IBM Security

Section 2: Qradar Data Sources

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

What to watch for?

- Lots of content – don’t drown in it.
- Look for the “Learning Point Star”

IBM Security

QRadar Event Data Sources

Agenda

- In this presentation you will learn the following:
  - How QRadar SIEM Collects Event Data
  - What are the key components to perform event collection from Third Party Devices
    - Log Sources
    - DSMs
    - Log Source Protocols
  - Integrating Windows Log Sources With QRadar (Agent based and Agentless)

IBM Security

How QRadar SIEM Collects Event Data

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

Event data pipeline

Event data is sent to or pulled by QRadar

Event Collector – Responsible for parsing and normalizing incoming Events

Protocols – Reads or pulls raw data from network devices (e.g: Windows Servers, Firewalls, etc)

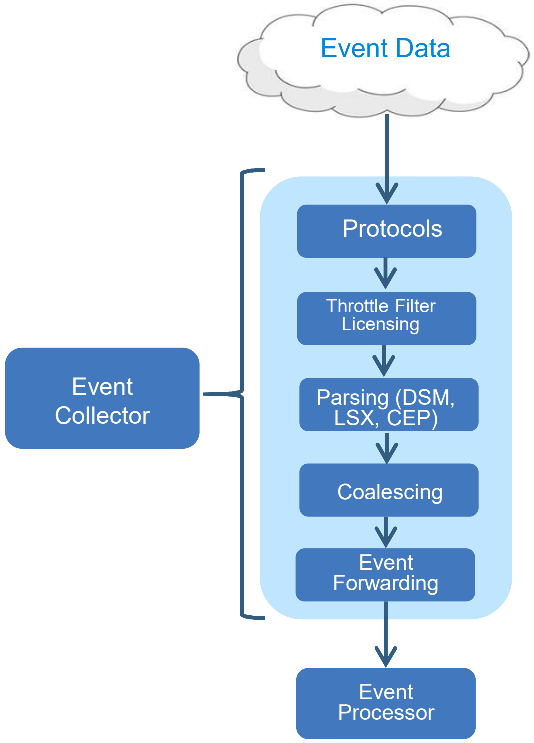
Throttle Filter - Licensing - On a second-by-second basis, slows down the incoming rate so it does not exceed the license on the appliance.

Parsing – DSMs / LSX / CEP – take the raw data and normalize it into a common structure.

Coalescing - "Event Compression". Find nearly identical events and delete one and increase the event count on the record. Key is: source IP, dest IP, dest port, QID, username

Forwarding - Applies routing rules for the system, such as sending event data to offsite targets, external Syslog systems, JSON systems, and other SIEMs.

Events are then sent to the **Event Processor** component and pass through the Custom Rules Engine (CRE). They are tested and correlated against the rules that are configured



Events not counted against the EPS licenses

- 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 Correlation and Processing

After Events are normalized they are then sent to the Event Processor for processing

Licensing is applied again on ingress to the EP

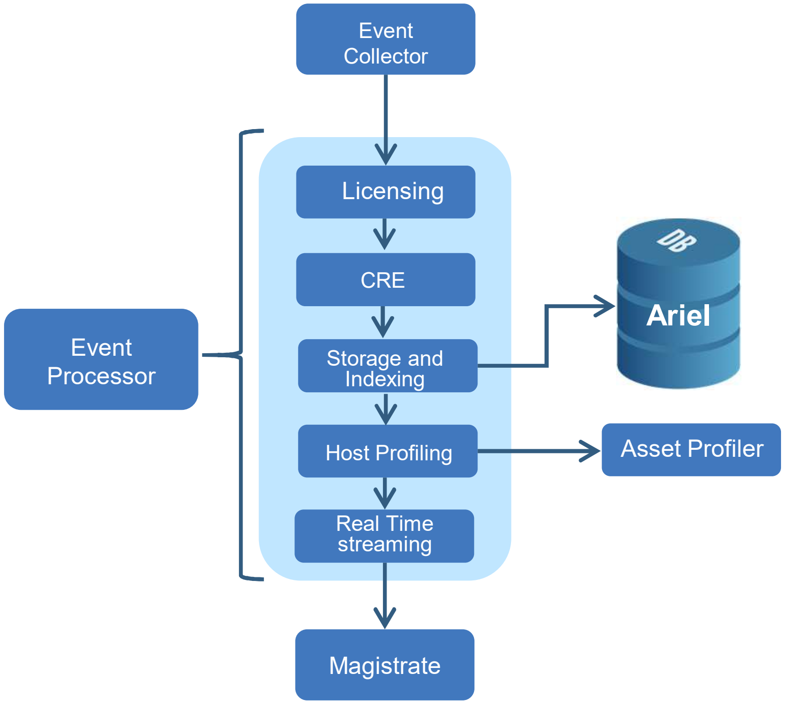
The **CRE or Custom Rules Engine** Applies the correlation rules that were created in the UI.

Event data is then sent to the **Ariel Database** for storage.

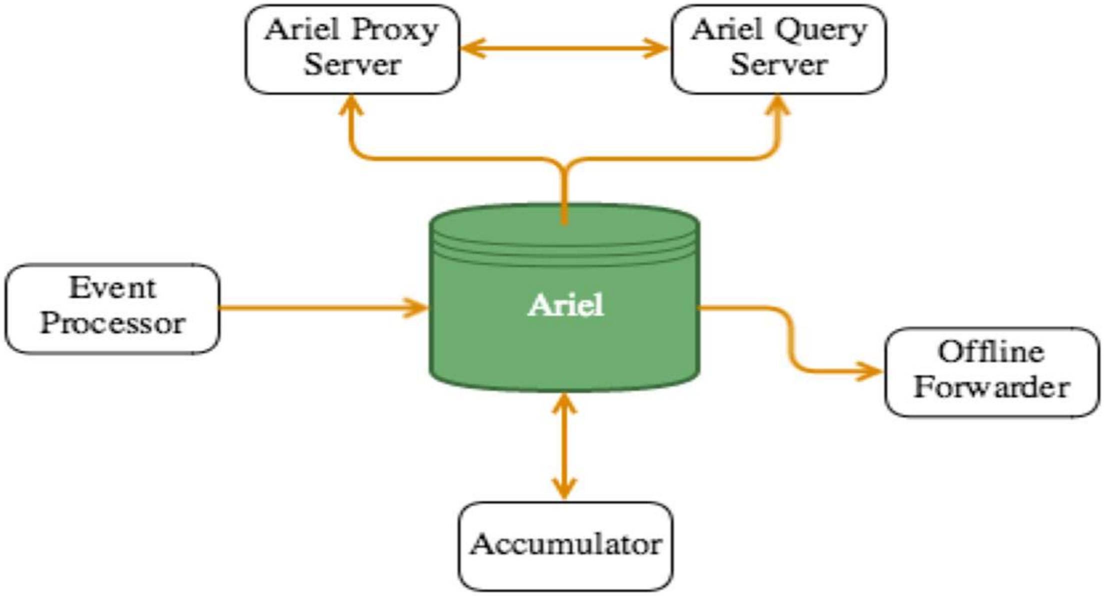
Host Profiling – Also called passive profiling or passive scanning. Watches event data from systems that contain Identity properties (e.g: Identity Username, Identity IP, Identity Mac, etc) on the network in order to make educated guesses about which Ips/assets exist and what ports are open.

Streaming – Responsible for the “real time (streaming)” view in User Interface

If an event matches a rule, the Magistrate component generates the response that is configure in the custom rule



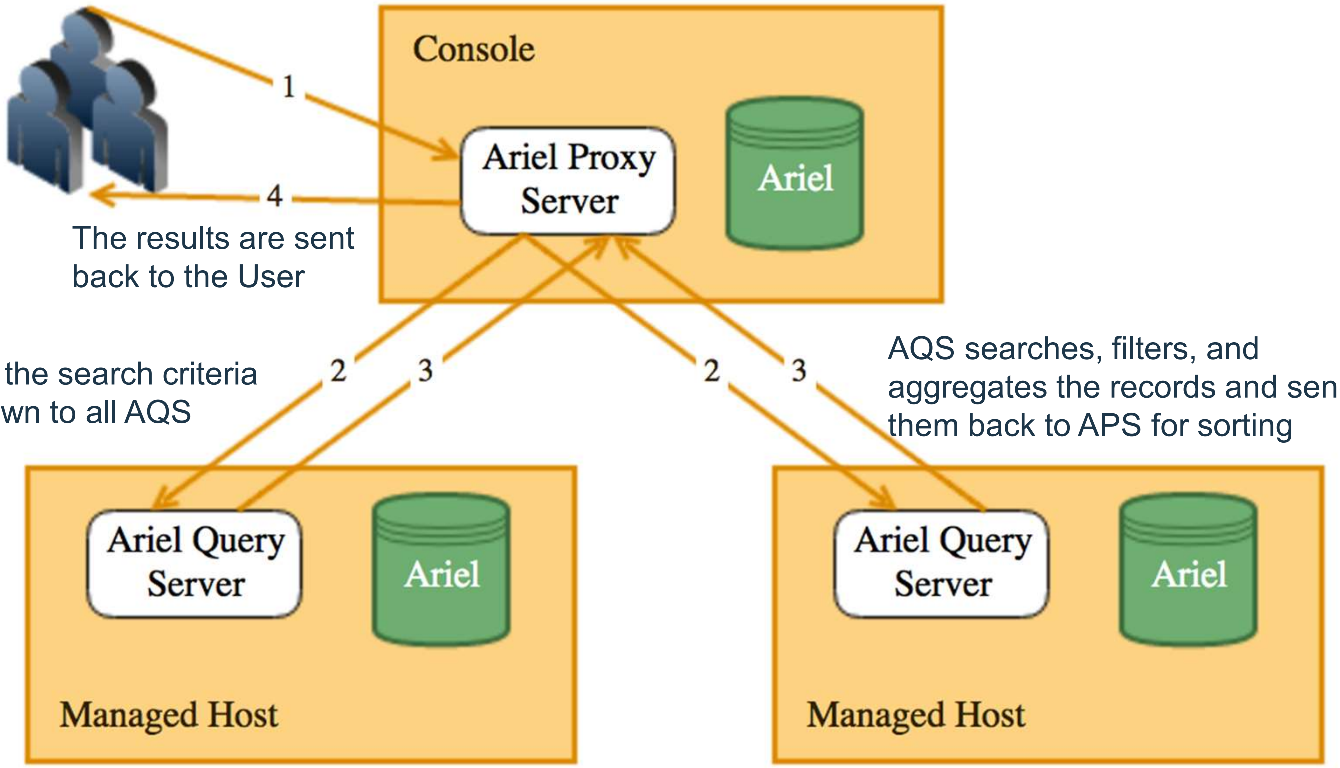
Ariel Components



Ariel Search Flow

User clicks on the “search” button in the Qradar UI

Tomcat sends the search criteria to the Ariel proxy server.

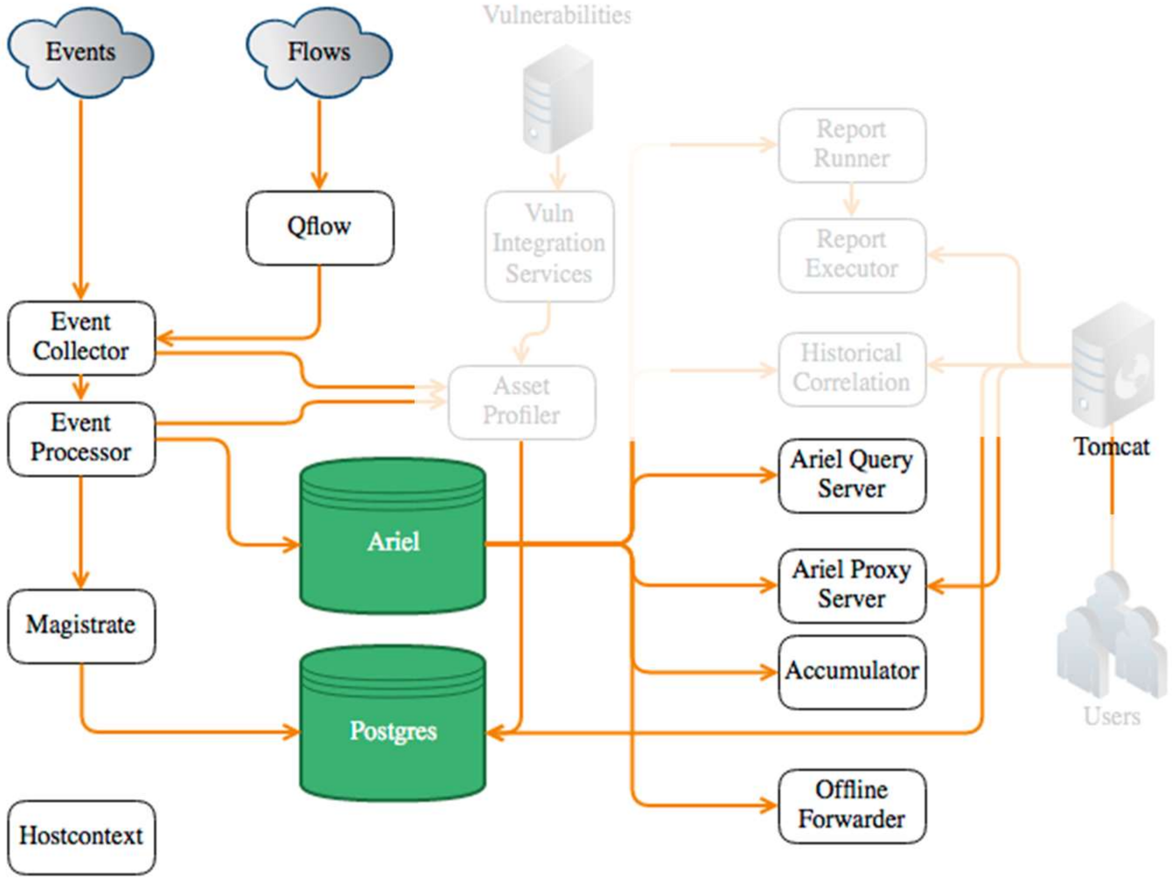


The results are sent back to the User

The APS takes the search criteria and sends it down to all AQS instances

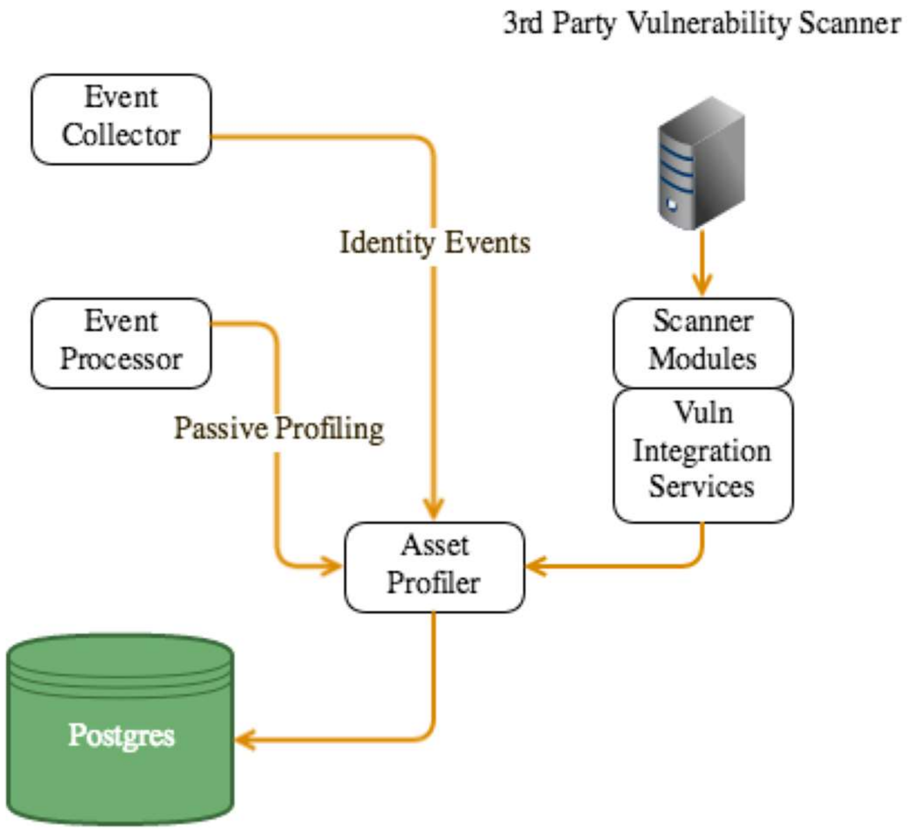
AQS searches, filters, and aggregates the records and sends them back to APS for sorting

Where we are

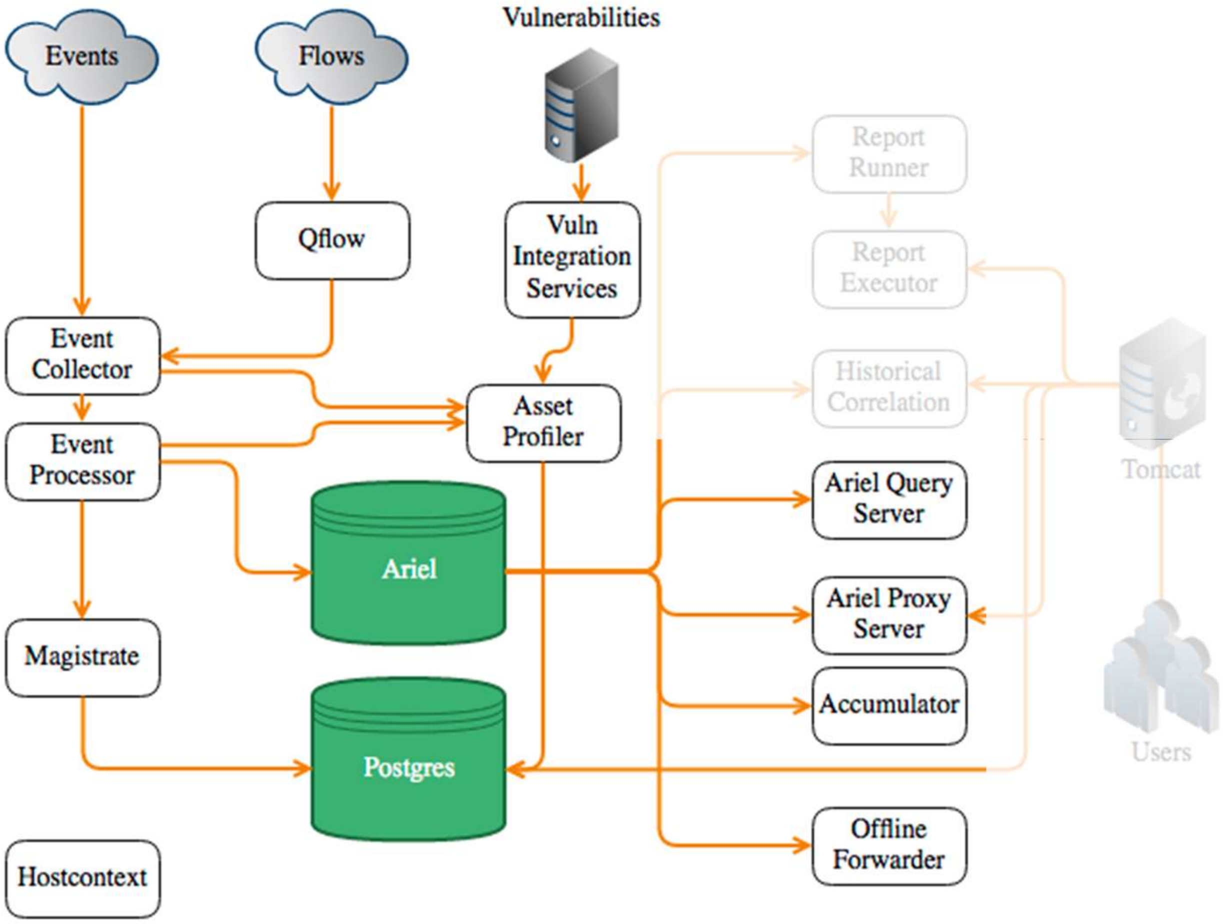


Events
Flows
Vulnerabilities
Qflow
Vuln Integration Services
Report Runner
Report Executor
Event Collector
Event Processor
Asset Profiler
Historical Correlation
Tomcat
Ariel Query Server
Ariel
Ariel Proxy Server
Magistrate
Accumulator
Users
Postgres
Offline Forwarder
Hostcontext

Asset and Vulnerability Flow



Where we are


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

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

Event Collection from Third Party Devices

Event collection from third-party devices

- To configure event collection from third-party devices, you need to complete configuration tasks on the third-party device, and your QRadar Console, Event Collector, or Event Processor.
- The key components that work together to collect events from third-party devices are :
  - Log sources
  - DSMs
  - Automatic Updates (Contains DSMs, Protocol and VIS updates)
  - Log Source Protocols

Log Sources

- A *log source* is any external device, system, or cloud service that is configured to either send events to your IBM Security QRadar system or be collected by your QRadar system.

- QRadar shows events from log sources in the **Log Activity** tab.

- To receive raw events from log sources, QRadar supports several protocols, including syslog from OS, applications, firewalls, IPS/IDS, SNMP, SOAP, JDBC for data from database tables and views.

- QRadar also supports proprietary vendor-specific protocols such as OPSEC/LEA from Checkpoint.

Device Support Module (DSM)

- A *Device Support Module (DSM)* is a jar file (compiled code) that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as output.

- Each type of log source has a corresponding DSM.

- For example, the IBM Fiberlink MaaS360 DSM parses and normalizes events from an IBM Fiberlink MaaS360 log source.

Automatic Updates

- QRadar provides daily and weekly automatic updates on a recurring schedule.
- The weekly automatic update includes new DSM releases, corrections to parsing issues, and protocol updates.
- For more information about automatic updates, see the *IBM Security QRadar Administration Guide*.

Auto Update

QRadar Log Source Protocols

Protocol configuration overview

- Log source protocols provide QRadar the ability to receive or actively collect log source events from external sources.
- Passive protocols actively listen for events on specific ports
- Active protocols leverage APIs or other communication methods to reach out to external systems to poll and retrieve events.
- Before you configure a log source, you must review and understand how the device, appliance, or software sends events to QRadar
- QRadar support multiple Log Source protocols such as:
  - Syslog and TLS Syslog, JDBC (Java Database Connectivity), SNMP, Log File Protocol, UDP and TCP Multiline Syslog, OPSEC/LEA, Microsoft (multiple protocols)

Protocol configuration overview

- Syslog Protocol
  - The Syslog protocol is the most common form of event collection.
  - QRadar can passively listen for Syslog events on TCP or UDP port 514
- TLS Syslog Protocol

  - TLS Syslog protocol enables log sources to receive encrypted syslog events from up to 50 network devices that support TLS Syslog event forwarding.
- JDBC Protocol
  - Log sources configured with the Java Database Connectivity (JDBC) protocol can remotely poll databases for events.
- SNMP Protocol
  - SNMP protocol provides log source the ability to receive SNMP Events.
  - QRadar supports SNMPv1, SNMPv2, SNMPv3

Protocol configuration overview

- Log File Protocol
  - The log file protocol retrieves event files that are stored from hosts to process events stored in remote locations.
  - The log file protocol is intended for systems that write daily event logs.
  - It is not appropriate to use the log file protocol for devices that appended information to their event files.
  - Log files are retrieved one at a time to be processed.
  - The log file protocol can manage plain text, compressed files, or file archives.
  - Archives must contain plain-text files that can be processed one line at a time.
  - When the log file protocol downloads an event file, the information received in the file updates the **Log Activity** tab.

Protocol configuration overview

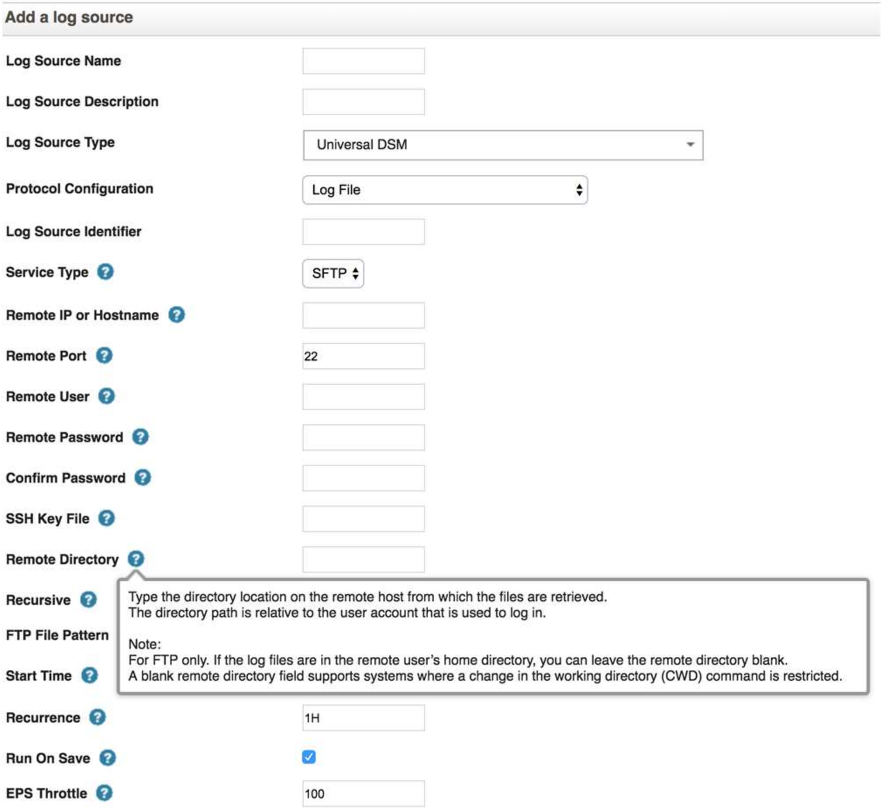
- UDP multiline syslog protocol
  - The UDP multiline protocol enables administrators to add a log source that creates a single-line syslog event from a multiline event.
  - The original event must contain a value that repeats that a regular expression can use identify and reassemble the multiline event.
- TCP multiline syslog protocol
  - Similar to the UDP multiline syslog protocol, The TCP multiline protocol enables administrators to add a log source that creates a single-line syslog event from a multiline event.
  - TCP multiline syslog protocol uses regular expressions to identify the start and end pattern of multiline events to create a single-line event.

Protocol configuration overview

- OPSEC/LEA protocol
  - The OPSEC/LEA protocol is a protocol that continuously polls for event data on 18184.
  - Typically used when configuring Checkpoint Firewalls.
- Microsoft (multiple protocols)
  - Microsoft Protocols will be covered in the section – “Integrating Windows Log Sources With QRadar”.

Protocols – UI Tooltips for Protocol Configurations

- QRadar 7.2.8 patch 8 and 7.3.0 patch 3 have support for UI Tooltips when configuring Protocols
- Initial content was pushed out via Weekly Autoupdate.
- Future updates will be included with Protocol RPMs
- Tooltip text matches what is in the QRadar documentation for that Protocol



Add a log source

Log Source Name	
Log Source Description	
Log Source Type	Universal DSM
Protocol Configuration	Log File
Log Source Identifier	
Service Type	SFTP
Remote IP or Hostname	
Remote Port	22
Remote User	
Remote Password	
Confirm Password	
SSH Key File	
Remote Directory	
Recursive	
FTP File Pattern	
Start Time	
Recurrence	1H
Run On Save	☑
EPS Throttle	100

Type the directory location on the remote host from which the files are retrieved.
The directory path is relative to the user account that is used to log in.

Note:
For FTP only. If the log files are in the remote user's home directory, you can leave the remote directory blank.
A blank remote directory field supports systems where a change in the working directory (CWD) command is restricted.

QRadar Data Protocols Challenges – Setup/Testing

Protocol Challenges – Forwarded/Funneled Syslog

- Syslog is one of the most commonly-used mechanisms for getting event data into the system.
- It’s usually easy to configure.
- However, if one aggregator or forwarder device is sending all syslog feeds from a set of original logging devices then you may end all events routed into a single log source.
- Caused if the events do not contain an RFC 3164 or 5424 compliant syslog header.
- Can be resolved using the Syslog Redirect protocol.
- Syslog Redirect (and now, the TCP Multiline, UDP Multiline, and soon TLS Syslog protocols) allow the user to define their own regular expression for capturing a value from the event payload to use as the sourceName.
- This lets you ‘break up’ a single event stream into separate feeds that QRadar can route to different log sources.

Protocol Challenges – Multiline Syslog

- Handling multiline events is often a challenge.
- QRadar offers some solutions for multiline syslog recombination.
- Some multiline logs involve a common field or tag that is present in each line of the multiline, and those lines need to be grouped based on that common value.
- Can be resolved using
  - The UDP Multiline Syslog
  - The TCP Multiline Syslog
- UDP Multiline Syslog (and soon, the TCP Multiline and TLS Syslog protocols) allow the user to define a regular expression for capturing a value from the event payload to use as the pivot point for determining which aggregate event an incoming message should be associated with.

Protocol Challenges – Multiline Syslog – Events with distinct beginnings and/or endings

- Some multiline logs have no common field or tag, but their structure/format is such that QRadar can tell, within a given stream of event data, where one event begins and another ends.
  - It can use the either an ‘Event Start Pattern’ regular expression, an ‘Event End Pattern’ regular expression, or both.
- Can use TCPMultilineSyslog (and soon, the TLSSyslog protocol) allow the user to define one or two regular expressions for defining how to extract multiline events out of a stream of multiline event data.
- **Example:**
- **Event Start Pattern** = (?:<(\d+)>\s?(\w{3} \d{2} \d{2}:\d{2}:\d{2}) (\S+))?(\d{2}/\d{2}/\d{4} \d{2}:\d{2}:\d{2} [AP]M)

Protocol Challenges – JDBC Setup/Testing

- JDBC is one of QRadar's more flexible protocol sources.
- JDBC, like the syslog-oriented protocols, is a 'generic' protocol.
- As a result, it's configuration can be confusing, since there are so many options:
  - **Log Source Identifier:** Traditionally this had to be <database name>@<IP or hostname>
    - The values had to match the IP or Hostname/Database Name below.
    - To accommodate cases where we have multiple JDBC log sources communicating with the same database, the table name can now be included also.
    - to ensure uniqueness in this value use the format <tablename>|<database name>@<IP or hostname>
  - **Database Type:** choose from MSDE, Postgres, Oracle, Sybase, DB2, Informix

Protocol Challenges – JDBC Setup/Testing

- **IP or Hostname:** The IP or hostname that the target database resides on
- **Port:** Port on database system to connect to.
  - Will be ignored if database type is MSDE and Database Instance is provided
- **Username:** the account to be used to log in to the database.
  - Generally this would be a database account, but for the MSDE type, you can use Windows authentication, and must use Windows credentials if Named Pipe communication is enabled.

– **Password/Confirm Password:** Password used to authenticate to the Database

– **Authentication Domain:** valid only for MSDE type, needed if using Windows authentication

Protocol Challenges – JDBC Setup/Testing

- **Database Instance:** valid only for MSDE and Informix database types.
  - If you wish to connect to a database instance other than the default instance, you have two options:
    - if you know which port the instance is listening on, and are using basic TCP/IP connection (NOT named pipe) you can supply it in the Port field and leave Instance blank.
    - If you don't know the port, or the port is dynamic, or you are using named pipe, you must supply the Instance name.
    - If you are using TCP/IP, the JDBC driver will automatically query the SQL Browser service (which listens on port 1434) to ask what port the named instance is running on.

Protocol Challenges – JDBC Setup/Testing

- **Predefined Query:** QRadar has some built-in queries for some device-specific specialized queries.
  - One can be selected here.
  - If anything but ‘none’ is selected, the Table Name, Select List and Compare Field configuration parameters will be hidden/suppressed.
- **Table Name:** available only if Predefined Query = none.
  - This is the name of the table or view to retrieve records from.
- **Database Locale:** available only for Informix type
- **Use Named Pipe Communication:** available only for MSDE type.
  - Use this to use Windows-based authentication to connect to a database.
  - Needed to hit an instance (aside from the default) if the instance listens on a dynamic port and the SQL Browser service is off or blocked.
  - Needed to interact with a database in a clustered environment

Protocol Challenges – JDBC Setup/Testing

- **Database Cluster Name:** Available only when Named Pipe is enabled.
  - Allows to connect to a clustered SQL Server instance.
- **Use NTLMv2:** available only for MSDE type.
  - On by default but might need to be turned off to work with some Windows configurations.
- **Use SSL:** available only for MDSE type (for now).
  - Allows for encrypted JDBC communication.
  - Requires that the database system be configured for encrypted connections.

Protocol Challenges – JDBC Setup/Testing

- JDBC is an ‘active’ protocol, which make outbound communication to retrieve event data from an external system.
- It has an on-disk ‘session tracking’ file for persisting information on the last event data seen, to avoid resets when ecs restarts.
- For JDBC, this tracking information is stored in simple name=value property files, which reside in /store/ec/jdbc/, with one file per JDBC log source.
- The files are named with the sensorprotocolconfig id value for the log source.
- This can be retrieved from the postgres database by using the following command:
  - **`psql –U qradar –c “select id from sensorprotocolconfig where configname =`** *‘<Log Source Name>’;”*
- This file can be used to identify when the JDBC protocol provider last polled the remote database, and also tells you what the comparable column is, and what the last observed value was.

Protocol Challenges – JDBC Setup/Testing

- You can force the JDBC protocol to re-read old data by tampering with this file – this is useful for testing or demonstration.
- Disable the log source, edit the file to reduce the ‘comparable’ to an older timestamp/counter/id/etc, then re-enable the log source.
- When the JDBC provider starts up, it will read from that file to determine where to start polling, and thus will look back in time and pull back the older data.
- JDBC also has some hidden configuration parameters.
- The postgres sensorprotocolconfigparameters table includes all the config parameters that can be seen in the protocol config section of the Log Sources UI.
- You can find all the parameters for a given log source with the query
  - ‘`select * from sensorprotocolconfigparameters where sensorprotocolconfigid = (select id from sensorprotocolconfig where configname = '`*<Log Source Name>*`');`’

Protocol Challenges – Log File Setup/Testing

- Log File is another ‘generic’ protocol, not intended for a specific product integration.
  - **Log Source Identifier:** Can be any value that applies to the log source. It needs to be unique among Log File log sources.
  - **Service Type:** choose from STFP, FTP, SCP.
  - **Remote IP or Hostname: T**he IP or hostname of system where files reside.
  - **Remote Port:** Port to connect to on remote system.
  - **Remote User:** the account to be used to log in to target.
  - **Remote User:** the account to be used to log in to target.
  - **Password/Confirm Password:** Password used to authenticate the Remote user.
  - **SSH Key File:** available only for SFTP and SCP.
  - **Remote Directory:** Directory on remote system where target files reside.

Protocol Challenges – Log File Setup/Testing

- **Recursive:** available only for SFTP and FTP service types.
  - If checked, the protocol will explore all subdirectories of the Remote Directory specified above, checking for files which match the specified pattern
- **FTP File Pattern:** available only for SFTP and FTP service types.
  - Uses a regular expression that will match any filenames that will be downloaded and processed in QRadar
- **FTP Transfer Mode:** available only for FTP. Choose BINARY or ASCII
- **SCP Remote File:** available only for SCP service type.
  - Must match the exact filename of file to download and process
- **Start Time:** Time of day offset to poll remote directory
- **Recurrence:** Interval for polling of remote directory

Protocol Challenges – Log File Setup/Testing

- **Run on Save:** Check if you want the protocol provider to run a poll on log source save.
- **EPS Throttle:** Event-per-second rate permitted
- **Processor:** Used if the files being downloaded are compressed and/or archived and thus need to be preprocessed for QRadar.
  - Default to NONE for plaintext files, or select from TAR, GZIP, ZIP, or TARGZ

- **Ignore Previously Processed File(s**): available only for SFTP and FTP service types.
  - Defines whether a given filename should only be read once, or should be re-downloaded and processed on every interval.
  - Should be checked in the case where filenames contain a timestamp or counter, meaning no file is ever written to more than once.
  - For cases where one filename is overwritten each day/hour/etc, this should be unchecked, and the Start Time and Recurrence values should be configured such that the Log File poll is timed to occur on the same schedule as file overwriting

Protocol Challenges – Log File Setup/Testing

- **Change Local Directory?**: Check to expose a text field for setting a different local directory to store the files in during processing (on the Qradar EC).
  - Each file will be written to disk as part of the download process, then read and converted to event payloads.
  - The file is cleaned up once reading is complete.
- **Event Generator:** A set of special processing options for handling some specific product integrations, and for some more general advanced configurations, like multiline events and exclusions.
- **File Encoding:** If the target files are not in UTF-8 encoding, provide their encoding here to ensure their contents can be converted to UTF-8 properly.
- **Folder Separator:** Character used by target filesystem for separation in file paths.

Protocol Challenges – Log File Setup/Testing

- Log File protocol, like JDBC, has an on-disk ‘session tracking’ file for persisting runtime information.
- For Log File, this tracking information is stored in sqlite databases, which reside in /store/ec/sqlite/, with one file per Log File log source.
- The files are named following the convention “sessiondata.db_<sensorprotocolconfig id>“
  - The id can be retrieved from the postgres database by using the following command:

    -
      ```
      psql -U qradar -c “select id from sensorprotocolconfig where configname = ‘<Log Source Name>’;”
      ```
- You can access the database using the sqlite3 command. Then look at the contents of the single table within by running ‘select * from remote_stream_source_session;’
- The most important parameter is likely the remoteFileList one, which shows the list of all files the protocol has run through – basically a skip list for the next poll.

Protocol Challenges – Log File Setup/Testing

- There are also parameter rows for the next day, hour and minute of the next poll time.
- Also parameters for keep place in a given file, in case ecs goes down unexpectedly midway through a file.
- As with JDBC, by disabling a log source, modifying the session tracking file, and re-enabling the log source, you can ‘hack’ it if you need to.

Protocol Challenges – AWS S3 RESTAPI Setup/Testing

- **Signature version**
  - AWS Signature Version 2 is the default – this can be used in some areas and uses HMAC-SHA1.
  - AWS Signature Version 4 is required in certain regions and can be used in ANY region – http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region - and is also required if your bucket is setup using the AWS Key Management Service.
- **Event format - Cloudtrail, W3C, LineByLine* (coming VERY soon)**
  - Cloudtrail (For use with AWS Cloudtrail only).
  - W3C (Currently supports .gz W3C files for Cisco CWS integration – near future plans for more flexibility).
  - LINEBYLINE – New processor being added to be able to take any “regular” file and put the data into the event pipeline a simple one line at a time.

Protocol Challenges – AWS S3 RESTAPI Setup/Testing

- **Logfile vs AWS S3 RESTAPI Protocol**
  - There is an AWS “Type” listed on Log File Protocol along with FTP, SFTP and SCP.
  - This was developed before the original AWS S3 RESTAPI Protocol and **should not be used as it does not support v4 signatures and is not actively maintained**.
  - t will be marked as deprecated soon but will still be available for current working setups.
- **Certificates**
  - Covered in the next slide regarding certificates for HTTPS protocols.
- **Session Track files**
  - Tracking files exist for the following:
    - /store/ec/amazonaws/ for Amazon AWS protocol
    - /store/ec/vcloud/ for Vmware vCloud protocol
    - /store/ec/ibmfiberlink/ for Fiberlink MaaS360 protocol

Protocols – HTTPS certificates

- The certificate for the URL relating to your connection must be downloaded into /opt/qradar/conf/trusted_certificates as outlined in the documentation.
  - You can convert the original certificate from various formats if you have it (PFX, PKCS12, etc).
  - Alternatively, you can export it from a browser sometimes directly in DER or sometimes an alternate format and then convert it.
  - The certificate must be in DER-encoded Binary or PEM format and have a file extension of .der, .crt, or .cert.
  - The easiest way to get the certificate in place is to use the “Automatically Acquire Server Certificate(s)” open which will take the certificates on the server now and mark them as trusted as they appear.
    - If there is ever a change you would want to verify the server identity first and then set this to “Yes” again to obtain the updated certificate.

Protocols – HTTPS certificates

- If your proxy re-writes the certificate or does anything else that may modify the SSL certificate that QRadar will receive, the Automatic option is the best choice as exporting from a browser may not present the same certificate QRadar will see using the proxy.

Third-party device installation process

Third-party device installation process

- To collect events from third-party device, you must complete installation and configuration steps on both the log source device and your QRadar system.
- For some third-party devices, extra configuration steps are needed, such as configuring a certificate to enable communication between that device and QRadar.
- The following steps represent a typical installation process:
  - Read the specific instructions for how to integrate your third-party device.
  - Download and install the RPM for your third-party device.
  - RPMs are available for download from the IBM support website (http://www.ibm.com/support).
    - **Tip:**If your QRadar system is configured to accept automatic updates, this step might not be required.
  - Configure the third-party device to send events to QRadar.

Third-party device installation process

- After some events are received, QRadar automatically detects some third-party devices and creates a log source configuration.
- The log source is listed on the Log Sources list and contains default information.
- You can customize the information.
- If QRadar does not automatically detect the log source, manually add a log source.
- The list of supported DSMs and the device-specific topics indicate which third-party devices are not automatically detected.
- Deploy the configuration changes and restart your web services.

Custom Log Source Types for unsupported third-party log sources

- After the events are collected and before the correlation can begin, individual events from your devices must be properly normalized.
- *Normalization* means to map information to common field names, such as event name, IP addresses, protocol, and ports.
- If an enterprise network has one or more network or security devices that QRadar does not provide a corresponding DSM, you can use the DSM Editor to:
  - Create Log Source Types
  - Log Source Extensions
  - Additionally, the DSM Editor can be used to enhance the parsing capabilities of supported Log Sources.

Adding a log source

- If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.
- The following table describes the common log source parameters for all log source types:

Parameter	Description
• Log Source Identifier	The IPv4 address or host name that identifies the log source.
• Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
• Credibility	Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events or adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
• Target Event Collector	Specifies the QRadar Event Collector that polls the remote log source. Use this parameter in a distributed deployment to improve Console system performance by moving the polling task to an Event Collector.
• Coalescing Events	Increases the event count when the same event occurs multiple times within a short time interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the Log Activity tab. When this check box is clear, events are viewed individually and events are not bundled.

Traffic Analysis Tuning

Traffic Analysis Tuning

- The TrafficAnalysis engine is how QRadar auto detection capability works.
- The Traffic Analysis engine loads up all DSMs capable of receiving inbound events through syslog.
- When events enter the system with a sourceName that does not match any configured log source, the Traffic Analysis engine tries parsing the event with each DSM it has loaded.
- The engine maintains success statistics for each sourceName/DSM combination and over time (as more events from the same sourceName come in), it determines which DSM (if any) the events “belong” to.
- If based on collected stats, it judges that an instance of a supported log source type exists in the customer’s environment, it will auto-create a log source for that sourceName, and start collecting events for it.

Traffic Analysis Tuning

- Fairly accurate but false positives can happen.
  - Usually because a set of events belonging to one device type are formatted sufficiently similarly to another log source type that has higher priority in the Traffic Analysis configuration file.
- Both DSMs may match the event set equally well, but one takes priority over the other.
- The Traffic Analysis Engine can simply fail to detect a log source at all.
- Often this is because events are coming to QRadar from the log source of interest that QRadar's DSMs cannot parse.
- They could be garbage events, or they could be genuine events that QRadar's DSM simply doesn't know how to process them.
- Even if a given DSM can parse some events from an unidentified source, if it isn't a high enough percentage of success, then the Traffic Analysis engine may give up because the results are inconclusive.

Traffic Analysis Tuning

- Fairly accurate but false positives can happen
  - Usually because a set of events belonging to one device type are formatted sufficiently similarly to another log source type that has higher priority in the Traffic Analysis configuration file.
- Both DSMs may match the event set equally well, but one takes priority over the other
- The Traffic Analysis Engine can simply fail to detect a log source at all.
- Often this is because events are coming to QRadar from the log source of interest that QRadar's DSMs cannot parse.
- They could be garbage events, or they could be genuine events that QRadar's DSM simply doesn't know how to process them.
- Even if a given DSM can parse some events from an unidentified source, if it isn't a high enough percentage of success, then the Traffic Analysis engine may give up because the results are inconclusive.

Traffic Analysis Tuning

- The Traffic Analysis engine can be tuned to remediate the false positives problem.
- On each event collector, there is a TrafficAnalysisConfig.xml file in /opt/qradar/conf/
- Every DSM registered with the Traffic Analysis engine has its own element.
- The 'order' attribute defines the precedence/priority of each DSM
  - The lower the number, the more important the DSM is.
  - So if one DSM has order 400 and another has 500, and both successfully parse 50 events of unknown origin, the one with order=400 will be autocreated
  - The order can be changed if you want to give greater priority to one DSM over another.
    - A common one is moving AIXServer ahead of LinuxServer, since their events are nearly identical.
    - A customer with a lot of AIX machines may see many LinuxServer false position autocreations.

Traffic Analysis Tuning

- Most DSM elements only have a ‘class’ and ‘order’ attribute.
- But they also inherit an additional set of Threshold and Template values from the defaults at the top of the file.
- These can be overridden on a per-DSM basis (the defaults can be changed too, if desired).
  - The Templates only affect how auto-detected log sources are assigned names and descriptions.

Traffic Analysis Tuning

- The Thresholds are statistical tuning parameters, affecting the runtime behavior of the Traffic Analysis engine
  - **MinNumEvents**
    - Defines how many successful event parses a DSM needs from a given sourceName to be eligible for autodetection.
  - **MinSuccessRate**
    - Defines the percentage of attempted parses from a given sourceName that must succeed for a DSM to be eligible for autodetection.
  - **MaxEventBeforeFail**
    - Defines how many total events can be attempted for a given DSM/sourceName pairing before the DSM is no longer considered for that sourceAddress.
  - **AbandonAfterSuccessiveFailures**
    - How many consecutive failed parses must occur for a given DSM/sourceName before the DSM is no longer considered for that sourceAddress.

Integrating Windows Log Sources With QRadar

Integrating with Windows

- At a really high level, there are two steps to any integration:
  - Collecting the event data
    - Getting it from point A (the Windows machine) to point B (QRadar)
    - This can be further divided into:
    - Agent-based collection – WinCollect, Snare, LOGbinder, Balabit Syslog-ng, Splunk
    - Agentless collection – WMI, MSRPC, SMBTail-based protocols

Integrating with Windows

- Parsing the data
  - Pulling out the useful properties/fields for QRadar to do something useful with it:
    - Rules, offenses, reports, correlation, security intelligence, etc.
- This also needs to be subdivided:
  - DSM parsing for normalized fields.
    - Source/Destination IPs, ports, MACs, NAT'd IPs, Username, Log Source Time, identity information.
  - Custom Event Property parsing for everything else.

Integrating with Windows – Agent based

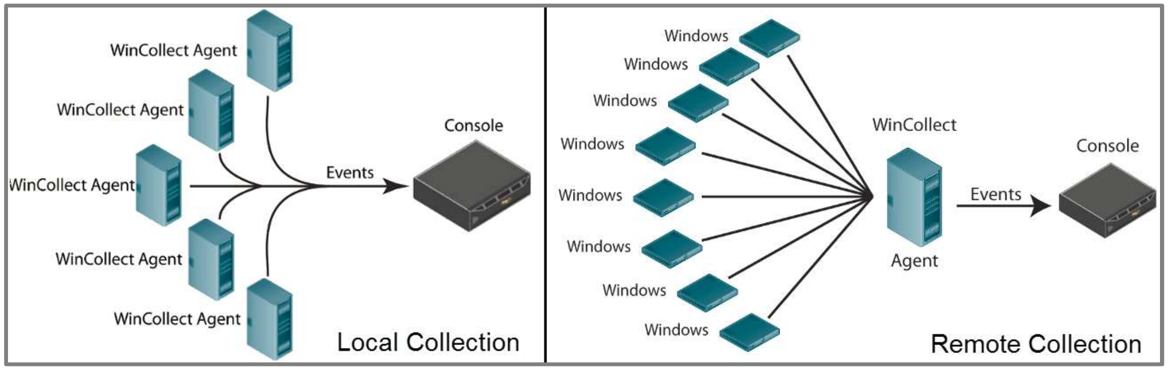
- Agents are pieces of software that need to be installed on a client’s Windows machine and send event data to QRadar (generally via syslog).
- Qradar supports several agent based offerings:
  - **WinCollect**
    - IBM’s recommended Windows event collection offering.
    - The WinCollect application is a Syslog event forwarder that administrators can use for Windows event collection with QRadar.
  - **Snare**
    - Snare Agents capture and immediately send the collected event logs to a third party SIEM or a Syslog server for central storage and reporting.
  - **Balabit Syslog-NG**
    - Syslog-ng Agent for Windows. It can collect log messages from Windows Servers and forward them to SIEM using Regular ot TLS – Encrypted TCP connections.

Integrating with Windows – Agent based

- **LOGbinder**
  - Three different 3rd party agents for obtaining audit, security and Admin/Mailbox events from various Microsoft products (Sharepoint, SQL and Exchange).
- **STEALTHbits**
  - Agent specializing in Windows event collection and analysis.
  - Agent can generate and send LEEF events to QRadar.
- **Splunk**
  - Not really an agent, but Splunk can forward Windows events to Qradar.
  - Splunk forwards Windows events in their original multiline format.
  - TCP Multiline Syslog protocol takes in an event stream of multiline events and uses regular expression(s) to correctly extract the multiline events from the stream.

Wincollect

- WinCollect uses the Windows Event Log API to gather events, and then WinCollect sends the events to QRadar.
- The Windows host can either gather information from itself, the local host, and, or remote Windows hosts.
- Remote hosts do not have the WinCollect software installed.
- The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to QRadar.



Wincollect

- Can be deployed in “**Managed**” mode or “**Standalon**e” mode.
- In both cases, the agent sends event data via syslog (either UDP or TCP or TLS) to QRadar.
  - TLS is supported for unmanaged/standalone mode since WinCollect version 7.2.4.
  - It will be available in the UI (for managed mode) starting in 7.3.1.
- Primarily these events will be from the Windows OS, from Microsoft products, or from flat files on Windows systems, i.e. log source events.
- Also can send system/status event data from the agent itself, as well as heartbeat messages.
- Right now, the agent’s own events can only be sent over UDP.

Wincollect

- In **managed mode**, the agent also maintains communication with QRadar:
  - Via an encrypted connection (on port 8413, by default).
  - Allowing it to check for configuration and software updates, downloading and installing them if necessary.
- The management communication is handled by a component which runs in the protocol source framework.
- It runs on any system in the deployment which is running the ecs-ec process (7.3.0 and earlier) or any system running ecs-ec-ingress (7.3.1 forward).
- Agents do not need to communicate directly with the console – can talk to an EC or EP.
- Agents in managed mode are essentially autonomous.
- Once the agent is installed on the Windows endpoint, there should be no need to access the Windows system again.
- It can be centrally controlled and updated from QRadar.

Wincollect

- In standalone mode, agents only send event data to QRadar.
- They do not poll QRadar for new configuration or software.
- They must be updated and configured directly, either by someone accessing the Windows system and making manual changes, or by a configuration management product such as BigFix or MS SCCM.
- They can still send in system/status syslog messages to a QRadar system, if desired (or to some other syslog receiver).
- This is set by using the StatusServer property in the install_config.txt file.
- Standalone is a good option for clients with large numbers (limit of 500 per EC) of Windows endpoints.
- It is recommended to control the agent if the client has a configuration management/endpoint management solution.

Wincollect

- The agent is installed using a single .exe (both 64-bit and 32-bit options available).
- There are two config files (**AgentConfig.xml and install_config.txt**).
- They may need to be updated thereafter if the agent's configuration needs to be changed.
- For single agent setups, the agent should immediately start up and work after installation.
- The WinCollect installation wizard can now output the command line installer text to reproduce the exact same configuration.
- It can set it up once manually, then easily push out the same install/configuration setup to all other systems.
- QRadar is not aware of standalone agents (that they are agents).
- QRadar just gets syslog event streams, without knowing where they originated.

WinCollect – Notable Capabilities

- **Event filtering**
  - for Windows Event Log only – Security, System, Application, DNS, File Replication, Directory Service log files).
  - Can now exclude events by Source/Event ID combination. Individually configurable for each log file.
- **Event throttling**
  - Limit the number of events per second an agent can send to Qradar.
- **Store and forward**
  - Both scheduled (to fit with data link limitations) and as automatic failover in the event of network outage.
- **Multiple destinations**
  - Configure the agent to send events to multiple destinations.
- **Xpath**
  - For flexibility, can collect from other event logs beyond standards (e.g. SYSMON, powershell).
  - Can use combinations of xpath and regular filters.
- Can customize heartbeat messages to include custom key/value attributes from a file.

WinCollect – Tuning

- Agents can handle:
  - Up to 5000 EPS for local collection.
  - Up to 2500 aggregate EPS if doing remote monitoring.
  - But not 5000 local AND 2500 remote – one or the other or a combination of both at lower rates.
- Script on Github – Event Log Report – calculates EPS for windows systems, makes recommendations for tuning.
  - https://github.com/ibm-security-intelligence/wincollect/tree/master/EventLogReport
- Event Rate Tuning Profiles are used to define roughly what EPS rate is expected a log source is expected to generate.

For more information on tuning Wincollect Agents:

http://www-01.ibm.com/support/docview.wss?uid=swg21672193

WinCollect – Available Plugins

- There is a Protocol Configuration option in the Log Source UI for each of the WinCollect event collection plugins
  - WinCollect – the original/standard one, for reading events from the Windows Event Log
    - Security, System, Application, DNS Server, File Replication Service, Directory Service logs, plus XPath
  - Microsoft DHCP
  - Microsoft IAS/NPS
  - Microsoft ISA/Forefront TMG
  - Microsoft IIS *
  - Microsoft SQL Server
  - Juniper SBR
  - NetApp Data ONTAP (improved performance and stability, historical event collection)
  - File Forwarder (generic flat file tailing plugin)
  - DNS Debug

* Currently local-only, but this will be addressed in WinCollect version 7.2.8

WinCollect – Utilities and debugging

- WinCollectPing utility (just for managed mode).
  - Included in agent install, found in the WinCollect bin directory.
  - Can be run from the command line with no parameters, simply reads the install_config.txt file and attempts to connect to the configuration console (a Qradar console or managed host) with the agent's configuration.
- Debugging the QRadar side (managed mode).
  - Turn on debug (using the /opt/qradar/support/mod_log4j.pl script).
  - Java classpath to enable debug for com.q1labs.sem.semsources.wincollectconfigserver.
- Debugging the agent side .
  - There are a set of log files in the 'logs' sub-directory of the WinCollect install directory.
  - New – INFOX starts in debug at startup, and goes into debug every 15 minutes (configurable) to get more detailed information.
    - Part of the regular logging system in WinCollect 7.2.8 (one logfile).

Agentless solutions

- Agentless solutions exist so QRadar can collect event data without having to install anything on a client system.
- Important for PoCs where potential customers may not want to install agents in their environment.
- Microsoft Security Event Log protocol
  - The Microsoft Security Event Log protocol provides remote agentless Windows event log collection for Windows with the Microsoft Windows Management Instrumentation (WMI) API.
  - The WMI API is a Microsoft technology that is used to communicate and exchange information between operating systems.
  - This API requires that firewall configurations accept incoming external communications on port 135 and any dynamic ports that are required for DCOM.

Agentless solutions

- Microsoft Security Event Log protocol (cont)
  - The following log source limitations apply when administrators deploy the Microsoft Security Event Log Protocol in your environment:
    - Systems that exceed 50 events per second (eps) can exceed the capabilities of this protocol. WinCollect can be used for systems that exceed 50 eps.
    - A QRadar all-in-one installation can support up to 250 log sources with the Microsoft Security Event Log protocol.
    - Dedicated Event Collectors can support up to 500 log sources with the Microsoft Security Event Log protocol.
    - The Microsoft Security Event Log protocol is not suggested for remote servers that are accessed over network links.

Agentless solutions

- Microsoft Security Event Log Over MSRPC Protocol
  - The Microsoft Security Event Log over MSRPC protocol is a method for QRadar to collect Windows events without the need of a local agent on the Windows host.
  - The protocol leverages Microsoft's implementation of DCE/RPC, which is commonly referred to as MSRPC.
  - The MSRPC protocols offers agentless, encrypted event collecting that provides higher event rates than the default 'Microsoft Windows Security Event Log' protocol, which uses WMI/DCOM for event collection.
  - The officially documented stance is that the MSRPC protocol can handle up to 100 events per second from a given endpoint, but attempting to pull events from a system with an event rate beyond is not officially supported.
  - Some additional limiting factors are 500 MSRPC log sources per QRadar event collector managed host, and 8500 total EPS per managed host.
- The Microsoft Security Event Log over MSRPC only supports standard Windows event logs for workstations and servers.

Agentless solutions

- This allows MSRPC to collect Security, System, Application, DNS Server, File Replication, and Directory Service event .

  MSRPC is **not** capable of retrieving or parsing non-Standard windows logs, such as Microsoft IIS, Microsoft SQL, Microsoft DHCP, Juniper Steel-Belted Radius, Microsoft IAS/NPS, Microsoft ISA, or NetApp Data ONTAP.
- If you require events from any of these systems, administrators can then install the WinCollect agent software.

Agentless solutions

- The SMBTail-based protocols
  - Protocols which use SMB/CIFS to remotely connect to a Windows file share and monitor a file or files
  - Microsoft Exchange' protocol
    - For tailing Outlook Web Access (OWA) logs, SMTP logs, and MSTRK logs
  - 'Microsoft DHCP' protocol
    - For tailing DHCP audit log
  - 'Microsoft IIS' protocol
    - For tailing W3C web server logs

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

IBM Security Understanding Flows in QRadar

Agenda

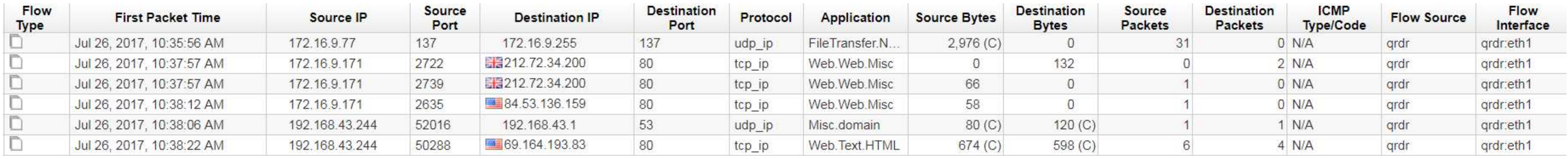
- Introduction to Flows
- Configuring Flow Sources
- Flow Source Aliases
- Viewing Flow Data in QRadar
- Flow Bias
- Flow Collector and Processor Appliances
- Introduction to QRadar Network Insights (QNI)
- Architecture, Sizing & Appliance Specifications
- How QNI deals with SSL encryption
- QNI Frequently Asked Questions (FAQ)

IBM Security

Introduction to Flows

What are Flows?

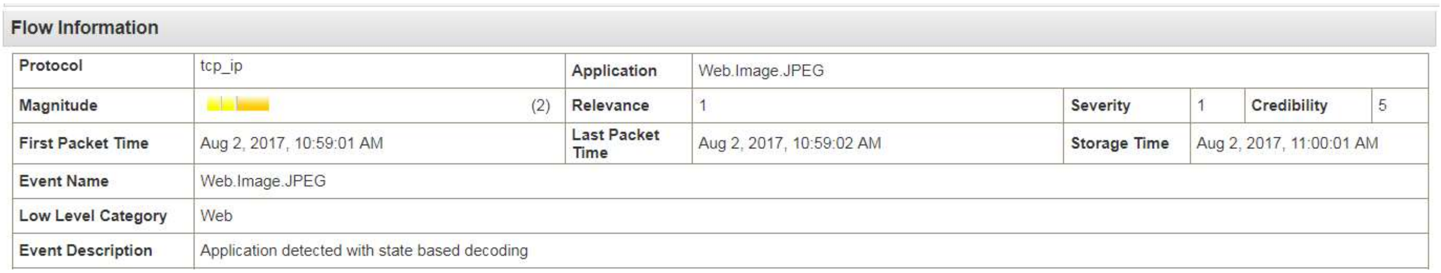
- QRadar collects network activity information, or what is referred to as "flow records".
- Flows represent network activity by normalizing IP addresses, ports, byte and packet counts, as well as other details, into "flow", which effectively represent a session between two hosts.
- For sessions that span multiple "intervals" (minutes), the pipeline reports a record at the end of each minute with the current metrics for each flow - bytes, packets etc.
- For this reason, you will see multiple records (per minute) in QRadar with the same "First Packet Time", but with "Last Packet Time" values that increment through time.



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	Flow Source	Flow Interface
□	Jul 26, 2017, 10:35:56 AM	172.16.9.77	137	172.16.9.255	137	udp_ip	FileTransfer.N...	2,976 (C)	0	31	0	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:37:57 AM	172.16.9.171	2722	212.72.34.200	80	tcp_ip	Web.Web.Misc	0	132	0	2	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:37:57 AM	172.16.9.171	2739	212.72.34.200	80	tcp_ip	Web.Web.Misc	66	0	1	0	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:38:12 AM	172.16.9.171	2635	84.53.136.159	80	tcp_ip	Web.Web.Misc	58	0	1	0	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:38:06 AM	192.168.43.244	52016	192.168.43.1	53	udp_ip	Misc.domain	80 (C)	120 (C)	1	1	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:38:22 AM	192.168.43.244	50288	69.164.193.83	80	tcp_ip	Web.Text.HTML	674 (C)	598 (C)	6	4	N/A	qrdr	qrdr:eth1

How do Flows and Events differ from each other?

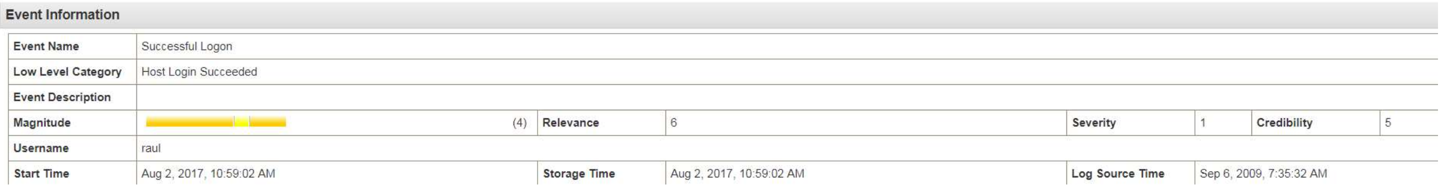
- A flow is different from an event
- Flows (for the most part) will have a start and end time, or, a life of multiple seconds.
- For example, when you connect to a website, the communication will include HTML files, images, flash files, longer file downloads, etc, and may take some time to transfer the data.



Flow Information

Protocol	tcp_ip	Application	Web.Image.JPEG				
Magnitude	(2)	Relevance	1	Severity	1	Credibility	5
First Packet Time	Aug 2, 2017, 10:59:01 AM	Last Packet Time	Aug 2, 2017, 10:59:02 AM	Storage Time	Aug 2, 2017, 11:00:01 AM		
Event Name	Web.Image.JPEG						
Low Level Category	Web						
Event Description	Application detected with state based decoding						

- An Event, in contrast, represents a single event on the network, such as the login action of a VPN session or a firewall deny by someone trying to connect to a network.

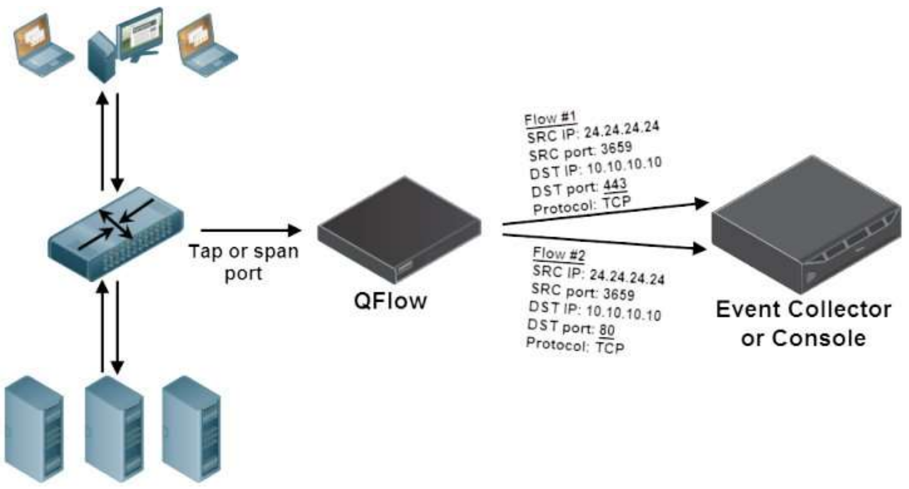


Event Information

Event Name	Successful Logon						
Low Level Category	Host Login Succeeded						
Event Description							
Magnitude	(4)	Relevance	6	Severity	1	Credibility	5
Username	raul						
Start Time	Aug 2, 2017, 10:59:02 AM	Storage Time	Aug 2, 2017, 10:59:02 AM	Log Source Time	Sep 6, 2009, 7:35:32 AM		

How are Flows licensed in QRadar?

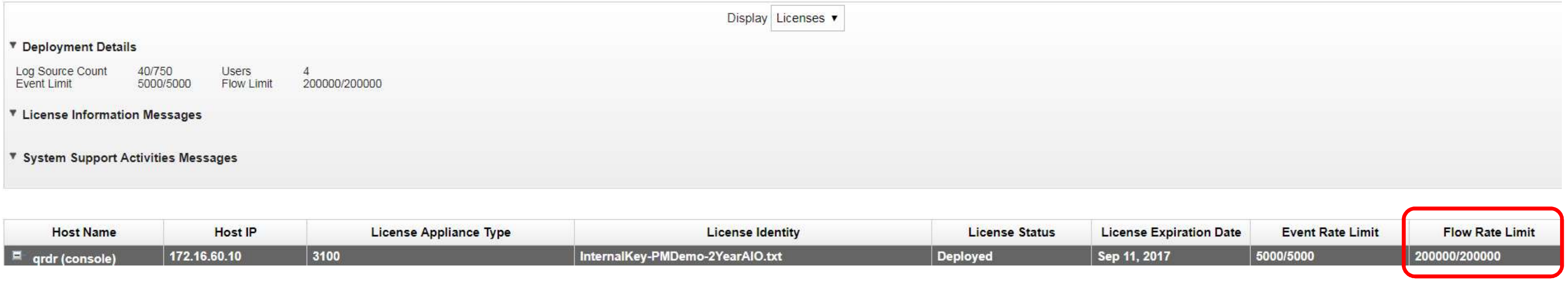
- Flows are a record of communication between two hosts over a one minute interval.
- QRadar licenses flow based on flows per minute (FPM).
- All packets, within a one minute interval, that contain the same source IP, destination IP, source port, destination port, and protocol are combined to become one flow record.
- This means that if you have a license of 25,000 FPM on your appliance, that the appliance can handle 25,000 flow records per minute.



- The flow record contains information such as the number of packets sent, how many bytes were transferred between the source and destination, and other data relevant to the communication.

How are Flows licensed in QRadar? (Cont)

- When administrators review their licenses for appliances or virtual machine (VM), they might notice that the appliances lists capabilities as two numbers.
- For example, an appliance might display a Flow Rate Limit of 200000/1200000 flows per minute.
- The first value represents the number of flows currently licensed to the appliance (200000)



▾ Deployment Details

Log Source Count	40/750	Users	4
Event Limit	5000/5000	Flow Limit	200000/200000

▾ License Information Messages

▾ System Support Activities Messages

Host Name	Host IP	License Appliance Type	License Identity	License Status	License Expiration Date	Event Rate Limit	Flow Rate Limit
qrdr (console)	172.16.60.10	3100	InternalKey-PMDemo-2YearAIO.txt	Deployed	Sep 11, 2017	5000/5000	200000/200000

- The second value represents the overall number of flows that the appliances is capable of handling (1200000)

How Flows are collected and Processed in QRadar

- The component in QRadar that collects and creates flow information is known as **Qflow.**
- QFlow can process & create flows from multiple sources
- A flow starts when the Flow Collector detects the first packet that has a unique source IP address, destination IP address, source port, destination port, and other specific protocol options.
- QRadar Flow collection is not full packet capture
- Each new packet is evaluated.
- Counts of bytes and packets are added to the statistical counters in the flow record.
- At the end of an interval, a status record of the flow is sent to a Flow Processor and statistical counters for the flow are reset.
- A flow ends when no activity for the flow is detected within the configured time.

Flow pipeline

The **QFlow** component collects and creates flow information from internal and external flow sources

Event Collector – Responsible for parsing and normalizing incoming flows

Asymmetric recombination - Responsible for combining two sides of each flow when data is provided asymmetrically

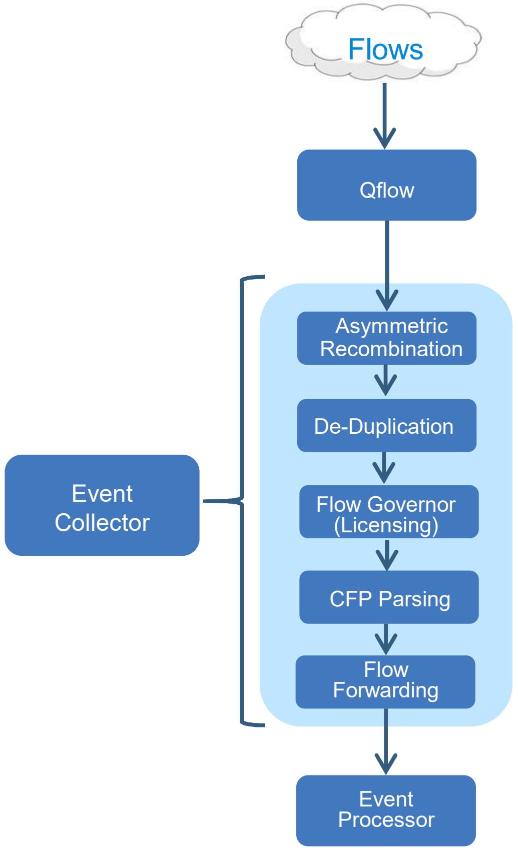
Deduplication - Flow deduplication is a process that removes duplicate flows when multiple Flow Collectors provide data to Flow Processors appliances.

Flow Governor - Monitors the number of incoming flows to the system to manage input queues and licensing.

Custom flow properties – extracts any properties defined in the Custom Flow Properties

Forwarding - Applies routing rules for the system, such as sending flow data to offsite targets, external Syslog systems, JSON systems, and other SIEMs.

Flows are then sent to the **Event Processor** component and pass through the Custom Rules Engine (CRE). They are tested and correlated against the rules that are configured



Flow Correlation and Processing

After flows are normalized they are then sent to the Event Processor for processing

Licensing is applied again on ingress to the EP

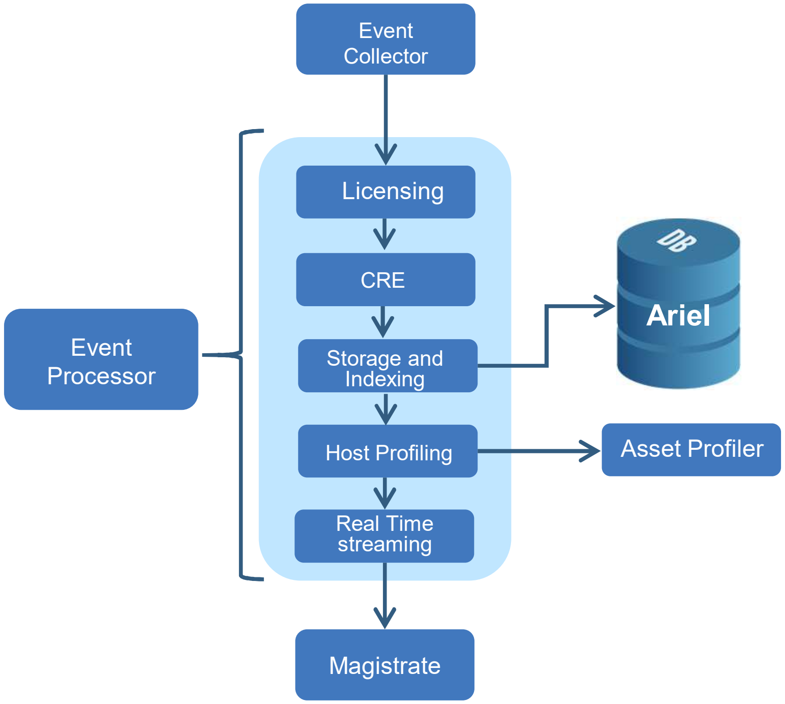
The CRE or Custom Rules Engine Applies the correlation rules that were created in the UI.

Flow data is then sent to the Ariel Database for storage.

Host Profiling – Also called passive profiling or passive scanning. Watches flows on the network in order to make educated guesses about which IPs/assets exist and what ports are open.

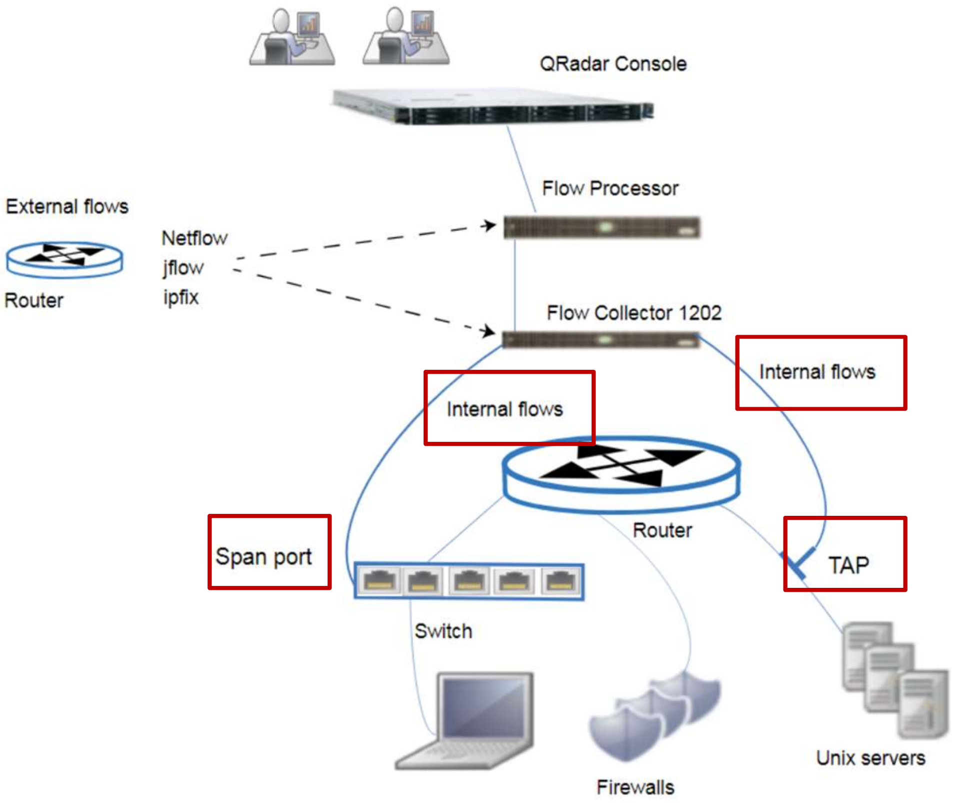
Streaming – Responsible for the “real time (streaming)” view in User Interface

If an event matches a rule, the Magistrate component generates the response that is configure in the custom rule



Types of Flow data - Internal Flow Sources

- **Sources that include packet data** by connecting a span/monitor port, or network tap, to a Flow collector are referred to as **internal flow sources**
- The internal type of collection requires a dedicated collector appliance, such as a 12XX or 13XX that varies in capacity based on traffic rates
- These sources provide raw packet data to a monitoring port on the QRadar flow collector, which then converts these packet details into **flow records**.
- The QRadar QFlow Collector is enabled by default, while the mirror port or tap is connected to a monitoring interface on your QRadar appliance.



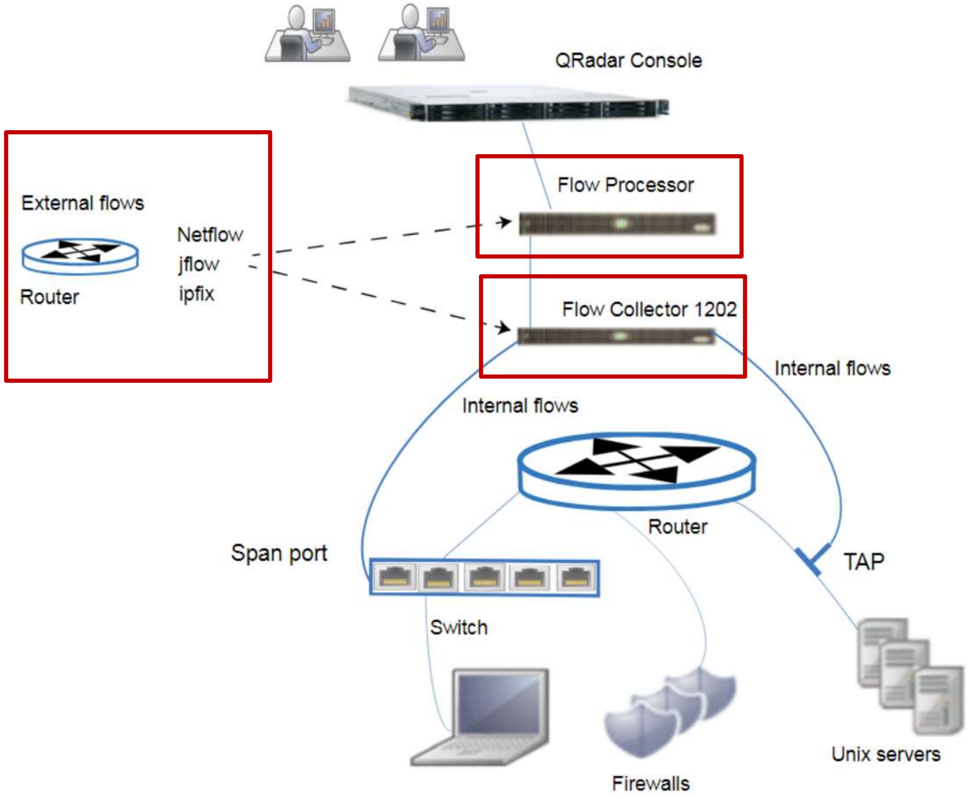
Types of Flow data - Internal Flow Sources (Cont)

- Common mirror port locations include core, DMZ, server, and application switches.
- QRadar QFlow Collector combined with QRadar and flow processors provides Layer 7 application visibility and flow analysis of network traffic regardless of the port on which the application is operating.
- For example, if the Internet Relay Chat (IRC) protocol is communicating on port 7500 (TCP), QRadar QFlow Collector identifies the traffic as IRC and provides a packet capture of the beginning of the conversation.
- This process differs from External Flow Sources, such as NetFlow or J-Flow, which indicate that there is traffic on port 7500 (TCP) without identifying the protocol.
- QRadar QFlow Collectors are not full packet capture engines, but you can adjust the amount of content that is captured per flow.
- The default capture size is 64 bytes, and you can collect helpful data by using this setting.

- However, you might want to adjust this setting to 256 bytes to capture more content per flow.
- Increasing the capture size increases network traffic between your QRadar QFlow Collector and Flow Processor, and more disk storage is required.

Types of Flow data - External Flow Sources

- **External sources** are flow sources such as NetFlow, IPFIX, sFlow, J-Flow, Packeteer and Flowlog file.
- Flows from external sources can be sent to a dedicated Flow Collector or to a Flow Processor.
- External sources do not require as much CPU processing because every packet is not processed to build flows.
- In smaller environments (less than 50 Mbps), an All-in-One appliance might handle all the data processing.



Supported External Flow Sources

- Netflow
  - Developed by Cisco Systems, NetFlow monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is used, counts the number of bytes and packets, and sends that data to a NetFlow collector.
- IPFIX
  - Internet Protocol Flow Information Export (IPFIX) is an accounting technology.
  - IPFIX monitors traffic flows through a switch or router, interprets the client, server, protocol, and port that is used, counts the number of bytes and packets, and sends that data to a IPFIX collector.
- Sflow
  - sFlow is a multi-vendor and user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously
- Jflow
  - A proprietary accounting technology used by Juniper Networks that allows you to collect IP traffic flow statistics. J-Flow enables you to export data to a UDP port on a J-Flow collector.
- Packeteer
  - Packeteer devices collect, aggregate, and store network performance data. After you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to IBM Security QRadar.
- Flowlog File
  - A Flowlog file is generated from the IBM Security QRadar flow logs.

IBM Security

Configuring Flow Sources

Configuring Flow Sources

- For IBM Security QRadar appliances, QRadar SIEM automatically adds default flow sources for the physical ports on the appliance.
- QRadar SIEM also includes a default NetFlow flow source.
- If QRadar SIEM is installed on your own hardware, QRadar SIEM attempts to automatically detect and add default flow sources for any physical devices, such as a network interface card (NIC).
- Also, when you assign a IBM Security QRadar QFlow Collector, QRadar SIEM includes a default NetFlow flow source.
- Flow sources are classed as either internal or external

Configuring Flow Sources (cont)

- **Internal Flow Sources**
  - Internal flow sources Includes any additional hardware that is installed on a managed host, such as a network interface card (NIC).
  - Depending on the hardware configuration of your managed host, the internal flow sources might include the following sources:
    - Network interface card or Napatech interface
- **External Flow Sources**
  - External flow sources Includes any external flow sources that send flows to the QRadar QFlow Collector.
  - If your QRadar QFlow Collector receives multiple flow sources, you can assign each flow source a distinct name.
  - When external flow data is received by the same QRadar QFlow Collector, a distinct name helps to distinguish external flow source data from each other.
  - External flow sources might include the following sources:
    - NetFlow, IPFIX, sFlow, J-Flow, Packeteer and Flowlog file

Configuring Flow Sources (Cont)

- QRadar SIEM can forward external flows source data by using the spoofing or non-spoofing method:
- **Spoofing**
  - Resends the inbound data that is received from flow sources to a secondary destination.
  - To ensure that flow source data is sent to a secondary destination, configure the Monitoring Interface parameter in the flow source configuration to the port on which data is received (management port).
  - When you use a specific interface, the QRadar QFlow Collector uses a promiscuous mode capture to obtain flow source data, rather than the default UDP listening port on port 2055.
  - As a result, QRadar QFlow Collector can capture flow source packets and forward the data.

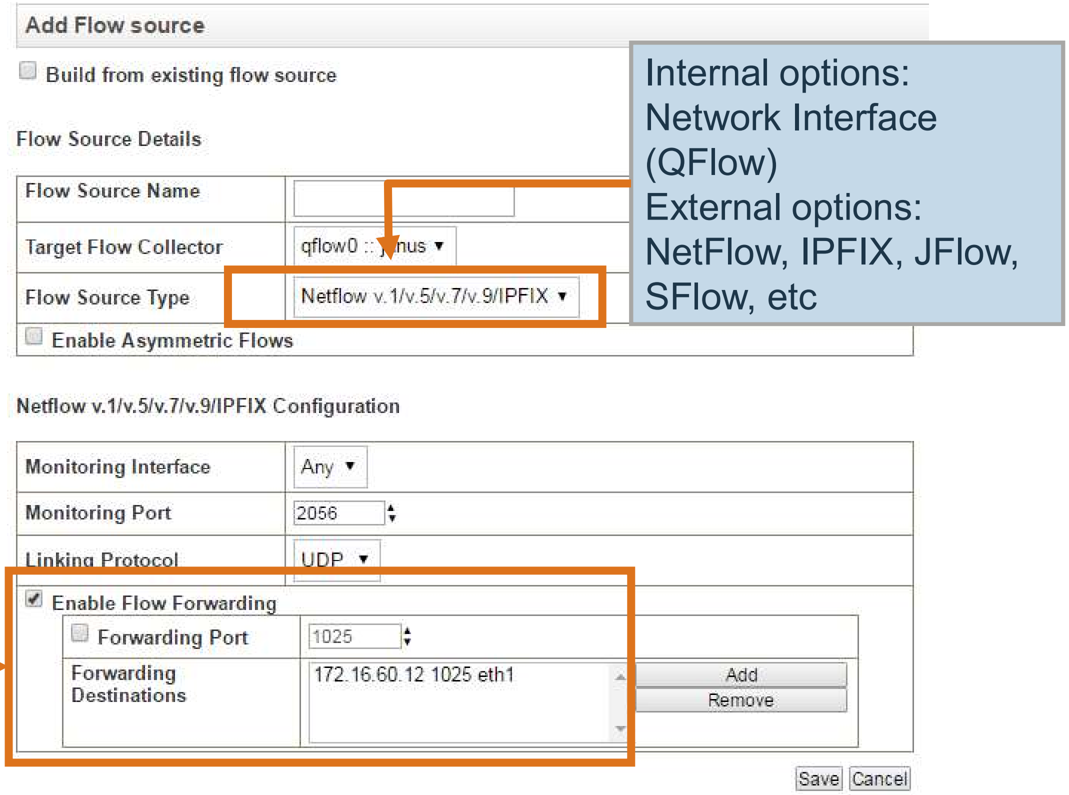
Configuring Flow Sources (Cont)

- **Non-Spoofing**
  - For the non-spoofing method, configure the Monitoring Interface parameter in the flow source configuration as **Any**.
  - The QRadar QFlow Collector opens the listening port, which is the port that is configured as the Monitoring Port to accept flow source data.
  - The data is processed and forwarded to another flow source destination.
  - The source IP address of the flow source data becomes the IP address of the QRadar SIEM system, not the original router that sent the data.

Configuring Flow Sources (cont)

In some cases you may need to create a Flow Source. You will need to follow these steps to create a new Flow Source

1. Specify a **Flow Source Name**
2. Select the **Target Flow Collector** that receives the flows
3. Select the **Flow Source Type**
4. Select **Enable Asymmetric Flows** if the Flow Processor should attempt unidirectional flow recombination
5. You can forward external flows to multiple destinations; use the original MAC address and original source IP for the forwarded flow



Add Flow source

□ Build from existing flow source

Flow Source Details

Flow Source Name	
Target Flow Collector	qflow0 :: janus ▾
Flow Source Type	Netflow v.1/v.5/v.7/v.9/IPFIX ▾
□ Enable Asymmetric Flows	

Netflow v.1/v.5/v.7/v.9/IPFIX Configuration

Monitoring Interface	Any ▾
Monitoring Port	2056
Linking Protocol	UDP ▾
☑ Enable Flow Forwarding	
□ Forwarding Port	1025
Forwarding Destinations	172.16.60.12 1025 eth1

Internal options: Network Interface (QFlow)
External options: NetFlow, IPFIX, JFlow, SFlow, etc

IBM Security

Flow Sources aliases

IBM

Flow Sources aliases

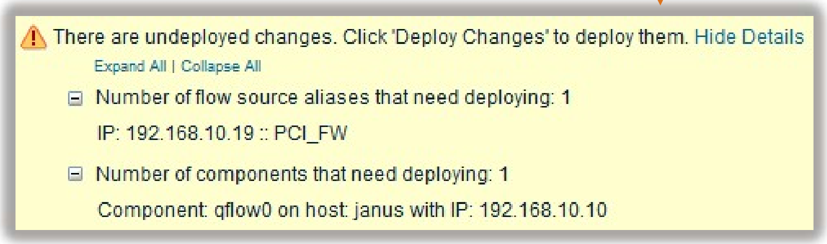
- You can use the Flow Source Alias window to configure virtual names, or aliases, for your flow sources.
- You can identify multiple sources that are sent to the same QRadar QFlow Collector by using the source IP address and virtual name.
- With an alias, a QRadar QFlow Collector can uniquely identify and process data sources that are sent to the same port.
- When QRadar QFlow Collector receives traffic from a device that has an IP address but does not have a current alias, the QRadar QFlow Collector attempts a reverse DNS lookup.
- The lookup is used to determine the host name of the device.
- If the lookup is successful, the QRadar QFlow Collector adds this information to the database and reports the information to all QRadar QFlow Collector components in your deployment.

Detecting Flow Source Aliases Automatically

- Use the Component Configuration to configure the QRadar QFlow Collector to automatically detect flow source aliases.
- To enable reverse DNS lookup, set **Alias Autodetection** to **Yes**

Note: The Component Configuration window is located in the System and License Management administration

To activate the Flow Source Alias, click **Deploy Changes**



⚠ There are undeployed changes. Click 'Deploy Changes' to deploy them. Hide Details

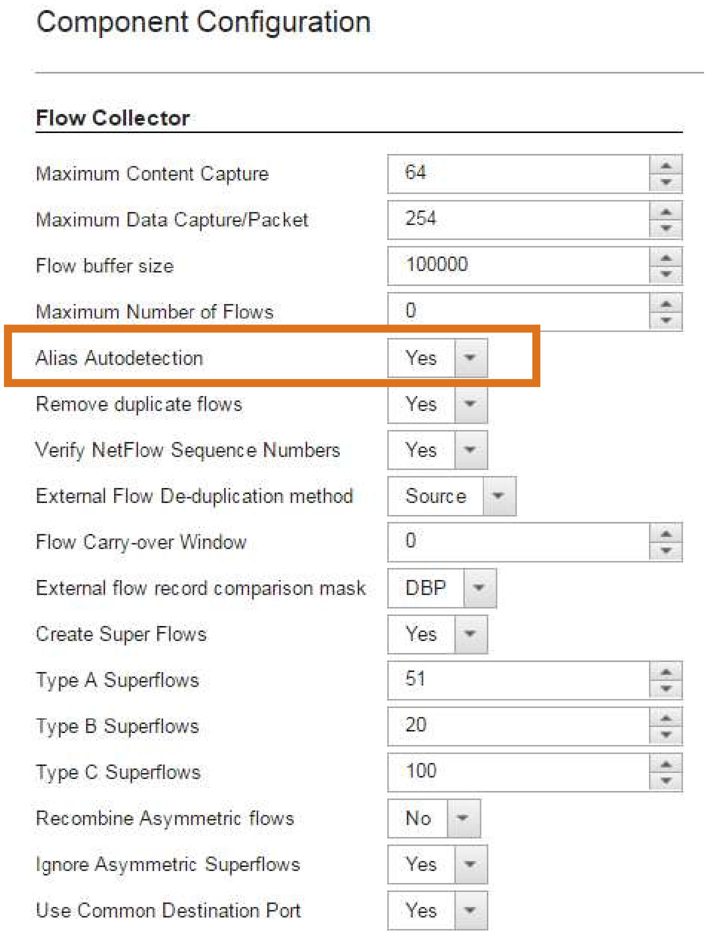
Expand All | Collapse All

⊟ Number of flow source aliases that need deploying: 1

IP: 192.168.10.19 :: PCI_FW

⊟ Number of components that need deploying: 1

Component: qflow0 on host: janus with IP: 192.168.10.10



Component Configuration

Flow Collector

Maximum Content Capture	64
Maximum Data Capture/Packet	254
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	51
Type B Superflows	20
Type C Superflows	100
Recombine Asymmetric flows	No
Ignore Asymmetric Superflows	Yes
Use Common Destination Port	Yes

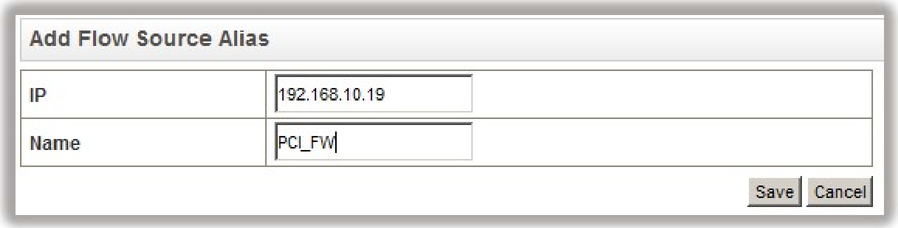
Adding or deleting a Flow Source Alias manually

If the reverse DNS lookup does not resolve the external flow source, you can add the Alias manually

- Click **Add**
- Specify an IP address
- Type a logical name for the external flow
- Click **Save**

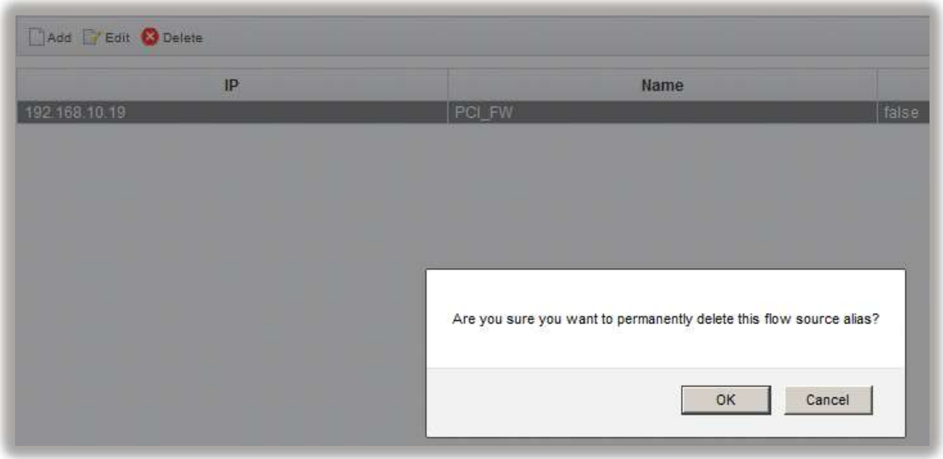
Follow these steps to delete a Flow Source Alias

- Select the Flow Source Alias
- Click **Delete**
- Click **OK**



Add Flow Source Alias

IP	192.168.10.19
Name	PCI_FW



IP	Name	
192.168.10.19	PCI_FW	false

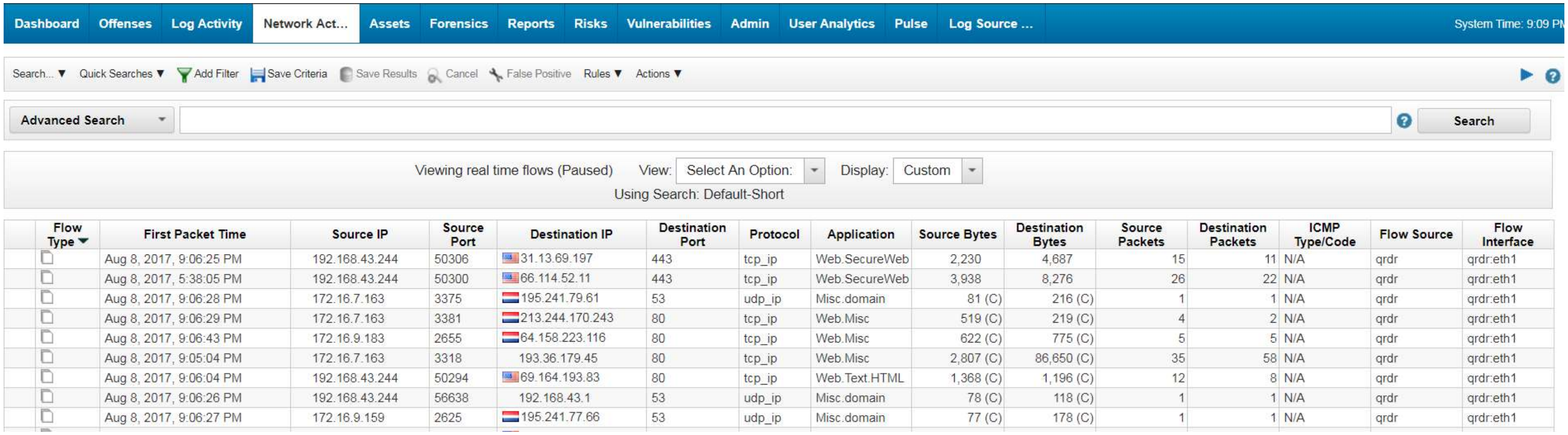
Are you sure you want to permanently delete this flow source alias?

IBM Security

Viewing Flow Data in QRadar

Network activity monitoring

- By default, the **Network Activity** tab displays flows in streaming mode, allowing you to view flows in real time.
- If you apply any filters on the Network Activity tab or in your search criteria before enabling streaming mode, the filters are maintained in streaming mode.
- Streaming mode does not support searches that include grouped flows.
- When you want to select a flow to view details or perform an action, you must pause streaming before you double-click an event.



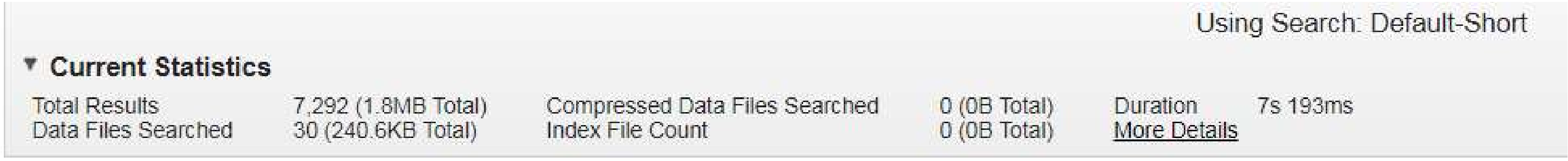
Viewing real time flows (Paused) View: Select An Option: Display: Custom

Using Search: Default-Short

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	Flow Source	Flow Interface
□	Aug 8, 2017, 9:06:25 PM	192.168.43.244	50306	31.13.69.197	443	tcp_ip	Web.SecureWeb	2,230	4,687	15	11	N/A	qrdr	qrdr:eth1
□	Aug 8, 2017, 5:38:05 PM	192.168.43.244	50300	66.114.52.11	443	tcp_ip	Web.SecureWeb	3,938	8,276	26	22	N/A	qrdr	qrdr:eth1
□	Aug 8, 2017, 9:06:28 PM	172.16.7.163	3375	195.241.79.61	53	udp_ip	Misc.domain	81 (C)	216 (C)	1	1	N/A	qrdr	qrdr:eth1
□	Aug 8, 2017, 9:06:29 PM	172.16.7.163	3381	213.244.170.243	80	tcp_ip	Web.Misc	519 (C)	219 (C)	4	2	N/A	qrdr	qrdr:eth1
□	Aug 8, 2017, 9:06:43 PM	172.16.9.183	2655	64.158.223.116	80	tcp_ip	Web.Misc	622 (C)	775 (C)	5	5	N/A	qrdr	qrdr:eth1
□	Aug 8, 2017, 9:05:04 PM	172.16.7.163	3318	193.36.179.45	80	tcp_ip	Web.Misc	2,807 (C)	86,650 (C)	35	58	N/A	qrdr	qrdr:eth1
□	Aug 8, 2017, 9:06:04 PM	192.168.43.244	50294	69.164.193.83	80	tcp_ip	Web.Text.HTML	1,368 (C)	1,196 (C)	12	8	N/A	qrdr	qrdr:eth1
□	Aug 8, 2017, 9:06:26 PM	192.168.43.244	56638	192.168.43.1	53	udp_ip	Misc.domain	78 (C)	118 (C)	1	1	N/A	qrdr	qrdr:eth1
□	Aug 8, 2017, 9:06:27 PM	172.16.9.159	2625	195.241.77.66	53	udp_ip	Misc.domain	77 (C)	178 (C)	1	1	N/A	qrdr	qrdr:eth1

Viewing normalized flows

- Data flow is collected, normalized and then displayed on the **Network Activity** tab.
- The **Network Activity** tab displays the following parameters when you view normalized flows:
  - Current Filters – displays the details of the filters that may be applied to the search results (if applicable)
  - Current Statistics - When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including:
  - **Total Results** - Specifies the total number of results that matched your search criteria.
  - **Data Files Searched** - Specifies the total number of data files searched during the specified time span.
  - **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span.
  - **Index File Count** - Specifies the total number of index files searched during the specified time span.
  - **Duration** - Specifies the duration of the search.



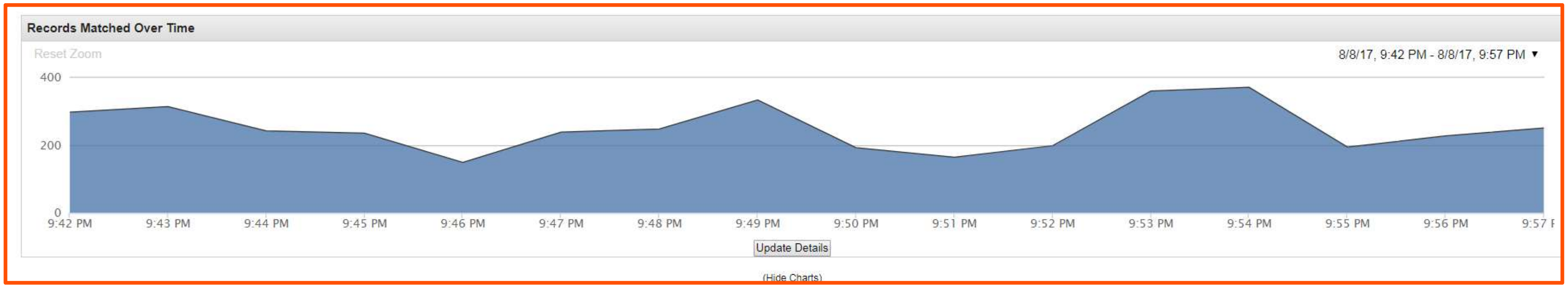
Using Search: Default-Short

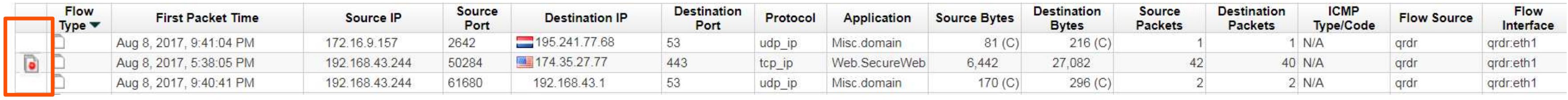
▼ Current Statistics

Total Results	7,292 (1.8MB Total)	Compressed Data Files Searched	0 (0B Total)	Duration	7s 193ms
Data Files Searched	30 (240.6KB Total)	Index File Count	0 (0B Total)	More Details	

Viewing normalized flows

- Charts - Displays configurable charts that represent the records that are matched by the time interval and grouping option.
- Click **Hide Charts** if you want to remove the charts from your display.
- The charts are only displayed after you select a time frame of Last Interval (auto refresh) or greater, and a grouping option to display.



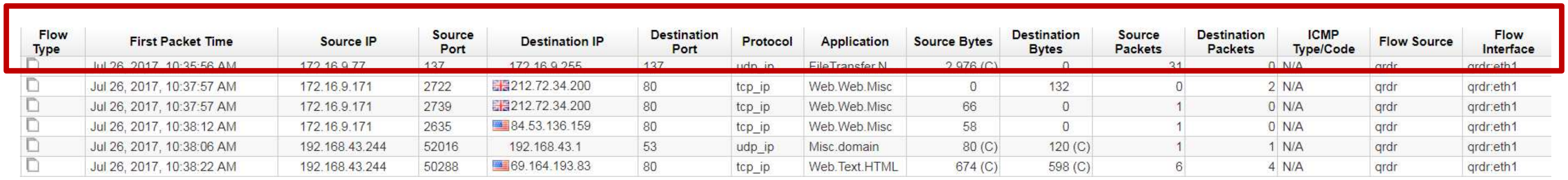


	Flow Type ▾	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Interface
	□	Aug 8, 2017, 9:41:04 PM	172.16.9.157	2642	195.241.77.68	53	udp_ip	Misc.domain	81 (C)	216 (C)	1	1	N/A	qrdr	qrdr:eth1
●	□	Aug 8, 2017, 5:38:05 PM	192.168.43.244	50284	174.35.27.77	443	tcp_ip	Web.SecureWeb	6,442	27,082	42	40	N/A	qrdr	qrdr:eth1
	□	Aug 8, 2017, 9:40:41 PM	192.168.43.244	61680	192.168.43.1	53	udp_ip	Misc.domain	170 (C)	296 (C)	2	2	N/A	qrdr	qrdr:eth1

- Offenses icon - Click the **Offenses** icon to view details of the offense that is associated with this flow.

What information do you get out of Flows in QRadar?

- Normalized view provides information on:
  - Flow Type
  - First Packet Time
  - Source IP & Port
  - Destination IP & Port, Protocol, Application
  - Source & Destination Bytes and Packets
  - ICMP Types
  - Flow Source and Interface

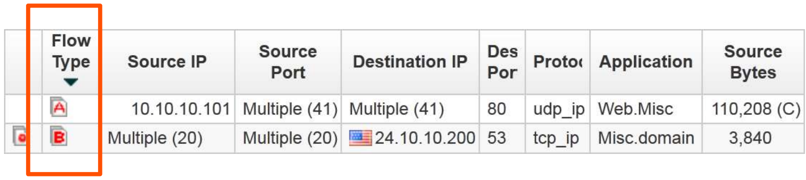


Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Interface
□	Jul 26, 2017, 10:35:56 AM	172.16.9.77	137	172.16.9.255	137	udp_ip	FileTransfer.N	2,976 (C)	0	31	0	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:37:57 AM	172.16.9.171	2722	212.72.34.200	80	tcp_ip	Web.Web.Misc	0	132	0	2	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:37:57 AM	172.16.9.171	2739	212.72.34.200	80	tcp_ip	Web.Web.Misc	66	0	1	0	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:38:12 AM	172.16.9.171	2635	84.53.136.159	80	tcp_ip	Web.Web.Misc	58	0	1	0	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:38:06 AM	192.168.43.244	52016	192.168.43.1	53	udp_ip	Misc.domain	80 (C)	120 (C)	1	1	N/A	qrdr	qrdr:eth1
□	Jul 26, 2017, 10:38:22 AM	192.168.43.244	50288	69.164.193.83	80	tcp_ip	Web.Text.HTML	674 (C)	598 (C)	6	4	N/A	qrdr	qrdr:eth1

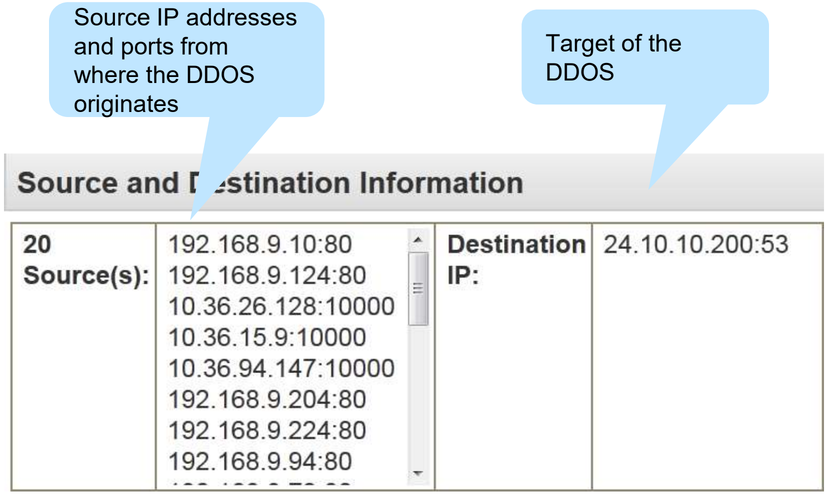
Viewing normalized flows – Flow Type

- Standard flow:
  - A single standard flow record.
- Superflows:
  - A superflow is a flow that is an aggregate of a number of flows that have a similar predetermined set of elements.
- Type A Superflow (Network scans):

  - One source to many destination IPs
  - This is a unidirectional flow, which has the same source, but multiple destinations.
- Type B Superflow (DDoS):
  - Multiple sources to a single destination IP
  - This is a unidirectional flow, which has the multiple sources, but has a single destination.
- Type C Superflow (Port scans):
  - One-to-one source and destination with many ports.
  - This is a one-to-one flow with different source or destination ports.



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



Source IP addresses and ports from where the DDOS originates

Target of the DDOS

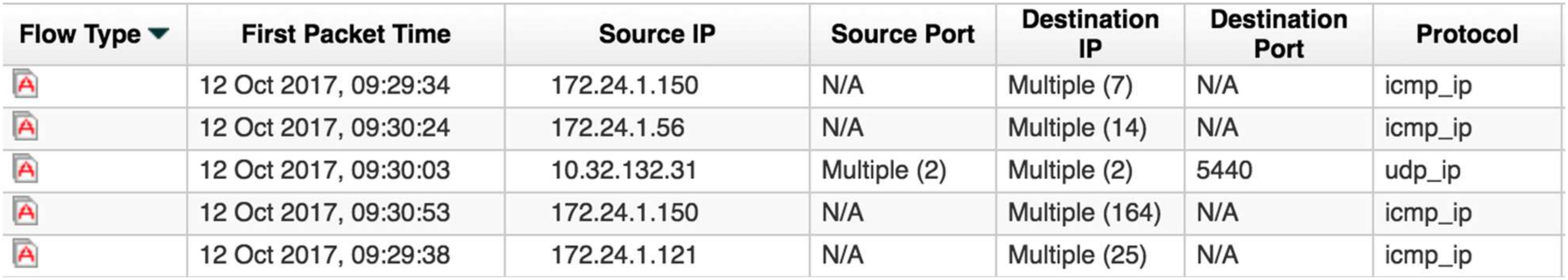
Source and Destination Information

20 Source(s):	192.168.9.10:80 192.168.9.124:80 10.36.26.128:10000 10.36.15.9:10000 10.36.94.147:10000 192.168.9.204:80 192.168.9.224:80 192.168.9.94:80	Destination IP:	24.10.10.200:53

Example: Type B Superflow

Superflow A

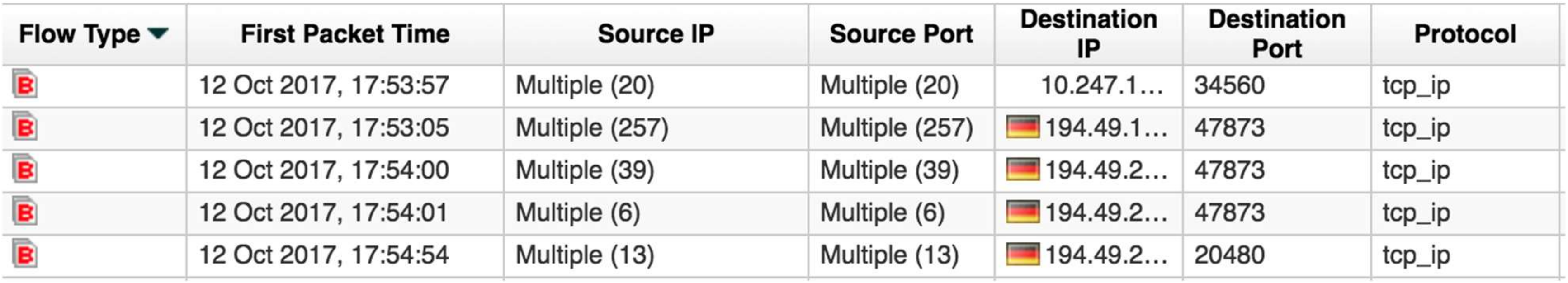
- Network scan – one source, many destinations
- Matching:
  - Protocol
  - Source bytes-to-packets ratio
  - Source IP
  - Destination port (TCP and UDP flows only)
  - TCP flags (TCP flows only)
  - ICMP type, and code (ICMP flows only)



Flow Type ▼	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol
A	12 Oct 2017, 09:29:34	172.24.1.150	N/A	Multiple (7)	N/A	icmp_ip
A	12 Oct 2017, 09:30:24	172.24.1.56	N/A	Multiple (14)	N/A	icmp_ip
A	12 Oct 2017, 09:30:03	10.32.132.31	Multiple (2)	Multiple (2)	5440	udp_ip
A	12 Oct 2017, 09:30:53	172.24.1.150	N/A	Multiple (164)	N/A	icmp_ip
A	12 Oct 2017, 09:29:38	172.24.1.121	N/A	Multiple (25)	N/A	icmp_ip

Superflow B

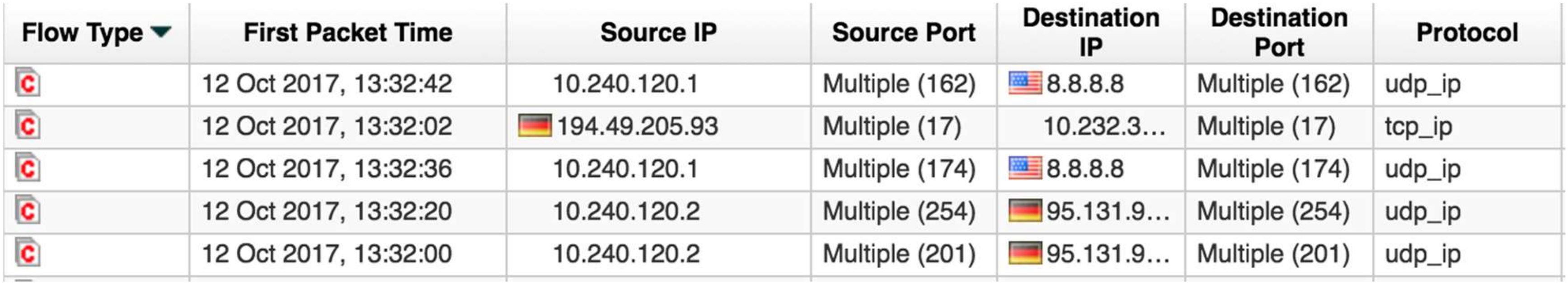
- Distributed denial of service (DDOS) – many sources, one destination
- Matching:
  - Protocol
  - Source bytes-to-packets ratio
  - Destination IP
  - Destination port (TCP and UDP flows only)
  - TCP flags (TCP flows only)
  - ICMP type, and code (ICMP flows only)



Flow Type ▼	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol
B	12 Oct 2017, 17:53:57	Multiple (20)	Multiple (20)	10.247.1...	34560	tcp_ip
B	12 Oct 2017, 17:53:05	Multiple (257)	Multiple (257)	🇩🇪 194.49.1...	47873	tcp_ip
B	12 Oct 2017, 17:54:00	Multiple (39)	Multiple (39)	🇩🇪 194.49.2...	47873	tcp_ip
B	12 Oct 2017, 17:54:01	Multiple (6)	Multiple (6)	🇩🇪 194.49.2...	47873	tcp_ip
B	12 Oct 2017, 17:54:54	Multiple (13)	Multiple (13)	🇩🇪 194.49.2...	20480	tcp_ip

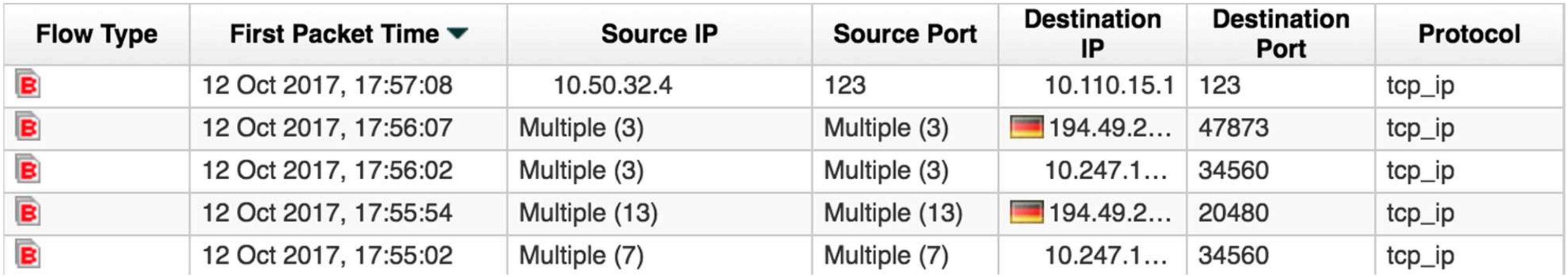
Superflow C

- Port scan – one source and destination, many ports
- Matching:
  - Protocol
  - Source IP
  - Destination IP
  - Source bytes-to-packets ratio
  - TCP flags (TCP flows only)



Flow Type ▼	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol
C	12 Oct 2017, 13:32:42	10.240.120.1	Multiple (162)	🇺🇸 8.8.8.8	Multiple (162)	udp_ip
C	12 Oct 2017, 13:32:02	🇩🇪 194.49.205.93	Multiple (17)	10.232.3...	Multiple (17)	tcp_ip
C	12 Oct 2017, 13:32:36	10.240.120.1	Multiple (174)	🇺🇸 8.8.8.8	Multiple (174)	udp_ip
C	12 Oct 2017, 13:32:20	10.240.120.2	Multiple (254)	🇩🇪 95.131.9...	Multiple (254)	udp_ip
C	12 Oct 2017, 13:32:00	10.240.120.2	Multiple (201)	🇩🇪 95.131.9...	Multiple (201)	udp_ip

Why do I have small superflows?



Flow Type	First Packet Time ▼	Source IP	Source Port	Destination IP	Destination Port	Protocol
B	12 Oct 2017, 17:57:08	10.50.32.4	123	10.110.15.1	123	tcp_ip
B	12 Oct 2017, 17:56:07	Multiple (3)	Multiple (3)	194.49.2…	47873	tcp_ip
B	12 Oct 2017, 17:56:02	Multiple (3)	Multiple (3)	10.247.1…	34560	tcp_ip
B	12 Oct 2017, 17:55:54	Multiple (13)	Multiple (13)	194.49.2…	20480	tcp_ip
B	12 Oct 2017, 17:55:02	Multiple (7)	Multiple (7)	10.247.1…	34560	tcp_ip

- Once the counter exceeds the threshold in an interval, all subsequent matching flows will be bundled into a superflow record to be sent in the following interval.
  - Given a threshold of 100, the first 99 flows will be sent as normal flow records.
  - The 100th flow and beyond will be included in the superflow record.
- The superflow record will continue to be reported in subsequent intervals until no matching traffic has been seen for a full interval.
  - A superflow could be kept alive for several intervals, even if just one flow record matches.

Superflows Default Values

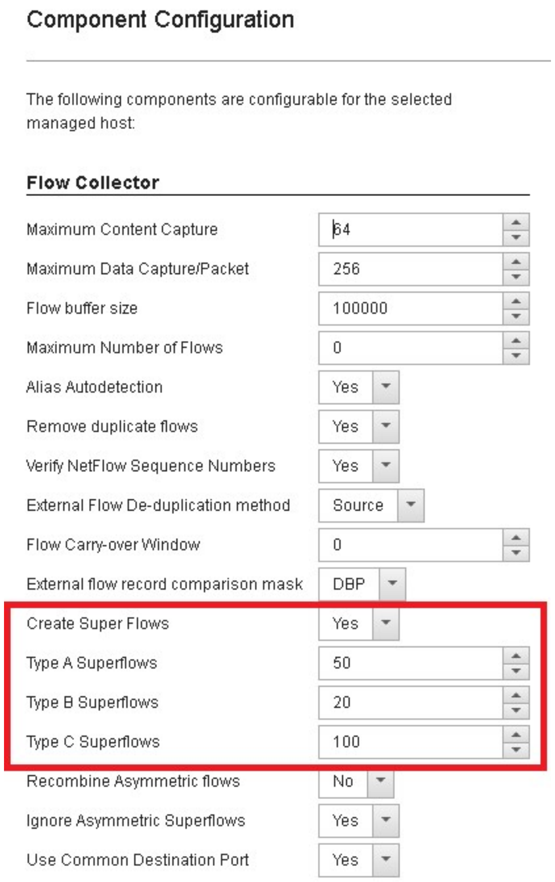
System and License Management

- Super Flows default values can be changed in “System and License Management

- Type A Superflows – 50

- Type B Superflows – 20

- Type C Superflows - 100



Component Configuration

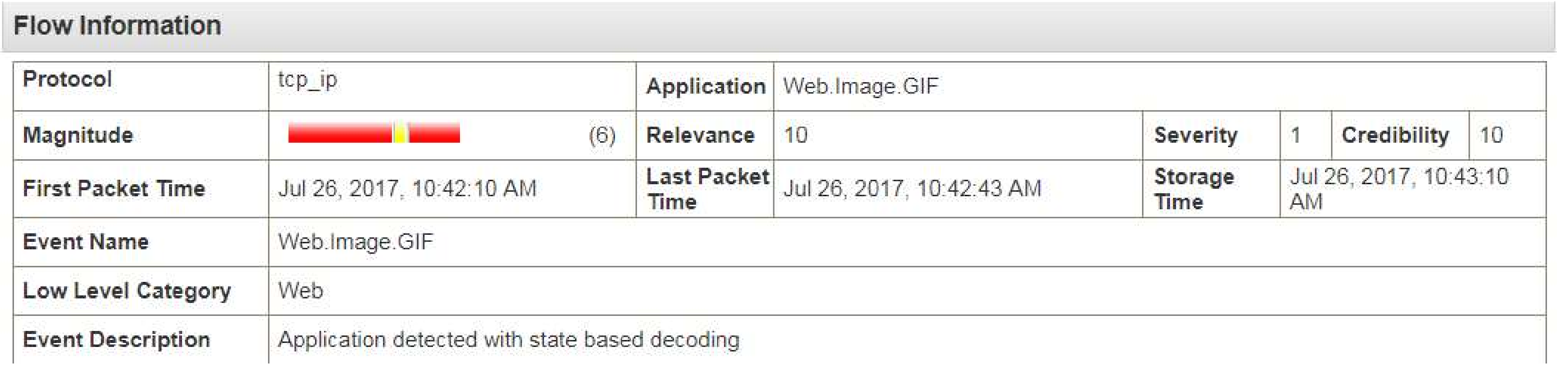
The following components are configurable for the selected managed host:

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

Flow Details

- The Flow Details provides more detailed information:
  - Protocol used in the flow
  - Application
  - Magnitude
  - First, Last Packet and the storage time
  - Event Name and Category
  - Event Description

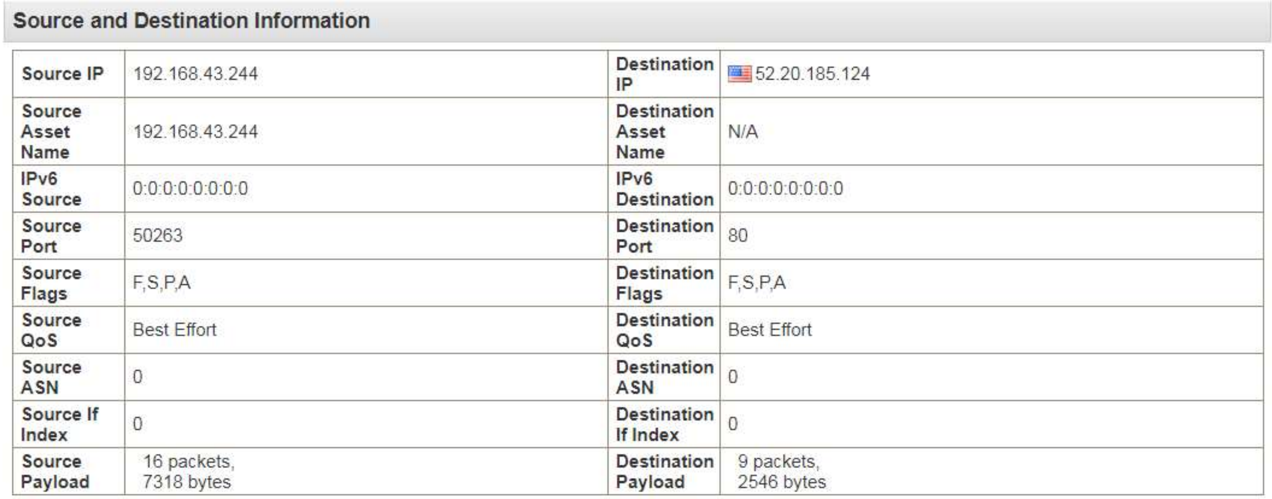


Flow Information

Protocol	tcp_ip	**Application**	Web.Image.GIF				
Magnitude	(6)	**Relevance**	10	**Severity**	1	**Credibility**	10
First Packet Time	Jul 26, 2017, 10:42:10 AM	**Last Packet Time**	Jul 26, 2017, 10:42:43 AM	**Storage Time**	Jul 26, 2017, 10:43:10 AM		
Event Name	Web.Image.GIF						
Low Level Category	Web						
Event Description	Application detected with state based decoding						

Flow Details (Cont)

- The Source and Destination Information of the Flow details include Source and Destination :
  - IP, Asset Names (if applicable), IPV6, Ports, Flags (e.g: FIN, SYN, PSH, ACK)
  - Quality of Service
  - Source and Destination Payload

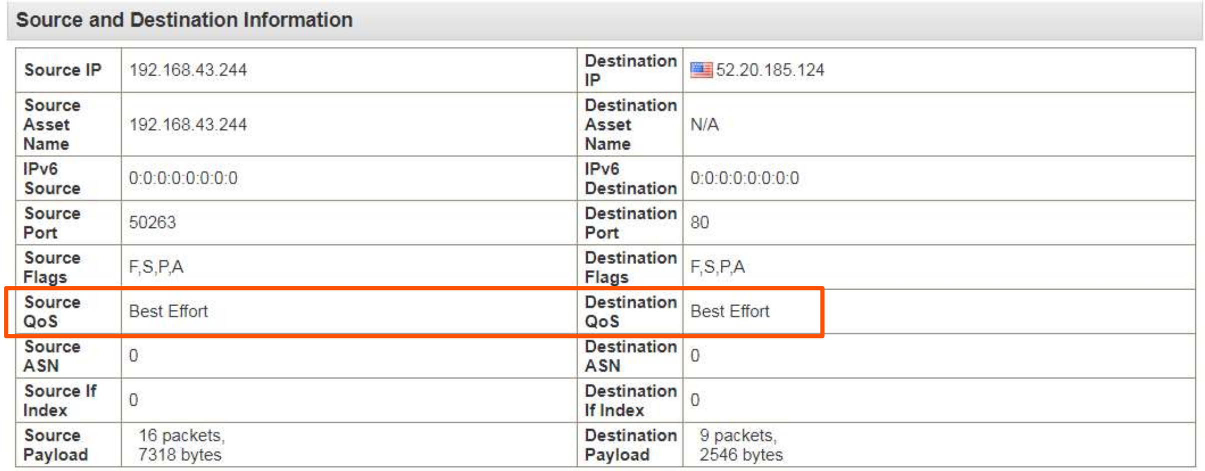


Source and Destination Information

Source IP	192.168.43.244	Destination IP	52.20.185.124
Source Asset Name	192.168.43.244	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	50263	Destination Port	80
Source Flags	F,S,P,A	Destination Flags	F,S,P,A
Source QoS	Best Effort	Destination QoS	Best Effort
Source ASN	0	Destination ASN	0
Source If Index	0	Destination If Index	0
Source Payload	16 packets, 7318 bytes	Destination Payload	9 packets, 2546 bytes

Flow Details (Cont)

- The Source and Destination QoS specifies the Quality of Service (QoS) service level for the flow.
- QoS provides the following basic service levels:
  - **Best Effort** - This service level does not guarantee delivery. The delivery of the flow is considered best effort.
  - **Differentiated Service** - Certain flows are granted priority over other flows. This priority is granted by classification of traffic.
  - **Guaranteed Service** - This service level guarantees the reservation of network resources for certain flows.

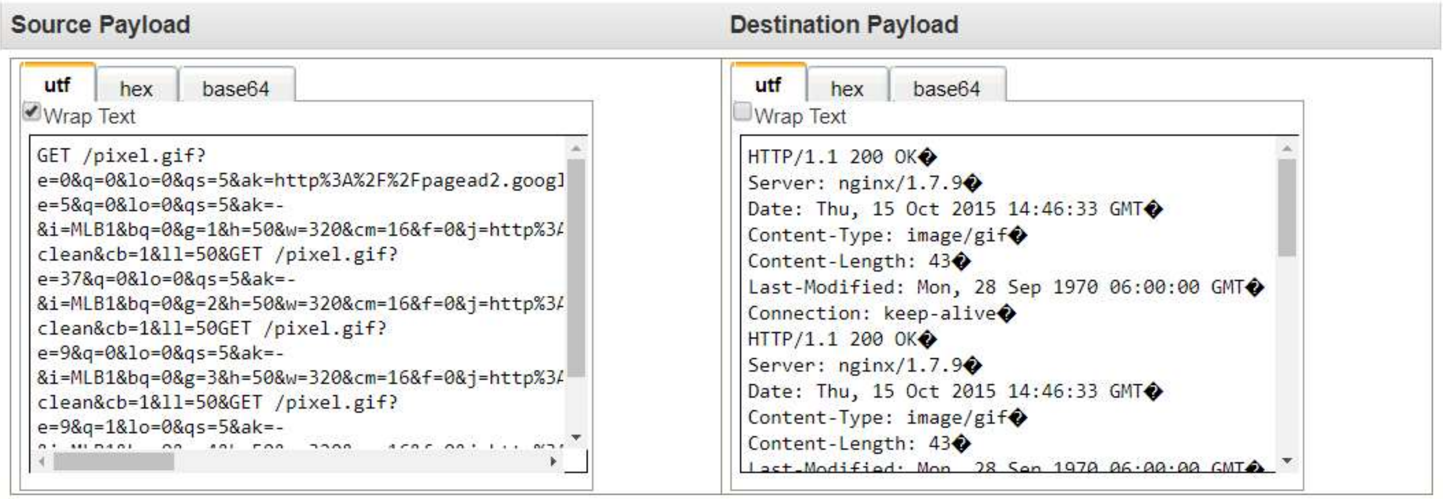


Source and Destination Information

Source IP	192.168.43.244	Destination IP	🇺🇸 52.20.185.124
Source Asset Name	192.168.43.244	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	50263	Destination Port	80
Source Flags	F,S,P,A	Destination Flags	F,S,P,A
Source QoS	Best Effort	Destination QoS	Best Effort
Source ASN	0	Destination ASN	0
Source If Index	0	Destination If Index	0
Source Payload	16 packets, 7318 bytes	Destination Payload	9 packets, 2546 bytes

Flow Details (Cont)

- You can view a snapshot of the Source and Destination Payload.
- QRadar QFlow Collectors can capture a configurable number of bytes at the start of each flow.
- Source and Destination Payload can be viewed in 3 formats: **UTF, HEX and Base 64**



Source Payload

☑ Wrap Text

```
GET /pixel.gif?
e=0&q=0&lo=0&qs=5&ak=http%3A%2F%2Fpagead2.googl
e=5&q=0&lo=0&qs=5&ak=-
&i=MLB1&bq=0&g=1&h=50&w=320&cm=16&f=0&j=http%3A
clean&cb=1&ll=50&GET /pixel.gif?
e=37&q=0&lo=0&qs=5&ak=-
&i=MLB1&bq=0&g=2&h=50&w=320&cm=16&f=0&j=http%3A
clean&cb=1&ll=50GET /pixel.gif?
e=9&q=0&lo=0&qs=5&ak=-
&i=MLB1&bq=0&g=3&h=50&w=320&cm=16&f=0&j=http%3A
clean&cb=1&ll=50&GET /pixel.gif?
e=9&q=1&lo=0&qs=5&ak=-
```

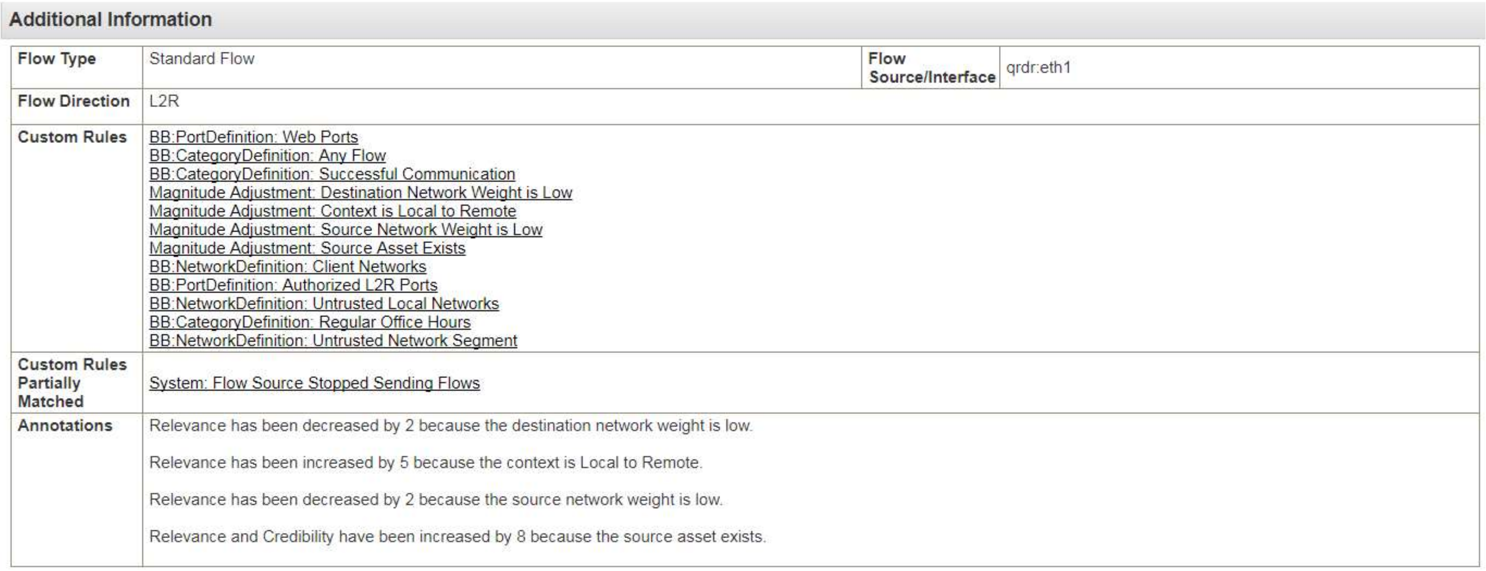
Destination Payload

□ Wrap Text

```
HTTP/1.1 200 OK�
Server: nginx/1.7.9�
Date: Thu, 15 Oct 2015 14:46:33 GMT�
Content-Type: image/gif�
Content-Length: 43�
Last-Modified: Mon, 28 Sep 1970 06:00:00 GMT�
Connection: keep-alive�
HTTP/1.1 200 OK�
Server: nginx/1.7.9�
Date: Thu, 15 Oct 2015 14:46:33 GMT�
Content-Type: image/gif�
Content-Length: 43�
Last-Modified: Mon, 28 Sep 1970 06:00:00 GMT�
```

Flow Details (Cont)

- In the Additional Information you can view
  - Flow Type – (Standard/Superflow)
  - The Flow Direction (L2L, L2R, R2L, R2R)
  - Flow Source/Interface
  - Custom Rules
  - Custom Rules Partially Matched
  - Annotations



Additional Information

Flow Type	Standard Flow	**Flow Source/Interface**	qrdr:eth1
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 Magnitude Adjustment: Source Asset Exists BB:NetworkDefinition: Client Networks BB:PortDefinition: Authorized L2R Ports BB:NetworkDefinition: Untrusted Local Networks BB:CategoryDefinition: Regular Office Hours BB:NetworkDefinition: Untrusted Network Segment		
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. Relevance has been decreased by 2 because the source network weight is low. Relevance and Credibility have been increased by 8 because the source asset exists.		

Network Hierarchy and Geographic data on Flow data

- When looking at Log and/or Network traffic, the country/region defined depends on type of traffic
  - L2L = Other
  - L2R = Destination IP (Looks up in geodata)
  - R2L = Source IP (Looks up in geodata)
  - R2R = Source & Destination IP (Looks up in geodata)

- So no matter what is defined in the Network Hierarchy, the lookup to the geodata.conf file will fill in the info based on the traffic direction.

IBM Security

Determining Applications for Flows

Application determination algorithm

- QFlow has 5 different algorithms to determine the application for a flow:
  - Application signatures
  - State Based Decoding (SBD)
  - QRadar port-based mapping
  - User port-based mapping
  - ICMP protocol mapping
- Flow exporters can also specify an application ID
  - IPFIX using the IBM PEN
  - Packeteer
- The algorithm used will be recorded in the new application determination algorithm field

Application Signatures

- Application detection based on the contents of the signatures.xml file.
- Main element is the “srccontent” or “dstcontent” of a signature:
  - A series of bytes to match against the source or destination payload
  - Starting offset for the search
  - Number of bytes to search (depth)
- This file is user-configurable.

- https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/t_DefAppCfg_guide_mapping_defnewapp.html

State Based Decoding (SBD)

- An internal mechanism for identifying applications by their payload
- Rules for a variety of protocols and applications:
  - aim
  - cerpc
  - ftp
  - h245
  - h323
  - http
  - ipsec
  - mms
  - msn
  - msnfile
  - msnssl
  - msnvideo
  - oracletns
  - rtp
  - rtsp
  - sccp
  - sip
  - skype
  - ssl
  - sunrpc
  - tftp
- Can be disabled if desired – set SBD_APP_DETECTION=NO in the NVA configuration on your console.

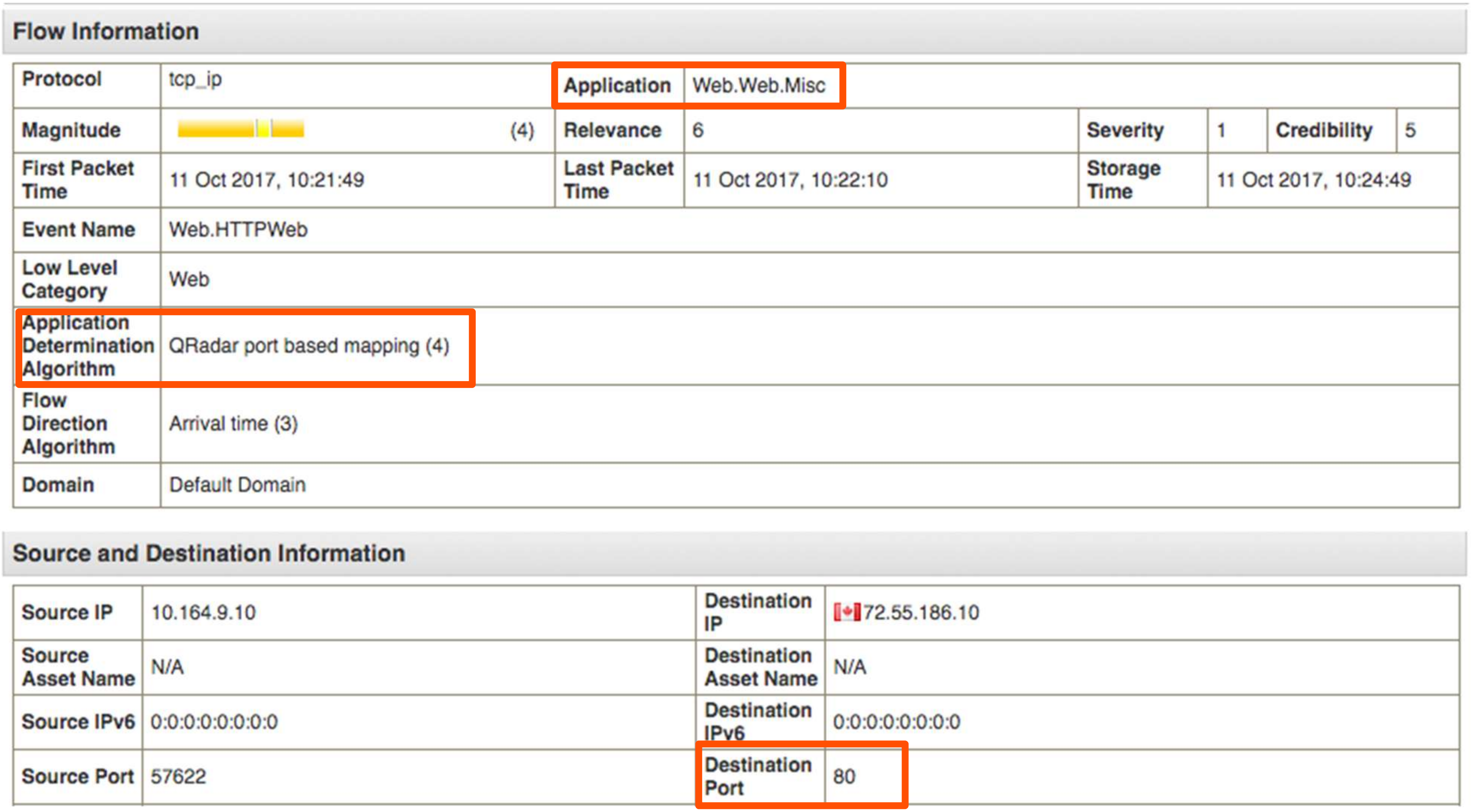
Port-Based Mapping (QRadar-defined and user-defined)

- QRadar port mapping is defined in appid_map.conf.
  - Maps destination ports to application IDs
- User port mapping allows one to define their own custom applications or reclassify incorrectly classified applications through the user_application_mapping.conf file.
- The format of the file is:
  - <New_ID> <Old_ID> <Source_IP_Address>:<Source_Port> <Dest IP Address>: <Dest_Port> <Name>
- https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/t_DefAppCfg_guide_mapping_defappmap.html

ICMP protocol mapping

- Classifies applications based on ICMP Type
- 0-41 IANA assigned types are supported in QRadar
- The remaining unassigned types will be displayed as unknown applications

Application determination algorithm



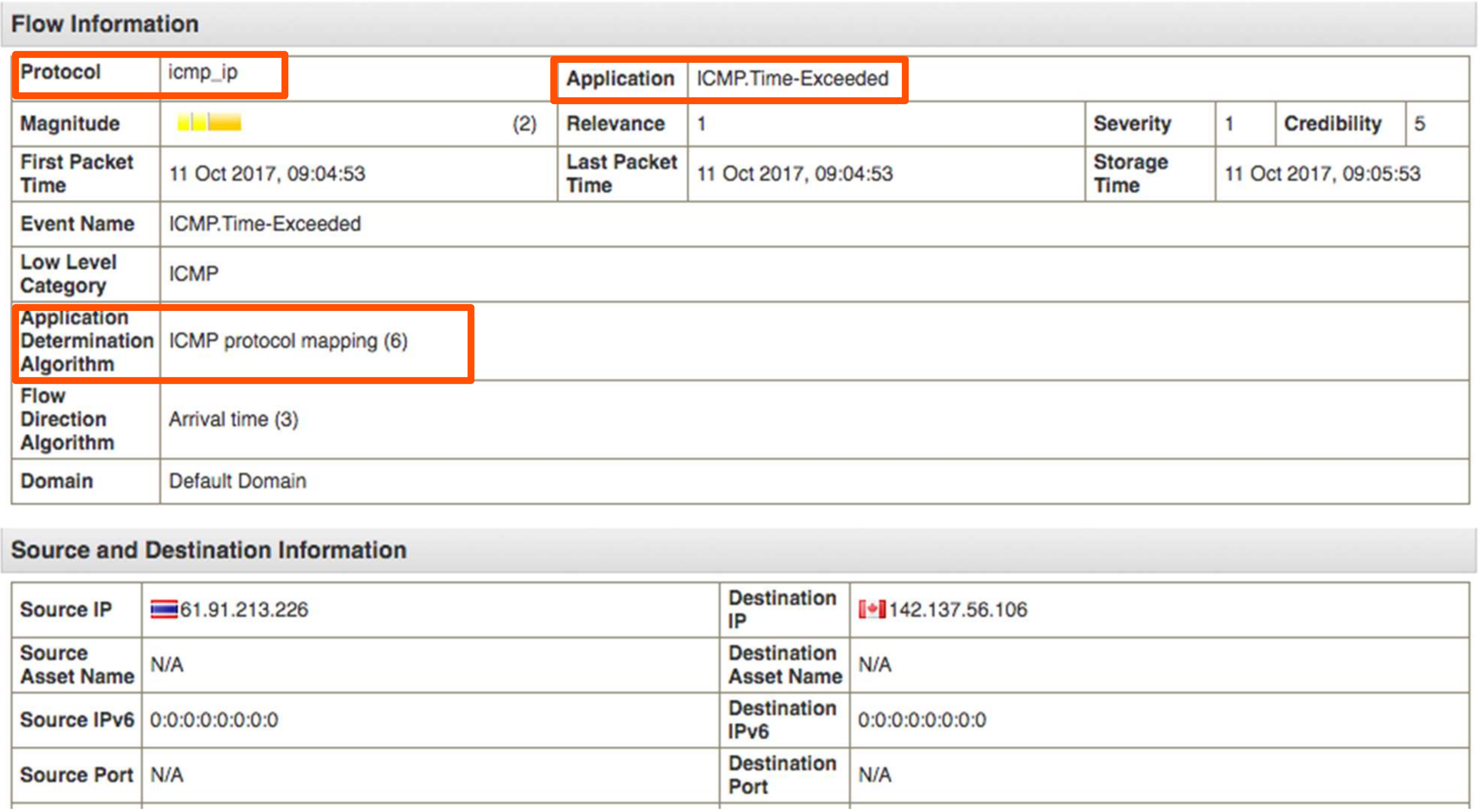
Flow Information

Protocol	tcp_ip	**Application**	Web.Web.Misc				
Magnitude	(4)	**Relevance**	6	**Severity**	1	**Credibility**	5
First Packet Time	11 Oct 2017, 10:21:49	**Last Packet Time**	11 Oct 2017, 10:22:10	**Storage Time**	11 Oct 2017, 10:24:49		
Event Name	Web.HTTPWeb						
Low Level Category	Web						
Application Determination Algorithm	QRadar port based mapping (4)						
Flow Direction Algorithm	Arrival time (3)						
Domain	Default Domain						

Source and Destination Information

Source IP	10.164.9.10	**Destination IP**	🇨🇦72.55.186.10
Source Asset Name	N/A	**Destination Asset Name**	N/A
Source IPv6	0:0:0:0:0:0:0:0	**Destination IPv6**	0:0:0:0:0:0:0:0
Source Port	57622	**Destination Port**	80

Application determination algorithm



Flow Information

Protocol	icmp_ip	Application	ICMP.Time-Exceeded				
Magnitude	(2)	Relevance	1	Severity	1	Credibility	5
First Packet Time	11 Oct 2017, 09:04:53	Last Packet Time	11 Oct 2017, 09:04:53	Storage Time	11 Oct 2017, 09:05:53		
Event Name	ICMP.Time-Exceeded						
Low Level Category	ICMP						
Application Determination Algorithm	ICMP protocol mapping (6)						
Flow Direction Algorithm	Arrival time (3)						
Domain	Default Domain						

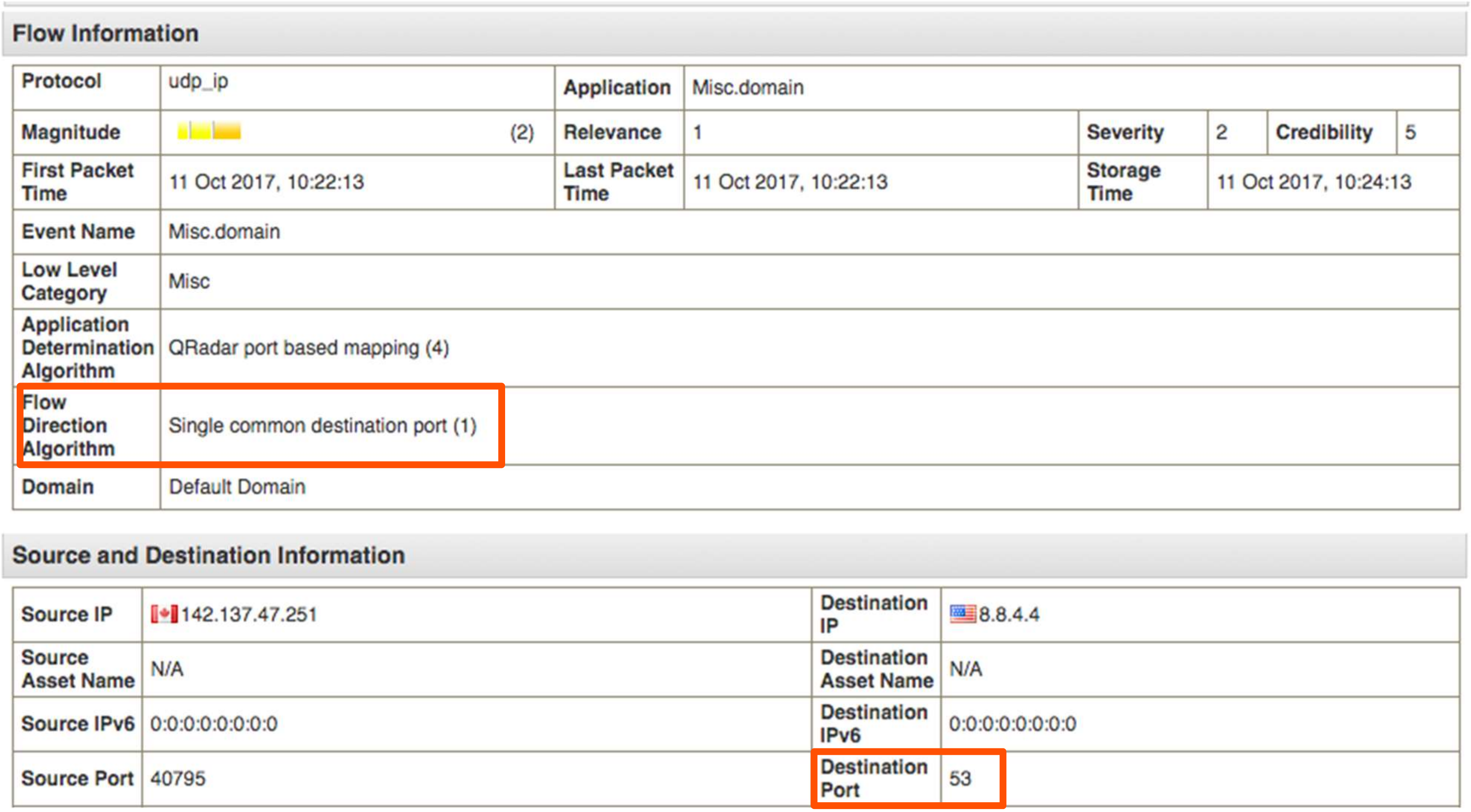
Source and Destination Information

Source IP	61.91.213.226	Destination IP	142.137.56.106
Source Asset Name	N/A	Destination Asset Name	N/A
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source Port	N/A	Destination Port	N/A

Flow direction algorithm

- QFlow will flip the direction of the flow if it has confidence that one side of the flow is a destination
- 3 algorithms could be used to determine the direction
  - Single common destination port
  - Both common destination port, RFC 1700 preferred
  - Arrival time (i.e. left as is, no direction change)
- Terminology:
  - “common destination port” is one which appears in the /opt/qradar/conf/appid_map.conf file
  - “RFC 1700 preferred” are well defined ports in the range of 0 to 1023, controlled and assigned by the IANA
- Packeteer flow exporters bypass these algorithms as they explicitly define direction

Flow direction algorithm



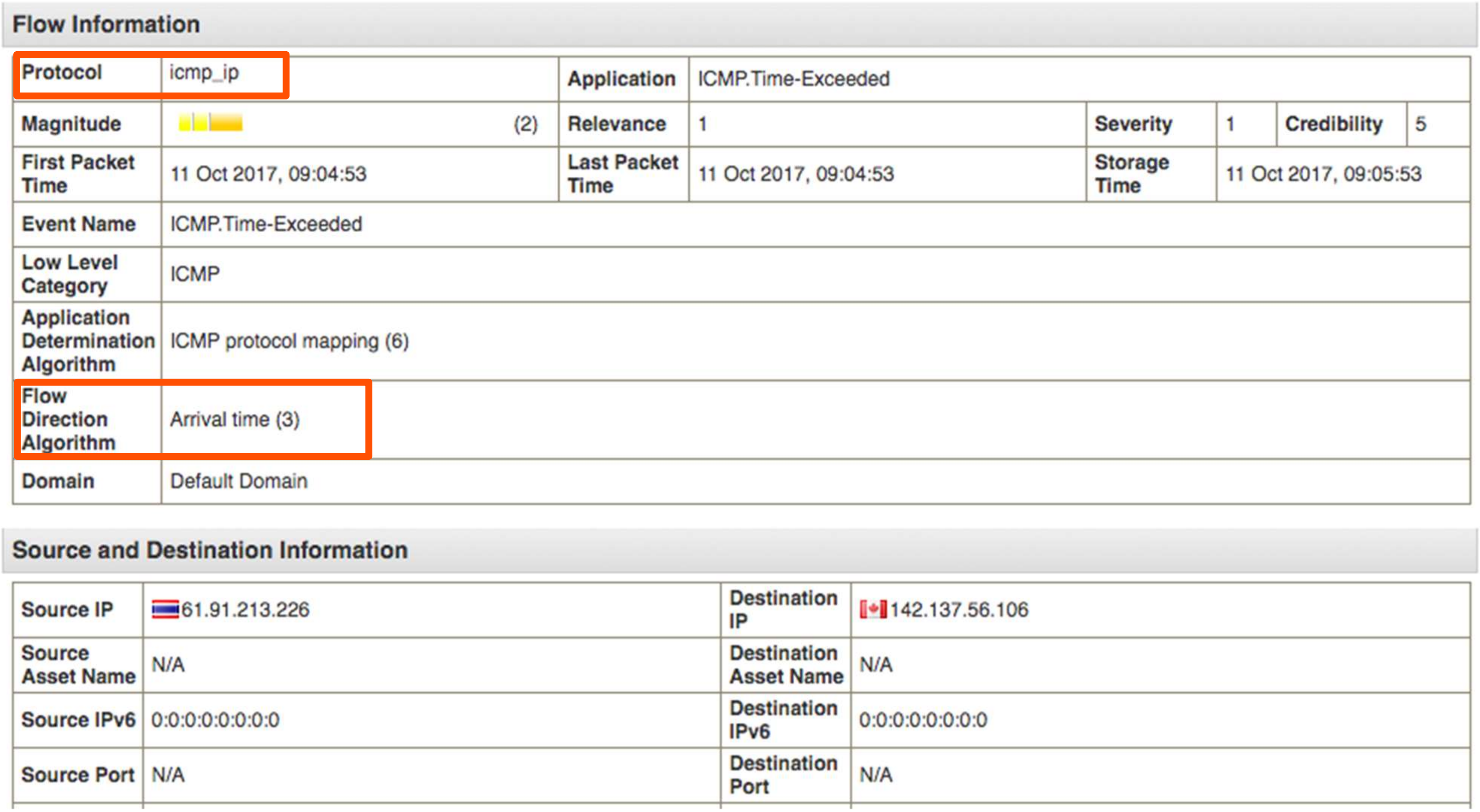
Flow Information

Protocol	udp_ip	Application	Misc.domain				
Magnitude	(2)	Relevance	1	Severity	2	Credibility	5
First Packet Time	11 Oct 2017, 10:22:13	Last Packet Time	11 Oct 2017, 10:22:13	Storage Time	11 Oct 2017, 10:24:13		
Event Name	Misc.domain						
Low Level Category	Misc						
Application Determination Algorithm	QRadar port based mapping (4)						
Flow Direction Algorithm	Single common destination port (1)						
Domain	Default Domain						

Source and Destination Information

Source IP	142.137.47.251	Destination IP	8.8.4.4
Source Asset Name	N/A	Destination Asset Name	N/A
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source Port	40795	Destination Port	53

Flow direction algorithm



Flow Information

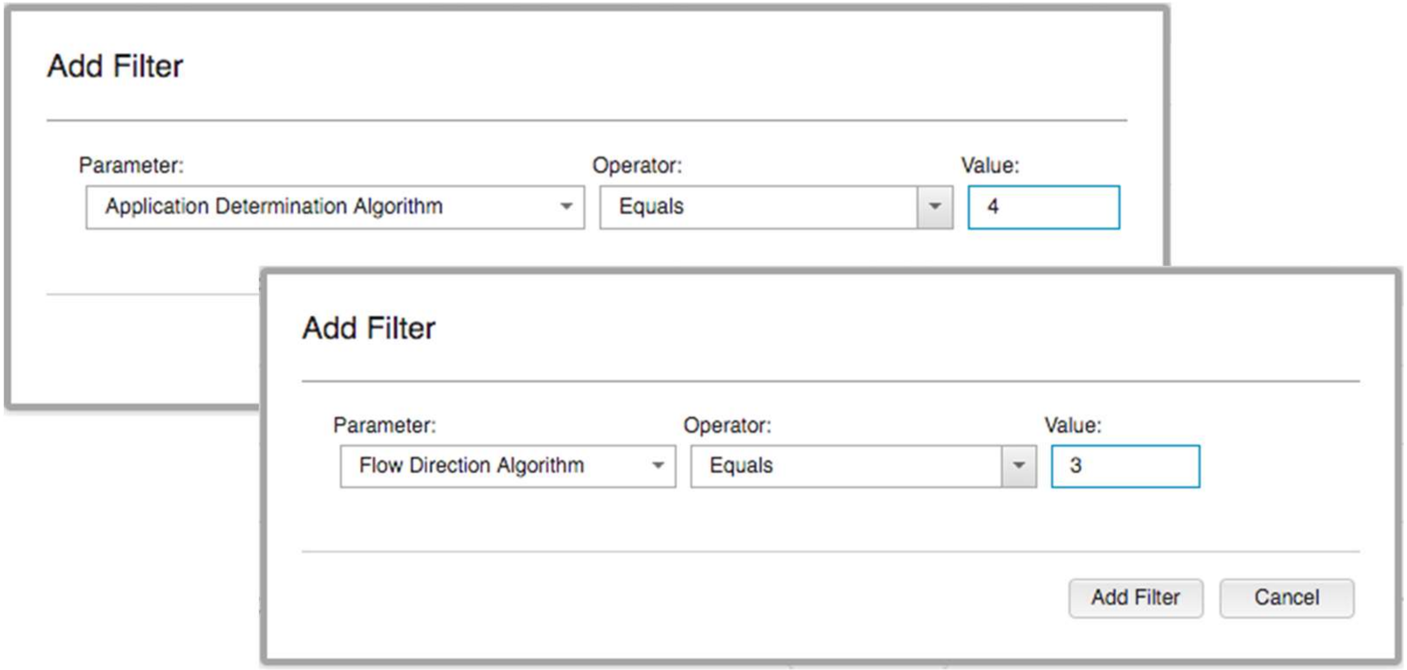
Protocol	icmp_ip	**Application**	ICMP.Time-Exceeded				
Magnitude	(2)	**Relevance**	1	**Severity**	1	**Credibility**	5
First Packet Time	11 Oct 2017, 09:04:53	**Last Packet Time**	11 Oct 2017, 09:04:53	**Storage Time**	11 Oct 2017, 09:05:53		
Event Name	ICMP.Time-Exceeded						
Low Level Category	ICMP						
Application Determination Algorithm	ICMP protocol mapping (6)						
Flow Direction Algorithm	Arrival time (3)						
Domain	Default Domain						

Source and Destination Information

Source IP	61.91.213.226	**Destination IP**	142.137.56.106
Source Asset Name	N/A	**Destination Asset Name**	N/A
Source IPv6	0:0:0:0:0:0:0:0	**Destination IPv6**	0:0:0:0:0:0:0:0
Source Port	N/A	**Destination Port**	N/A

Application and flow direction algorithms

- Available in the Add Filter dialog



Add Filter

Parameter: Application Determination Algorithm

Operator: Equals

Value: 4

Add Filter

Parameter: Flow Direction Algorithm

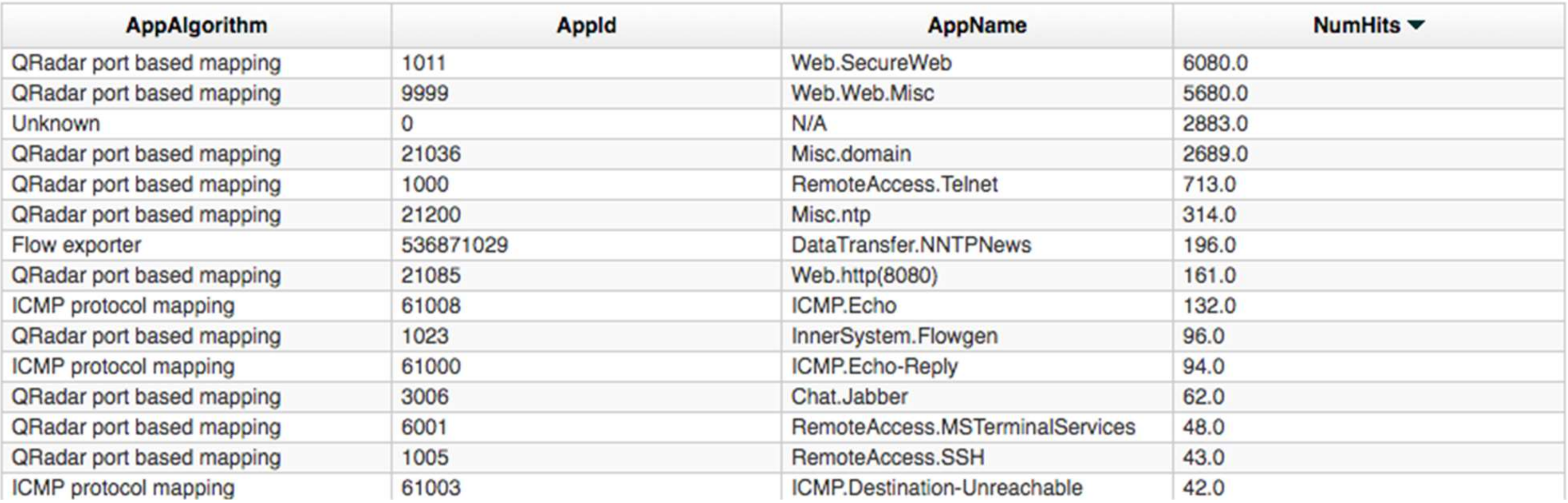
Operator: Equals

Value: 3

Application and flow direction algorithms

- Available in advanced AQL searches

```
SELECT  LOOKUP('application determination algorithm', "application determination algorithm") as AppAlgorithm,
        applicationid as AppId,
        APPLICATIONNAME(applicationid) as AppName,
        COUNT(*) as NumHits
FROM flows
GROUP BY AppAlgorithm, applicationid
ORDER BY NumHits DESC
```



AppAlgorithm	AppId	AppName	NumHits ▼
QRadar port based mapping	1011	Web.SecureWeb	6080.0
QRadar port based mapping	9999	Web.Web.Misc	5680.0
Unknown	0	N/A	2883.0
QRadar port based mapping	21036	Misc.domain	2689.0
QRadar port based mapping	1000	RemoteAccess.Telnet	713.0
QRadar port based mapping	21200	Misc.ntp	314.0
Flow exporter	536871029	DataTransfer.NNTPNews	196.0
QRadar port based mapping	21085	Web.http(8080)	161.0
ICMP protocol mapping	61008	ICMP.Echo	132.0
QRadar port based mapping	1023	InnerSystem.Flowgen	96.0
ICMP protocol mapping	61000	ICMP.Echo-Reply	94.0
QRadar port based mapping	3006	Chat.Jabber	62.0
QRadar port based mapping	6001	RemoteAccess.MSTerminalServices	48.0
QRadar port based mapping	1005	RemoteAccess.SSH	43.0
ICMP protocol mapping	61003	ICMP.Destination-Unreachable	42.0

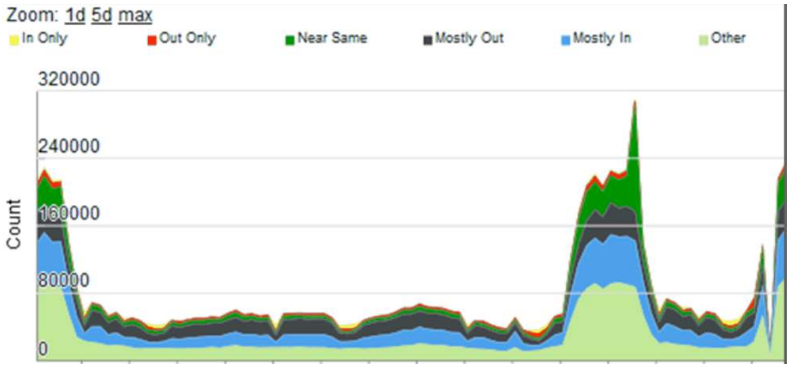
IBM Security

Flow Bias

IBM

Flow Bias

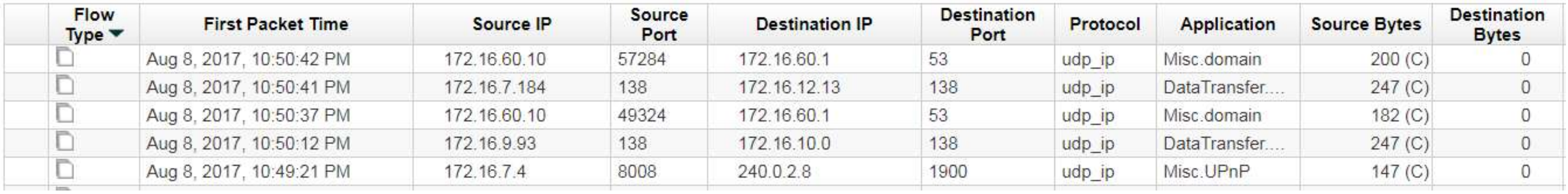
- Flow Bias is used to describe the relative **size**, or **data transfer** bias, of a flow, based on transfer into or out of the network, where local network resources are defined as those entered into the Network Hierarchy.
- Any address not defined in the Network Hierarchy are thus ‘unknown’, and are effectively considered as external or ‘Remote’.
- **In/Out** Bias requires traffic to be entering into or leaving your network.



Flows in	Flows out	Flow Bias
0%	100%	**Out Only**
1% to 30%	70% to 99%	**Mostly Out**
31% to 69%	31% to 69%	**Near Same**
70% to 99%	1% to 30%	**Mostly In**
100%	0%	**In Only**

Flow Bias - In/Out Only

- **In/Out Only** Communication
  - These are considered Unidirectional Flows, one way only, where there are only bytes & packet counts on the Source or Destination address, but not **both.**
- **In/Out Only** traffic can indicate: Host or network scanning.
- Communication that is being blocked by a Firewall/IDS.
- The QRadar Flow collector is not seeing the other side of the traffic due to a problem with a span or tap being mis-configured.
- A routing issue at the network level, where external traffic is actually entering, then exiting your network.
- External flow (Netflow) data collection not sending both sides of a communication. For example you are only seeing traffic on an inbound communication, but not the corresponding outbound communication.



Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes
□	Aug 8, 2017, 10:50:42 PM	172.16.60.10	57284	172.16.60.1	53	udp_ip	Misc.domain	200 (C)	0
□	Aug 8, 2017, 10:50:41 PM	172.16.7.184	138	172.16.12.13	138	udp_ip	DataTransfer....	247 (C)	0
□	Aug 8, 2017, 10:50:37 PM	172.16.60.10	49324	172.16.60.1	53	udp_ip	Misc.domain	182 (C)	0
□	Aug 8, 2017, 10:50:12 PM	172.16.9.93	138	172.16.10.0	138	udp_ip	DataTransfer....	247 (C)	0
□	Aug 8, 2017, 10:49:21 PM	172.16.7.4	8008	240.0.2.8	1900	udp_ip	Misc.UPnP	147 (C)	0

Flow Bias - Out/In

- **Mostly Out/In** Communication
  - The ratio on these Flows is more than 70% in one direction.
  - For most enterprise users, the majority of your traffic should be **Mostly In**, if most of your endpoints are user workstations, which would be pulling information towards the local workstations.
  - **Mostly out**, could represent local file or web servers, which are sending out more data in the form of html responses or file downloads than they are receiving URL requests.
  - An example use case for monitoring for DLP in QRadar, is to watch your user segments for "**Mostly Out**" traffic, indicating some sort of large outbound file transfer.

Flow Bias - Near Same

- **Near Same** Communication
- The ratio of these flows is between 30% and 70% per direction.
- **Near Same** communication is not as common as **Mostly In/Out**.

  Examples of Near Same could be: Video conference call, where video streams are Inbound & Outbound.
- VOIP voice call, where audio streams are both Inbound & Outbound.
- Interactive (text based) user session, where a user is navigating around a command line based operating system, such as SSH or Telnet.
- Internet messaging or chat applications.
- Any other example, where two hosts are connected directly, and would send and receive similar amounts of data.

Flow Bias – Other

- Local to Local (Internal) and Remote to Remote (both Source and Destination address unknown) traffic.
- If you are monitoring Internal Network Points within your organization, you should expect to see a fair amount of **Other** or **Local to Loca**l data.
- If you see a large amount of “Other” or “Remote to Remote”, it is often the case that one of the IP address ranges in use on your network was not included in the Network Hierarchy.
- It can also be an indicator of some device on your network being incorrectly configured with a non-internal address range, or perhaps some device is spoofing an internet based IP address, although this is normally quite rare.
- ISP users may see a large amount of Communication if they have a large internet transit point and do not define all their customer downstream networks within their Hierarchy.
- A **rare** possibility is that you are seeing traffic in your network that should not be there.
- Another possibility is that something on your network, by design (malicious intent) or by mis-configuration, is spoofing or using an incorrect, **Non-Loca**l defined IP Address.

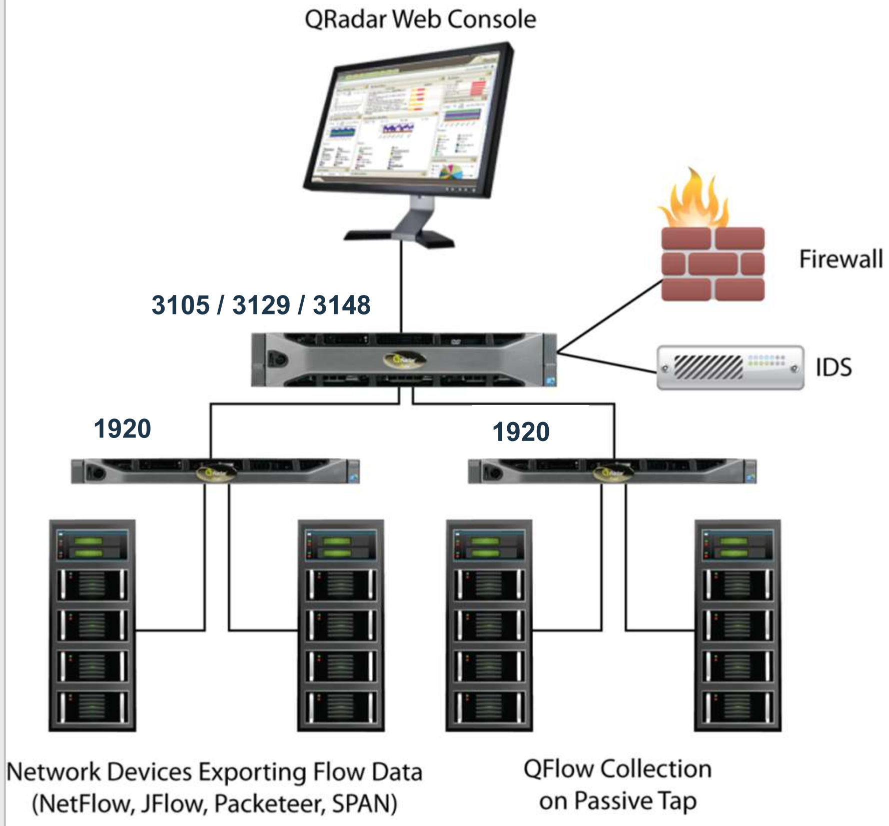
IBM Security

Flow Collector and Processor Appliances

IBM

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

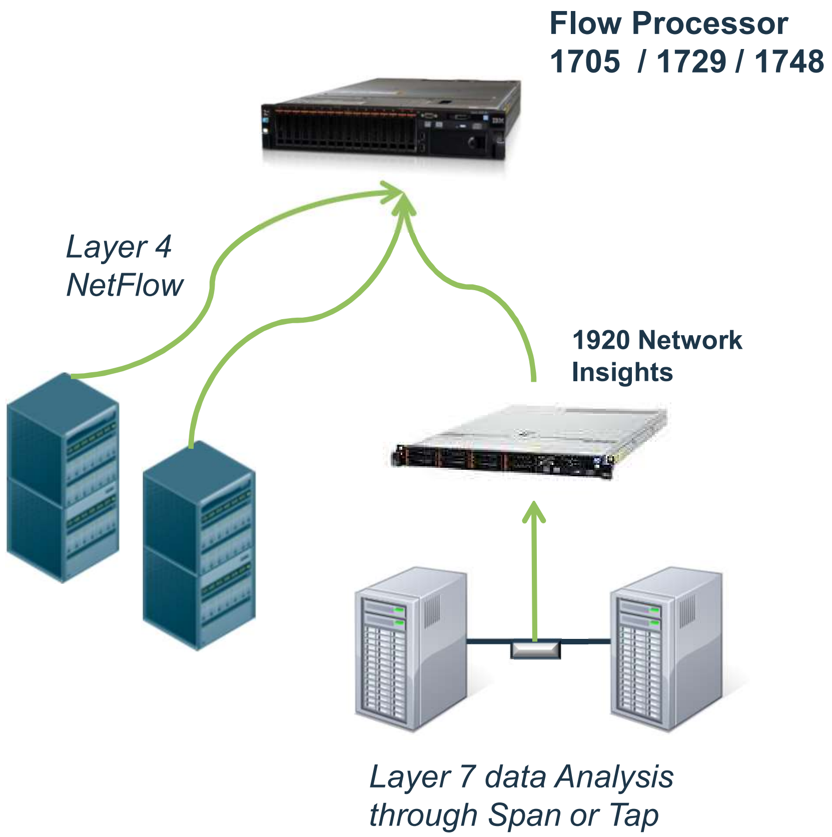
- **Positioning**
  - – QRadar appliance for centralized deployment in a small/medium/large enterprise
  - – Contains event & flow processing capabilities
- **Characteristics and Capacity**
  - ▪**Memory Capacity**
  - - 3015 – 64 GB
  - - 3129/3128-C/3148 – 128 GB
  - – Requires ***external*** QFlow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


QRadar Web Console
Firewall
3105 / 3129 / 3148
IDS
1920
1920
Network Devices Exporting Flow Data (NetFlow, JFlow, Packeteer, SPAN)
QFlow Collection on Passive Tap

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**

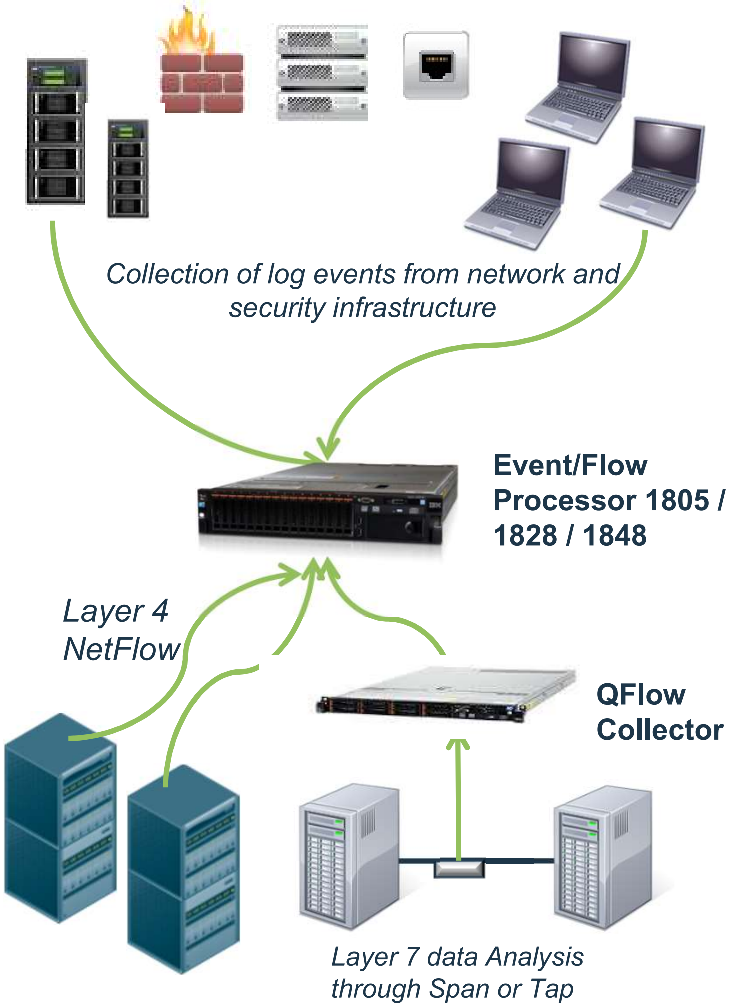
*May vary based on configuration



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


Collection of log events from network and security infrastructure
Event/Flow Processor 1805 / 1828 / 1848
Layer 4 NetFlow
QFlow Collector
Layer 7 data Analysis through Span or Tap

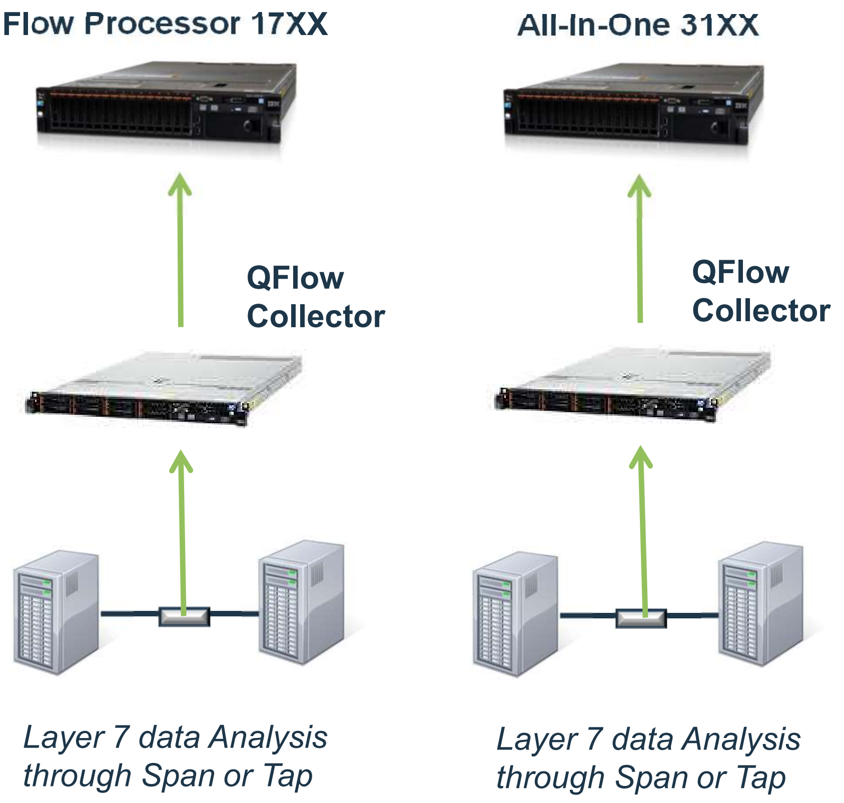
QFlow Collector 1201, 1202, 1301, and 1310 Appliances

- **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:
    - 1202 – 3 Gbps (Copper Inserts)
    - 1301 – 3 Gbps (Fiber Inserts)
    - 1310-SR – 10 Gbps (Short Range Inserts)
    - 1310-LR – 10 Gbps (Long Range Inserts)
    - 1202/1301-C – 3 Gbps (Copper & Fiber Inserts Included)
    - 1310SR/LR-C – 10 Gbps (Short and Long Range Inserts Included
- **Upgradability**
  - – No upgrade available

–**HA/DR NOT available**

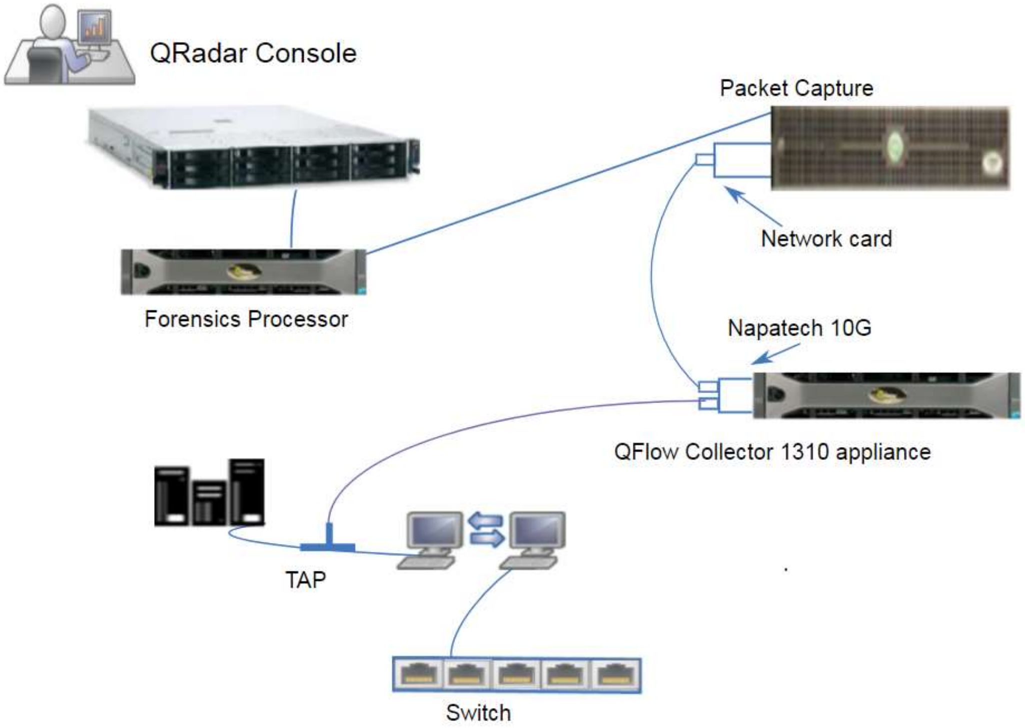
QFlow Collector can send collected layer 7 application data to a Flow Processor or a Console directly.



Flow Processor 17XX
All-In-One 31XX
QFlow Collector
QFlow Collector
Layer 7 data Analysis through Span or Tap
Layer 7 data Analysis through Span or Tap

Configuring a QRadar QFlow Collector

- You can monitor network traffic by sending raw data packets to a IBM QRadar QFlow Collector 1310 appliance.
- The QRadar QFlow Collector uses a dedicated Napatech monitoring card to copy incoming packets from one port on the card to a second port that connects to a IBM Security QRadar Packet Capture appliance.
- If you already have a QRadar QFlow Collector 1310 with a 10G Napatech network card, you can mirror the traffic to QRadar Packet Capture.
- As shown in the following diagram, if you already have a QRadar QFlow Collector 1310 with a 10G Napatech network card, you can mirror the traffic to QRadar Packet Capture.



IBM Security

Introduction to QRadar Network Insights (QNI)

IBM

Taking network analysis to the next level

***QRadar Incident Forensics and Network Packet Capture** will capture, reconstruct and replay the entire conversation*

Incident Response

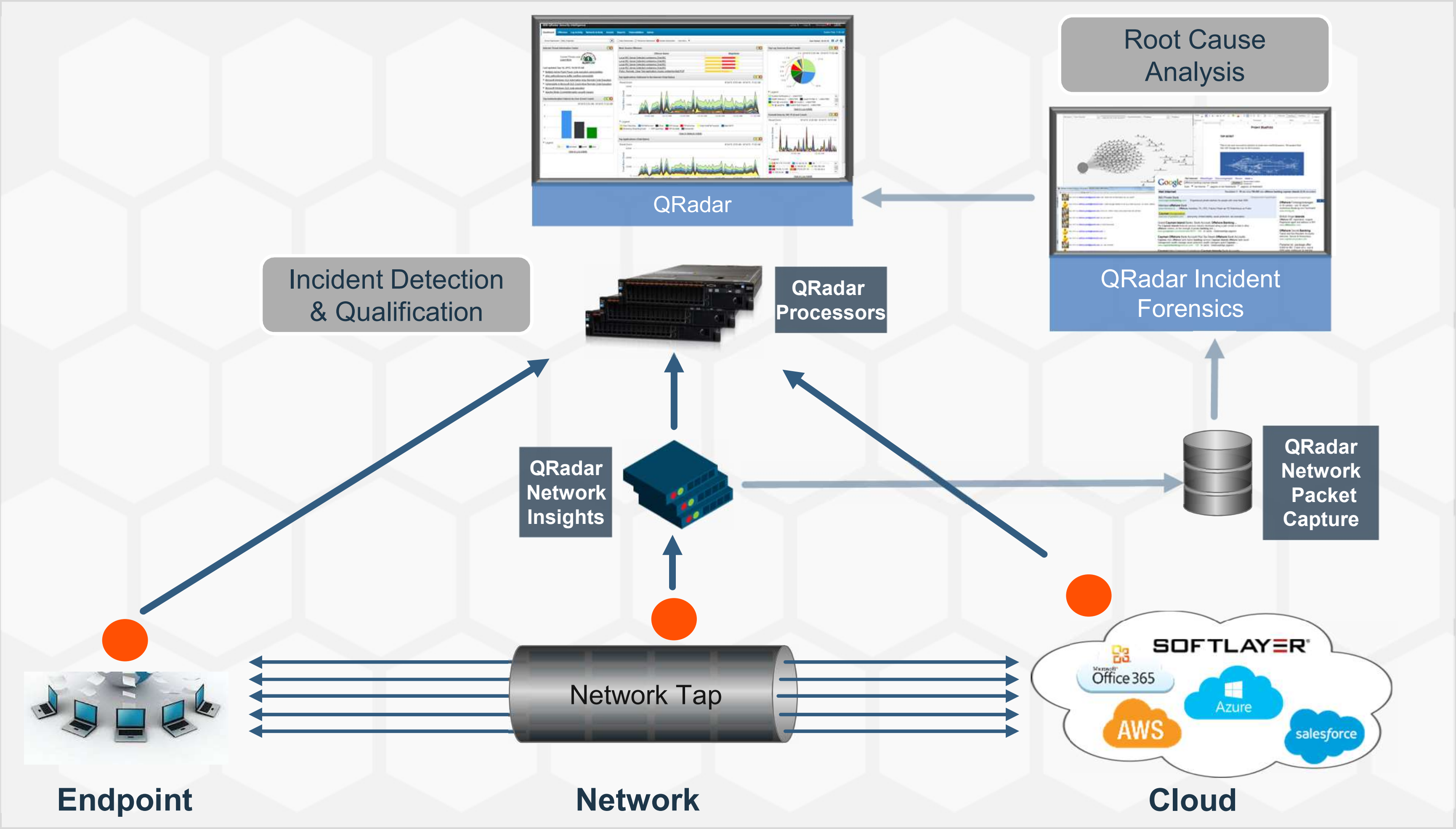
Incident Detection

***QRadar Network Insights** will also let you know if suspect items or topics of interest were discussed at anytime during the conversation*

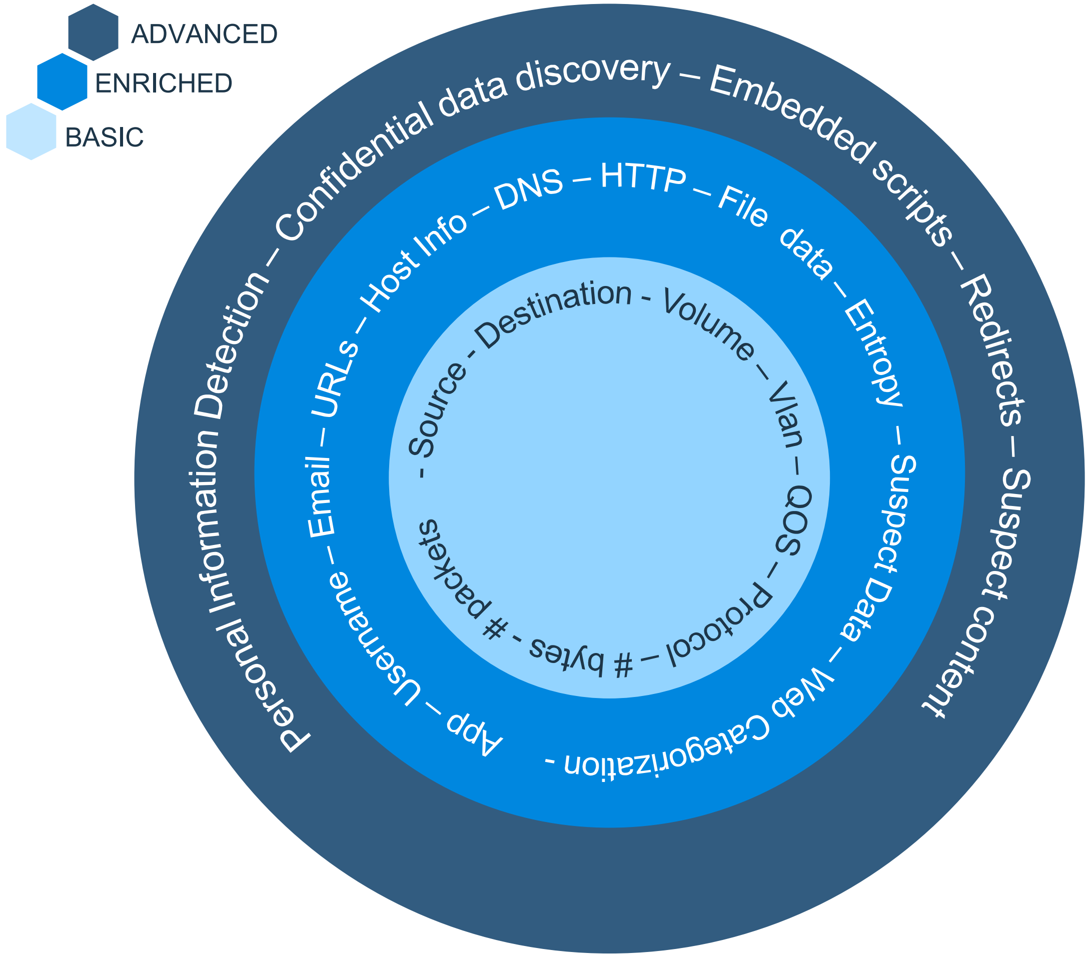
***QFlow** provides all the benefits of network flows but will also recognize layer 7 applications and allows you to capture the beginning of the sessions*

*"**A network flow** is, in essence, a record of a given conversation between two hosts on a network… this information is much like a phone bill: you can't tell what was said during the conversation, but you can use it to prove who talked to who"*
– SANS Institute

Providing complete coverage and threat detection



QRadar QNI – Completing the picture



ADVANCED

ENRICHED

BASIC

Personal Information Detection – Confidential data discovery – Embedded scripts – Redirects – Suspect content

App – Username – Email – URLs – Host Info – DNS – HTTP – File data – Entropy – Suspect Data – Web Categorization -

- Source - Destination - Volume – Vlan – QOS – Protocol – # bytes - # packets

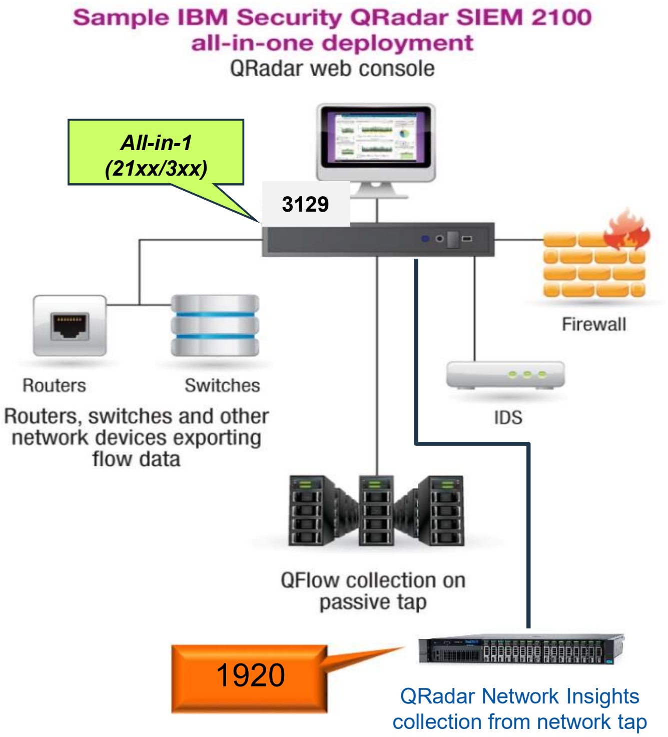
Filling in the important gaps

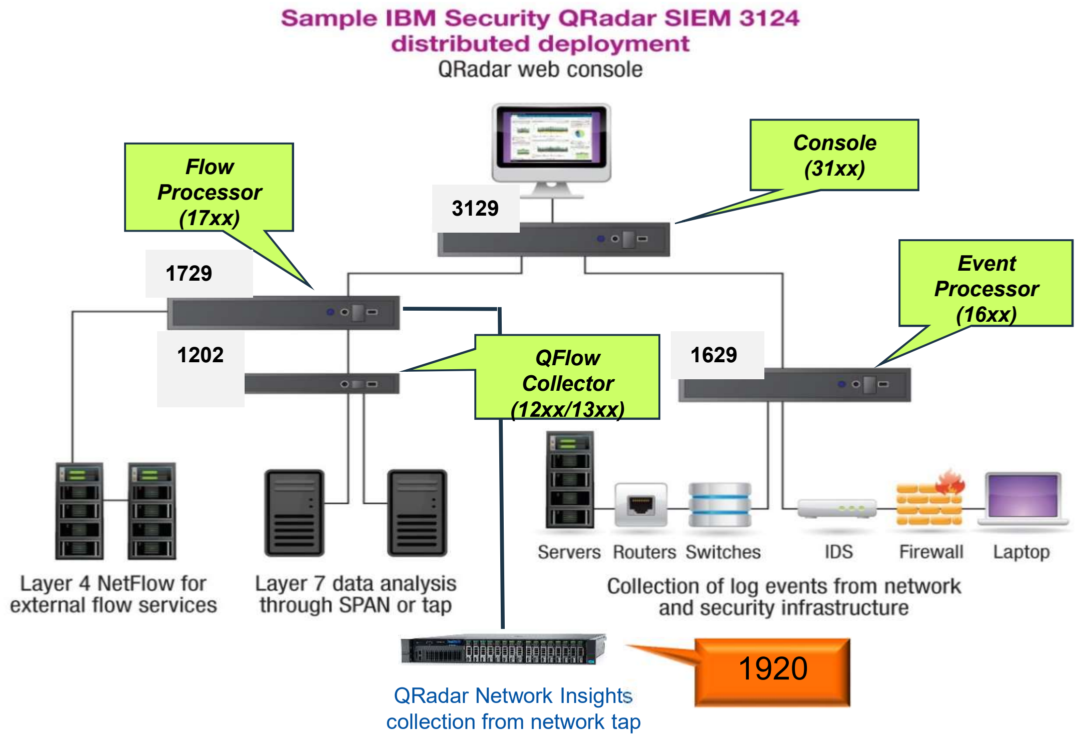
- What is out there ?
- Who is talking to whom ?
- What files and data are being exchanged ?
- Do they look malicious ?
- Do they contain any important or sensitive data ?
- Is this malicious application use ?
- Is this new threat on my network ?
- If so, it where is it and what did it do ?

IBM Security

Architecture, Sizing & Appliance Specifications

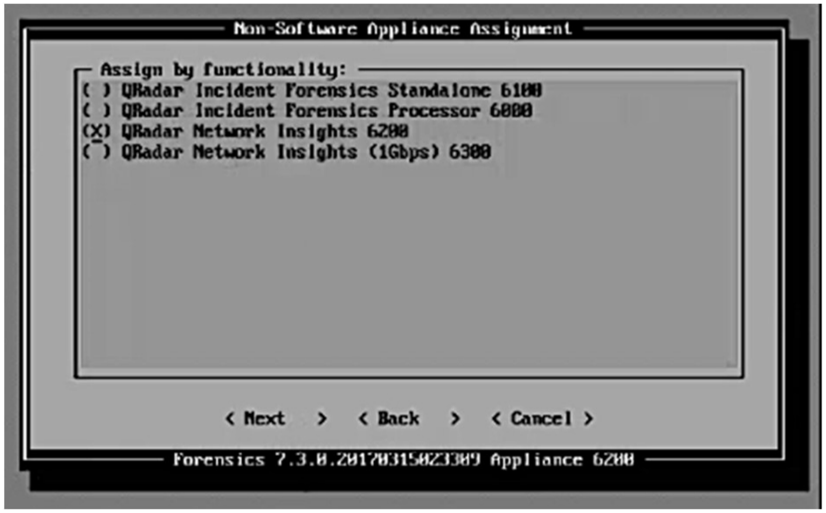
QRadar Network Insights Deployment Models


Sample IBM Security QRadar SIEM 2100
all-in-one deployment
QRadar web console
All-in-1
(21xx/3xx)
3129
Firewall
Routers
Switches
Routers, switches and other network devices exporting flow data
IDS
QFlow collection on passive tap
1920
QRadar Network Insights collection from network tap


Sample IBM Security QRadar SIEM 3124
distributed deployment
QRadar web console
Flow
Processor
(17xx)
3129
Console
(31xx)
1729
Event
Processor
(16xx)
1202
QFlow
Collector
(12xx/13xx)
1629
Servers
Routers
Switches
IDS
Firewall
Laptop
Layer 4 NetFlow for external flow services
Layer 7 data analysis through SPAN or tap
Collection of log events from network and security infrastructure
1920
QRadar Network Insights collection from network tap

QRadar Network Insights

- IBM® QRadar® Network Insights is a managed host that you attach to the QRadar console.
- For a QRadar Network Insights deployment, you must select the 6200 appliance option during the installation.
- QRadar Network Insights requires a separate license for the 6200 appliance
- QRadar Network Insights requires only a connection to the QRadar console or a Flow Processor



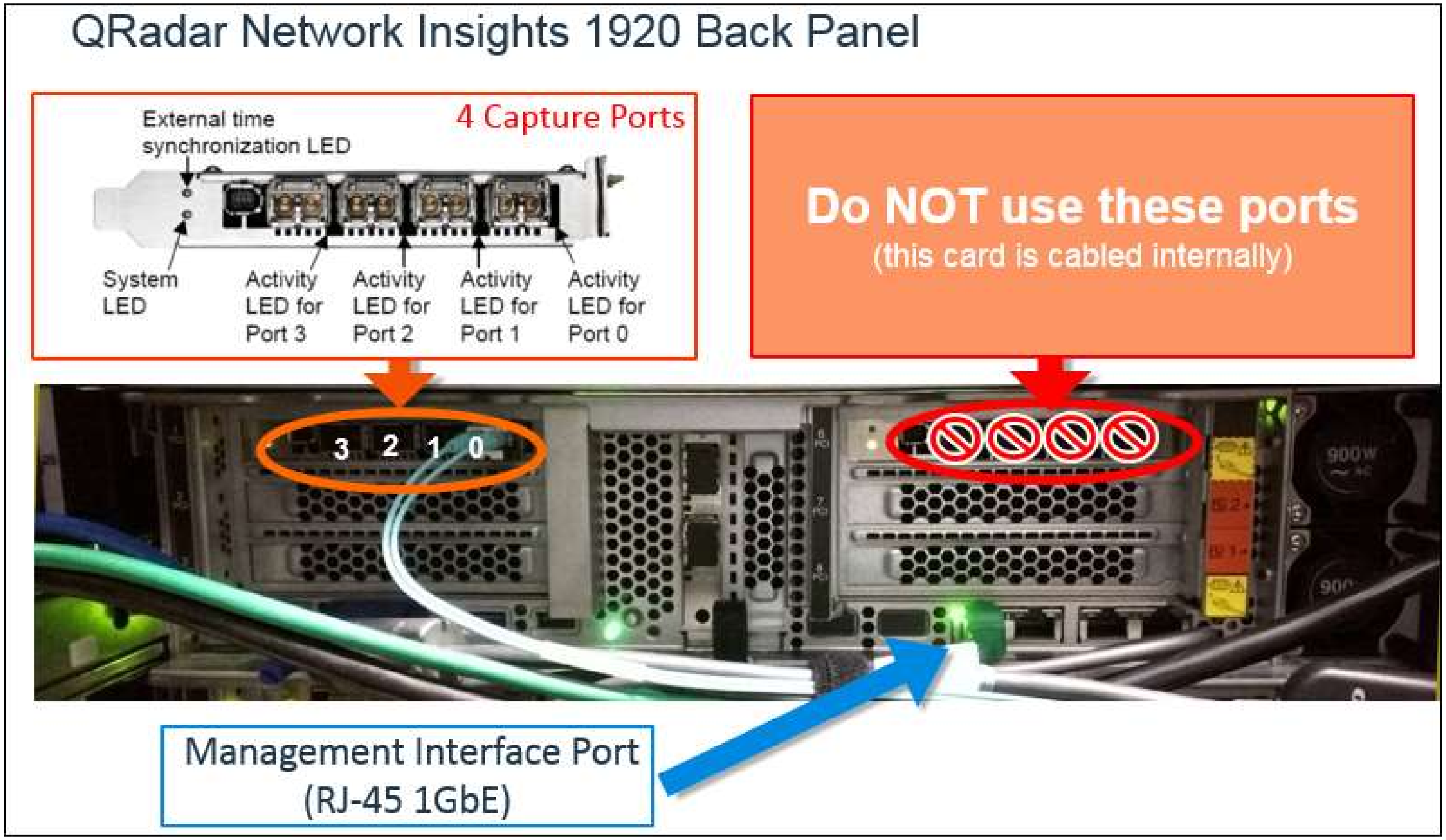
```
Non-Software Appliance Assignment

Assign by functionality:
( ) QRadar Incident Forensics Standalone 6100
( ) QRadar Incident Forensics Processor 6000
(X) QRadar Network Insights 6200
( ) QRadar Network Insights (1Gbps) 6300

< Next    >  < Back    >  < Cancel >

Forensics 7.3.0.20170315023309 Appliance 6200
```

QRadar Network Insights Appliances

- The IBM® Security QRadar® Network Insights 1920 (MTM 4412-F3F) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM Security QRadar.
- 10Gbps connectivity with 4 ports available (by default captures on all 4 ports).
  - Note: Overall appliance performance limited to 10Gbps.
  - Configurable flow forwarding capability enables load-balancing across multiple appliances.
  - Hardware configuration optimized to reduce costs and facilitate in-memory processing.
- Transceivers included with Appliance **and** available as standalone orderable Option PNs.

Appliance	Server	CPU	RAM	HDD	ServeRAID	I/O Cards	P/S
1920	X3650 M5	2x E5-2680 v4 14C 2.4GHz 35MB 2400MHz 120W	8x 16GB	2 x 200GB SSD	M1215	Intel X520 2P 10GbE + 2x 10G SR 2x NT40E3 4P 40G + 2x 10G SR + 2x 10G LR	2x 900W

QRadar Network Insights Appliances



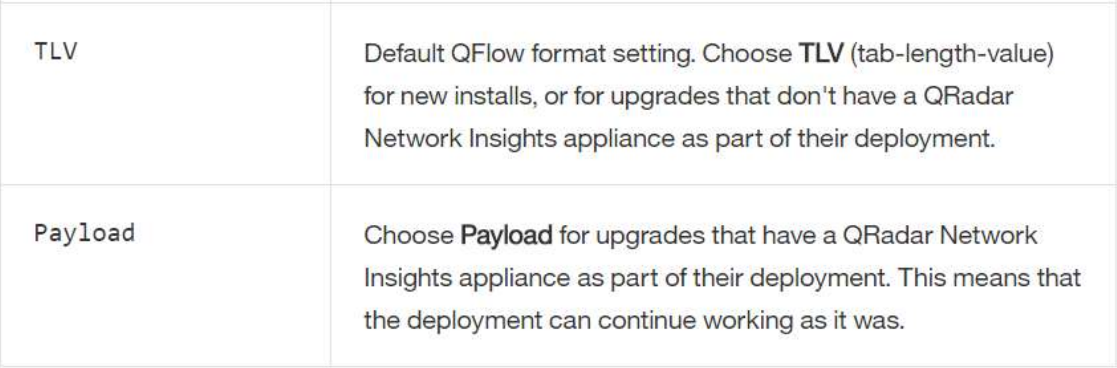
QRadar Network Insights Appliances

- The IBM® Security QRadar® Network Insights 1901 (MTM 4412-F4Y) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM Security QRadar.
- The QRadar Network Insights 1901 appliance provides the same capabilities as the QRadar Network Insights 1920 appliance but on a lower-price hardware platform that is designed for 1 Gbps network connectivity.

Appliance	Server	CPU	RAM	HDD	ServeRAID	I/O Cards	P/S
1901	X3550 M5	X1 E5-2680 v4 14C 2.4GHz 35MB Cache 2400MHz 120W	X4 16GB	X2 S3710 200GB Enterprise Performance SATA G3HS 2.5" SSD	M1215 / RAID 1	Intel X520 2P 10GbE + x2 10G SR NT40E3 4P 1GbE + x2 SFP SX + 2 SFP CU	X2 750W

Configure Network Insights

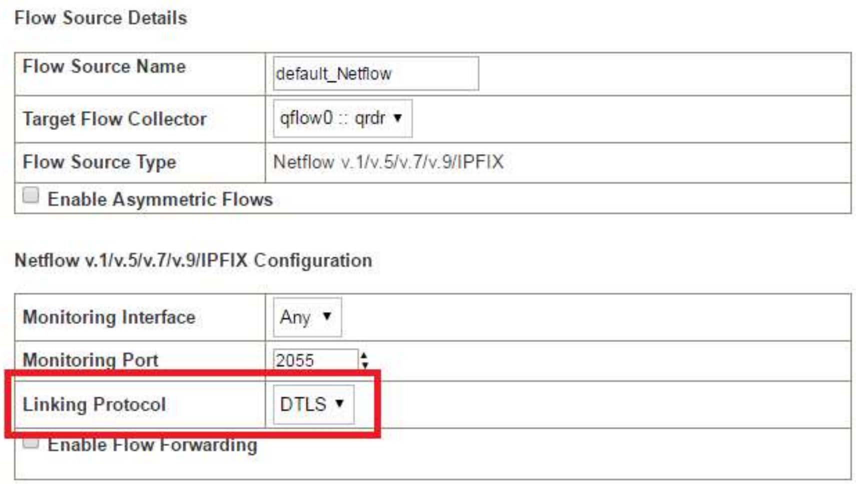
- You must configure your appliance before you can begin to use it for investigating threats on your network.
- The QRadar Network Insights appliance reads the raw packets from a network tap or span port and then generates IPFIX packets
- The IPFIX packets are sent to the QFlow process on the QRadar Console or Flow Processor
- You can choose the format that your QFlow Collectors use to export data to the QFlow Processor: TLV or Payload.



`TLV`	Default QFlow format setting. Choose **TLV** (tab-length-value) for new installs, or for upgrades that don't have a QRadar Network Insights appliance as part of their deployment.
`Payload`	Choose **Payload** for upgrades that have a QRadar Network Insights appliance as part of their deployment. This means that the deployment can continue working as it was.

Setting up DTLS on a QRadar Network Insights managed host

- To prevent eavesdropping and tampering, you must set up Datagram Transport Layer Security (DTLS) on a QRadar® Network Insights managed host.
- The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees
- A flow source must be configured first



Flow Source Details

Flow Source Name	default_Netflow
Target Flow Collector	qflow0 :: qrdr ▾
Flow Source Type	Netflow v.1/v.5/v.7/v.9/IPFIX
□ Enable Asymmetric Flows	

Netflow v.1/v.5/v.7/v.9/IPFIX Configuration

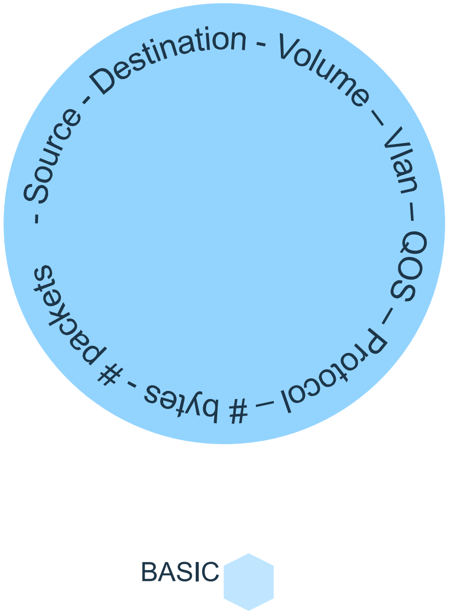
Monitoring Interface	Any ▾
Monitoring Port	2055
Linking Protocol	DTLS ▾
□ Enable Flow Forwarding	

QRadar Network Insights Flow Inspection Levels

- To improve performance, you must choose the appropriate flow rate that is required by configuring the **Flow Inspection Level** setting.
- The flow rate is related to the levels of visibility through the available content, such as source, destination, protocol, and specific file types.
- The flow inspection levels are cumulative, so each level takes the properties of the preceding level.
    - **Flows**
    - **Enriched Flows**
    - **Content enriched flows**

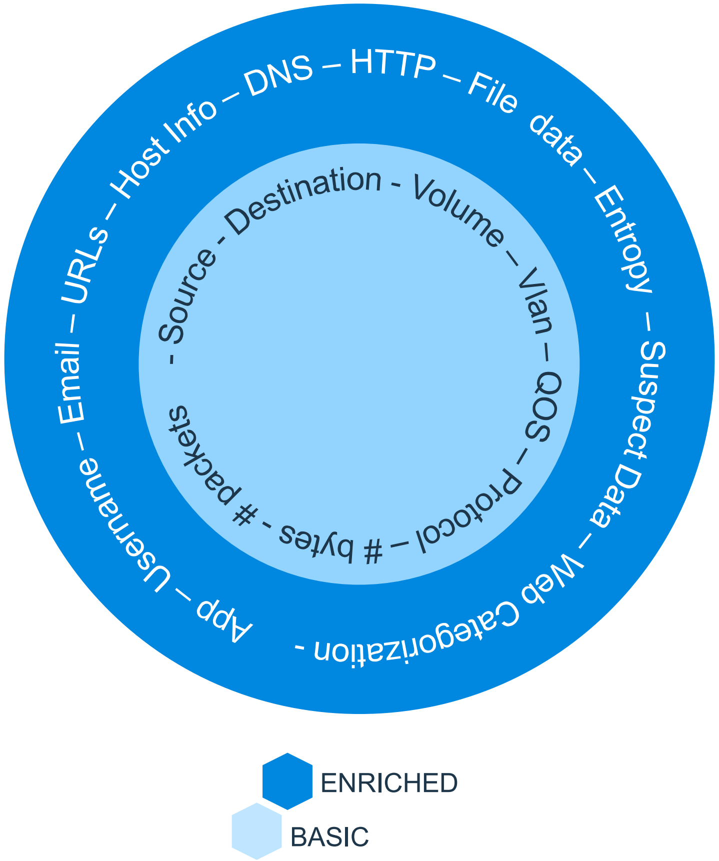
Inspection Levels - Flow

- Flows is the lowest level of inspection.
- Flows are detected by 5-tuple, and the number of bytes and packets that are flowing in each direction are counted.
- Similar to what you get out of a router or network switch that does not perform deep packet inspection.
- This level supports the highest bandwidth, but generates the least amount of flow information.
- The attributes that QRadar® Network Insights generates using the flows inspection level are: 5-tuple values, a flow ID, packet and octet counts in each direction, and flow start and end times.


- Source - Destination - Volume – Vlan – QOS – Protocol – # bytes - # packets
BASIC

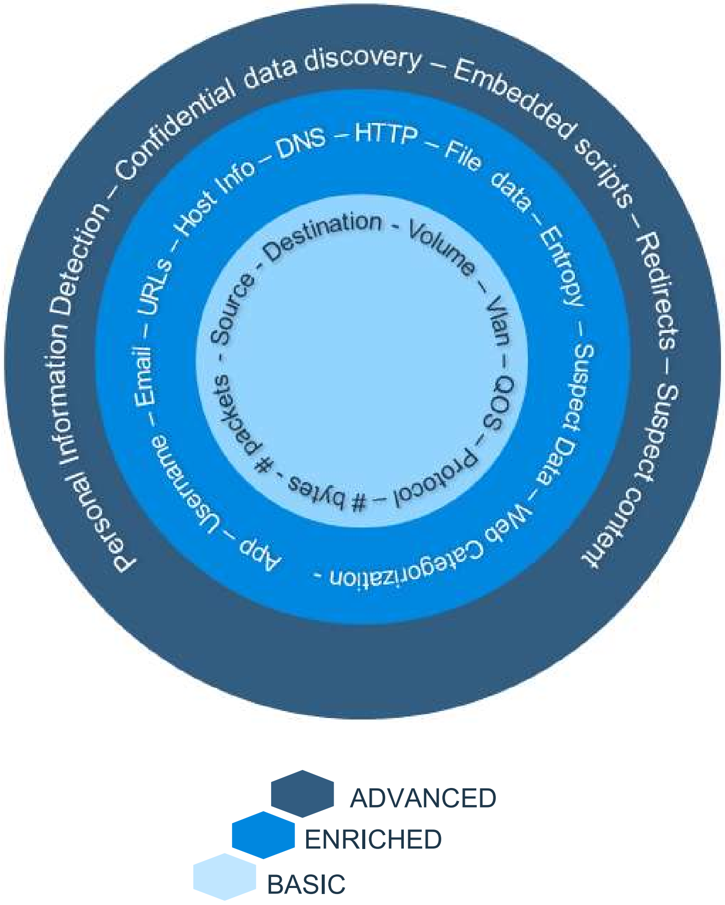
Flow Inspection Levels - Enriched

- Each flow is identified and inspected by one of the protocol or domain inspectors, and many kinds of attributes can be generated from that inspection.
- The attributes that QRadar Network Insights generates by using the enriched flows inspection level are:
  - HTTP metadata values - including categorization of URLs
  - Application ID and action
  - File information (name, size, hash)
  - Originating and recipient user names
  - Limited suspect content values


Host Info – DNS – HTTP – File data – Entropy – Suspect Data – Web Categorization - App – Username – Email – URLs –
- Source - Destination - Volume – Vlan – QOS – Protocol – # bytes - # packets
ENRICHED
BASIC

Flow Inspection Levels – Content Enriched

- Content enriched flows is the default setting and the highest level of inspection.
- It contains all the attributes that the enriched flows level does and it also scans and inspects the content of the files that it finds.
- This results in a more accurate content-type determination, and can yield more suspect content values that result from the inspection of the file contents.
- The attributes that QRadar Network Insights generates by using the content enriched flows inspection level:
  - Personal information
  - Confidential data
  - Embedded scripts
  - Redirects
  - Configurable content-based suspect content

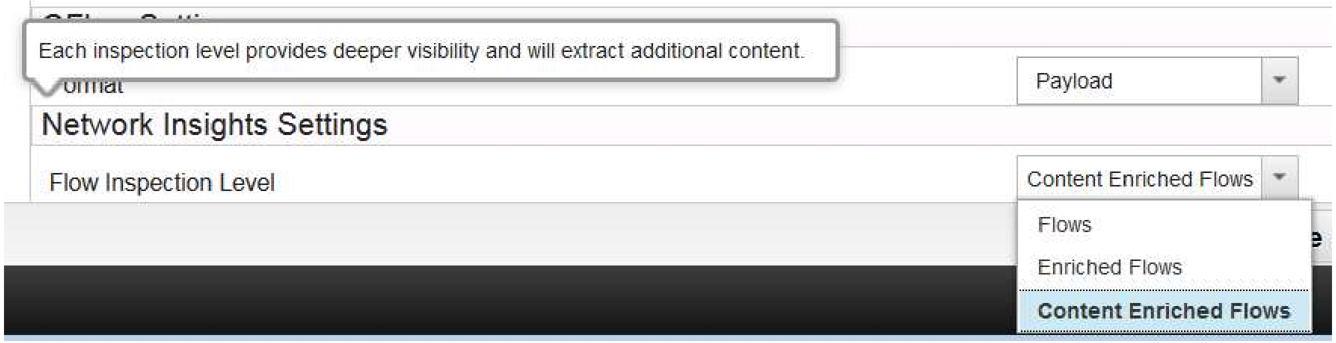


Personal Information Detection – Confidential data discovery – Embedded scripts – Redirects – Suspect content
App – Username – Email – URLs – Host Info – DNS – HTTP – File data – Entropy – Suspect Data – Web Categorization -
# packets - Source - Destination - Volume – Vlan – QOS – Protocol – # bytes -
ADVANCED
ENRICHED
BASIC

Changing Flow Inspection Levels

System Settings

- To change Flow Inspection Levels
  - From the Admin Tab Select System Settings.
  - In Network Insight Settings select the appropriate Flow Inspection Level.
  - Deploy Changes.



Each inspection level provides deeper visibility and will extract additional content.

ormat: Payload

Network Insights Settings

Flow Inspection Level: Content Enriched Flows

QRadar Network Insights Sizing

SETTING	PERFORMANCE
BASIC	10Gbps
ENRICHED	~10Gbpsa [a]
ADVANCED	~ 3.5Gbps [b]

[a] Performance will vary depending on QRadar Network Insights setting, search / extraction criteria and network data

[b] 10Gbps performance achievable with multiple appliances

Setting	Stacking: # Appliances / Tap*		
	Up to 3.5Gbps	Up to 7.0Gbps	Up to 10Gbps
ENRICHED	1	1	**1**
ADVANCED	1	2	**3**

*Performance will vary depending on QNI setting, search / extraction criteria and network data

QRadar Network Insights Sizing

- How many flows does QNI generate compared to QFlow?
- Given the same network traffic, QNI and QFlow **generate the same number of licensable flows**
- However, QNI generates more flows overall compared to QFlow
  - The best number to use for scaling is QNI generates QFlow x 2
  - Empirical evidence suggests it could be slightly more
  - There will be variation from client to client and network to network
  - The number of overall flows impacts
    - Retention scaling
    - FPM scaling

IBM Security

How QNI deals with SSL encryption

QRadar Network Insights – How to deal with SSL encryption

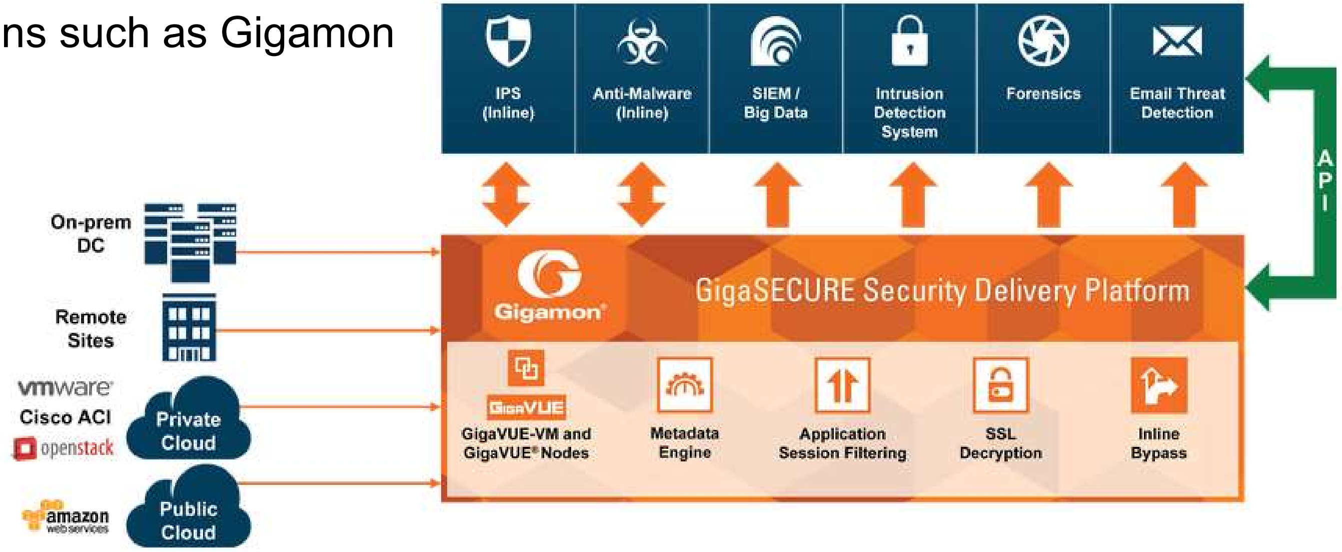
- Key based decryption

QNI: Use keys uploaded to QNI to decrypt traffic in real-time

– Private key based decryption (inbound SSL)

– Session key based decryption (outbound SSL)

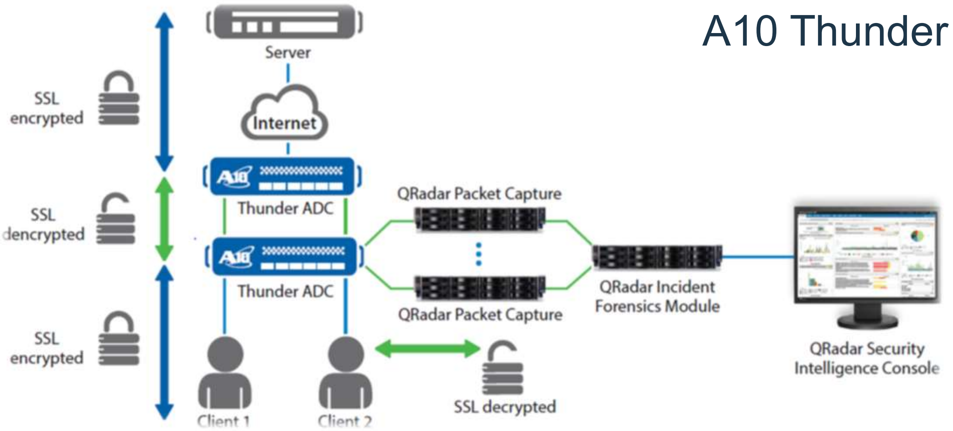
3rd party solutions such as Gigamon

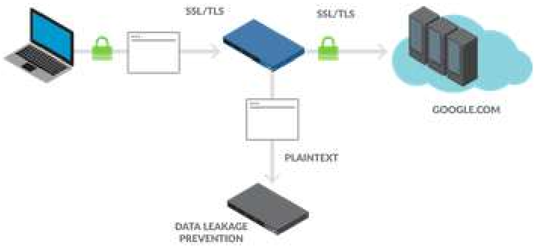


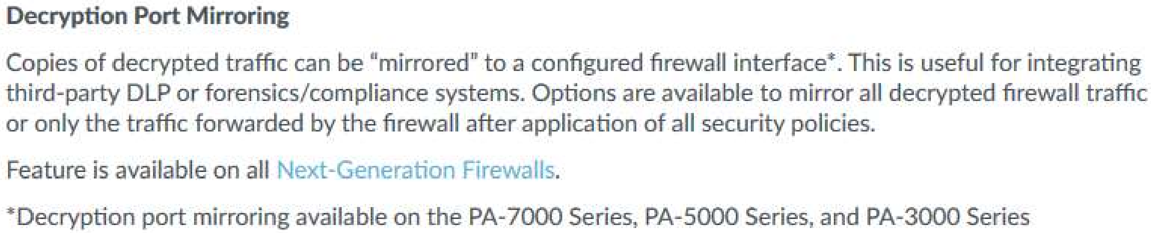
QRadar Network Insights – How to deal with SSL encryption

- Man in the Middle
  - Dedicated Solutions (A10 Thunder)
  - Firewalls (Palo Alto and others)

A10 Thunder







Decryption Port Mirroring

Copies of decrypted traffic can be "mirrored" to a configured firewall interface*. This is useful for integrating third-party DLP or forensics/compliance systems. Options are available to mirror all decrypted firewall traffic or only the traffic forwarded by the firewall after application of all security policies.

Feature is available on all Next-Generation Firewalls.

*Decryption port mirroring available on the PA-7000 Series, PA-5000 Series, and PA-3000 Series

- Palo Alto Next-Gen Firewalls

IBM Security

Frequently Asked Questions (FAQ)

IBM

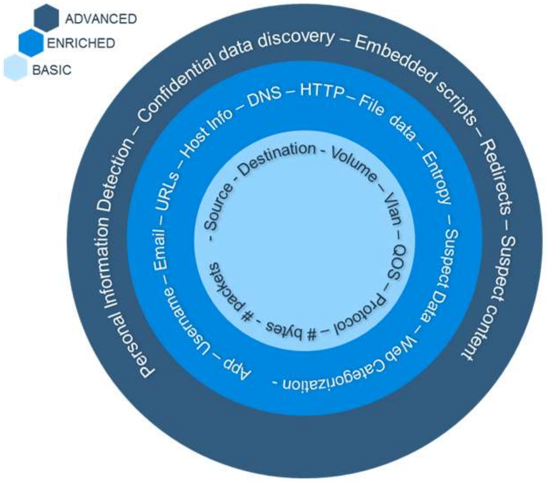
What is different between QNI and QFlow?

- While QFlow analyzes network data to collect basic flow information, identify applications and can extract the beginning of the payload.
- QRadar Network Insights does all of that plus delves much deeper in its analysis.
- QNI can uniquely extract metadata such as:
  - File information (name, size, type, hash, entropy, etc.)
  - User information (across e-mails, chat sessions, applications)
  - HTTP parameters and DNS strings
  - And more
- QNI can also detect a wide range of suspicious activity using Suspect Content which customers can add to with their own unique criteria using Yara rules.

What is the difference in positioning QNI compared to QFlow? What is really new in QNI'?

- The diagram depicts the difference between QFlow and QNI:

  QFlow does the center of the circle plus application detection.
- QNI adds the capability in the outer rings.


ADVANCED
ENRICHED
BASIC
Personal Information Detection – Confidential data discovery – Embedded scripts – Redirects – Suspect content
App – Username – Email – URLs – Host Info – DNS – HTTP – File data – Entropy – Suspect Data – Web Categorization -
- Source - Destination - Volume – Vlan – QOS – Protocol – # bytes - # packets

The added flow analysis and data extraction of QNI allows us to address a number of key use cases such as:

- phishing detection,
- malware analysis
- tracking, later movement detection, etc

What is the difference in positioning QNI compared to QFlow? What is really new in QNI'?

- QFlow can extract packet payload by capturing the first N bytes of payload (64 bytes default setting).

  Limitations:

  - Customer may misses key data they need (if not enough bytes are captured)
  - May require large amounts of storage (since some of the captured bytes contain data that will not be used.

- QNI takes a very different approach.
- QNI analyzes the flows (both header and payload) and extract only the information needed while also sending records to QRadar of suspect content and activity.
- This approach not only provides more visibility but it also guarantees that only data needed to be analyzed will be captured while minimizing storage requirements.

QFlow appliances

- Can QFlow appliances be upgraded to run QNI?
  - QNI is currently offered only as an appliance (the 1920/1901)
  - QFlow users will continue to utilize their existing hardware / QFlow offering
  - A new version of QNI is being developed that will run on M4 Qflow appliances (Roadmap)
  - This new version will allow for a free upgrade for customers who purchased M4 Qflow Appliances
  - Limited Performance (due to hardware limitations with the M4 Qflow Appliances)
  - Upgrading will permit customers to leverage their existing hardware investment and perform deeper flow and content analysis than they can with Qflow
- Is Qflow reaching the end of life?
  - Qflow is still available for customers as a software only offering
  - It is recommended that customers use the QNI appliances to achieve greater visibility

QFlow Technology

- QFlow technology available for free in the near future
- Customers that require an appliance can make use of a QNI Appliance.
- Which technology to use?

  QFlow (software-only): provides low cost option for basic flow analysis

  QNI (Appliance-only): provides the deepest level of network analysis

  - 1920 appliance provides 10G connectivity on 4 ports (10Gbps max per appliance) with stacking option
  - 1901 Appliance provides 1G performance on 4 ports

- Customers who have purchased QFlow from IBM in the past will generally be interested in the more advanced capabilities of QNI.
- QFlow software remain an option and is great for expanding the number of network nodes where flow data is collected (QNI on primary nodes such as internet ingress / egress and QFlow on secondary network nodes).

If we provide Q-Flow technology for free in SW, why not include this into Flow capacity parts? And separately position QNI?

- QFlow is free for flow collection.
- Customers can also ingest flow information from a number of other sources such as QNI, XGS and switches / routers.
- All of these flows require processing and licensing which needs to be managed across all QRadar flow sources.
- QNI is IBM’s most advanced flow collection offering.
- Customers are encouraged to bring in flow information from as many sources / points on the network as possible to improve their threat visibility and detection capability.
- When sizing a QNI deployment, size the FPM entitlement the same as you would for a Qflow deployment.
- Only the basic flow records are counted from QNI for the capacity entitlement which aligns with QFlow.

Differences between QNI and XGS

- XGS is an IPS / IDS IDS/IPS solution that can be used to hunt for specific threat or risk indicators while also providing flow information to QRadar.
- QNI can not only detect known threats or risks it also enables security teams to harvest the necessary content for security analysis of previously unknown threats and performs deep content analysis.
- QNI is also a managed host of QRadar and work exclusively to provide QRadar with the deepest network analysis possible.

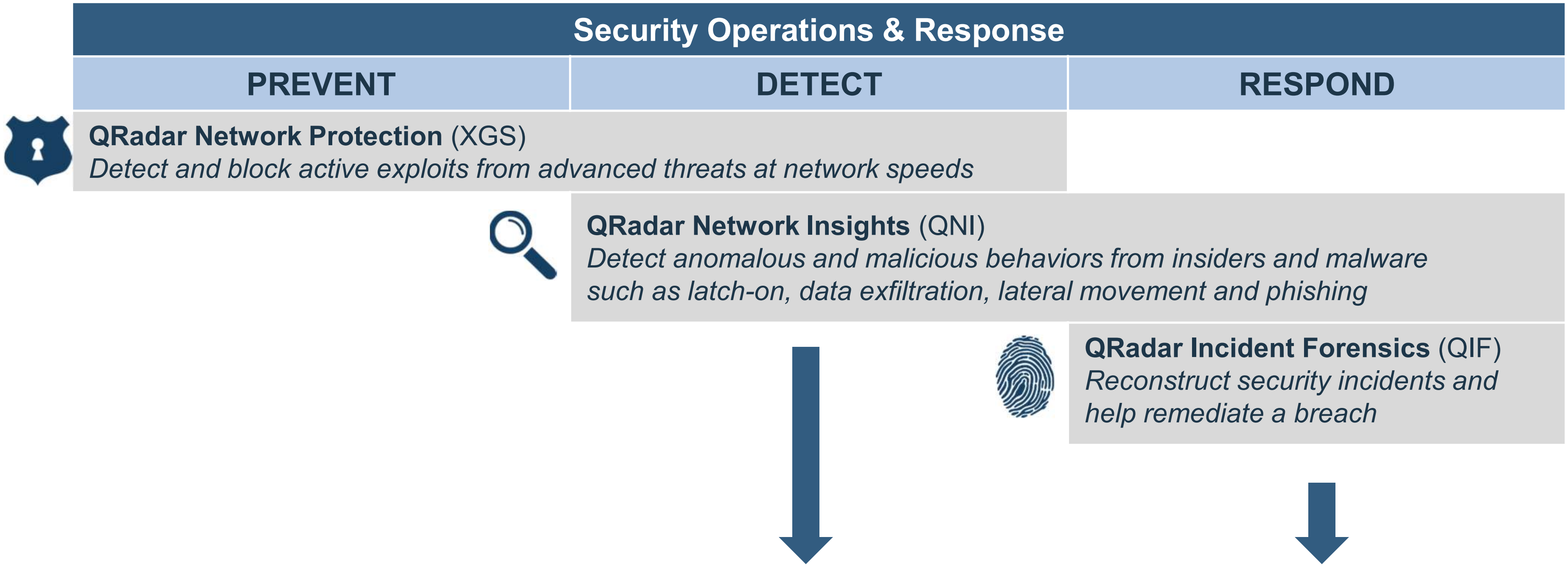
Flow options

	Network flow from routers/ switches	QFlow Collector software	XGS appliance	QRadar Network Insights appliance
Includes basic network traffic info	Yes	Yes	Yes	Yes
Includes application info	No	Yes	Yes	Yes
Includes user info	No	No	Yes	Yes
Includes deep content visibility	No	No	No	Yes
Includes attack/exploit identification	No	No	Yes	No
Can inspect SSL traffic	No	No	Inbound and outbound	Inbound and outbound (with keys)
Can block traffic	No	No	Yes	No
Deployment modes	TAP / SPAN port	TAP / SPAN port	TAP / SPAN port or in-line	TAP / SPAN port
Speed	Varies	Depends on underlying hardware used	400 Mbps – 25 Gbps	3.5 Gbps–10 Gbps per appliance; stackable
List price	N/A	$30,500	$12k - $350k	$120k

QRadar analyzes network traffic in real-time to generate deep network intelligence and provide comprehensive threat protection

SECURITY GUARD	DECTECTIVE	CRIME SCENE INVESTIGATOR
QRadar Network Protection (XGS)	**QRadar Network Insights** (QNI)	**QRadar Incident Forensics** (QIF)
Stops threats at the point of attack nearly instantly and provides visibility • **Behavior-based analysis** and heuristics stops known and unknown threats • **Network visibility and control** over users and applications • **Inbound and outbound encryption** inspection • Powered by **IBM X-Force** threat intelligence and research	Identifies and qualifies active threats and attacks in real-time • **Network analytics** detects insider threats, data exfiltration and malware • **Records** application activities, captures artifacts, and identifies assets, applications and users • Configurable analysis from network traffic for **real time threat detection** and long-term retrospective analysis	Methodical attack investigation and re-creation after the fact • **Re-traces the step-by-step actions** of cyber criminals • **Reconstructs raw network data** related to a security incident • **Available Packet capture** (PCAP)

QRadar delivers network intelligence across the lifecycle of security operations & response



Security Operations & Response

PREVENT | **DETECT** | **RESPOND**

QRadar Network Protection (XGS)
Detect and block active exploits from advanced threats at network speeds

QRadar Network Insights (QNI)
Detect anomalous and malicious behaviors from insiders and malware such as latch-on, data exfiltration, lateral movement and phishing

QRadar Incident Forensics (QIF)
Reconstruct security incidents and help remediate a breach

XGS + QNI

Enables deeper network insights, detecting threats performing recon and DDOS

QNI + QIF

Enables complete forensic investigation, providing a holistic picture of network activity

QRadar Network Insights

- Is QNI available as software?
  - QRadar Network Insights GA's on December 9th, 2016 as an appliance based offering
  - A software based version of QNI is in development with target availability in late 2017

- Is QNI available on Dell?
  - The 1920/1901 appliances are currently using a Lenovo platform
  - A Dell version of the 1920 appliance is being qualified with target availability in late 2017

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

IBM Security QRadar Vulnerability Assessment

QRadar Vulnerability Assessment Overview

- This presentation covers only QRadar integration with third party scanners
- For QRadar Vulnerability Manager please review:
  - Understanding and Using QRadar Vulnerability Manager

QRadar Vulnerability Assessment Overview

- Vulnerability assessment is the evaluation of assets in the network to identify and prioritize potential security issues.
- QRadar products that support Vulnerability Assessment can import vulnerability data from external scanner products to identify vulnerabilities profiles for assets.
- As external scanners generate scan data, QRadar can retrieve the vulnerability data with a scan schedule.
- QRadar imports the scan results to provide vulnerability assessment profiles for network assets.
- Vulnerability assessment profiles use correlated event data, network activity, and behavioral changes to determine the threat level and vulnerabilities present on critical business assets in your network.

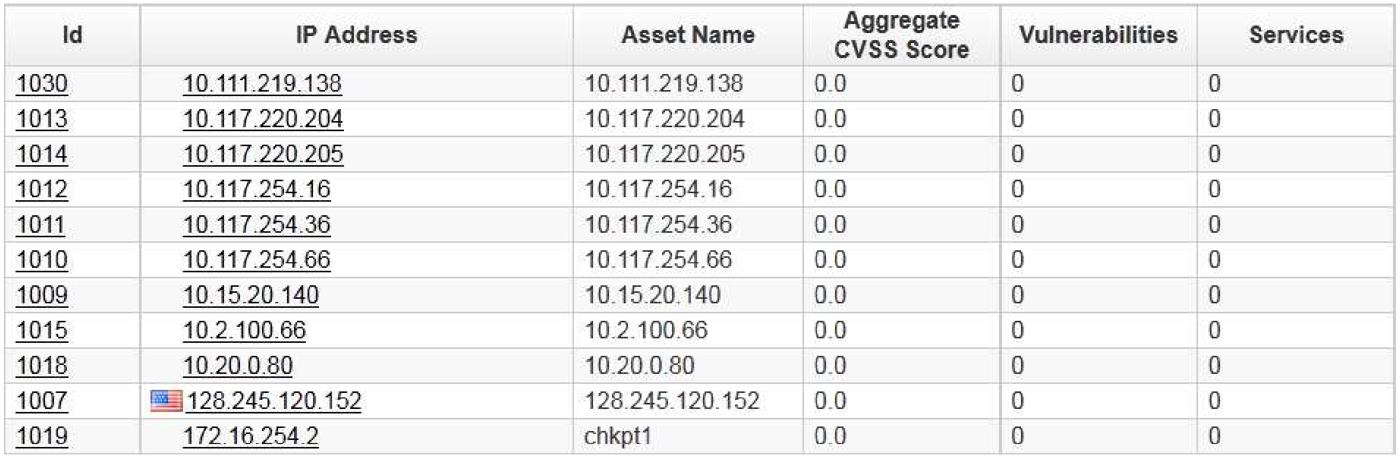
Active scanners

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

QRadar Vulnerability Assessment Overview

- Asset profiles for servers and hosts in your network provide information that can help you to resolve security issues.
- Using asset profiles, you can connect offenses that occur on your system to the physical or virtual assets as part of your security investigation.
- Asset data is helpful to identify threats, to identify vulnerabilities, services, ports, and monitor asset usage in your network.



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

IBM Security

Supported third party scanner integrations

Supported third party scanner integrations

- AXIS scanner
  - You can import vulnerability data from any scanner that outputs data in Asset Export Information Source (AXIS) format. Axis is an XML data format that was created specifically for asset and vulnerability compatibility with IBM® Security QRadar® products.
  - To successfully integrate an AXIS scanner with QRadar, XML result files must be available on a *remote server* or a scanner that supports SFTP or SMB Share communication.
  - A remote server is a system or third-party appliance that can host the XML scan results.
- Beyond Security AVDS scanner
  - Beyond Security Automated Vulnerability Detection System (AVDS) appliances create vulnerability data in Asset Export Information Source (AXIS) format. AXIS formatted files can be imported by XML files that can be imported.
- Digital Defense Inc AVS scanners
  - Before you add this scanner, a server certificate is required to support HTTPS connections. QRadar supports certificates with the following file extensions: .crt, .cert, or .der.

Supported third party scanner integrations

- eYe scanner
  - QRadar® can collect vulnerability data from eEye REM Security Management Console or eEye Retina CS scanners.
  - The following protocol options are available to collect vulnerability information from eEye scanners:
    - SNMP protocol eEye scanner AND JDBC protocol eEye scanner.
- IBM AppScan Enterprise scanner
  - QRadar retrieves AppScan Enterprise reports with the Representational State Transfer (REST) web service to import vulnerability data and generate offenses for your security team.
  - You can import scan results from IBM Security AppScan Enterprise report data, providing you a centralized security environment for advanced application scanning and security compliance reporting.
  - You can import IBM Security AppScan Enterprise scan results to collect asset vulnerability information for malware, web applications, and web services in your deployment.

Supported third party scanner integrations

- IBM Guardium scanner
  - IBM InfoSphere Guardium appliances are capable of exporting database vulnerability information that can be critical to protecting customer data.
  - IBM Guardium audit processes export the results of tests that fail the Common Vulnerability and Exposures (CVE) tests generated when running security assessment tests on your IBM Guardium appliance.
  - The vulnerability data from IBM Guardium must be exported to a remote server or staging server in Security Content Automation Protocol (SCAP) format.
  - IBM Security QRadar can then retrieve the scan results from the remote server storing the vulnerability using SFTP.
  - IBM Guardium only exports vulnerability from databases containing failed CVE test results.
  - If there are no failed CVE tests, IBM Guardium may not export a file at the end of the security assessment.

Supported third party scanner integrations

- IBM BigFix scanner
  - The IBM® BigFix scanner module accesses vulnerability data from IBM BigFix by using the SOAP API that is installed with the Web Reports application.
  - To retrieve vulnerability data from BigFix for IBM Security QRadar, the Web Reports application for BigFix is required.
  - Administrators create a user in IBM BigFix for QRadar to use when the system collects vulnerabilities.
  - QRadar is compatible with IBM BigFix for versions 8.2.x to 9.5.2.
- Juniper Profiler NSM scanner
  - QRadar® can collect vulnerability data from the PostgreSQL database on the Juniper Profiler NSM scanner by polling for data with JDBC.
  - The Juniper Networks Netscreen Security Manager (NSM) console passively collects valuable asset information from your network through deployed Juniper Networks IDP sensors.
  - QRadar connects to the Profiler database stored on the NSM server to retrieve these records. The QRadar server must have access to the Profiler database.

Supported third party scanner integrations

- McAfee Vulnerability Manager scanner
  - The McAfee Vulnerability Manager scanner enables QRadar® to import vulnerabilities from an XML file or query for a results file from the McAfee OpenAPI.
  - QRadar can collect vulnerability data from McAfee Vulnerability Manager appliances. The following software versions are supported: v6.8 and v7.0 for the McAfee Vulnerability Manager SOAP API and v6.8, v7.0, and v7.5 for remote XML imports
- Microsoft SCCM scanner
  - IBM® Security QRadar® can import scan reports from Microsoft System Center Configuration Manager (SCCM) scanners
  - Before you configure a Microsoft SCCM scanner, configure your system DCOM settings for each host that you want to monitor.

Supported third party scanner integrations

- Nessus scanner
  - QRadar® can use a Nessus client and server relationship to retrieve vulnerability scan reports.
  - You can also use the Nessus XMLRPC API or JSON API to access scan data directly from Nessus.
  - When you configure your Nessus client, you need to create a Nessus user account for your QRadar system.
  - A unique user account ensures that QRadar has the correct credentials to log in and communicate with the Nessus server.
  - After you create the user account, a connection test verifies the user credentials and remote access.
- The following options are available for data collection of vulnerability information from Nessus scanners:
- Scheduled Live Scan, Scheduled Results Import, Scheduled Live Scan - XMLRPC API, Scheduled Live Scan - JSON API, Scheduled Completed Report Import - XMLRPC API, Scheduled Completed Report Import - JSON API

Supported third party scanner integrations

- Nmap scanner
  - QRadar uses SSH to communicate with the Nmap server to either start remote Nmap scans or download the completed Nmap scan results.
  - Note: Although there is an NMap binary on each QRadar host, it is reserved for internal QRadar use only. Configuring an NMap vulnerability scanner to use a QRadar Console or QRadar managed host as the remote NMap scanner is not supported and can cause instabilities.
  - When administrators configure an Nmap scan, a specific Nmap user account can be created for the QRadar system.
  - A unique user account ensures that QRadar possesses the credentials that are required to log in and communicate with the Nmap server.
  - After the user account creation is complete, administrators can test the connection from QRadar to the Nmap client with SSH to verify the user credentials.
  - This test ensures that each system can communicate before the system attempt to download vulnerability scan data or start a live scan.

Supported third party scanner integrations

- Outpost24 Vulnerability Scanner
  - QRadar uses HTTPS to communicate with the Outpost24 vulnerability scanner API to download asset and vulnerability data from previously completed scans.
  - A server certificate is required to support HTTPS connections.
- Positive Technologies MaxPatrol Scanner
  - QRadar imports XML file results by scheduling regular scan imports that contain MaxPatrol vulnerabilities.
  - The MaxPatrol scanner imports files from a remote server that contains the exported scan data.
- Qualys scanner
  - QRadar can retrieve vulnerability information from the QualysGuard Host Detection List API or download scan reports directly from a QualysGuard appliance.
  - The data that the query returns contains the vulnerabilities as identification numbers, which QRadar compares against the most recent Qualys Vulnerability Knowledge Base.
  - The Qualys Detection Scanner does not support live scans, but enables the Qualys Detection Scanner to retrieve vulnerability information aggregated across multiple scan reports.

Supported third party scanner integrations

- Rapid7 Nexpose scanner
  - Rapid7 Nexpose scanners can provide site data reports to QRadar® to import vulnerabilities known about your network.
  - The following options are available to collect vulnerability information from Rapid7 Nexpose scanners:
    - Site import of an adhoc report through the Rapid7 API.
    - Site import of a Local file or of a Remote File.
- SAINT scanner
  - QRadar may collect SAINT vulnerability data for hosts, including Mac addresses, ports, and service information.
  - The SAINT scanner identifies vulnerabilities based on the specified scan level and uses SAINT writer to generate custom reports.
  - Therefore, your SAINT system must include a custom SAINTwriter report template and scans that runs regularly to ensure the results are current.
  - The following data collection types are supported for SAINT scanner configurations: Live Scan and Report Only.

Supported third party scanner integrations

- Tenable Security Center scanner
  - A Tenable SecurityCenter scanner can be used to schedule and retrieve any open vulnerability scan report records from Nessus vulnerability scanners on your network.
  - QRadar can collect host and vulnerability information through the Tenable API.

Supported third party scanner integrations (as of QRadar 7.3)

Vendor	Scanner name	Supported versions	Configuration name	Connection type
Beyond Security	Automated Vulnerability Detection System (AVDS)	AVDS Management V12 (minor version 129) and above	Beyond Security AVDS Scanner	File import of vulnerability data with SFTP
Digital Defense Inc	AVS	N/A	Digital Defense Inc AVS	HTTPS
eEye Digital Security	eEye REM	REM V3.5.6	eEye REM Scanner	SNMP trap listener
	eEye Retina CS	Retina CS V3.0 to V4.0		Database queries over JDBC
Generic	Axis	N/A	Axis Scanner	File import of vulnerability data with SFTP
IBM®	IBM AppScan® Enterprise	V8.6	IBM AppScan Scanner	IBM REST web service with HTTP or HTTPS
IBM	InfoSphere® Guardium®	v9.0 and above	IBM Guardium SCAP Scanner	File import of vulnerability data with SFTP
IBM	BigFix®	V8.2x to V9.5.2	IBM BigFix Scanner	SOAP-based API with HTTP or HTTPS
IBM	InfoSphere SiteProtector™	V2.9.x	IBM SiteProtector Scanner	Database queries over JDBC
IBM	Tivoli®			
	Now known as IBM BigFix			

Supported third party scanner integrations (as of QRadar 7.3)

Vendor	Scanner name	Supported versions	Configuration name	Connection type
Juniper Networks	NetScreen Security Manager (NSM) Profiler	2007.1r2 2007.2r2 2008.1r2 2009r1.1 2010.x	Juniper NSM Profiler Scanner	Database queries over JDBC
McAfee	Vulnerability Manager	V6.8 V7.0 V7.5	McAfee Vulnerability Manager	SOAP-based API with HTTPS XML file import
Microsoft	Microsoft System Center Configuration Manager (SCCM)	Microsoft Windows	Microsoft SCCM	DCOM must be configured and enabled
nCircle or Tripwire	IP360	VnE Manager V6.5.2 to V6.8.28	nCircle ip360 Scanner	File import of vulnerability data with SFTP
netVigilance	SecureScout	V2.6	SecureScout Scanner	Database queries over JDBC
Open source	NMap	V3.7 to V6.0	NMap Scanner	File import of vulnerability data over SFTP with SSH command execution
Outpost24	Outpost24	HIAB V4.1 OutScan V4.1	Outpost24	API over HTTPS
Positive Technologies	MaxPatrol	V8.24.4 and later	Positive Technologies MaxPatrol	SFTP or SMB Share

Supported third party scanner integrations (as of QRadar 7.3)

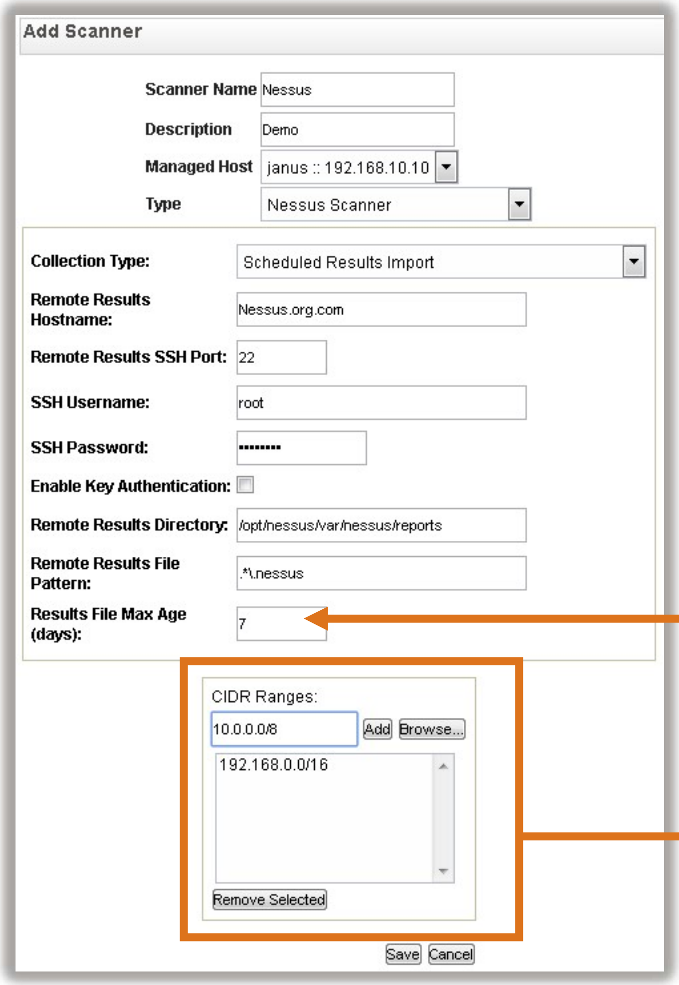
Vendor	Scanner name	Supported versions	Configuration name	Connection type
Qualys	QualysGuard	V4.7 to V8.1	Qualys Scanner	APIv2 over HTTPS
Qualys	QualysGuard	V4.7 to V8.1	Qualys Detection Scanner	API Host Detection List over HTTPS
Rapid7	NeXpose	V4.x to V6.3.3	Rapid7 NeXpose Scanner	Remote Procedure Call (RPC) over HTTPS
				Local file import of XML file over SCP or SFTP to a local directory
Saint Corporation	Security Administrator's Integrated Network Tool (SAINT)	V7.4.x	Saint Scanner	File import of vulnerability data over SFTP with SSH command execution
Tenable Network Security	SecurityCenter	V4 and V5	Tenable SecurityCenter	JSON request over HTTPS
Tenable Network Security	Nessus	Linux V4.0.2 to V4.4.x	Nessus Scanner	File import over SFTP with SSH command execution
		Microsoft Windows V4.2 to V4.4.x		
		Linux V4.2 to V5.x		XML-RPC API over HTTPS
		Microsoft Windows V4.2 to V5.x		

IBM Security

Adding and Scheduling a Vulnerability Scanner

IBM

Vulnerability Scanners



Add Scanner

Scanner Name: Nessus

Description: Demo

Managed Host: janus :: 192.168.10.10

Type: Nessus Scanner

Collection Type: Scheduled Results Import

Remote Results Hostname: Nessus.org.com

Remote Results SSH Port: 22

SSH Username: root

SSH Password: ••••••••

Enable Key Authentication: □

Remote Results Directory: /opt/nessus/var/nessus/reports

Remote Results File Pattern: .*\.nessus

Results File Max Age (days): 7

CIDR Ranges: 10.0.0.0/8

192.168.0.0/16

Set the maximum age of the result sets to be imported

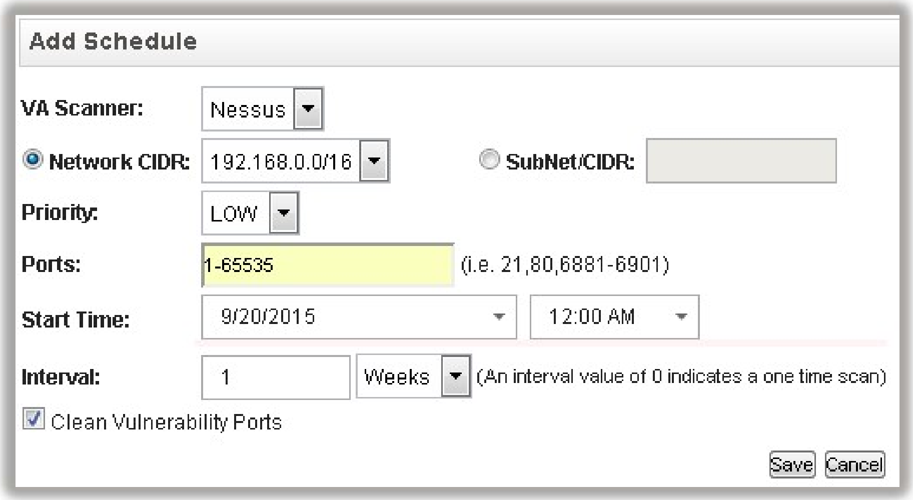
Use CIDR ranges to import only VA Scanner results from machines within the CIDR range

VA Scanners

Schedule VA Scanners

- Each VA Scanner requires specific configuration settings; use the *Vulnerability Assessment Configuration Guide* for configuration guidance
- You can import vulnerability data from any scanner that outputs data in Asset Export Information Source (AXIS) format using the Axis scanner

Configure the scheduled import of VA results



Add Schedule

VA Scanner: Nessus

● Network CIDR: 192.168.0.0/16 ○ SubNet/CIDR:

Priority: LOW

Ports: 1-65535 (i.e. 21,80,6881-6901)

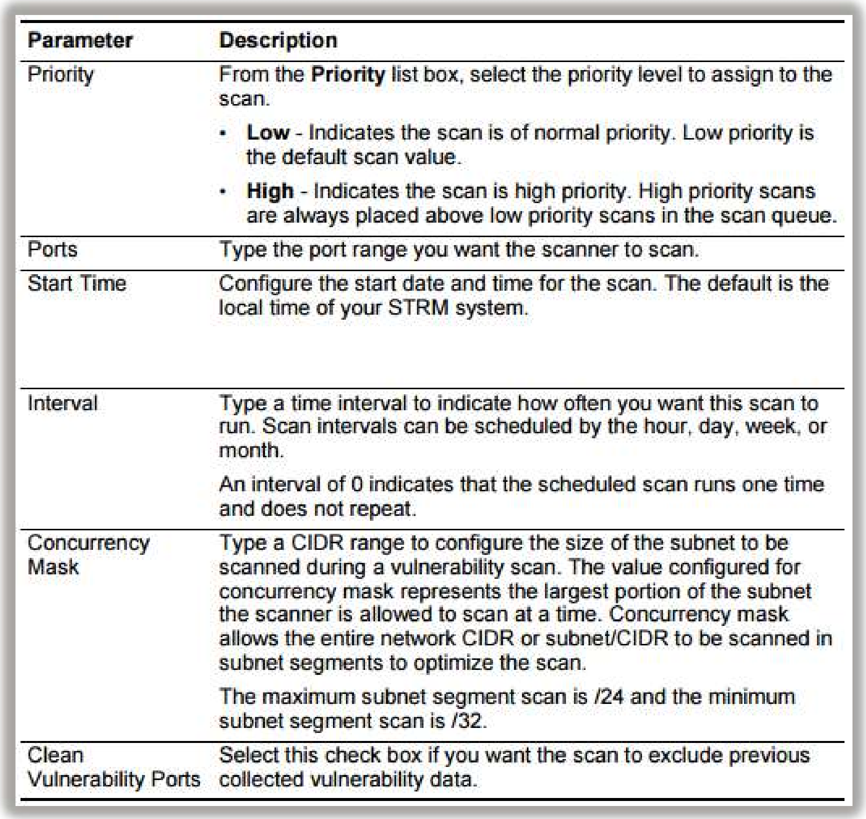
Start Time: 9/20/2015 12:00 AM

Interval: 1 Weeks (An interval value of 0 indicates a one time scan)

☑ Clean Vulnerability Ports

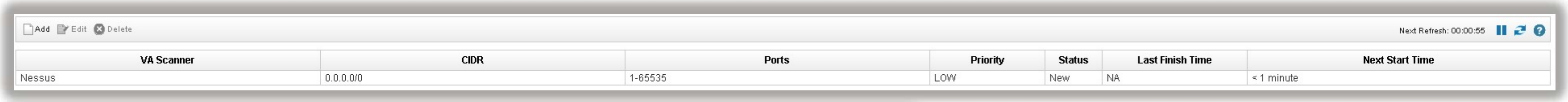
- To import VA scanner results into the asset profile database, click **Schedule**
- You can select specific CIDR ranges and Ports for the VA scan

Note: Usually, QRadar VA Scanner schedules are ***not*** used to run VA Scanners because of the considerable impact on the network, and QRadar VA Scanner schedules are only used to import scanner results

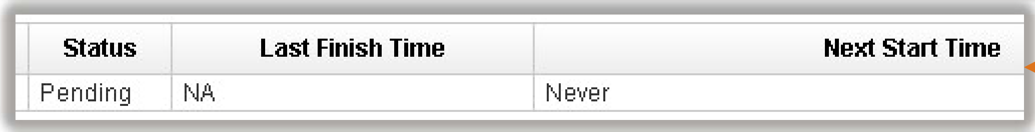


Parameter	Description
Priority	From the **Priority** list box, select the priority level to assign to the scan. • **Low** - Indicates the scan is of normal priority. Low priority is the default scan value. • **High** - Indicates the scan is high priority. High priority scans are always placed above low priority scans in the scan queue.
Ports	Type the port range you want the scanner to scan.
Start Time	Configure the start date and time for the scan. The default is the local time of your STRM system.
Interval	Type a time interval to indicate how often you want this scan to run. Scan intervals can be scheduled by the hour, day, week, or month. An interval of 0 indicates that the scheduled scan runs one time and does not repeat.
Concurrency Mask	Type a CIDR range to configure the size of the subnet to be scanned during a vulnerability scan. The value configured for concurrency mask represents the largest portion of the subnet the scanner is allowed to scan at a time. Concurrency mask allows the entire network CIDR or subnet/CIDR to be scanned in subnet segments to optimize the scan. The maximum subnet segment scan is /24 and the minimum subnet segment scan is /32.
Clean Vulnerability Ports	Select this check box if you want the scan to exclude previous collected vulnerability data.

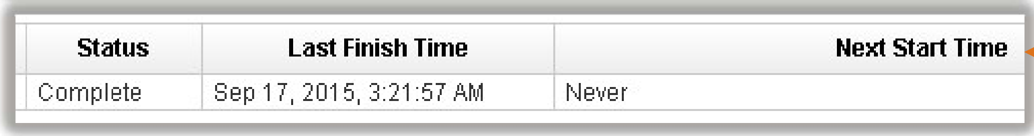
Configure the scheduled import of VA results



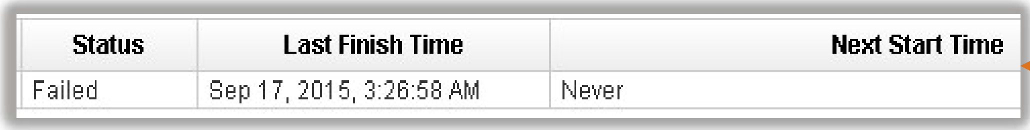
VA Scanner	CIDR	Ports	Priority	Status	Last Finish Time	Next Start Time
Nessus	0.0.0.0/0	1-65535	LOW	New	NA	< 1 minute



Status	Last Finish Time	Next Start Time
Pending	NA	Never

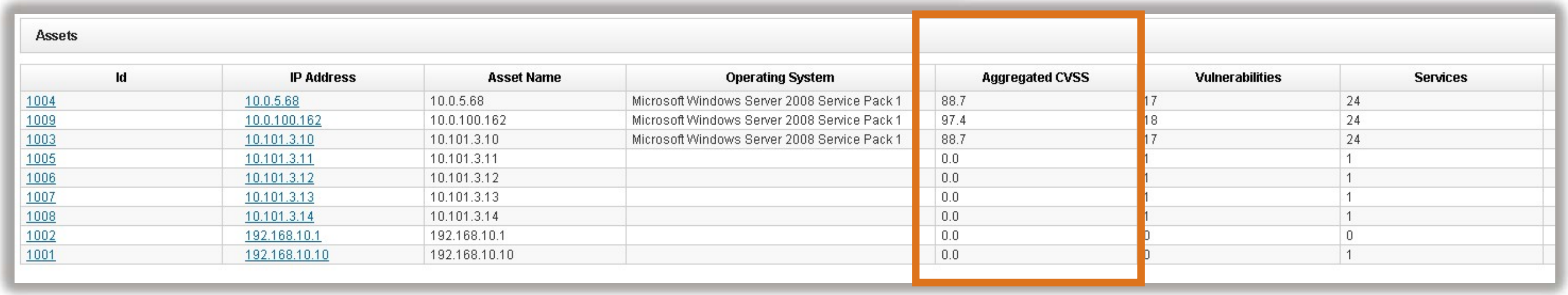


Status	Last Finish Time	Next Start Time
Complete	Sep 17, 2015, 3:21:57 AM	Never



Status	Last Finish Time	Next Start Time
Failed	Sep 17, 2015, 3:26:58 AM	Never

To view the scheduled import progress and results, monitor the VA Scanner’s **Status** field



Assets

Id	IP Address	Asset Name	Operating System	Aggregated CVSS	Vulnerabilities	Services
1004	10.0.5.68	10.0.5.68	Microsoft Windows Server 2008 Service Pack 1	88.7	17	24
1009	10.0.100.162	10.0.100.162	Microsoft Windows Server 2008 Service Pack 1	97.4	18	24
1003	10.101.3.10	10.101.3.10	Microsoft Windows Server 2008 Service Pack 1	88.7	17	24
1005	10.101.3.11	10.101.3.11		0.0	1	1
1006	10.101.3.12	10.101.3.12		0.0	1	1
1007	10.101.3.13	10.101.3.13		0.0	1	1
1008	10.101.3.14	10.101.3.14		0.0	1	1
1002	192.168.10.1	192.168.10.1		0.0	0	0
1001	192.168.10.10	192.168.10.10		0.0	0	1

To view imported scan results by asset, click the **Asset** tab and drill down to the vulnerability list

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®