

QRadar Tuning



IBM SECURITY SUPPORT OPEN MIC

Slides and additional dial in numbers: <http://ibm.biz/qradartuning1>

NOTICE: BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS ON YOUTUBE. IF YOU OBJECT, PLEASE DO NOT CONNECT TO THIS CALL.

May 16, 2017

Panelists

- Adam Frank – Executive IT Architect
- Sterling Jones – Cybersecurity Technical Lead
- Nick LaPlaca – Product Professional Services, Consultant
- Alaa Ali – Product Professional Services, Consultant
- Paul Ford-Hutchinson – Security Intelligence SWAT
- Shane Lundy – Offering Management – QRadar App Management

Presenter: Jonathan Pechta – Support Technical Writer / Support Content Lead

Moderator: Jack Cam – Support Manager

Assisting: Michael Hunt – Support Knowledge Co-op student



Announcements



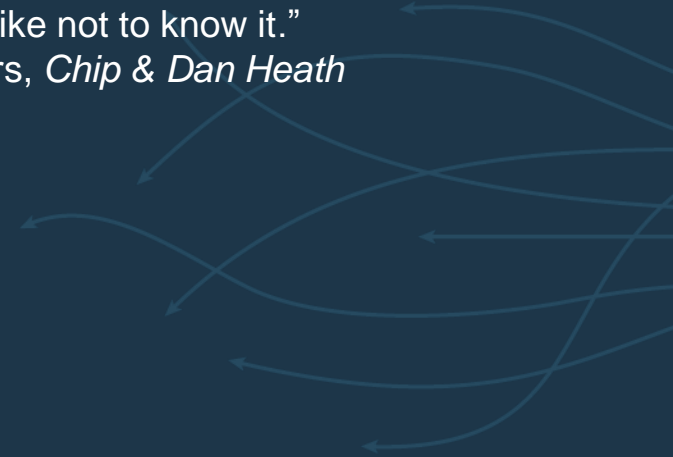
General Information / Announcements

- QRadar 7.3.0 Patch 1 has been released. There is both a published ISO and SFS file.
 - The SFS file is intended for users at QRadar 7.3.0 to update to Patch 1.
 - The ISO file is intended for users at 7.2.8 Patch 1 or later to update to QRadar 7.3.0 Patch 1.
- April wrap-up newsletter is available here:
<http://ibm.biz/newsapril2017>
- Next week: QRadar Open Mic on Optimizing QRadar Advisor w/Watson (23rd of May)



Agenda

“Once we know something, we find it hard to imagine what it was like not to know it.”
- Authors, *Chip & Dan Heath*



QRadar Tuning Feature Discussion

Tuning Methodology

Getting Started (The Core Foundation)

- Network Hierarchy

- Host Definitions BB / Reference sets

- Server Discovery

- Content Packs (pre-built use cases, e.g. PCI)

Tuning (Initial Rule Tuning)

- 1a. Tuning using Sim Tuning Report

- 1b. Tuning using Offenses by Category

- 1c. Offenses by rules, sorted by Offense Count

- 1d. False positive rules and use of False positive button – last resort

The Core Foundations

Network Hierarchy

You can't build a great building on a weak foundation. You must have a solid foundation if you're going to have a strong superstructure.

- Gordon B. Hinckley



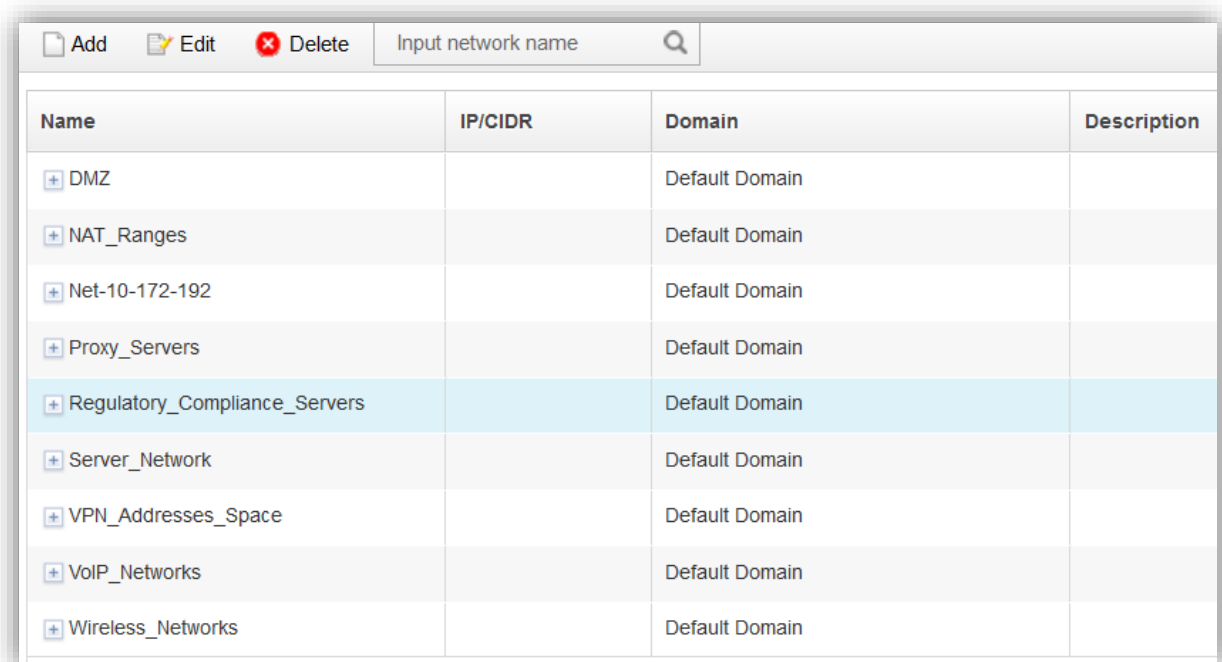
What is Network Hierarchy?

Network Hierarchy defines what address spaces for assets are in your network (Local) and what is outside of your network (Remote). This is done by defining CIDR ranges that allows administrators to segment the network in to logical groups for rules, searches, reports, network anomaly behavior patterns, etc. This list should include both routable and non-routable addresses for assets you own.

Rule of thumb: Make your network hierarchy as deep and specific as you need to monitor critical systems and important network segments.

Did you know?

64 enabled rules in QRadar refer to the Network Hierarchy.



Name	IP/CIDR	Domain	Description
+ DMZ		Default Domain	
+ NAT_Ranges		Default Domain	
+ Net-10-172-192		Default Domain	
+ Proxy_Servers		Default Domain	
+ Regulatory_Compliance_Servers		Default Domain	
+ Server_Network		Default Domain	
+ VPN_Addresses_Space		Default Domain	
+ VoIP_Networks		Default Domain	
+ Wireless_Networks		Default Domain	

How deep do I go with Network Hierarchy?

A well-defined network hierarchy can help users quickly identify where an offense is occurring.

The more specific you get, the better, but more maintenance is likely required to keep the list up-to-date with network changes.

Brainstorming: Think of your organization's network and attempt to classify it into 10 segments. Use these 10 segments to become the top level networks in your hierarchy. Note: Each top level can have multiple-sub segments; however, disregard that for this thought exercise.

Example of top level segments:

1. Corporate Network
2. Remote Sites
3. Data Centers
4. Critical Assets (PCI Zone)
5. Server Types
6. Network Management Devices
7. Local Catch-all

Example :

1. Corporate Network
 1. Corporate 1 wired 10.1.0.0/24
 2. Corporate 2 wired 10.2.0.0/24
 3. Wireless 10.3.0.0/24
2. Remote Sites
 1. Fredericton 10.4.0.0/24
 2. Atlanta 10.5.0.0/24
 3. Belfast 10.6.0.0/24
3. Data Centers 10.7.0.0/24
4. Critical Assets (PCI Zone) 10.8.0.0/24
5. Server Types
 1. Windows Servers 10.9.0.0/24
 2. Linux 10.10.0.0/24
 3. Active Directory 10.11.0.0/24
 4. Mail 10.12.0.0/24
6. Local Catch-all
 1. 10.0.0.0/8
 2. 192.168.0.0/24
 3. 172.20.0.0/24
7. Network Management Devices 10.14.0.0/24
8. Lab Networks 10.13.0.0/24

Network Hierarchy and Rules

The larger the network segment the easier it is to maintain from a rule standpoint. The smaller the network hierarchy segment, then the more granular you can get from an offense standpoint. The rule engine isn't affected by the size of the range. It's simply going to analyze each IP and see which network object the event or flow falls in to based on CIDR.

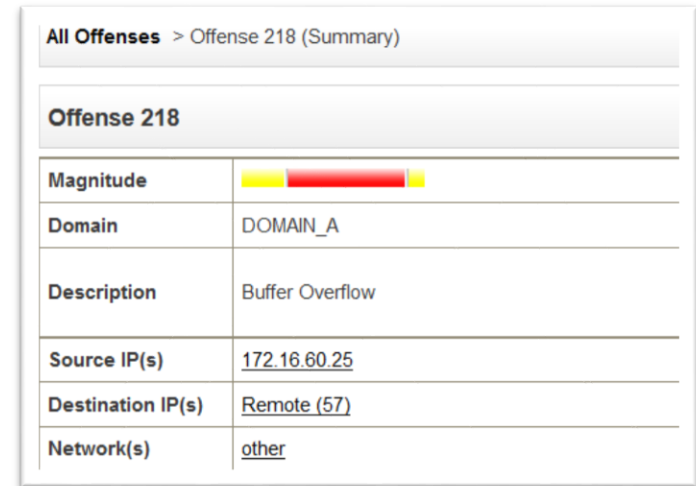
How granularity can work to your advantage (anomalies and tracking behavior):

- For example, you probably expect all of the AD servers in your North America Finance department to exhibit roughly the same behaviors and patterns. Keeping these two networks in their own hierarchy allows you to write rules around similar networks and let QRadar detect deviations. You might want to compare AD servers in North America Finance to AD servers in Europe Finance.
- Another typical use case is to allow you to write rules around data moving between zones, such as communications between A and B outside certain hours, weekends, or meeting other criteria should trigger an anomaly.


Network Hierarchy and keeping up-to-date

Administrators can use searches to determine addresses that are outside of the network hierarchy. If you run searches that look for data that is Remote-to-Remote and get hits back on the search, then you likely have an issue in your network hierarchy.

1. Talk with your Subject Matter Experts and schedule reviews or reports of IP addresses to keep up-to-date.
2. Use automation such as Infoblox or other network management utilities to keep track of IP addresses in large networks and leverage the API to update data.
3. Look for Remote-to-Remote (R2R) events, this indicates a network hierarchy configuration issue.
4. Schedule reviews to identify addresses that are classified as “other”. Other is a hidden network hierarchy address that uses 0.0.0.0/0 as the CIDR range to catch all addresses that are undefined to a network.



The screenshot shows a summary for 'Offense 218' with the following details:

All Offenses > Offense 218 (Summary)	
Offense 218	
Magnitude	
Domain	DOMAIN_A
Description	Buffer Overflow
Source IP(s)	172.16.60.25
Destination IP(s)	Remote (57)
Network(s)	other

The Core Foundations

Host Definitions BB / Reference data



Quick Review: What are Building Blocks?

A building block are a subset of rule tests without any responses. Think of it as a container of rules without an resulting action. The idea being that building blocks are a reusable set of rule tests that users can leverage within other rules when required.

A common example of this is to populate the BB:Host Definition building blocks with the addresses of servers. This allows administrators to either exclude or include rule tests by specific server types, such as VPN servers, Mail servers, LDAP servers, etc.

In order to leverage a building block, a rule test must be added to reference the building block.

In a default QRadar 7.2.7 installation without any content extensions added, there are 123 rules (89 enabled) and 198 building blocks (188 building blocks).

Such as:

BB:ComplianceDefinition

BB:CategoryDefinition

BB:PortDefinition

BB:DeviceDefinition

BB:Flowshape

BB:FalsePositive

BB:ProtocolDefinition

and more...

What are Host Definition: Building Blocks?

Host definition building blocks (BB:HostDefinition) are used by QRadar to discover and classify server types on the network. If a particular server is not automatically detected, you can manually add the server to its corresponding host definition building block using an IP or CIDR range.

This ensures that the appropriate rules are applied to a particular server type. However, building blocks are used as categorizers for rule and have no action of their own.

If there is not a category that fits common server types in your network, you can copy/modify a Host Definition:BB to meet your requirements.

By default, there are 27 HostDefinition:BB categories.

- BB:HostDefinition: Consultant Assets
- BB:HostDefinition: Database Servers
- BB:HostDefinition: DHCP Servers
- BB:HostDefinition: DMZ Assets
- BB:HostDefinition: DNS Servers
- BB:HostDefinition: FTP Servers
- BB:HostDefinition: Host with Port Open
- BB:HostDefinition: LDAP Servers
- BB:HostDefinition: Local Assets
- BB:HostDefinition: Mail Servers
- BB:HostDefinition: MailServer Assets
- BB:HostDefinition: Network Management Servers
- BB:HostDefinition: Protected Assets
- BB:HostDefinition: Proxy Servers
- BB:HostDefinition: Regulatory Assets
- BB:HostDefinition: Remote Assets
- BB:HostDefinition: RPC Servers
- BB:HostDefinition: Servers
- BB:HostDefinition: SNMP Sender or Receiver
- BB:HostDefinition: SSH Servers
- BB:HostDefinition: Syslog Servers and Senders
- BB:HostDefinition: VA Scanner Source IP
- BB:HostDefinition: Virus Definition and Other Update Servers
- BB:HostDefinition: VoIP PBX Server
- BB:HostDefinition: VPN Assets
- BB:HostDefinition: Web Servers
- BB:HostDefinition: Windows Servers

Host Definition: Building Blocks (continued)

Why are host definition building blocks important?

These building blocks categorize assets / server types in to CIDR/IP ranges. Populating host definition building blocks allows QRadar to understand the type of appliance that belongs to an address or address range.

These building blocks can then be leveraged in rules to exclude or include entire asset categories in rule tests.

Rule

Apply Database Remote Login Failure on events which are detected by the Local system
and when the source is Remote
and when an event matches any of the following BB:HostDefinition: Database Servers, BB:HostReference: Database Servers
and when an event matches all of the following BB:CategoryDefinition: Authentication Failures

Alternately, use reference sets to capture data or categorize appliances and use these instead of Host Definition:BB.

The downside is that default QRadar rules do not leverage reference sets by default. However, some content packs do include reference sets, with building blocks and matching rule definitions.

The Core Foundations

Server Discovery



What is Server Discovery?

Server discovery uses existing asset profile data to allow administrators to define unknown server types and assign them to a server definition and also the Network Hierarchy.

You must have asset data on your Assets tab. Asset data is populated by:

1. Vulnerability scan data
2. Flows – passive asset identification

Administrators who have asset data populated using Vulnerability (VA) scanners or asset data from passive flow data can define server types by port information.

Server Discovery

To discover servers (assets) in your deployment based on standard server ports, select the desired role in the Server Type drop-down list box and click 'Discover Servers'.

Server Type:	Database Servers <input type="button" value="v"/> <input type="radio"/> All <input type="radio"/> Assigned <input checked="" type="radio"/> Unassigned
Ports:	1433, 1434, 3306, 66, 1521, 1525, 1526, 1527, 1528, 1529, 1571, 1575, 1630, 1748, 1754, 1808, 1809, 2481, 2482, 2484, 3872, 3891, 3938 Edit Ports
Server Type Definition:	Edit this BB to define typical database servers. This BB is used in conjunction with the BB.FalsePositive: Database Server False Positive Categories blocks. Edit Definition
Network:	Select an object... <input type="button" value="v"/>

Matching Servers:

Approved	Name	IP Address	
<input type="checkbox"/>	10.101.140.111	10.101.140.43	Net-10-172-192.Net_10_0_0_0
<input type="checkbox"/>	10.101.140.43	10.101.140.43	Net-10-172-192.Net_10_0_0_0
<input type="checkbox"/>	10.101.161.85	10.101.161.85	Net-10-172-192.Net_10_0_0_0
<input type="checkbox"/>	10.103.77.143	10.103.77.143	Net-10-172-192.Net_10_0_0_0
<input type="checkbox"/>	10.103.77.211	10.103.77.211	Net-10-172-192.Net_10_0_0_0
<input type="checkbox"/>	10.103.78.111	10.103.78.111	Net-10-172-192.Net_10_0_0_0

Server Discovery does **not** scan your network.
Server Discovery does **not** look into events and flows.
Server Discovery only searches asset profiles.

The Core Foundations

QRadar Content Extensions



Content Extensions

QRadar by default includes 321 entries in the custom rule table in QRadar (7.2.7). This includes 123 rules (89 enabled) and 198 building blocks (188 building blocks).

During the QRadar 7.2.6 release, QRadar shipped with ~660 default rules in our enterprise template. The enterprise template was broken in to core SIEM rules and categories. There are currently 20 content extensions available for QRadar on the X-Force App Exchange.

For example:

- QRadar Intrusion Content Extension
- QRadar Anomaly Content Extension
- QRadar Reconnaissance Content Extension
- QRadar Threat Content Extension
- QRadar Baseline Maintenance Content Extension
- QRadar Security Compliance Content Extension

Specific product extensions and compliance specific extensions are also released:

- QRadar ISO 27001 Content Extension
- Microsoft Security Event Log Content Extension
- SOX, HIPPA, PCI, GPG13, FISMA, GLBA, NERC
- ThreatStream Content Extension
- VMware Content Extension

Tuning Methodology

“Computers are like Old Testament gods; lots of rules and no mercy.”
- Joseph Campbell



Where to start?

A common misconception when tuning is to start looking at the data on **Offenses > All Offenses**. This can be time consuming and doesn't provide an initial direction to administrators who have to tune the system.

In this section, we are going to discuss two tuning methods that can help increase success for most administrators:

1. Creating a SIEM Tuning Report
2. Tuning by Offense Category

Don't start on the All Offenses Page.

The screenshot shows the IBM QRadar Security Intelligence interface. The main panel displays a list of offenses with columns for ID, Description, Offense Type, Offense Source, Magnitude, Source IP(s), Destination IP(s), and User. An arrow points from the text 'Don't start on the All Offenses Page.' to the 'All Offenses' page in the interface. A detailed view of Offense 173 is shown in a pop-up window.

ID	Description	Offense Type	Offense Source	Magnitude	Source IP(s)	Destination IP(s)	User
1471	Multiple Login Failures for the Same User containing Root Login Failed	Multiple (10)	Local (11)	root			root
1408	Assess potential inbound connections from the Internet to regulatory assets	Event Name	Assess potential inbound	Multiple (5)	Local (5)		admin
1463	Assess actual inbound connections from the Internet to regulatory assets	Event Name	Assess actual inbound	Multiple (5)	Local (5)		admin
1482	Potentially Successful Exploit preceded by Exploit Followed by Suspicious Host Activity - Chained preceded by Multiple Vector Attacker Detected preceded...	Source IP	10.0.240.4		dhcp-4-users-1.a...	Multiple (1,185)	Multiple (7)
1511	Attack Followed by an Attack Response preceded by Policy: Chat or IM Traffic Detected preceded by Exploit Followed by Suspicious Host Activity - Chained...	Source IP	10.0.230.231		dhcp-231-vpn.ac...	Multiple (1,750)	Multiple (3)
1481	Compliance: assess regulatory assets using insecure protocols	Event Name	Compliance: assess re...	Multiple (5)	Local (5)		admin
2448	Excessive Firewall Denies Between Hosts containing Firewall Drop	Source IP	61.19.50.229		61.19.50.229	Local (2)	N/A
2453	Traffic from Untrusted Network to Trusted Network	Source IP	0.0.0.0		0.0.0.0	10.0.120.200	Multiple (7)
2483	SMTP Mail Sender containing Mail SMTP	Source IP	10.0.220.30		10.0.220.30	Remote (8)	N/A
2446	Sensitive Data in Transit containing Web Application: XAMMS/COPIE	Source IP	10.0.240.179		10.0.240.170	10.0.220.153.11	N/A
906	OS Attack: MS SMB2 Validate Provider Callback CVE-2009-3183	Event Name	OS Attack: MS SMB2 Val...	Multiple (26)	Local (20)	Multiple (2)	
2452	Authentication attempted by unauthorized user	Username	victoria_ennis		dhcp-235-users-2...	10.0.10.42	victoria_ennis
2486	Local UDP Scanner Detected containing HTTP/IPv6	Source IP	10.0.100.23		dhcp-23-building...	Remote (83)	N/A
2489	Multiple Login Failures for the Same User containing Logon Failed	Username	T05		10.15.101.12	127.0.0.1	T05
2125	Unauthorised Users on Credentials Objects - Alert	Username	usdc0571		dhcp-83-users-1	10.0.10.42	usdc0571
1487							
1476							
2455							
1480							
901							
2459							
2457							
1518							
1512							
1007							
2482							
2479							
2460							
2451							
2488							
1720							
2447							
2449							

Offense 173	
Magnitude	
Domain	Default Domain
Description	Potentially Successful Exploit preceded by Local Database Scanner Detected preceded by Policy: Chat or IM Traffic Detected preceded by Local UDP Scanner Detected preceded by Large Outbound Transfer High Rate of Transfer preceded by Internal Connection to Possible Malware Host
Source IP(s)	10.0.240.143 (10.0.240.143)
Destination IP(s)	10.0.240.143 (10.0.240.143)Remote (75)
Network(s)	Multiple (2)
Offense Source Summary	

Tuning Methodology

Creating a SIEM Tuning Report

“Computers are like Old Testament gods; lots of rules and no mercy.”
- Joseph Campbell



Step 1: SIEM Tuning Report

IBM QRadar Security Intelligence

Dashboard Offenses Log Activity Network Activity Assets Forensics Reports

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Pos

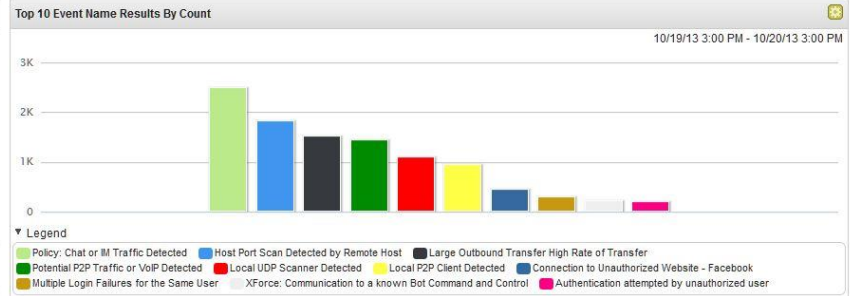
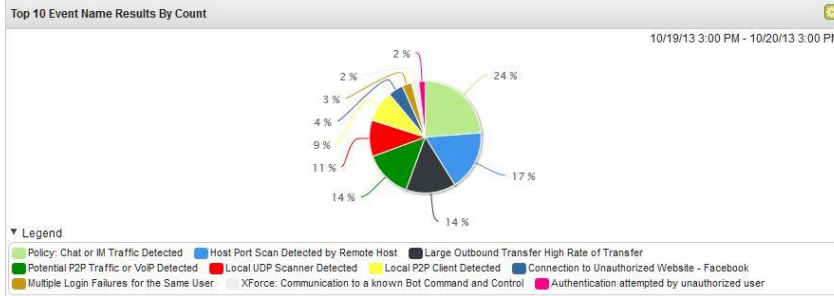
Advanced Search

Viewing event... 2013. 3

Grouping By:
Event Name

Current Filters:
Log Source is Custom Rule Engine-8 :: QRDemoV2 (Clear Filter)

► Current Statistics



(Hide Charts)


Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
Policy: Chat or IM Traffic Detected	Multiple (15)	Multiple (16)	Multiple (6)	Custom Rule Engine-8 :: QRDemoV2	IRC/IM Policy Violation	Multiple (2)	None	6	2,496	2,496
Host Port Scan Detected by Remote Host	80.96.34.22	10.0.52.60	Multiple (612)	Custom Rule Engine-8 :: QRDemoV2	Host Port Scan	tcp_ip	None	8	1,825	1,825
Large Outbound Transfer High Rate of Transfer	Multiple (83)	Multiple (230)	Multiple (34)	Custom Rule Engine-8 :: QRDemoV2	Data Loss Possible	Multiple (2)	None	6	1,513	1,513
Potential P2P Traffic or VoIP Detected	Multiple (63)	Multiple (1,175)	Multiple (1,140)	Custom Rule Engine-8 :: QRDemoV2	Host Port Scan	Multiple (2)	None	8	1,449	1,449
Local UDP Scanner Detected	Multiple (63)	Multiple (948)	Multiple (911)	Custom Rule Engine-8 :: QRDemoV2	UDP Reconnaissance	udp_ip	None	7	1,103	1,103
Local P2P Client Detected	Multiple (64)	Multiple (103)	Multiple (57)	Custom Rule Engine-8 :: QRDemoV2	P2P Policy Violation	Multiple (2)	None	8	947	947
Connection to Unauthorized Website - Facebook	Multiple (59)	Multiple (30)	80	Custom Rule Engine-8 :: QRDemoV2	Web Policy Violation	tcp_ip	None	6	456	456
Multiple Login Failures for the Same User	Multiple (16)	Multiple (7)	0	Custom Rule Engine-8 :: QRDemoV2	User Login Failure	Other	Multiple (4)	8	292	292
XForce: Communication to a known Bot Command a...	Multiple (46)	Multiple (3)	Multiple (2)	Custom Rule Engine-8 :: QRDemoV2	Potential Botnet Con...	tcp_ip	None	8	222	222
Authentication attempted by unauthorized user	Multiple (20)	Multiple (20)	0	Custom Rule Engine-8 :: QRDemoV2	Multiple (2)	Other	Multiple (4)	6	192	192
Local SSH Scanner Detected	10.0.52.60	Multiple (131)	22	Custom Rule Engine-8 :: QRDemoV2	Misc Recon Event	tcp_ip	None	7	179	179
Local Web Scanner Detected	10.0.52.60	Multiple (122)	Multiple (2)	Custom Rule Engine-8 :: QRDemoV2	Web Reconnaissance	tcp_ip	None	7	152	152

Displaying 1 to 40 of 42 items (Elapsed time: 0:00:00.114)

Step 2: SIEM Tuning Report – Save it

It is also recommended that admins make this tuning report in to a dashboard to view how tuning changes reduce unnecessary offenses over time.

Save Criteria

 Please enter the name of this search below.

Search Name:

Assign Search to Group(s) [Manage Groups](#)

- Authentication, Identity and User Activity
- Identity Exclusion
- Compliance
- Log Sources
- AntiVirus

Timespan options:

Last Interval (auto refresh) Recent Specific Interval

Include in my Quick Searches Set as Default

Share With Everyone Include in my Dashboard

Step 3: Review – What rules are generating offenses?

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)
Policy: Chat or IM Traffic Detected	Multiple (14)	Multiple (18)	Multiple (6)	Custom Rule Engine-8 :: QRDemoV2	IRC/IM Policy Violation	Multiple (2)	None	6	2,471
Host Port Scan Detected by Remote Host	🇺🇸 80.96.34.22	10.0.52.60	Multiple (610)	Custom Rule Engine-8 :: QRDemoV2	Host Port Scan	tcp_ip	None	8	1,806
Large Outbound Transfer-High Rate of Transfer	Multiple (83)	Multiple (229)	Multiple (34)	Custom Rule Engine-8 :: QRDemoV2	Data Loss Possible	Multiple (2)	None	6	1,497
Potential P2P Traffic or VoIP Detected	Multiple (63)	Multiple (1,157)	Multiple (1,122)	Custom Rule Engine-8 :: QRDemoV2	Host Port Scan	Multiple (2)	None	8	1,427
Local UDP Scanner Detected	Multiple (63)	Multiple (935)	Multiple (898)	Custom Rule Engine-8 :: QRDemoV2	UDP Reconnaissance	udp_ip	None	7	1,087
Local P2P Client Detected	Multiple (64)	Multiple (102)	Multiple (56)	Custom Rule Engine-8 :: QRDemoV2	P2P Policy Violation	Multiple (2)	None	8	932
Connection to Unauthorized Website - Facebook	Multiple (58)	Multiple (30)	80	Custom Rule Engine-8 :: QRDemoV2	Web Policy Violation	tcp_ip	None	6	446
Multiple Login Failures for the Same User	Multiple (15)	Multiple (7)	0	Custom Rule Engine-8 :: QRDemoV2	User Login Failure	Other	Multiple (4)	8	292
XForce: Communication to a known Bot Command a...	Multiple (46)	Multiple (3)	Multiple (2)	Custom Rule Engine-8 :: QRDemoV2	Potential Botnet Con...	tcp_ip	None	8	221
Custom Rule Engine Message	172.16.60.150	172.16.60.150	0	Custom Rule Engine-8 :: QRDemoV2	Stored	Other	None	4	220
Authentication attempted by unauthorized user	Multiple (20)	Multiple (21)	0	Custom Rule Engine-8 :: QRDemoV2	Multiple (2)	Other	Multiple (4)	6	195
Local SSH Scanner Detected	10.0.52.60	Multiple (131)	22	Custom Rule Engine-8 :: QRDemoV2	Misc Recon Event	tcp_ip	None	7	177
Local Web Scanner Detected	10.0.52.60	Multiple (121)	Multiple (2)	Custom Rule Engine-8 :: QRDemoV2	Web Reconnaissance	tcp_ip	None	7	151
Local FTP Scanner	10.0.52.60	Multiple (106)	21	Custom Rule Engine-8 :: QRDemoV2	FTP Reconnaissance	tcp_ip	None	7	142
Login Failures Followed By Success from the same ...	Multiple (5)	Multiple (4)	0	Custom Rule Engine-8 :: QRDemoV2	Suspicious Pattern D...	Other	Multiple (3)	8	137
Login Failures Followed By Success to the same De...	Multiple (3)	127.0.0.1	0	Custom Rule Engine-8 :: QRDemoV2	Suspicious Pattern D...	Other	Multiple (4)	6	116
Exploit Followed by Suspicious Host Activity	Multiple (114)	Multiple (52)	0	Custom Rule Engine-8 :: QRDemoV2	Misc Exploit	Multiple (2)	Multiple (51)	9	114
Sensitive Data in Transit	Multiple (3)	Multiple (48)	80	Custom Rule Engine-8 :: QRDemoV2	User Activity	tcp_ip	None	8	90
Vulnerability Discovered on Local Host	127.0.0.1	127.0.0.1	0	Custom Rule Engine-8 :: QRDemoV2	New Vuln Discovered	Other	None	5	90
Local LDAP Scanner	10.0.52.60	Multiple (60)	389	Custom Rule Engine-8 :: QRDemoV2	Misc Recon Event	tcp_ip	None	7	63
Local Windows Scanner Detected	10.0.52.60	Multiple (55)	Multiple (5)	Custom Rule Engine-8 :: QRDemoV2	Windows Reconnaiss...	tcp_ip	None	7	62
Multiple Vector Attacker Detected	Multiple (37)	Multiple (43)	Multiple (15)	Custom Rule Engine-8 :: QRDemoV2	Misc Exploit	Multiple (3)	Multiple (18)	8	53
Log Source Stopped Sending Events	Multiple (40)	Multiple (20)	Multiple (5)	Custom Rule Engine-8 :: QRDemoV2	System Failure	Multiple (3)	Multiple (9)	9	49
Exploit Followed by Suspicious Host Activity - Chained	Multiple (27)	Multiple (13)	0	Custom Rule Engine-8 :: QRDemoV2	Misc Exploit	Multiple (2)	Multiple (26)	8	40
Multiple Login Failures to the Same Destination	Multiple (2)	127.0.0.1	0	Custom Rule Engine-8 :: QRDemoV2	Remote Access Logi...	Other	Multiple (3)	7	38
Traffic from Untrusted Network to Trusted Network	Multiple (3)	Multiple (2)	0	Custom Rule Engine-8 :: QRDemoV2	Compliance Policy Vi...	Other	Multiple (28)	6	37
Attack Followed by an Attack Response	Multiple (27)	Multiple (24)	Multiple (22)	Custom Rule Engine-8 :: QRDemoV2	Misc Exploit	Multiple (3)	Multiple (10)	9	34
DDOS Detected	127.0.0.1	127.0.0.1	0	Custom Rule Engine-8 :: QRDemoV2	User Activity	Other	None	6	28
SMTP Mail Sender	Multiple (2)	Multiple (15)	Multiple (2)	Custom Rule Engine-8 :: QRDemoV2	Mail Policy Violation	tcp_ip	None	8	15
Excessive Firewall Denies Between Hosts	🇺🇸 61.19.50.229	Multiple (4)	0	Custom Rule Engine-8 :: QRDemoV2	ACL Deny	Other	None	7	11
Potentially Successful Exploit	Multiple (7)	Multiple (7)	Multiple (3)	Custom Rule Engine-8 :: QRDemoV2	Misc Exploit	Multiple (2)	None	10	7
Potential Data Loss	Multiple (4)	Multiple (3)	Multiple (3)	Custom Rule Engine-8 :: QRDemoV2	ACL Deny	Multiple (2)	None	8	4
Local P2P Scanner	192.168.2.207	Multiple (3)	6881	Custom Rule Engine-8 :: QRDemoV2	Misc Recon Event	udp_ip	None	4	3
Communication to a known Bot Command and Control Information - Event CRE	Multiple (3)	Multiple (2)	6667	Custom Rule Engine-8 :: QRDemoV2	Potential Botnet Con...	tcp_ip	None	5	3
Botnet: Successful Inbound Connection from a Know...	🇺🇸 108.61.240.240	Multiple (2)	Multiple (2)	Custom Rule Engine-8 :: QRDemoV2	Web	tcp_ip	None	6	2
Flow Source/Interface Stopped Sending Flows	Multiple (2)	Multiple (2)	80	Custom Rule Engine-8 :: QRDemoV2	Potential Botnet Con...	tcp_ip	None	4	2
Local P2P Client Connected to more than 100 Servers	192.168.2.207	🇺🇸 84.104.18.64	6881	Custom Rule Engine-8 :: QRDemoV2	P2P Policy Violation	udp_ip	None	5	1
Local IRC Server Detected	🇺🇸 108.61.240.240	192.168.2.46	53987	Custom Rule Engine-8 :: QRDemoV2	IRC Session Opened	tcp_ip	None	6	1
Local TCP Scanner Detected	10.0.110.46	🇺🇸 80.3.209.196	45201	Custom Rule Engine-8 :: QRDemoV2	TCP Reconnaissance	tcp_ip	None	7	1

Step 4: Start to tune rules as required based on your report

Administrators should review the content from Step 3 to determine what rules are firing most. Then review what is making those rules fire and adjust any of the following conditions:

1. Add/Remove Tests
2. Modify Tests/Thresholds
3. Change the Response

4a/4b. Modifying Rule Tests & Thresholds

Add/remove rule tests to tune for data you care about:

- Only to a specific country
- Only from a critical network
- Working hours
- Assets w/vulnerabilities

Adjust the existing rule tests:

- Source bytes greater than 2M
- 30 min window instead of 12

Create a note about changed made to the rule



The screenshot shows the 'Rule Wizard: Rule Test Stack Editor' window. It features a list of test groups with a search filter. The selected rule is 'Apply Policy: Large Outbound Transfer High Rate of Transfer' on flows detected by the 'Local' system. The rule conditions include: 'and when the source bytes is greater than 2000', 'and when at least 5 flows are seen with the same Source IP, Destination Port, Destination IP in 12 minutes', and 'and when the flow context is Local to Remote'. Below the rule, there is a section for selecting groups (Anomaly, Asset Reconciliation Exclusion, Authentication, Botnet, Category Definitions) and a 'Notes' field containing the text: 'Detects a single host that is sending more data out of the network than received. This rule detects over 2 MB of data transferred over a 12 minute period.'

4c. Adjust Your Rule Responses

Examples:

- Enable response limiters
- Trigger scans
- Add to reference set / data

Rule Wizard

Rule Action
Choose the action(s) to take when a flow triggers this rule

Severity Set to 0

Credibility Set to 0

Relevance Set to 0

Ensure the detected flow is part of an offense

Index offense based on Source IP

Annotate this offense:

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

Annotate flow

Drop the detected flow

Rule Response
Choose the response(s) to make when a flow triggers this rule

Dispatch New Event

Enter the details of the event to dispatch

Event Name: Large Outbound Transfer High Rate of Transfer

Email

Send to Local SysLog

Notify

Add to a Reference Set

Add the Source IP of the detected event/flow to the Reference Set:

SuspiciousIPs - IP

Add to Reference Data

Trigger Scan

IBM Security

Tip: Use event searches to quickly find the contributing rule

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)
Policy: Chat or IM Traffic Detected	Multiple (14)	Multiple (18)	Multiple (6)	Custom Rule Engine-8 :: QRDemoV2	IRC/IM Policy Violation	Multiple (2)	None	6	2,471
Host Port Scanned	Multiple (14)	Multiple (18)	Multiple (6)	80.96.34.22	Multiple (83)	Multiple (2)	None	8	1,806
Large Outbound Transfer High Rate of Transfer	Multiple (14)	Multiple (18)	Multiple (6)	Multiple (83)	Multiple (2)	Multiple (2)	None	6	1,497
Potential P2P Traffic or VoIP Detected	Multiple (14)	Multiple (18)	Multiple (6)	Multiple (63)	Multiple (2)	Multiple (2)	None	8	1,427
Local UDP Scanner	Multiple (14)	Multiple (18)	Multiple (6)	Multiple (63)	Multiple (2)	Multiple (2)	None	7	1,087
Local P2P Client	Multiple (14)	Multiple (18)	Multiple (6)	Multiple (63)	Multiple (2)	Multiple (2)	None	8	932
Connection to Remote Host	Multiple (14)	Multiple (18)	Multiple (6)	Multiple (63)	Multiple (2)	Multiple (2)	None	6	446
Multiple Logins	Multiple (14)	Multiple (18)	Multiple (6)	Multiple (63)	Multiple (2)	Multiple (2)	Multiple (4)	8	292
XForce: Command and Control	Multiple (14)	Multiple (18)	Multiple (6)	Multiple (63)	Multiple (2)	Multiple (2)	None	8	221
Custom Rule	Multiple (14)	Multiple (18)	Multiple (6)	Multiple (63)	Multiple (2)	Multiple (2)	None	4	220

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)
Authentication attempted by unauthorized user	Multiple (20)	Multiple (21)	0
Local SSH Scanner Detected	10.0.52.60	Multiple (131)	22
Local Web Scanner Detected	10.0.52.60	Multiple (121)	Multiple (2)
Local FTP Scanner	10.0.52.60	Multiple (106)	21
Login Failures Followed By Success from the same ...	Multiple (5)	Multiple (4)	0
Login Failures Followed By Success to the same De...	Multiple (3)	127.0.0.1	0
Exploit Followed by Suspicious Host Activity	Multiple (114)	Multiple (52)	0
Sensitive Data in Transit	Multiple (3)	Multiple (48)	80
Vulnerability Discovered on Local Host	127.0.0.1	127.0.0.1	0
Local LDAP Scanner	10.0.52.60	Multiple (60)	389
Local Windows Scanner Detected	10.0.52.60	Multiple (55)	Multiple (5)
Multiple Vector Attacker Detected	Multiple (37)	Multiple (43)	Multiple (15)
Log Source Stopped Sending Events	Multiple (40)	Multiple (20)	Multiple (5)
Exploit Followed by Suspicious Host Activity - Chained	Multiple (27)	Multiple (13)	0
Multiple Login Failures to the Same Destination	Multiple (2)	127.0.0.1	0
Traffic from Untrusted Network to Trusted Network	Multiple (3)	Multiple (2)	0
Attack Followed by an Attack Response	Multiple (27)	Multiple (24)	Multiple (22)
DDOS Detected	127.0.0.1	127.0.0.1	0
SMTP Mail Sender	Multiple (2)	Multiple (15)	Multiple (2)
Excessive Firewall Denies Between Hosts	61.19.50.229	Multiple (4)	0
Potentially Successful Exploit	Multiple (7)	Multiple (7)	Multiple (3)
Potential Data Loss	Multiple (4)	Multiple (3)	Multiple (3)
Local P2P Scanner	192.168.2.207	Multiple (3)	6881
Communication to a known Bot Command and Control	Multiple (3)	Multiple (2)	6667
Information - Event CRE	Multiple (2)	Multiple (2)	80
Botnet: Successful Inbound Connection from a Know...	108.61.240.240	Multiple (2)	Multiple (2)
Flow Source/Interface Stopped Sending Flows	Multiple (2)	Multiple (2)	80
Local P2P Client Connected to more than 100 Servers	192.168.2.207	84.104.18.64	6881
Local IRC Server Detected	108.61.240.240	192.168.2.46	53987
Local TCP Scanner Detected	10.0.110.46	80.3.209.196	45201

Return to Event List | Offense | Map Event | False Positive | Extract Property | Previous | Next | Print

Payload Information

utf | hex | base64

Wrap Text

```
Large Outbound Transfer High Rate of Transfer Detects a single host that is sending more data out of the network than received. This rule detects over 2 MB of data transferred over a 12 minute period.
```


Additional Information

Protocol	Log Source	Custom Rules	QID	Event Count
tcp_ip	Custom Rule Engine-8 :: QRDemoV2	Policy: Large Outbound Transfer High Rate of Transfer	70750	1

[Bot Definition: Trojans](#)
[BB:Local To Remote](#)
[Compliance:Load ISO 27001 Building Blocks](#)
[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](#)
[System: Load Building Blocks](#)



Tuning Offenses by Category



Tuning Offenses by Category

The goal of tuning by category is to eliminate the number of offenses being generated by category to quickly reduce the volume of offenses generated in QRadar.

In this example, we see that 700+ offenses are generated under the Audit & Potential Exploit category. Let's expand this for more information.

Step 1: Start your investigation based on what categories are generating the most events. In this case, there are two core categories that are generating large numbers of events.

The screenshot displays the IBM QRadar Security Intelligence interface. The main navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Acti...', 'Assets', 'Forensics', 'Reports', 'Risks', and 'V'. The 'Offenses' section is active, showing a list of offense categories and their counts. A detailed view of the 'Audit' category is expanded on the right, showing sub-categories and their respective counts.

Category Name	Offense Count
▶ Access	3
▶ Malware	3
▶ System	124
▼ Audit	722
Disable Activity Succeeded	1
General Audit Event	30
Read Activity Attempted	123
Delete Activity Succeeded	164
Update Activity Succeeded	189
Create Activity Succeeded	272
Read Activity Succeeded	435
Enable Activity Succeeded	578
▼ Potential Exploit	729
Potential Botnet Connection	729

Viewing the Offenses Summary

1. Double click the Category and then double click an event to view the Offense summary.

▼ Audit	722	0	722	1,037,996
Disable Activity Succeeded	1	0	1	2
General Audit Event	30	0	30	215
Read Activity Attempted	123	0	123	444
Delete Activity Succeeded	164	0	164	848
Update Activity Succeeded	189	0	189	4,458
Create Activity Succeeded	272	0	272	1,564
Read Activity Succeeded	435	0	435	3,662
Enable Activity Succeeded	578	0	578	1,026,803
▼ Potential Exploit	729	0	729	24,493
Potential Botnet Connection	729	0	729	24,493

2. Review the basic summary, note that this offense is not part of a network hierarchy and the description is “New-Non-Servers Communicating with External IP Classified as Dynamic containing File downloaded”.
3. This does not tell use the rules that triggered though, so select **Display > Rules**.

Viewing the Offenses Summary

Review the list of rules that contributed to the offense.

All Offenses > Offense 31,315 (Rules)

Offense 31315 Summary Display ▼ Events Connections Flows View Attack Path Actions ▼ Print Send to Resilient

Magnitude		Status		Relevance	0	Severity	4	Credibility	2
Domain	DomainA								
Description	New-Non-Servers Communicating with External IP Classified as Dynamic containing Read Activity Succeeded			Offense Type	Source IP				
				Event/Flow count	589 events and 0 flows in 4 categories				
Source IP(s)	98.26.119.237			Start	May 11, 2017, 6:30:54 PM				
Destination IP(s)	52.168.128.89			Duration	3d 18h 38m 13s				
Network(s)	other			Assigned to	Unassigned				

List of Rules Contributing to Offense

	Rule Name	Events/Flows	First Event/Flow	Last Event/Flow
	X-Force Premium: Non-Servers Communicating with External IP Classified as Dynamic	589	4d 14h 32m 33s	19h 54m 19s

NOTE: It is a X-Force Premium Rule for Non-Servers Communicating with an External IP Classified as Dynamic.

Viewing the Offenses Summary

Double click the rule to view the rule tests.

In this case, since the NOT exclusion is unable to trigger due to a network hierarchy configuration issue, all Source IP addresses categorized as Dynamic IPs were triggering the rule, if they have a confidence factor of 75 or higher.

Remember that the network hierarchy showed 'other' telling us that the IP in the offense was not part of any Network hierarchy.

What to do next:

1. The administrator could populate the network hierarchy with CIDR ranges.
2. Raise the confidence values
3. Disable the rule

Apply **X-Force Premium: Non-Servers Communicating with External IP** on events or flows which are detected by the **Local** system

and NOT when a flow or an event matches any of the following BB:HostDefinition: Database Servers, BB:HostDefinition: DHCP Servers, BB:HostDefinition: DMZ Assets, BB:HostDefinition: DNS Servers, BB:HostDefinition: FTP Servers, BB:HostDefinition: LDAP Servers, BB:HostDefinition: Mail Servers, BB:HostDefinition: Network Management Servers, BB:HostDefinition: Proxy Servers, BB:HostDefinition: RPC Servers, BB:HostDefinition: Servers, BB:HostDefinition: SSH Servers, BB:HostDefinition: Syslog Servers and Senders, BB:HostDefinition: Virus Definition and Other Update Servers, BB:HostDefinition: VoIP PBX Server, BB:HostDefinition: Web Servers, BB:HostDefinition: Windows Servers

and when Source IP is categorized by X-Force as Dynamic IPs with confidence value greater than 75



False positive rule

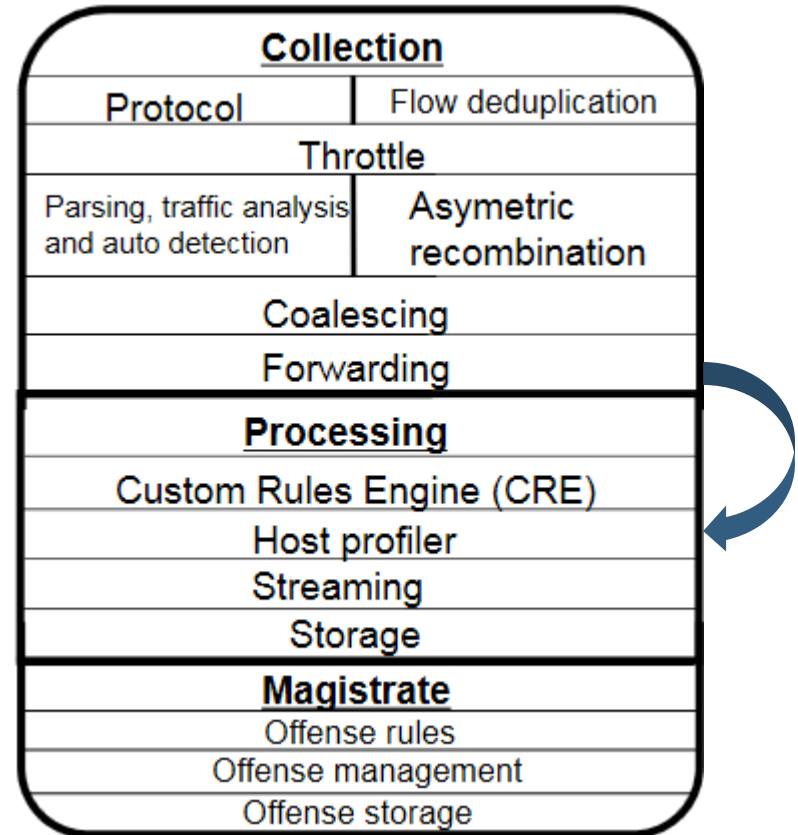


Where to start?

Users can tune out rules that are known to be false positives. False positives act as a bypass CRE action to prevent a rule from generating an offense or any notifications.

The goal of using false positives is to tune out expected behavior to reduce the noise and identify true risks. False positives building blocks are special because they are loaded and evaluated first when they appear as part of a rule test.

False positive rules should only be added as a last resort. There are better methods of reducing false positives such as tuning specific rules, verifying that baseline data is updated, or even using a routing rule to prevent an offense from being triggered.



False Positive – ONLY when it's NOT TRUE!

The screenshot shows a web browser window with the URL `https://172.16.60.150/console/qradar/jsp/ArielSearchWrapper.jsp?`. The navigation bar includes buttons for "Return to Event List", "Offense", "Map Event", "False Positive", and "Extra". Below this is the "Event Information" section, which contains a table with the following data:

Event Name	Botnet: Successful Inbound Connection from a Known
Low	
Cate	
Event	

A context menu is open over the table, listing several options:

- Event: Filter on Event Name is User Login
- Event: Filter on Event Name is not User Login
- Event: Quick Filter...
- Event: **False Positive** (highlighted)
- Event: View path from 172.16.60.10 to 172.16

The screenshot shows a "False Positive" tuning configuration window in Mozilla Firefox. The URL is `https://172.16.60.150/console/do/events/falsePositive`. The window title is "False Positive".

False positive tuning allows you to prevent event/flow(s) from correlating into offenses.

Event/Flow Property

- Event/Flow(s) with a specific QID of 70750173 (*Botnet: Successful Inbound Connection from a Known Botnet CandC*)
- Any Event/Flow(s) with a low level category of *Potential Botnet Connection*
- Any Event/Flow(s) with a high level category of *Potential Exploit*

Traffic Direction

- 108.61.240.240 to 192.168.2.46
- 108.61.240.240 to Any Destination
- Any Source to 192.168.2.46
- Any Source to any Destination

Buttons: Cancel, Tune

Where do I find my false positives?

To edit this tuning, look in 'User-BB-FalsePositive: User Defined False Positives Tunings' building block in the Rules section of the Offense Manager.

Questions


“Good questions outrank easy answers.”
- Paul Samuelson






THANK YOU

FOLLOW US ON:

 <https://www.facebook.com/IBM-Security-Support-221766828033861/>

 QRadar Forums: <https://ibm.biz/BdR2kC>

 [youtube/user/ibmsecuritysupport](https://www.youtube.com/user/ibmsecuritysupport)

 [@askibmsecurity](https://twitter.com/askibmsecurity)

 securityintelligence.com

 xforce.ibmcloud.com

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

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