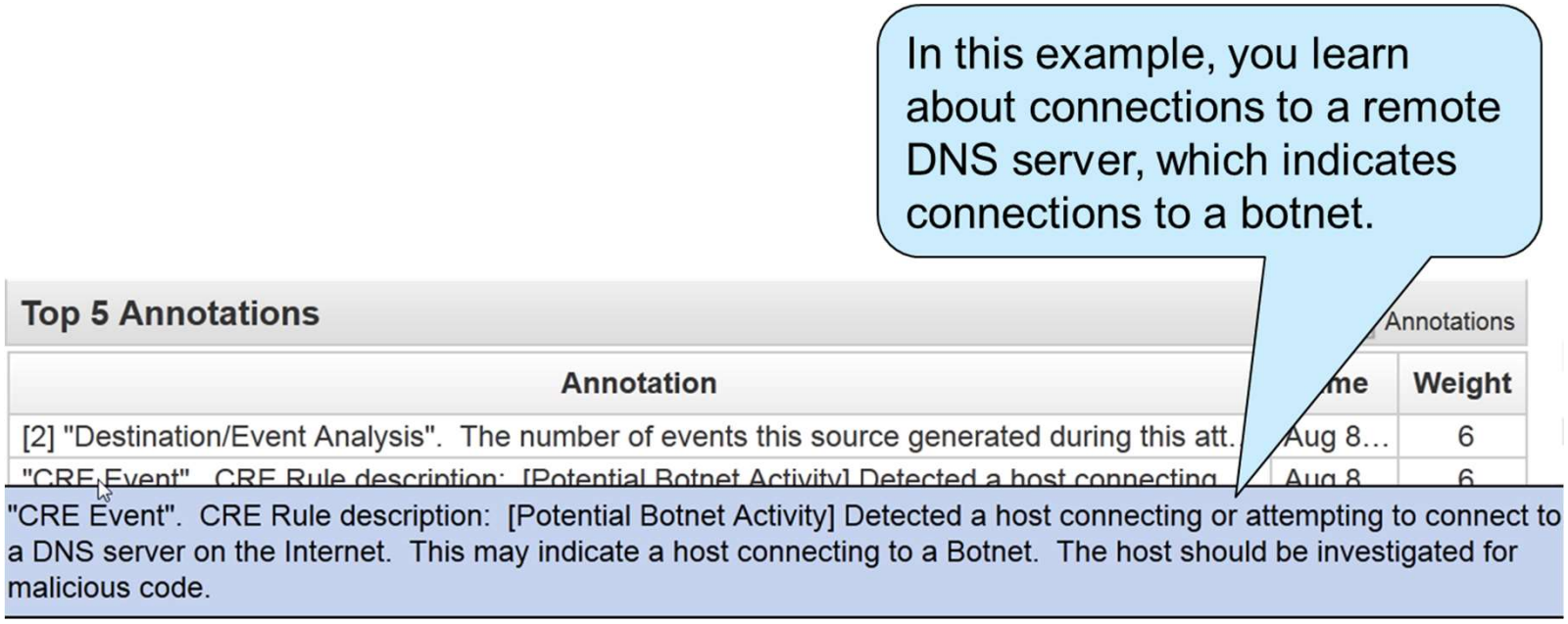
Double-click a row to open a window with details about the flow

Last 10 Flows Flows

Application	Source IP	Source Port	...ination 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

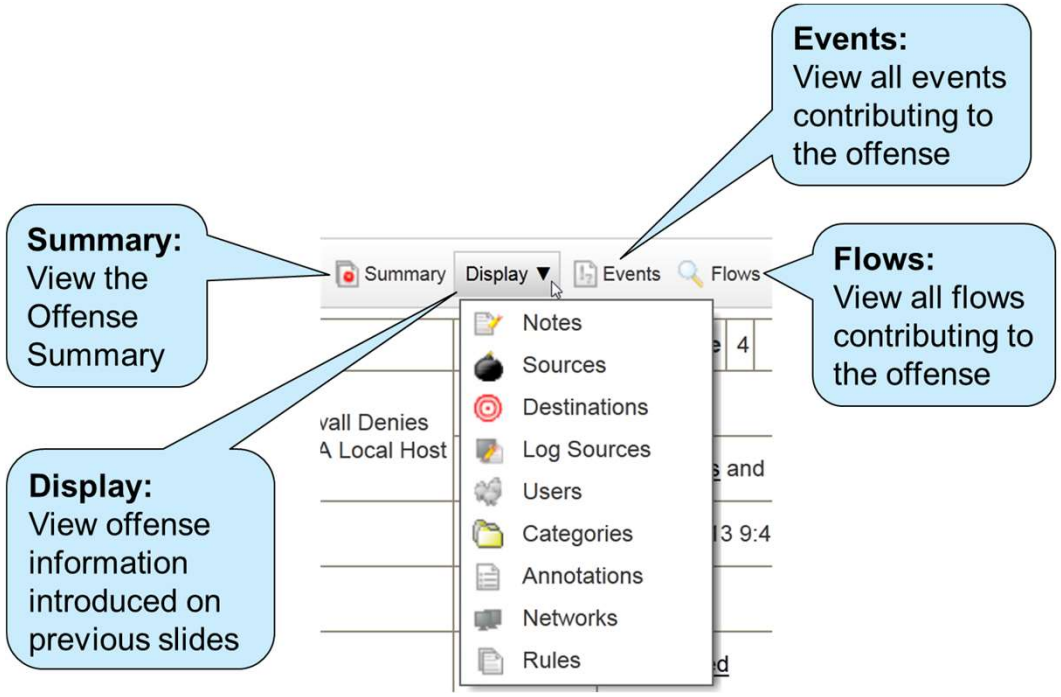
Annotations

- 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



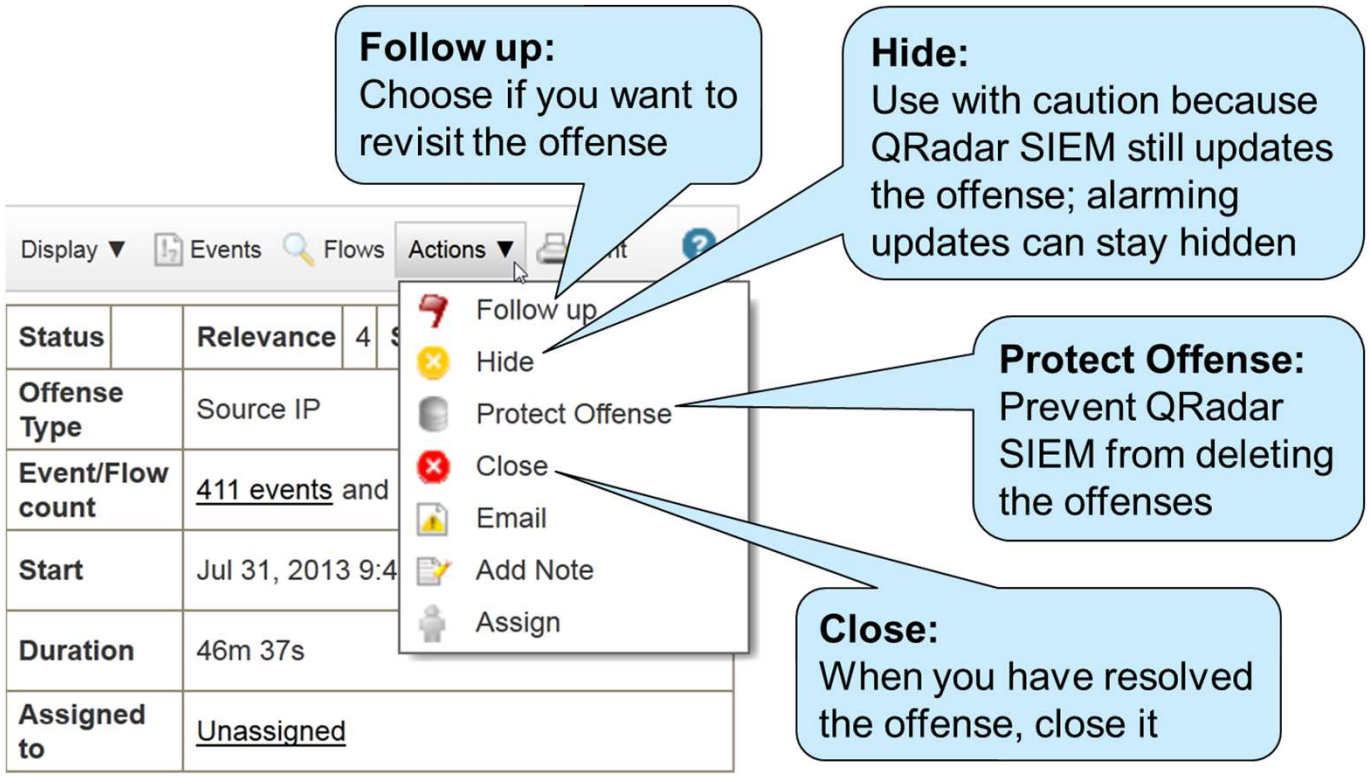
Offense Summary toolbar

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



Offense actions

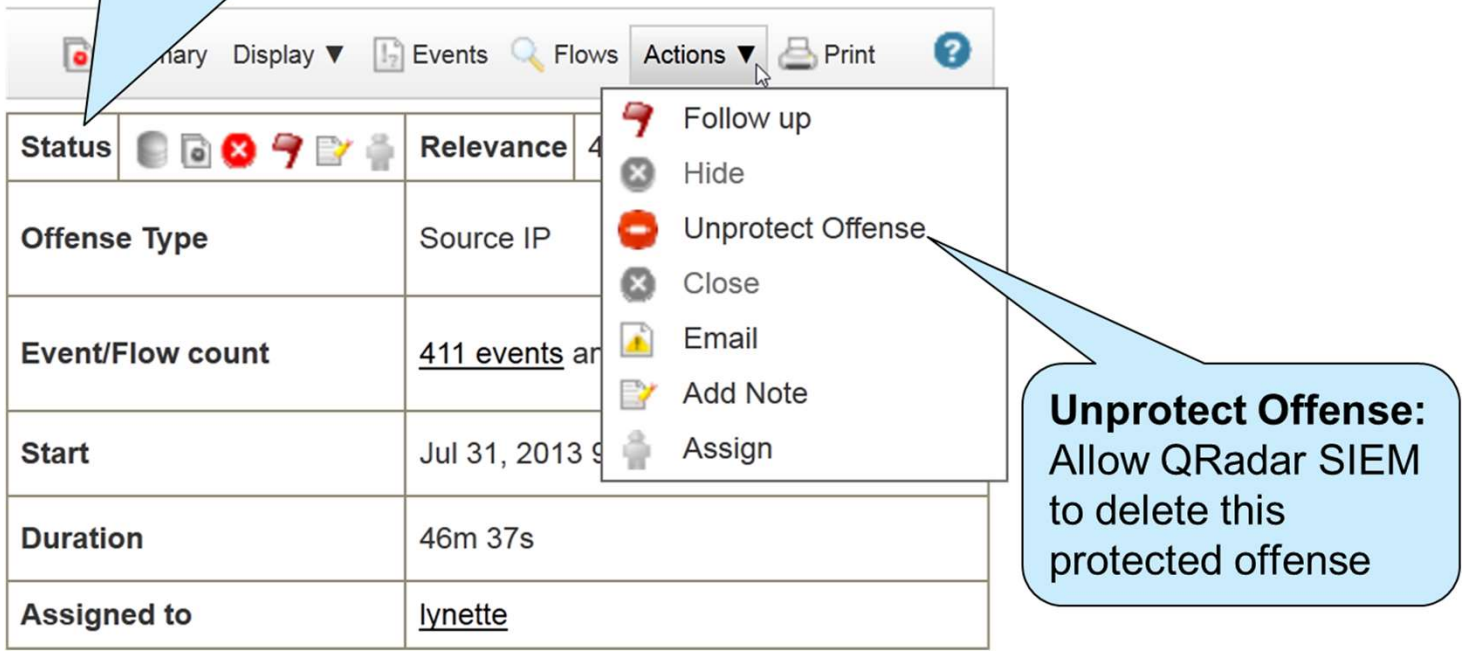
- After investigating an offense, click **Actions** at the top of the Offense Summary page to set flags and status



Offense status and flags

Status: Icon indicates
- Protected
- Inactive
- Closed
- Follow up
- Notes
- Assigned

The actions available depend on the status of the offense



Unprotect Offense: Allow QRadar SIEM to delete this protected offense

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

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.

IBM

Introduction to Rules

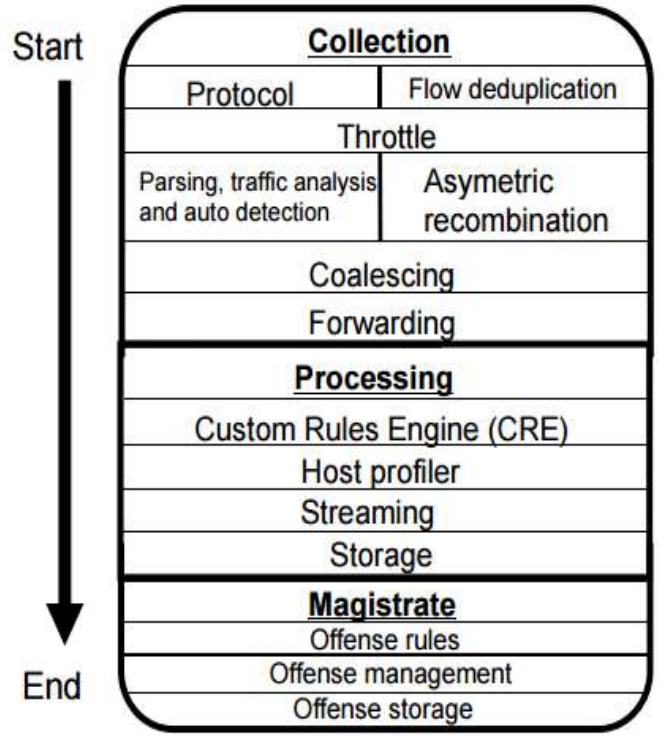
What are rules

- 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

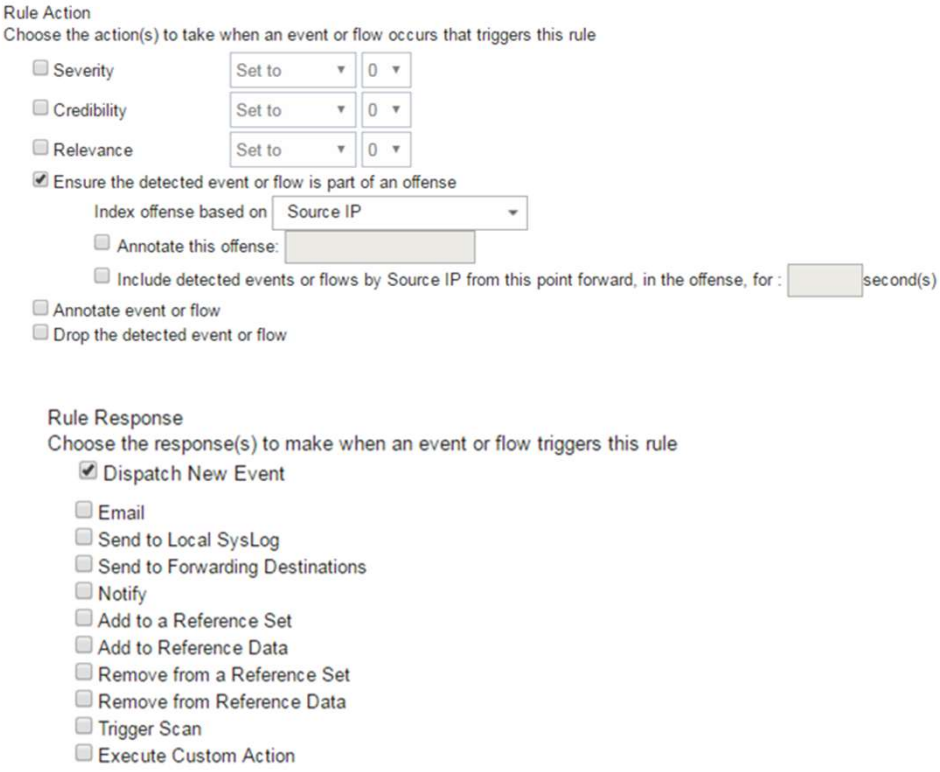
- Event Rules
  - Test against incoming log source data that is processed in real time and previously processed data (historical data) by the QRadar Event Processor.
  - Event rules can perform tests against a single event or event sequences
- Flow Rules
  - Test against incoming flow data that is processed 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

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.



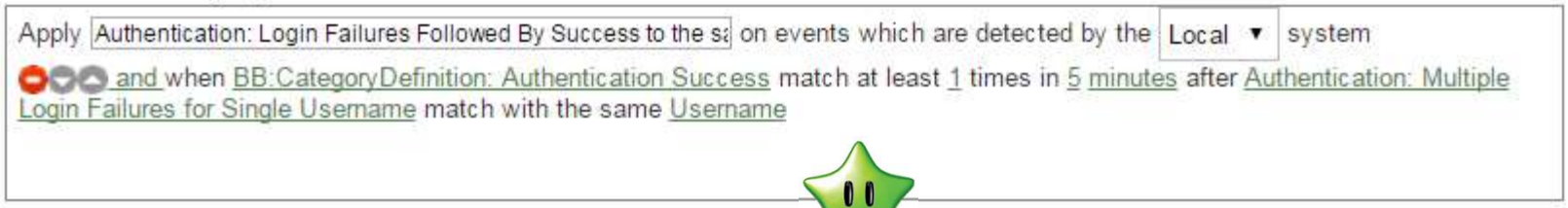
Rules and Building Blocks

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



- 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"*

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

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

  - Rule:

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

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

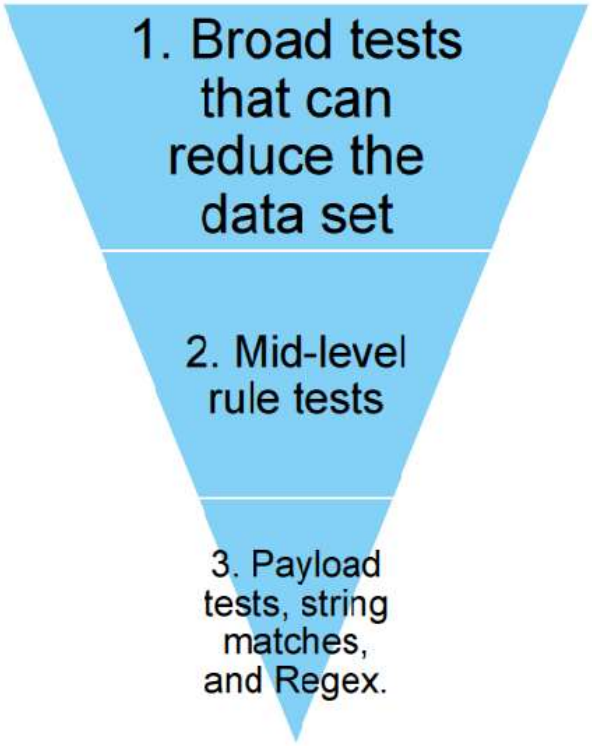
Optimizing Linking Tests (1/2)

- 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

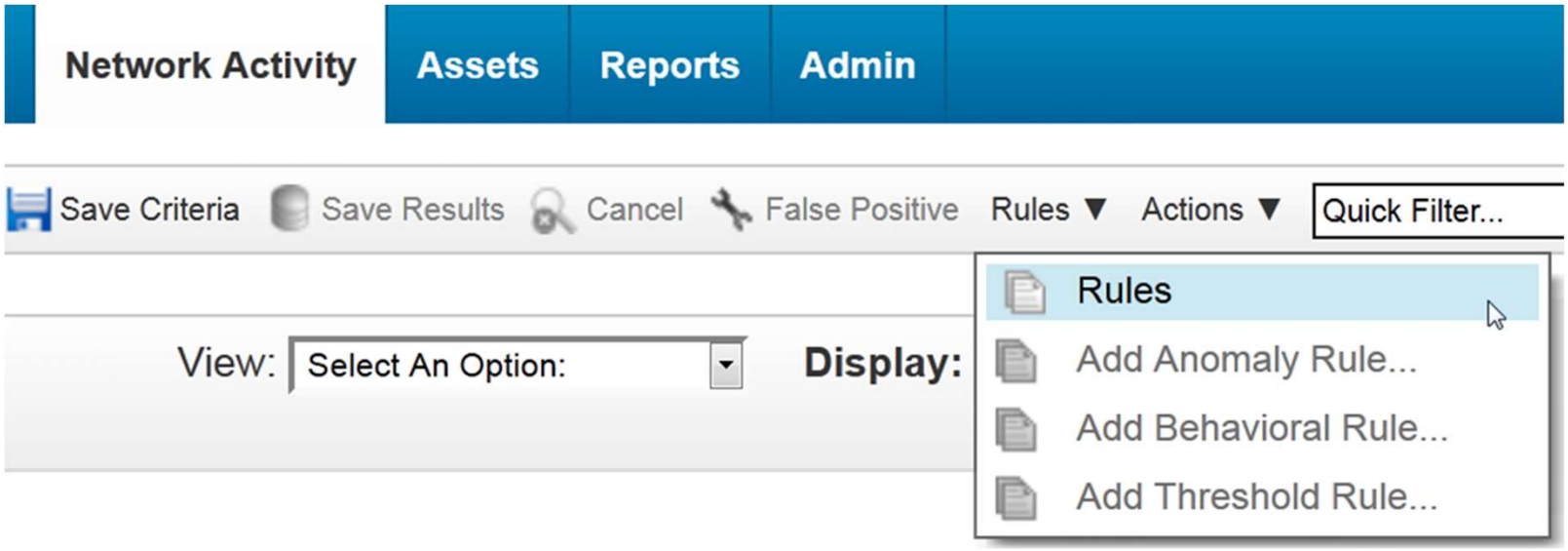
Creating a Custom Rule

- 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

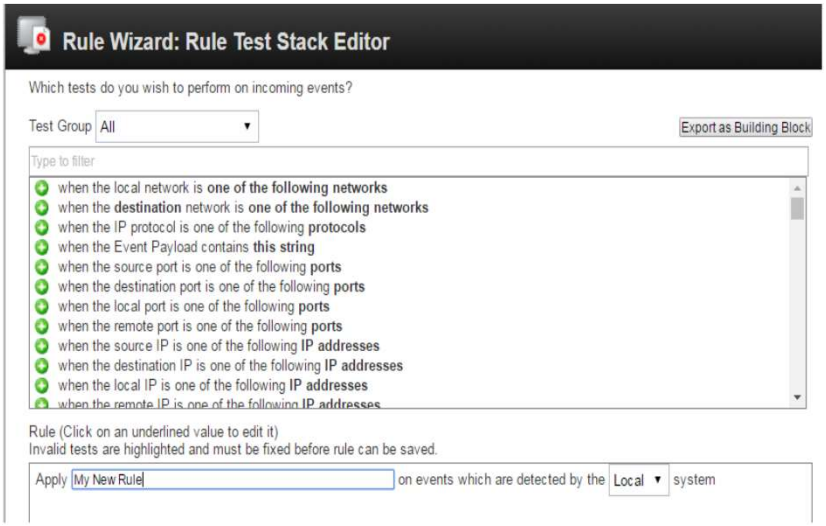
Rules can be accessed from:

- 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



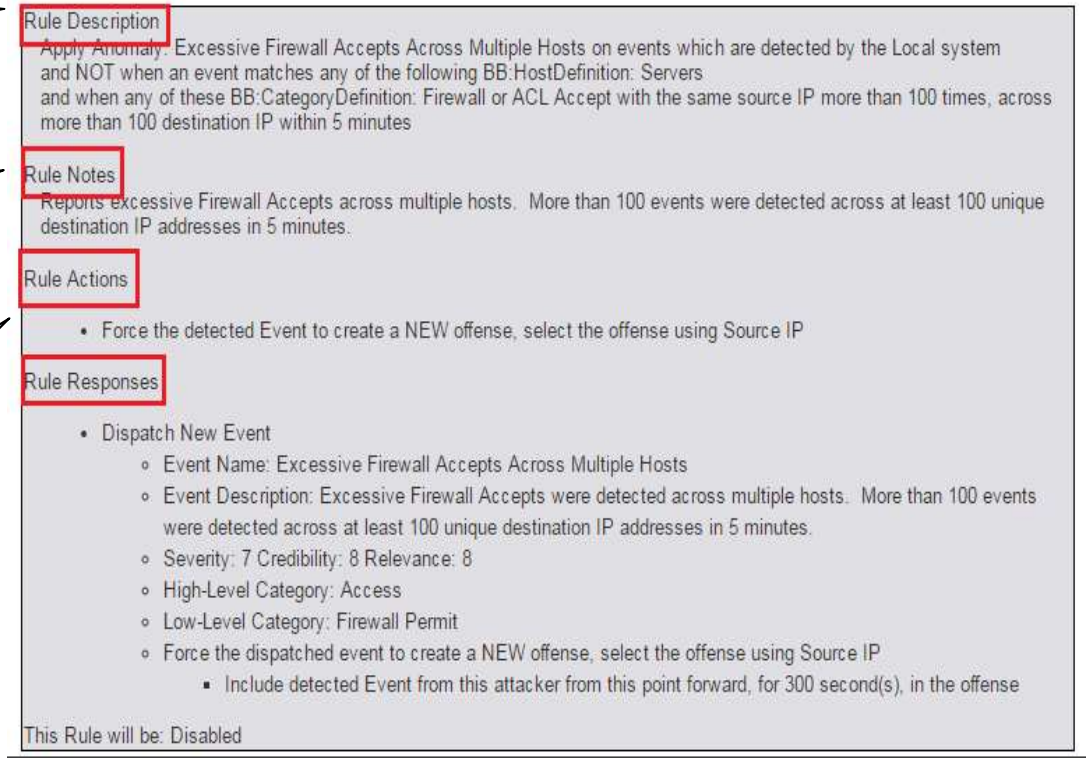
- On the Rule Responses page, configure the responses and Action that you want this rule to generate

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

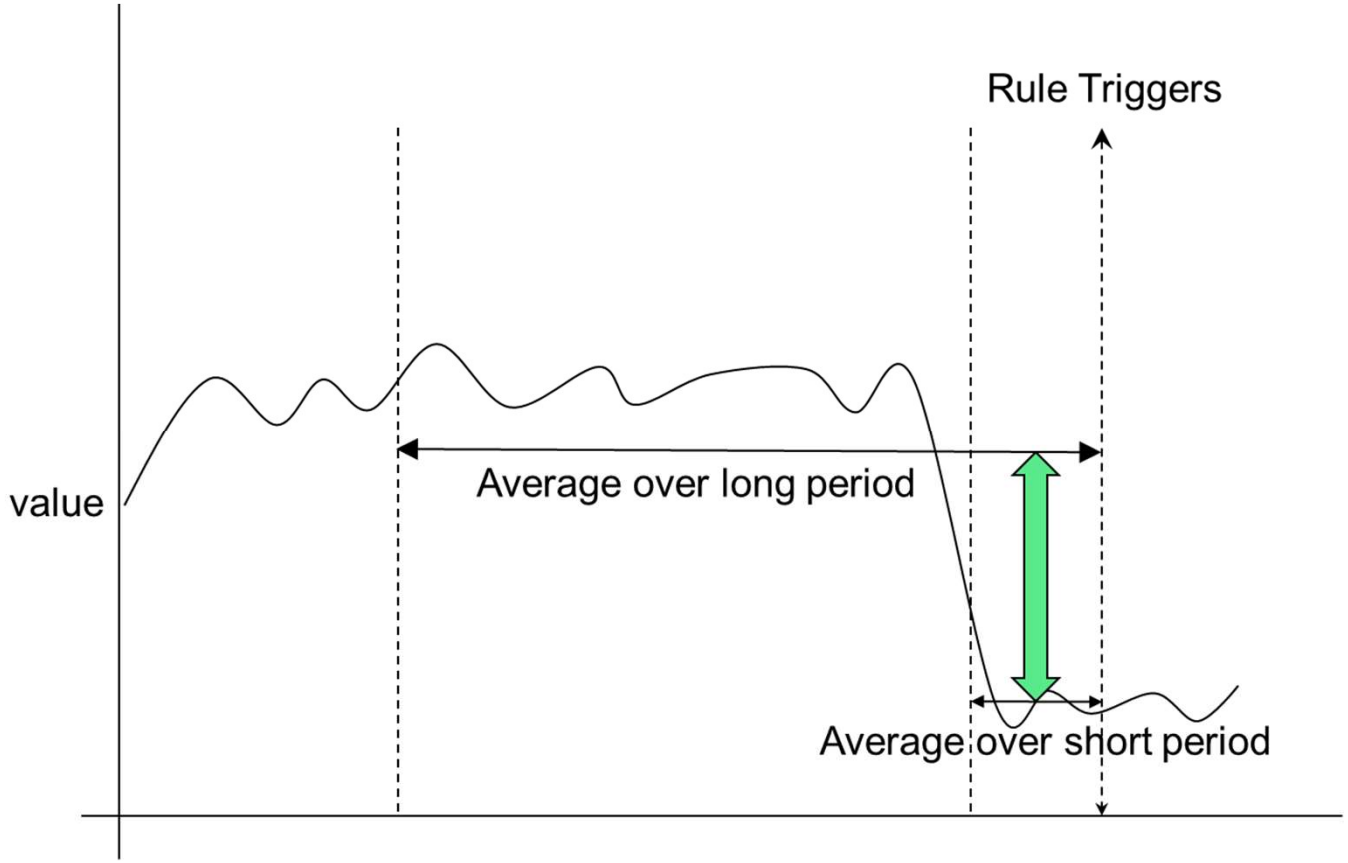


Anomaly Detection Rules

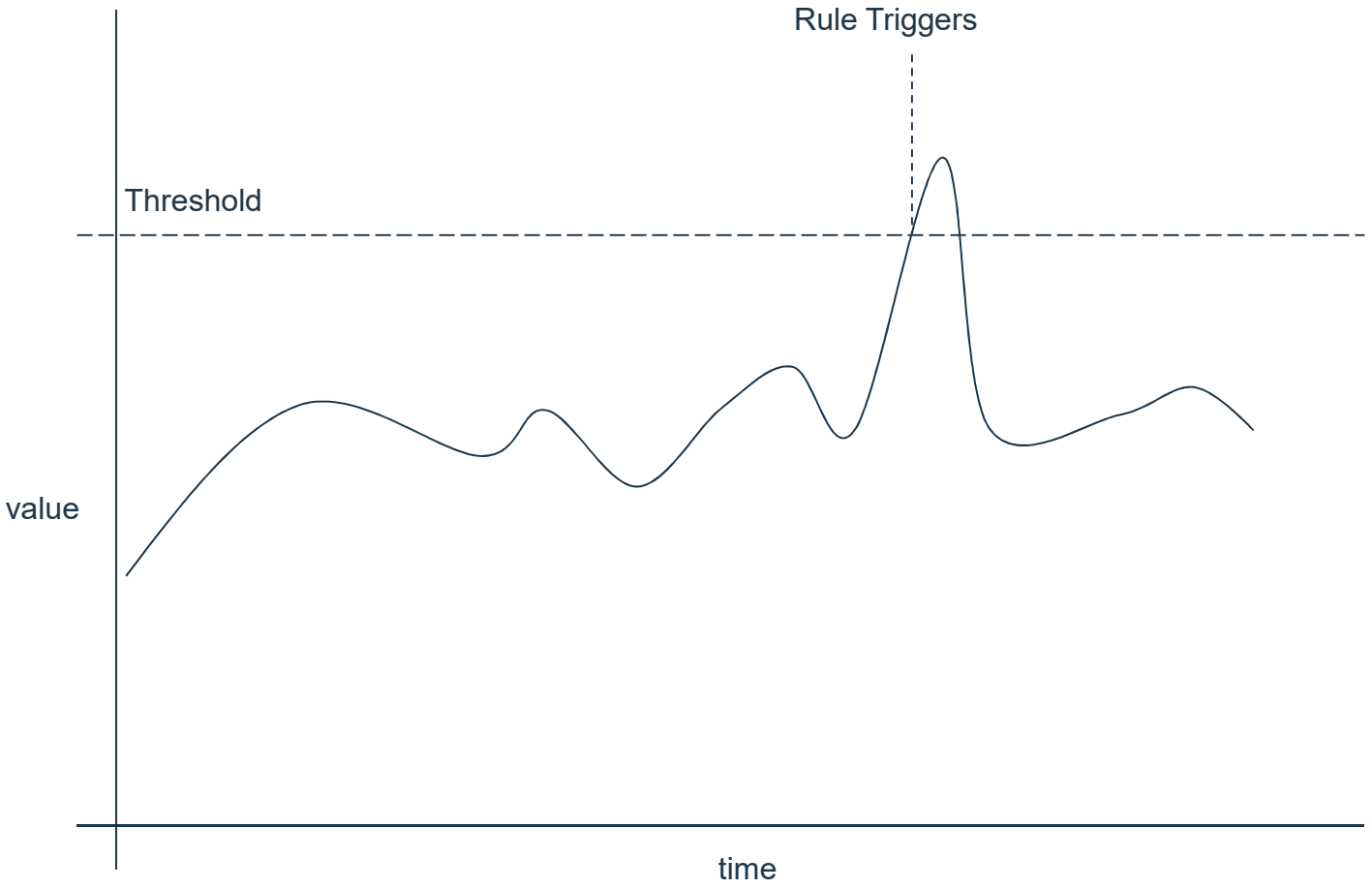
Anomaly Detection Rules

- 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

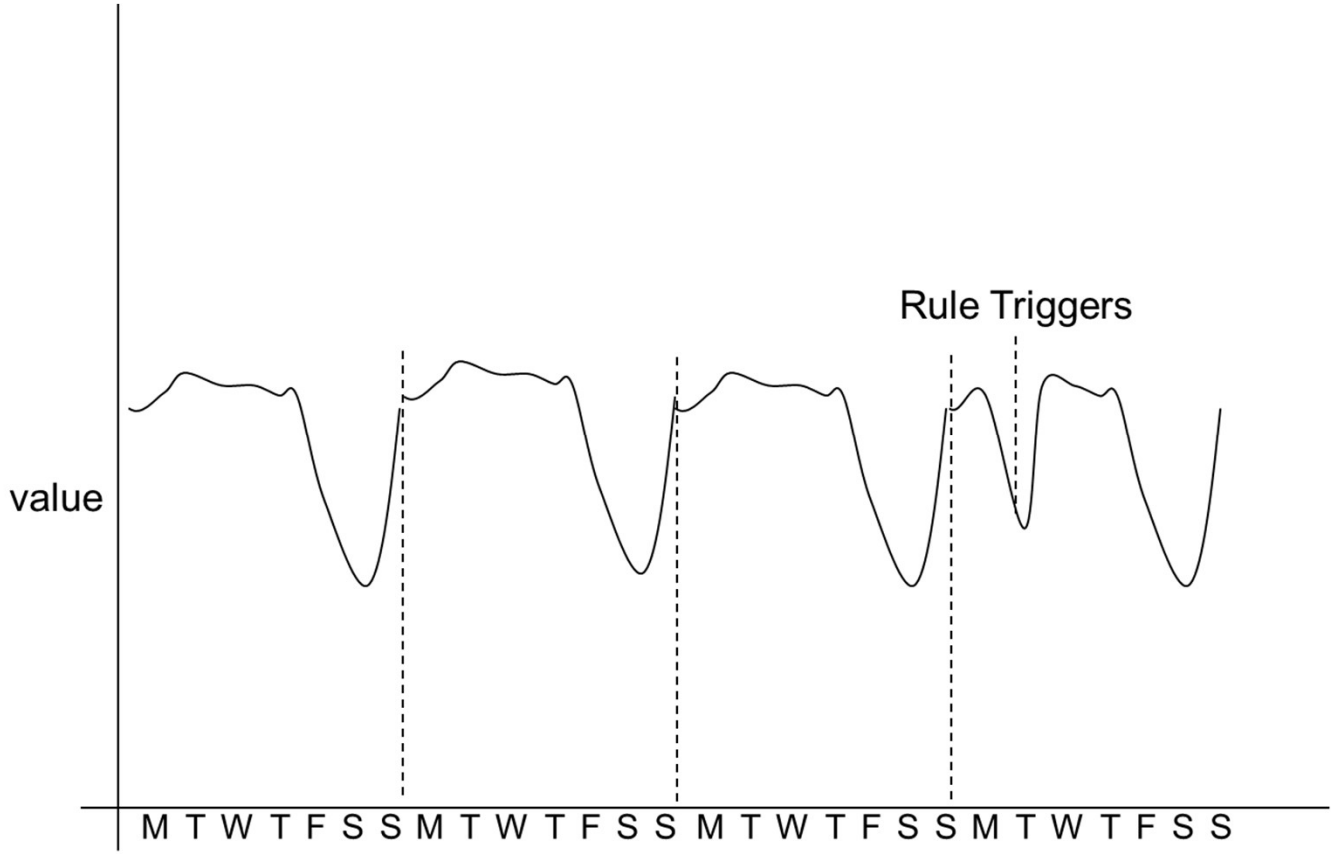
Anomaly Rules



Threshold Rules



Behavioral rules



IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

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.

IBM

Reports

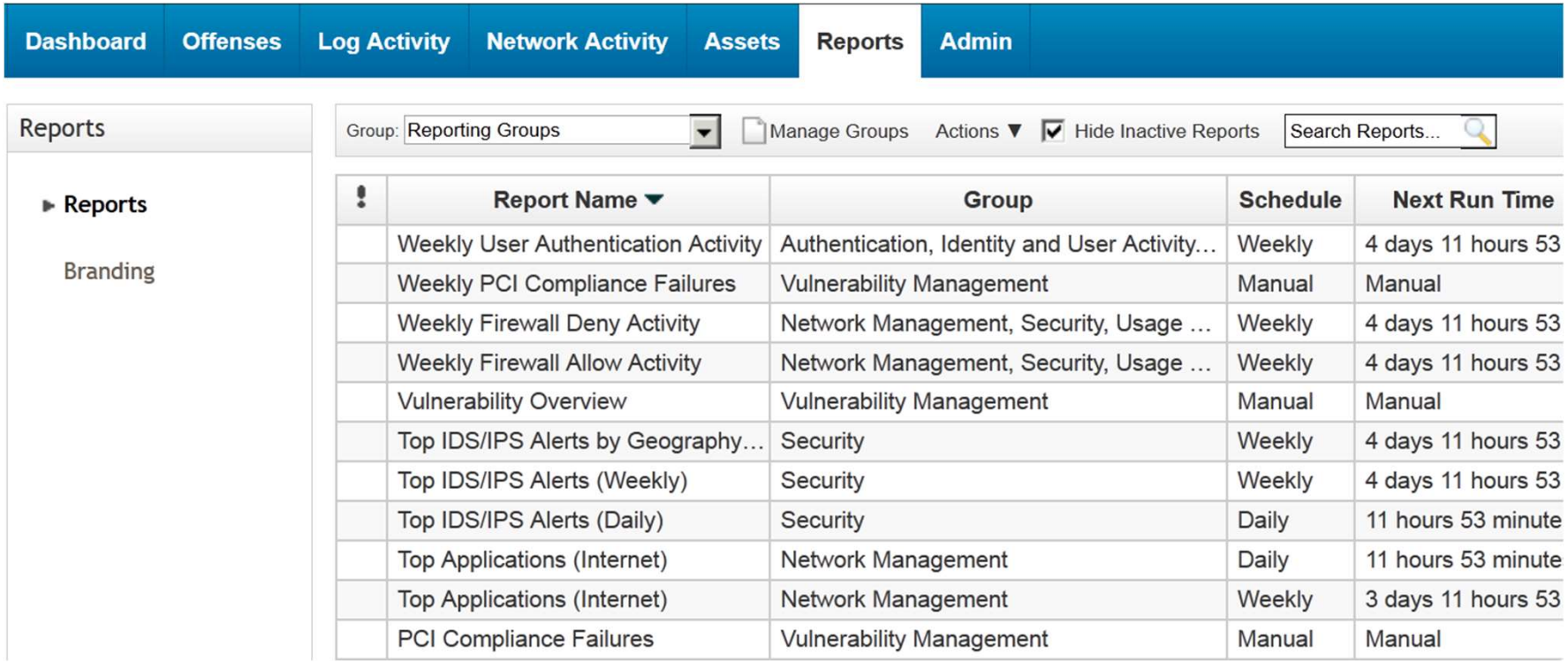
Reporting introduction

- 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

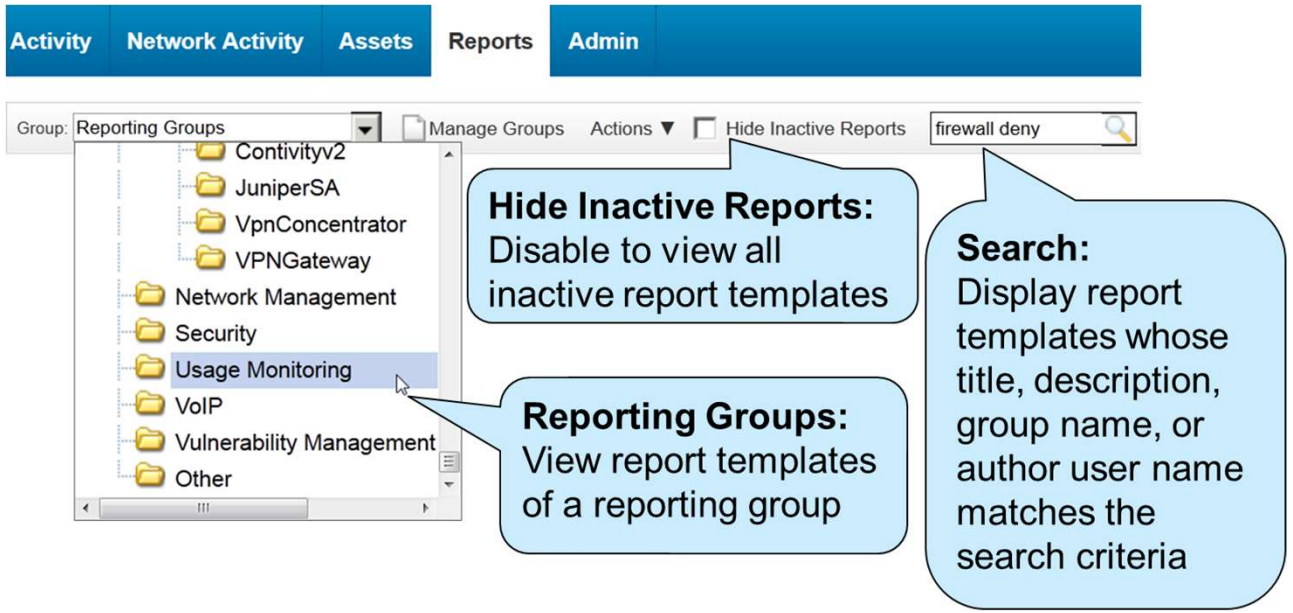
Reports tab

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

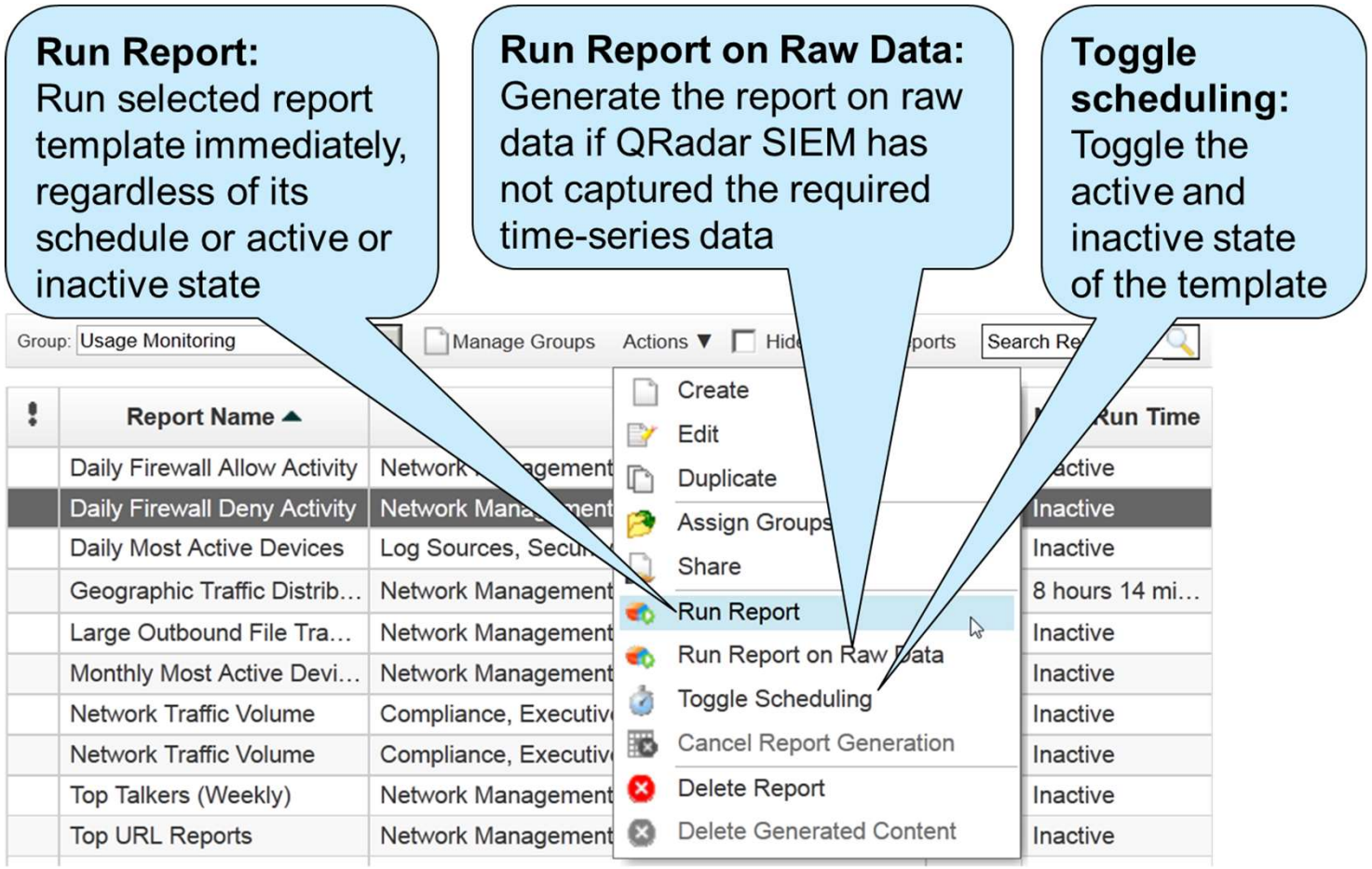


Finding a report

- 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



Running a report



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

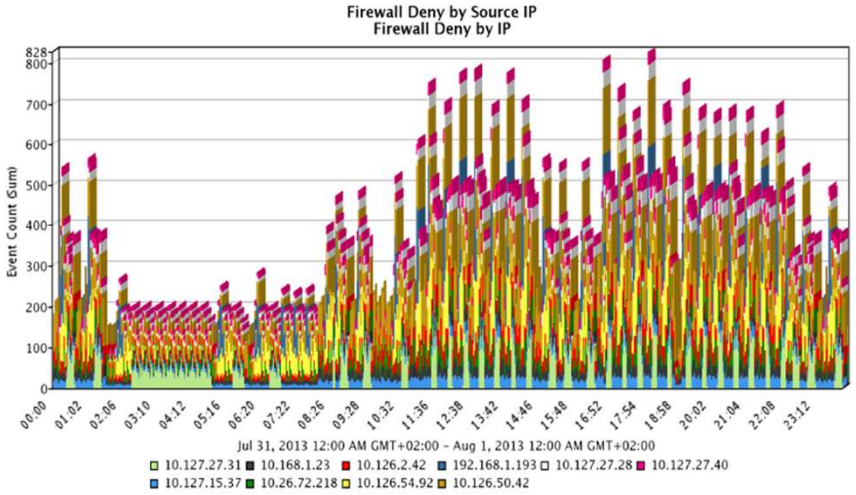
Next Run Time	Last Modifi	Owner	Author	Generated Reports	Formats
Inactive	Sep …	admin	admin	None	
Inactive	Sep …	admin	admin	Jul 31, 2013 4:49 PM	

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

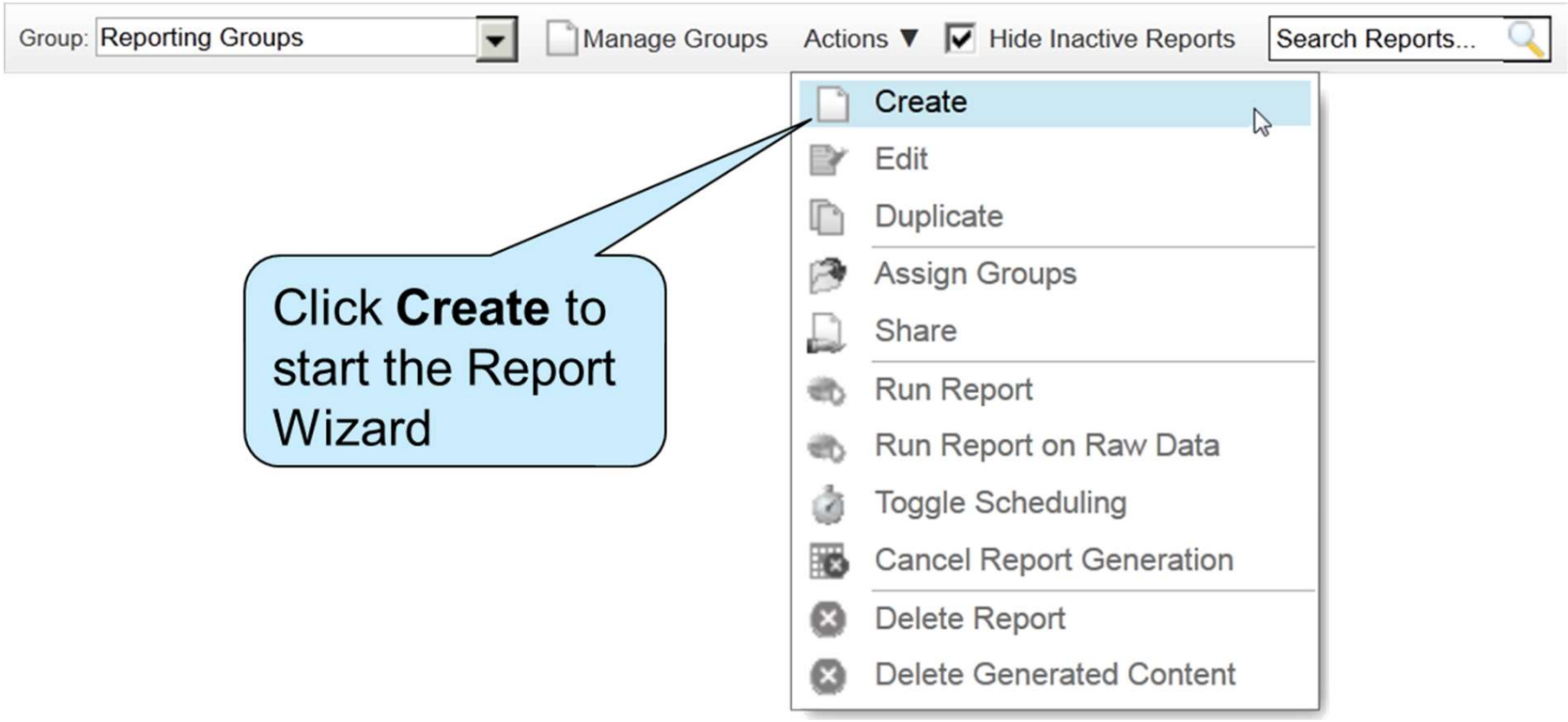


Firewall Deny by Device
Firewall Deny by Log Source
Jul 31, 2013 12:00:00 AM - Aug 1, 2013 12:00:00 AM

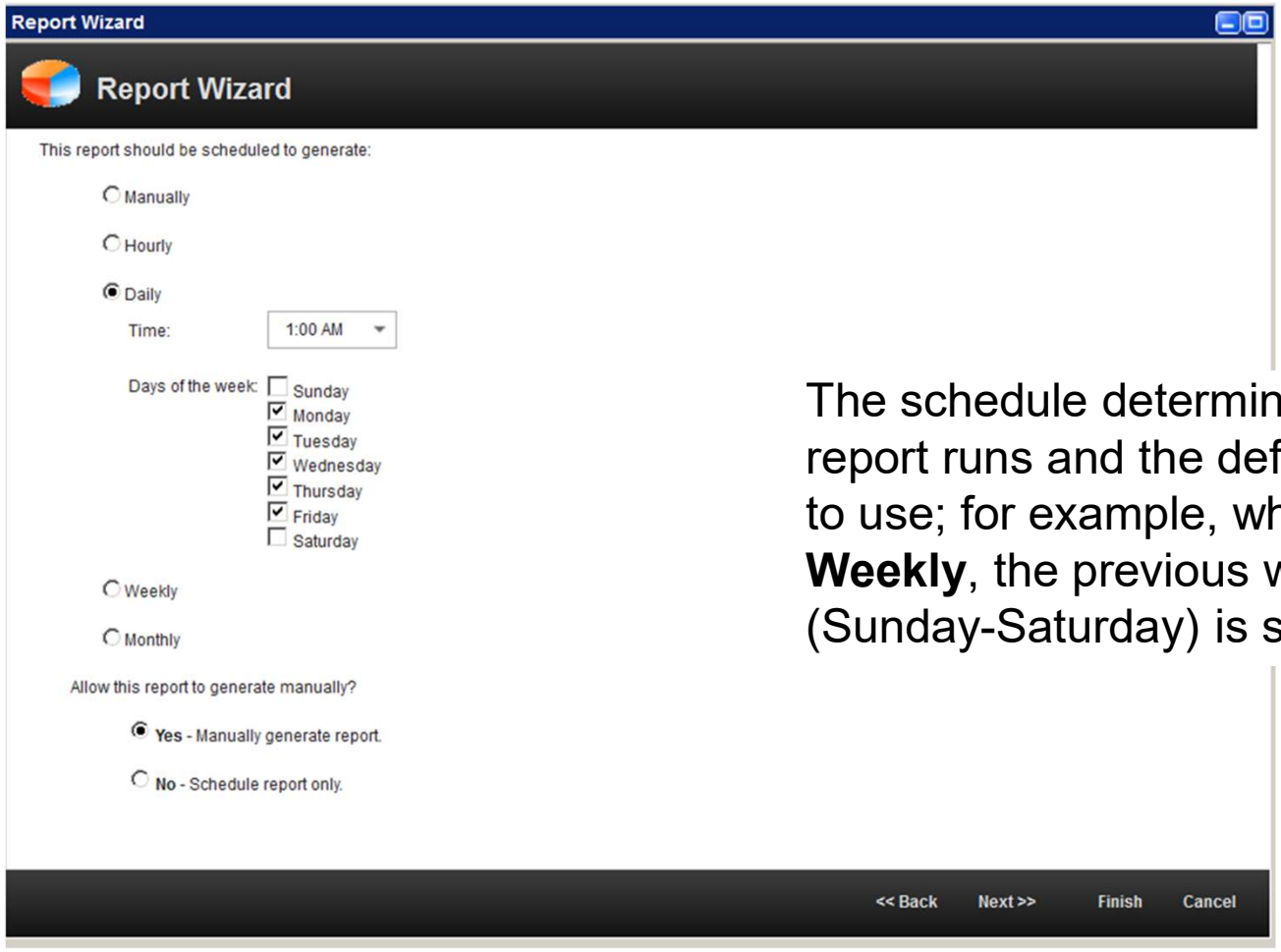
Log Source	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
CheckPoint @ FW-1Machine	Multiple (13,157)	Multiple (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



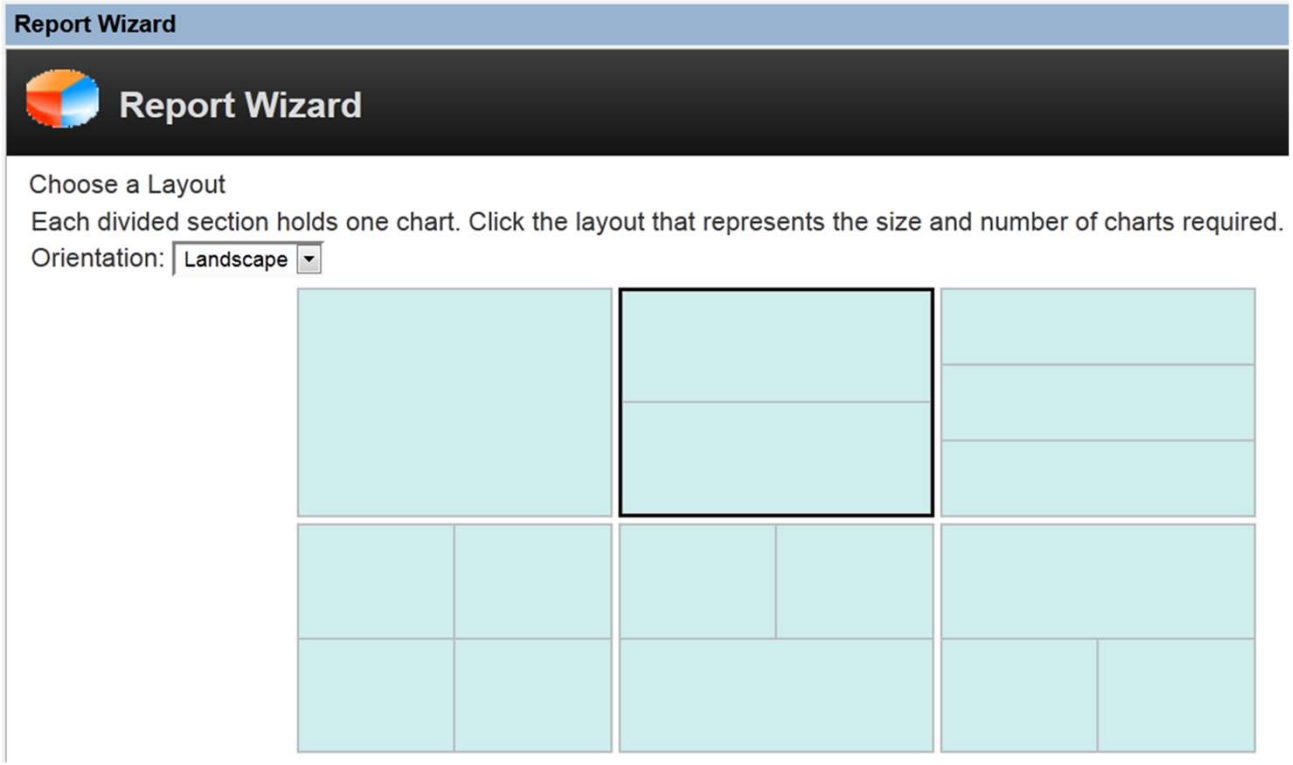
Choosing a schedule



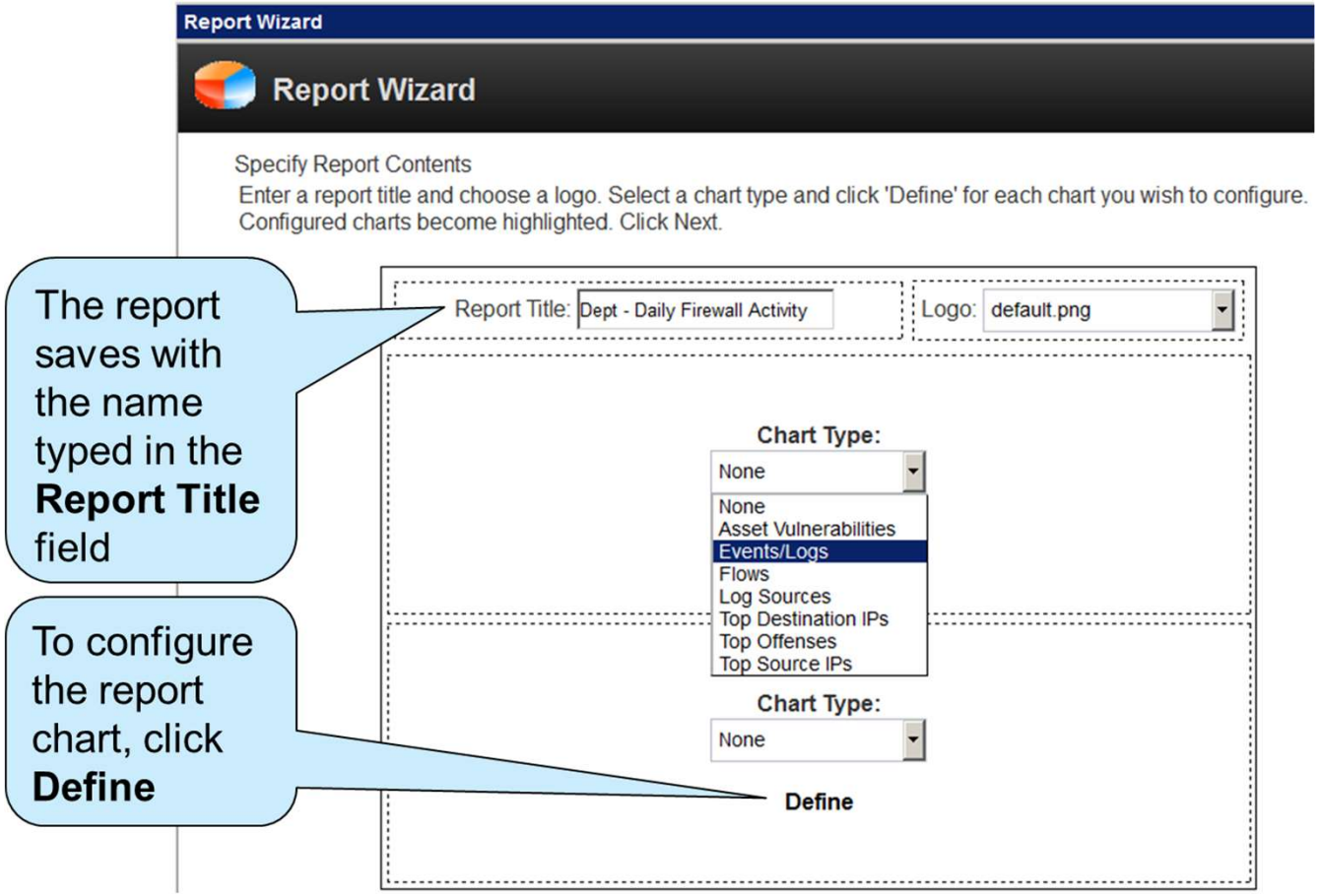
The schedule determines when the report runs and the default data range to use; for example, when you select **Weekly**, the previous week's data (Sunday-Saturday) is selected

Choosing a layout

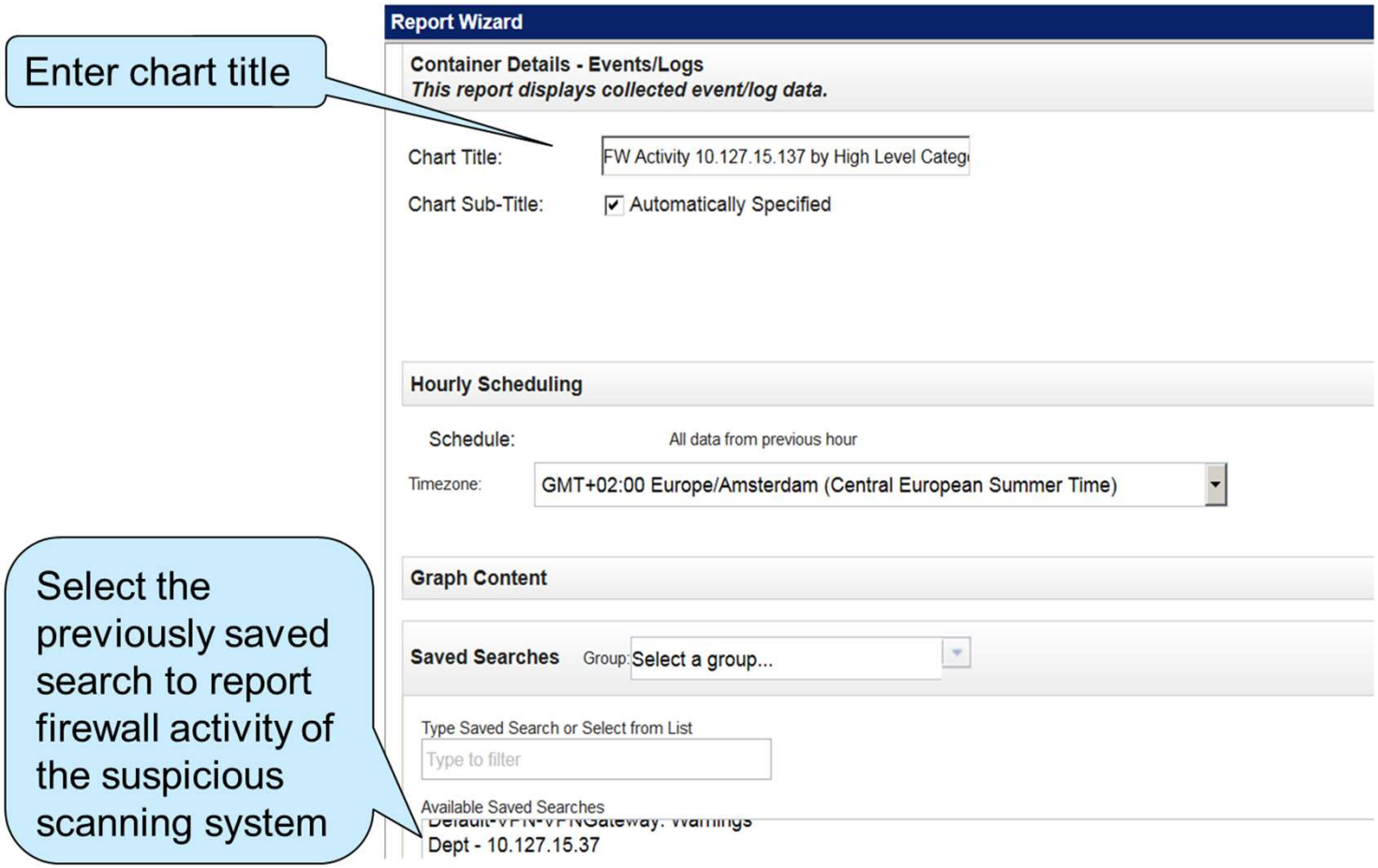
- QRadar SIEM uses containers to segregate report pages so that different data sets can show on the same report page



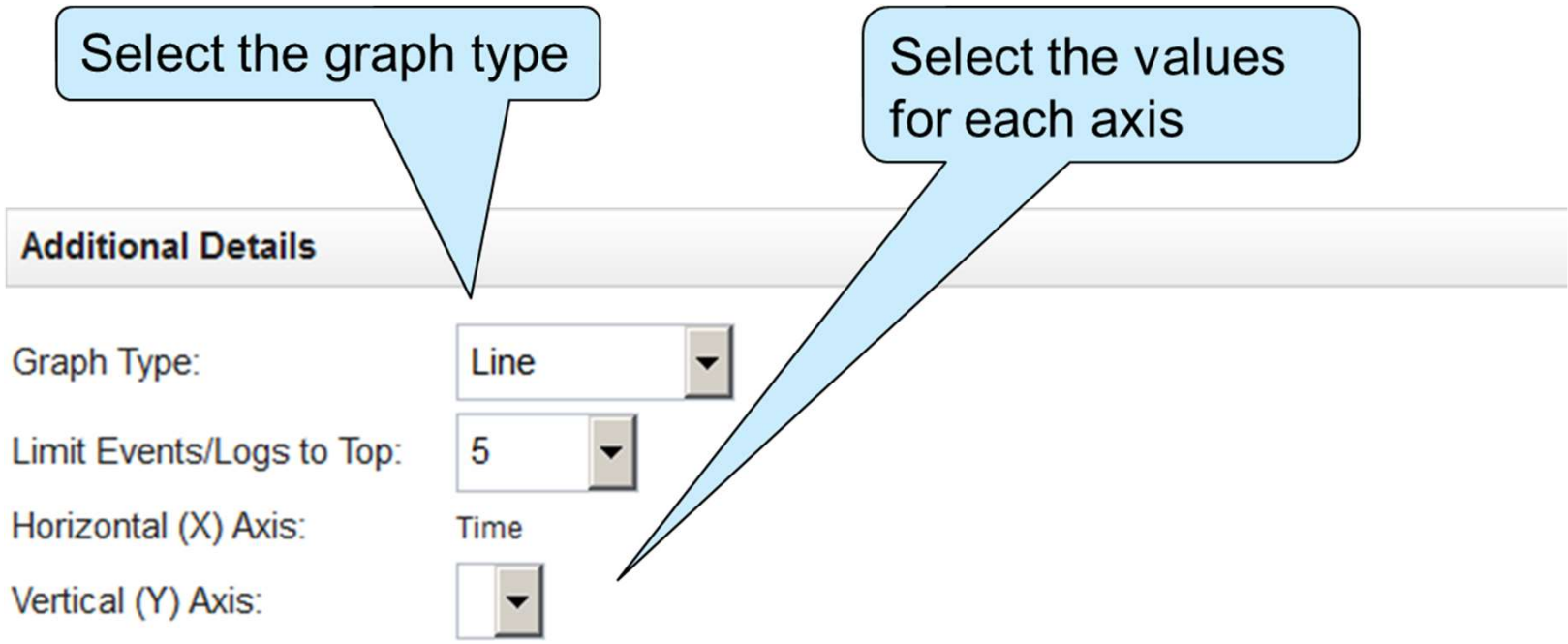
Defining report contents



Configuring the upper chart



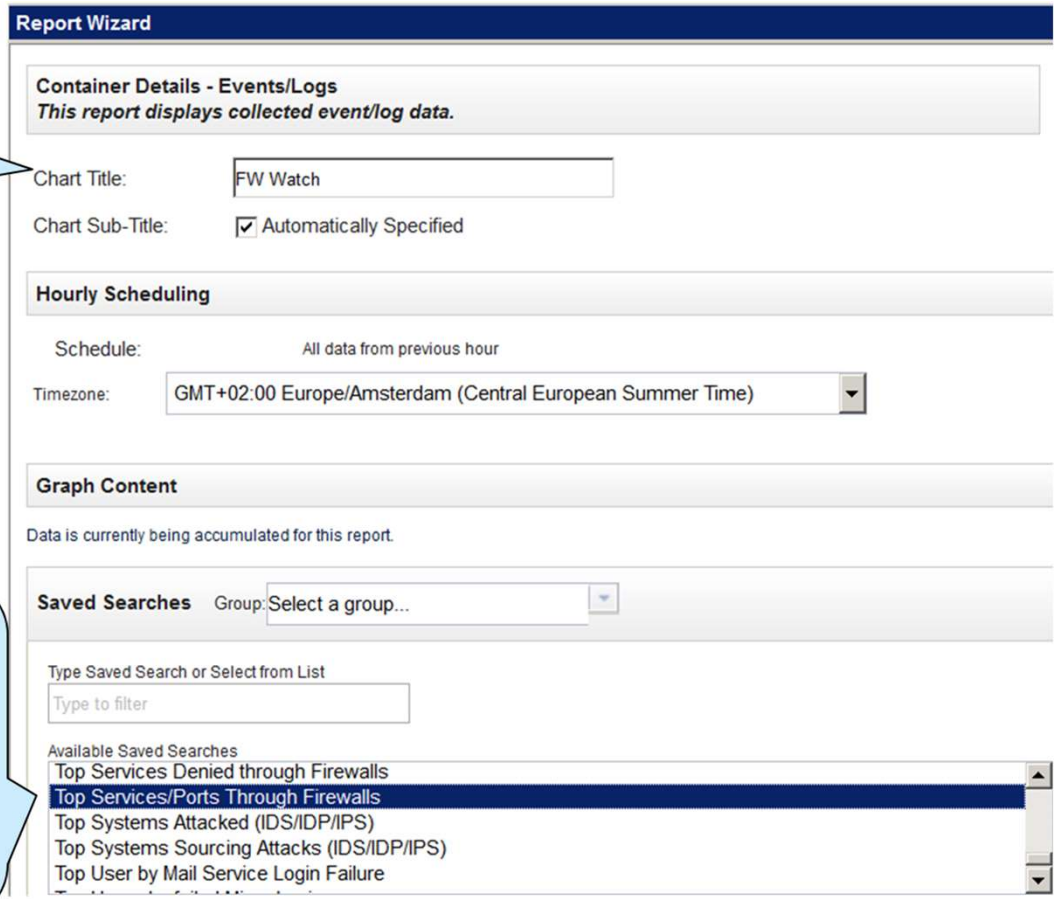
Configuring the upper chart (continued)



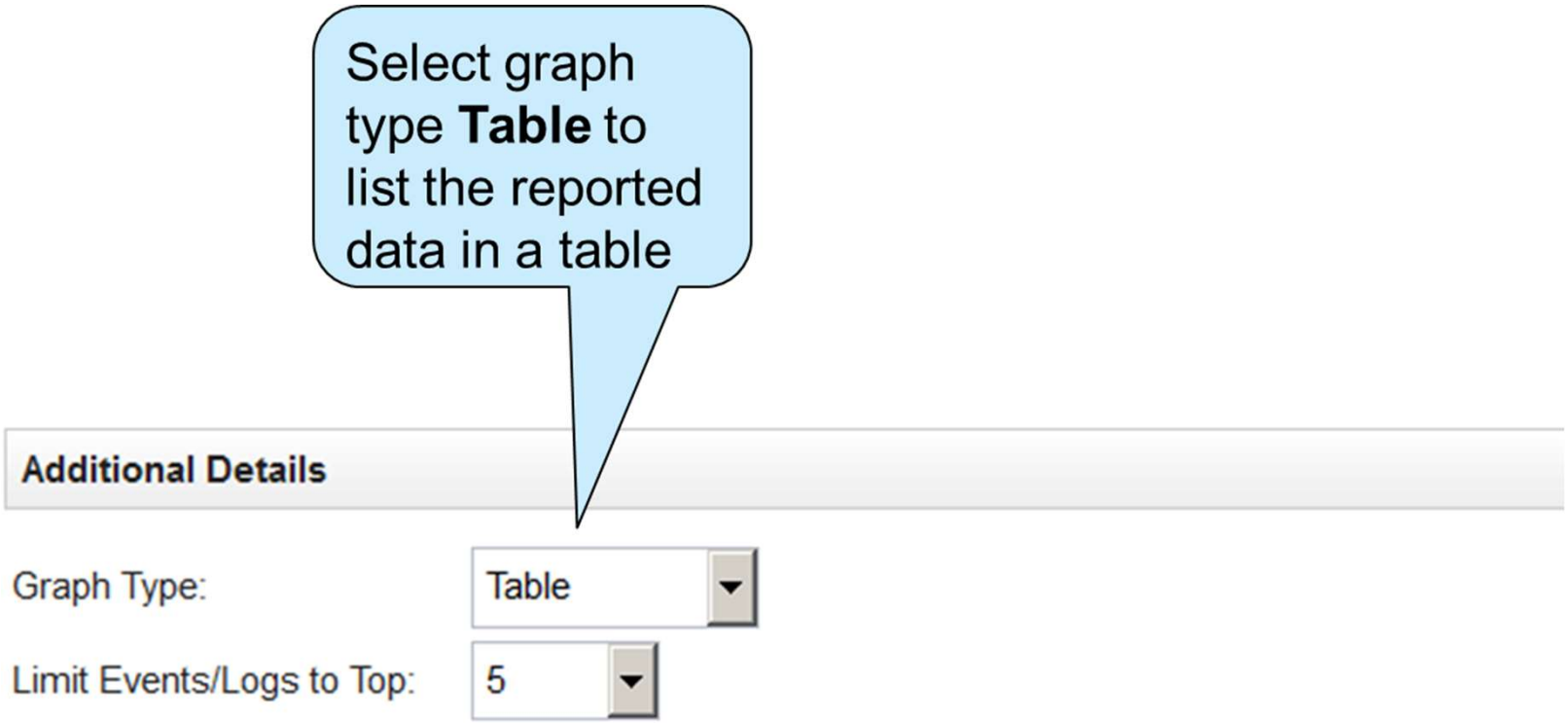
Configuring the lower chart

Define a chart for firewall activity

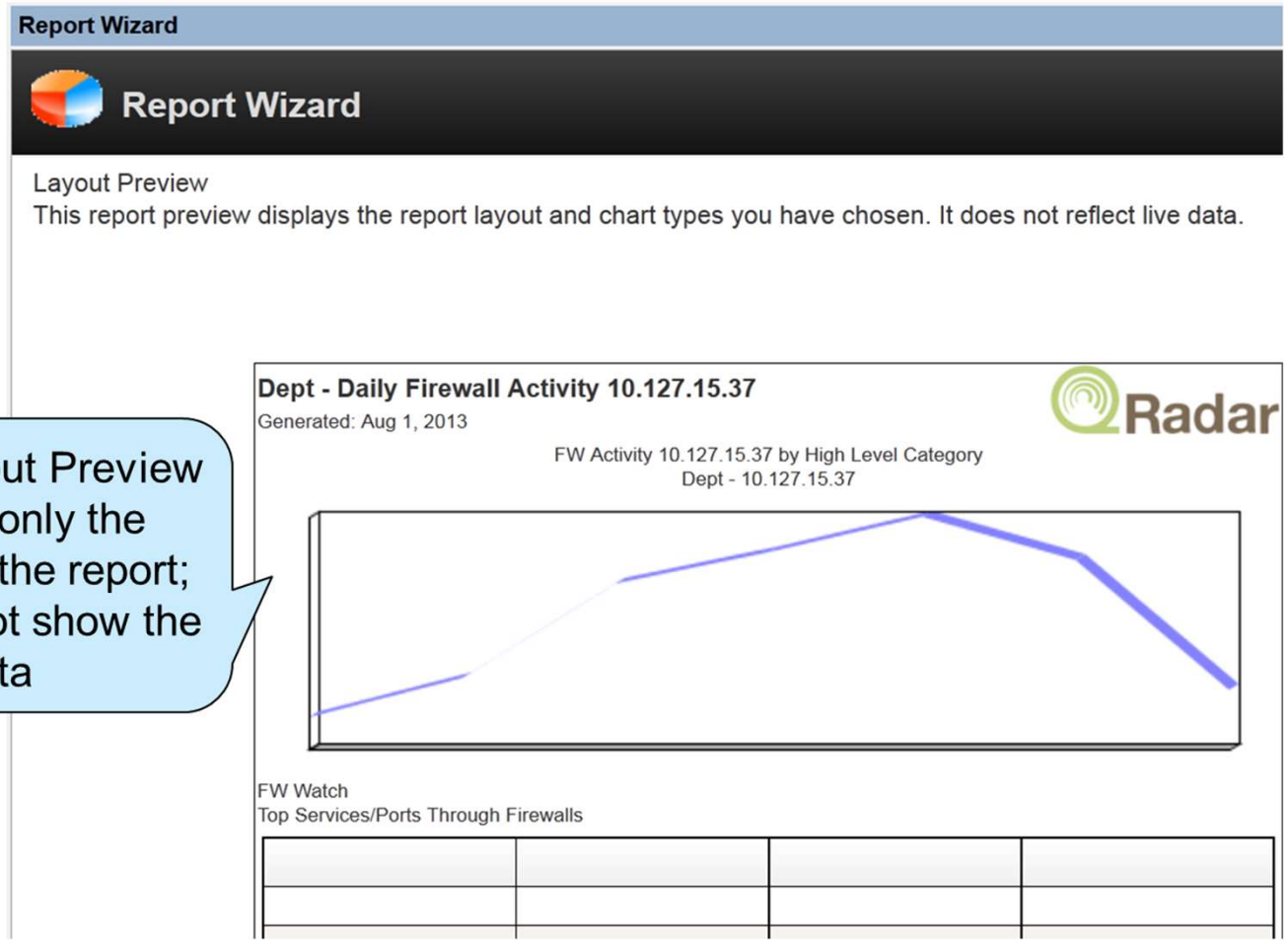
Select a predefined search to report the top services and port numbers of traffic through firewalls



Configuring the lower chart (continued)



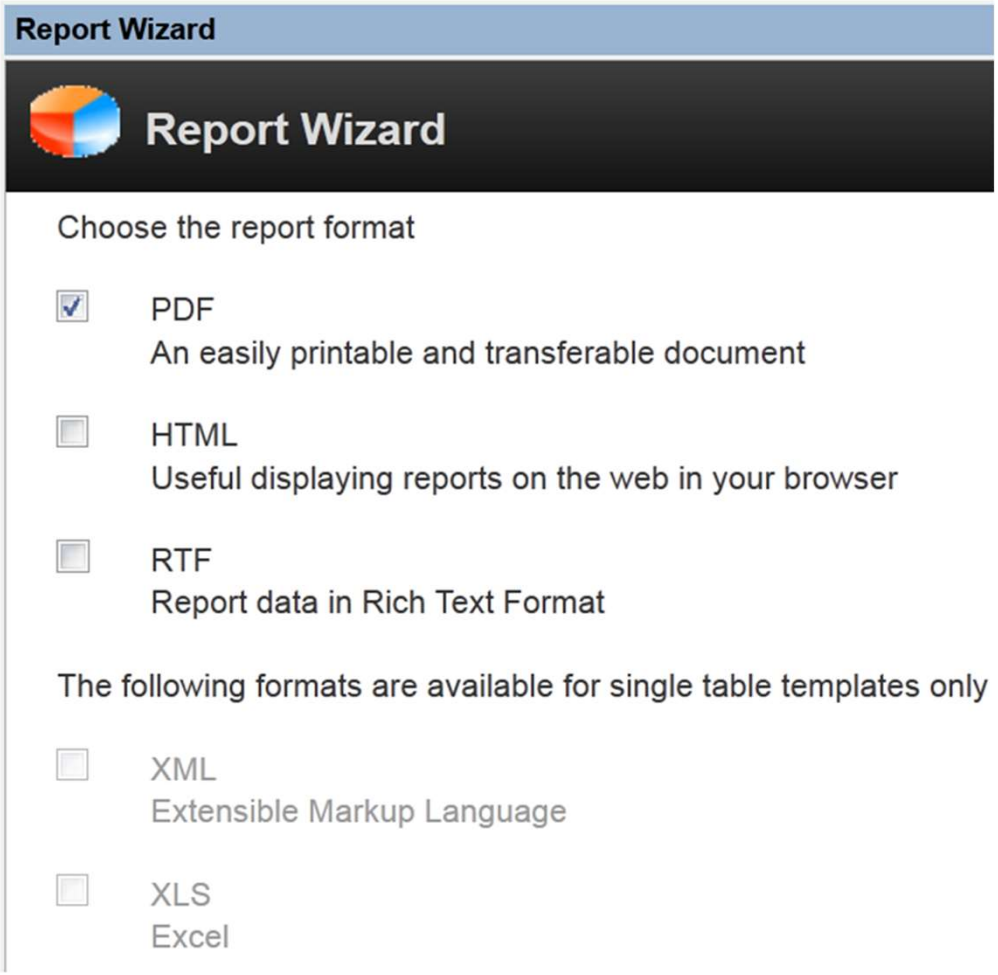
Verifying the layout preview



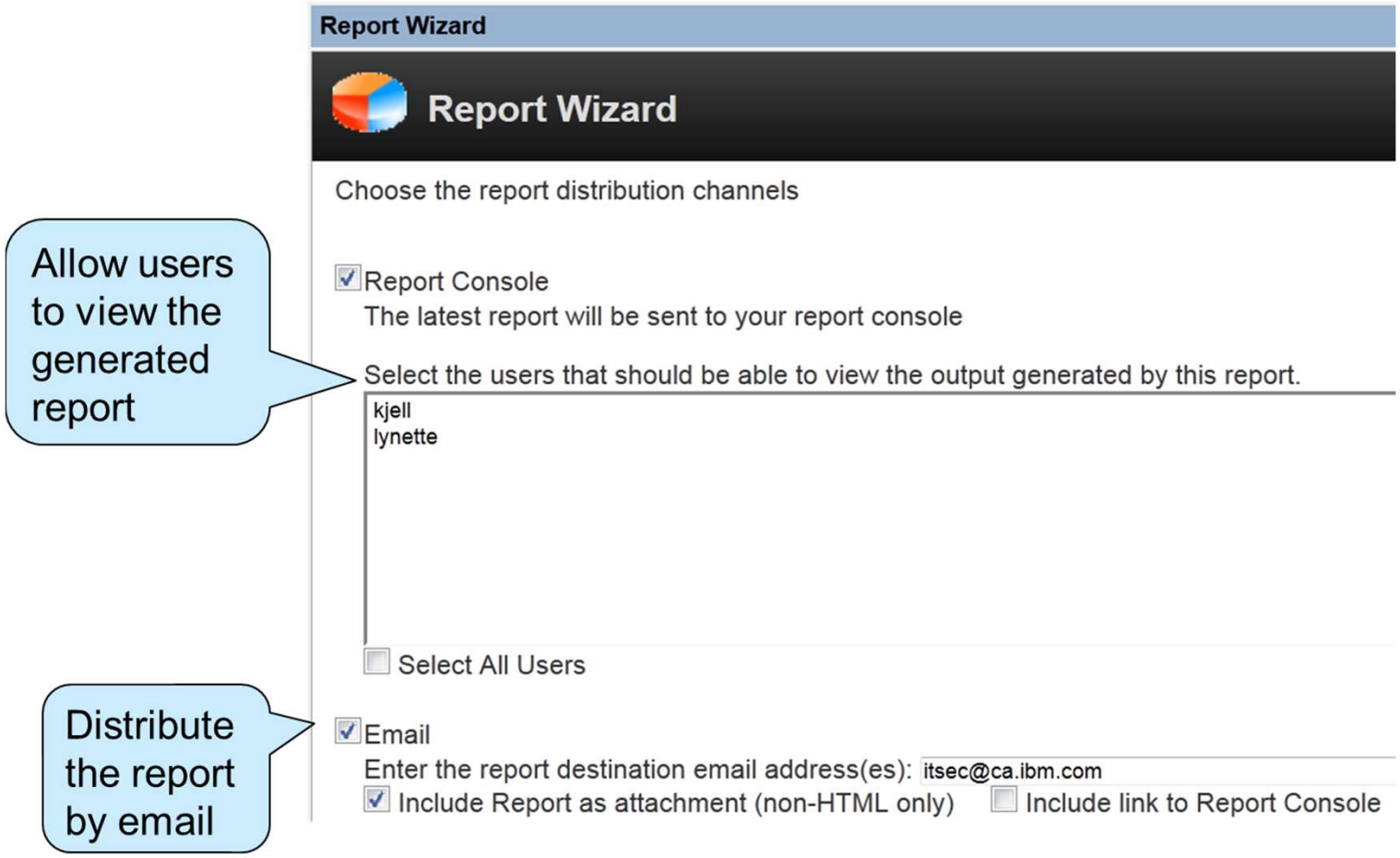
The Layout Preview provides only the layout of the report; it does not show the actual data

Choosing a format

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

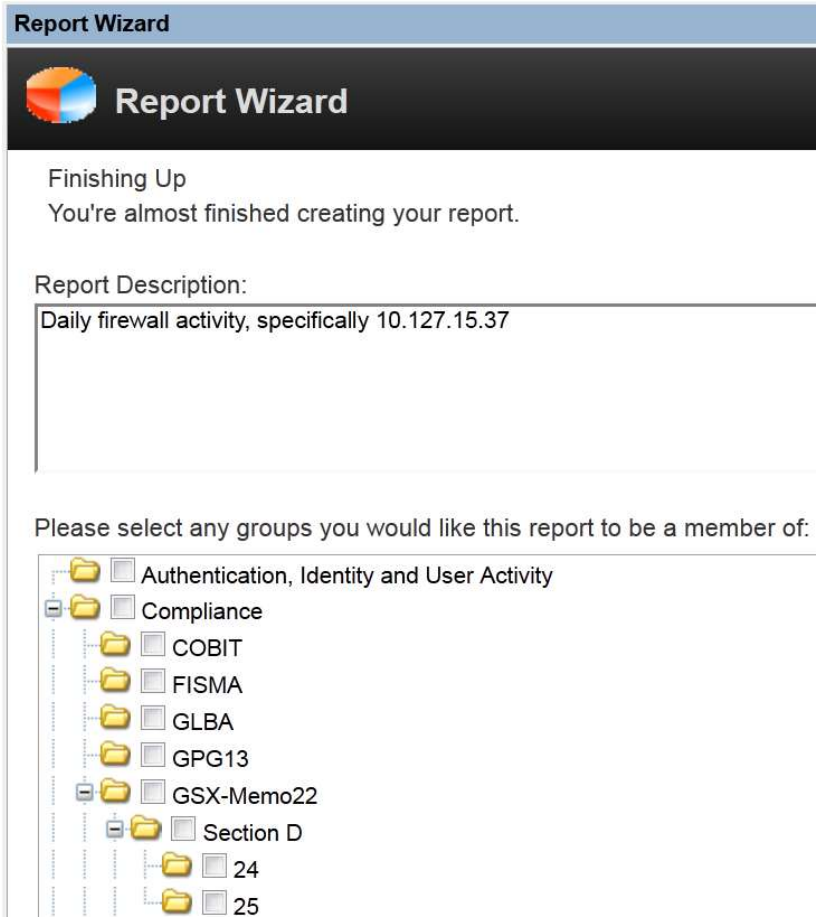


Distributing the report

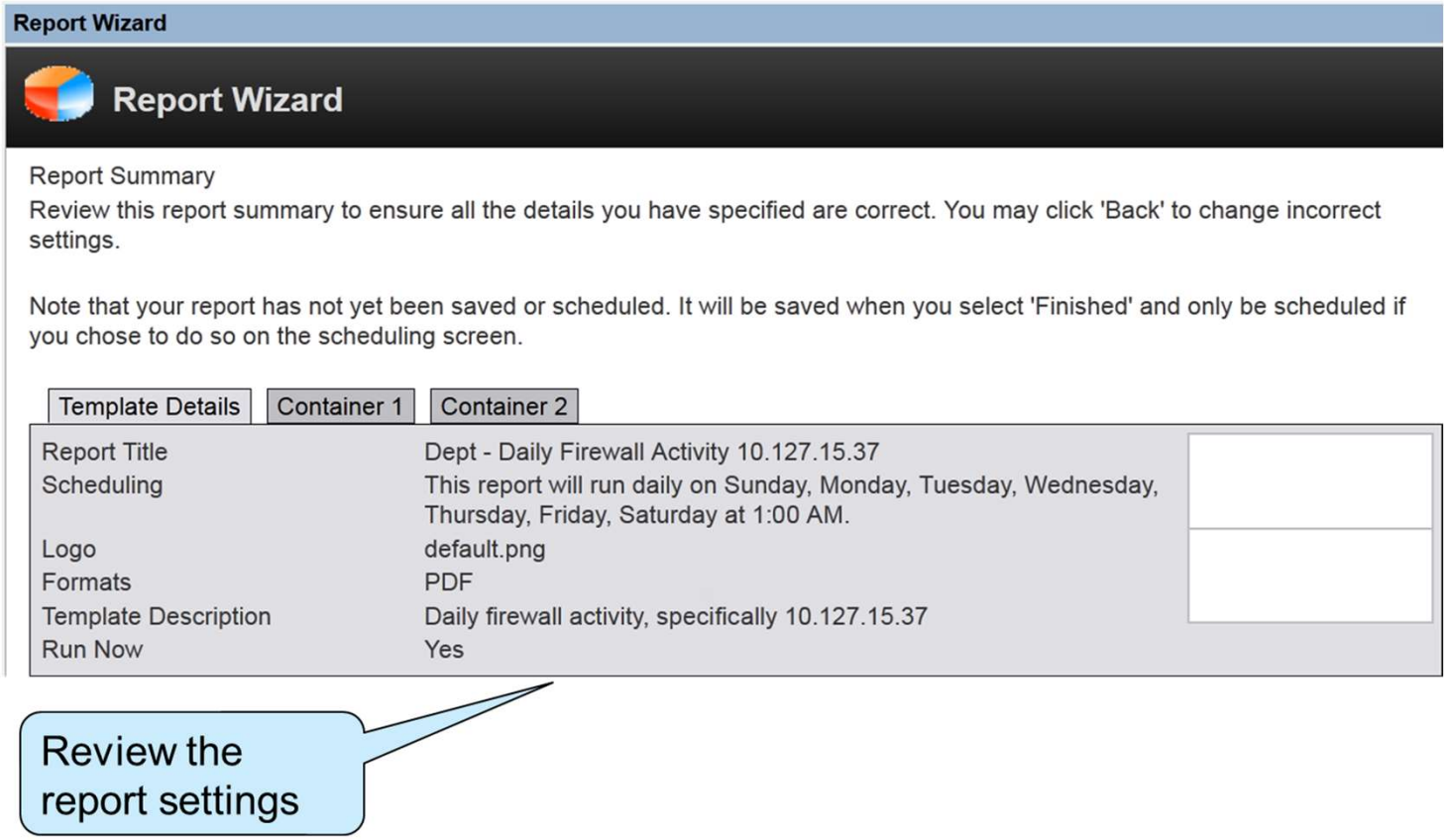


Adding a description and assigning the group

- 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



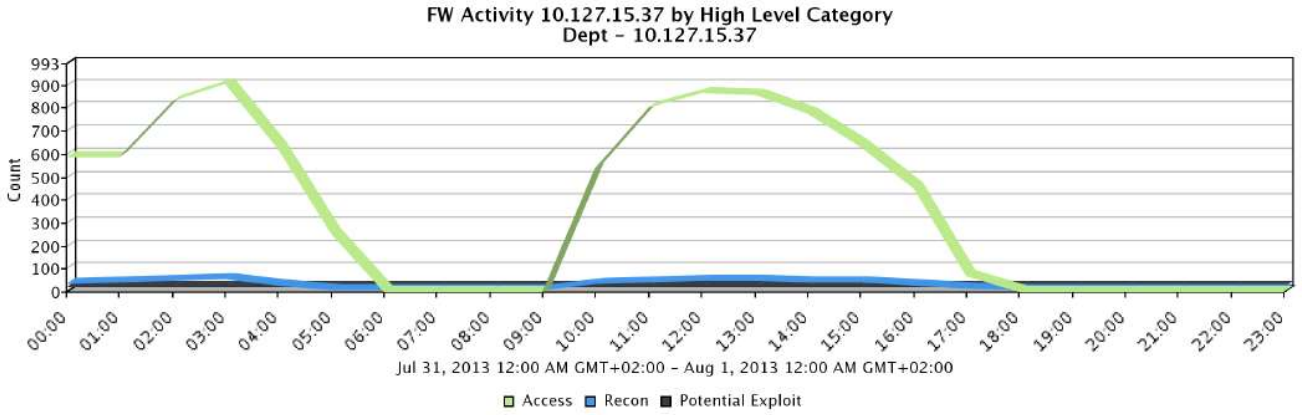
Verifying the report summary



Viewing the generated report

Dept - Daily Firewall Activity 10.127.15.37

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



FW 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 acces 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

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

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.

IBM