

NELOGUJTE BEZ LOGIKY

Security information and event management

marek.deters@soitron.com



SOITRON*
INSPIRE TO ASPIRE

CONTENT

- **SIEM?**
 - Roles, functions
- **IBM QRadar**
 - History, now, future
- **Inputs**
 - Asets, logs, netflow
- **How to's with QRadar**
 - Rules, corellations, reference sets, offense chaining, log/flow view, search, licence
- **Outputs**
 - Offenses, forward, export, custom actions, alert, magnitude



HOW DO YOU LOG?

SIEM?



- How do you log?
- Security information and event management
- Event and log collection
- Archive
- Layered Centric Views
- Normalization
- Like really FAST search on big data
- Reporting
- Compliance
- Correlation of events – context
- Scalable
- SIEM is NOT monitoring platform or is it?

IBM QRADAR

- History – Q1 Labs 2011, engine
- Now – IBM, X-Force, cloud
- Future – Watson, X-Force, home, CLOUD
- Integration, API, X-Force APP Exchange
- Requirements, maintenance, people



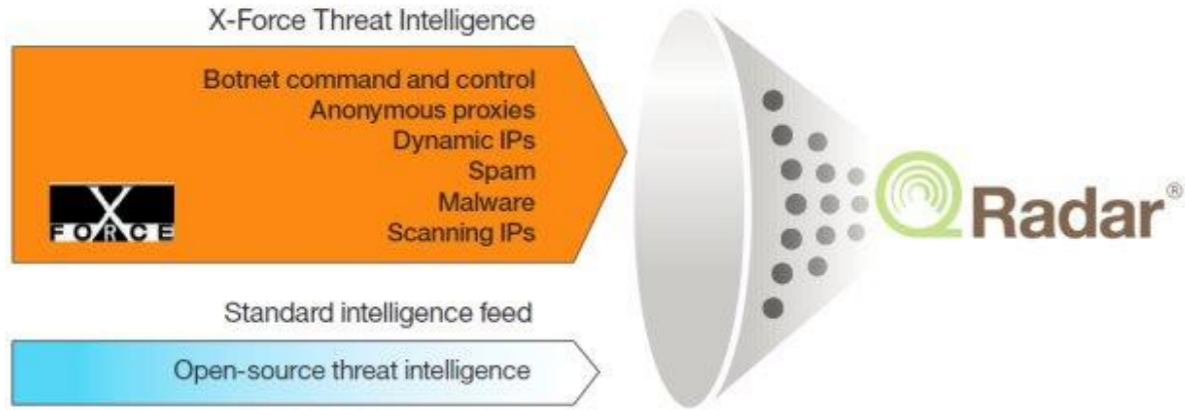
- It's all **“The 24/7 nature of security operations presents a challenge that is costly for most organizations to staff, which is where the appeal of cognitive-enabled security comes in — it never sleeps or fatigues.”**

Michael Pinch

Chief Information Security Officer
University of Rochester

X-FORCE?

<http://ibm.co/2nolbiJ>



Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply X-Force Premium: Internal Host Communicating with Botnet Comma on events which are

- and when the event context is Local to Remote
- and when URL (custom) is categorized by X-Force as Social Media

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

- Anomaly
- Asset Reconciliation Exclusion

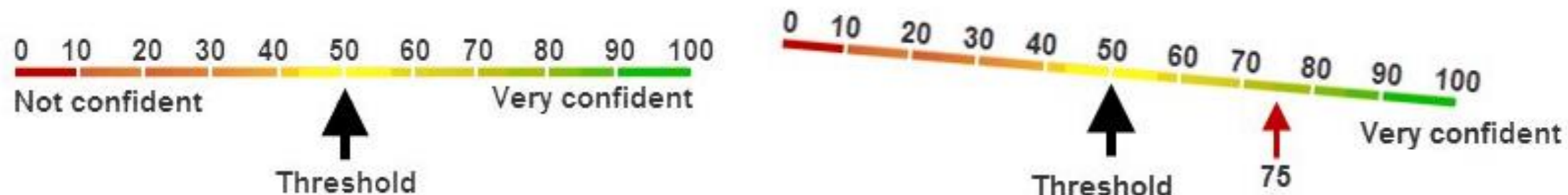
The screenshot shows the 'Rule Wizard - Mozilla Firefox: IBM Edition' window. The address bar contains a redacted URL. The main content area has the instruction 'Select an X-Force URL category and click "Submit"'. Below this is a search box labeled 'Type to filter' with a list of categories: Social Media, Social Networking, Software / Hardware, Software as a Service, Spam URLs, and Sports. An 'Add +' button is located to the right of the list.

X-FORCE FOR FREE IN 7.2.8+

<http://ibm.co/2nolbiJ>

How do I enable X-Force Threat Intelligence in QRadar 7.2.8?

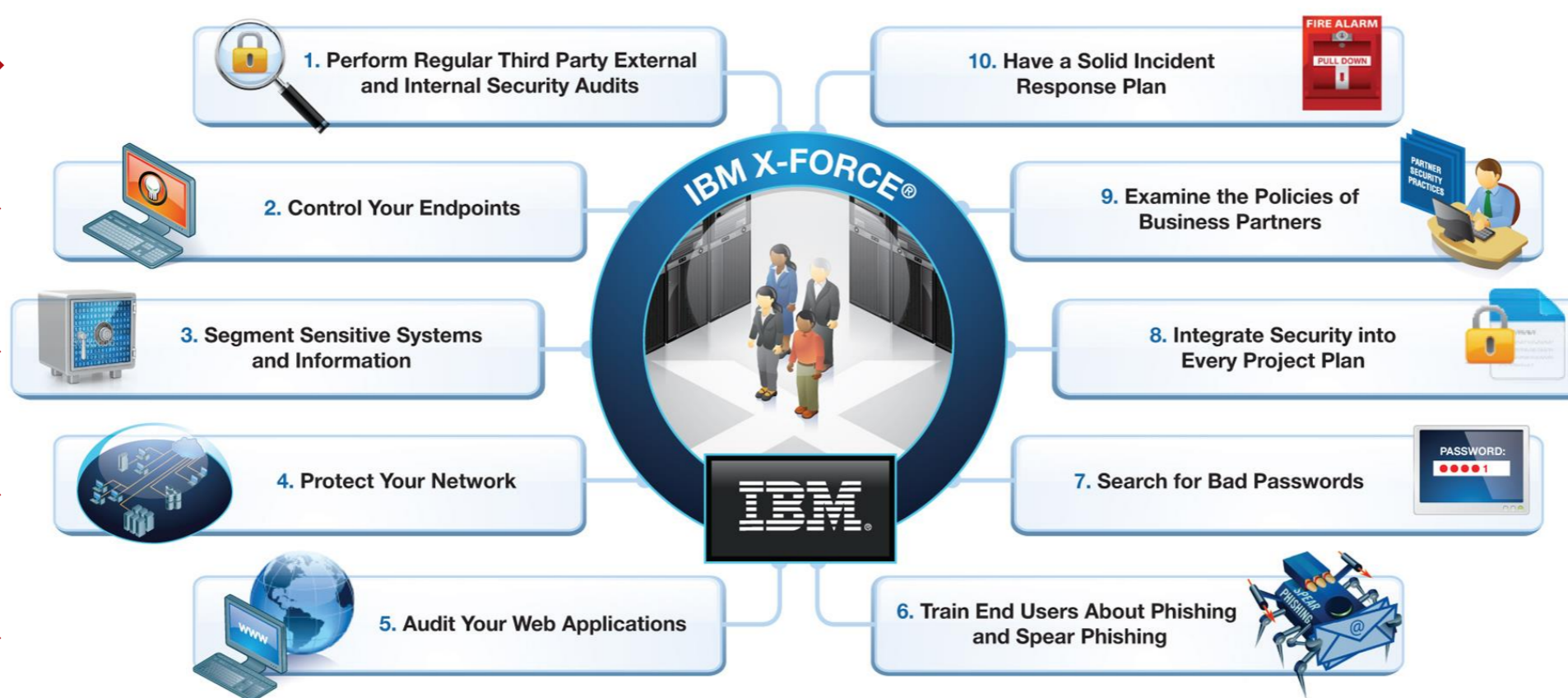
In QRadar 7.2.8, X-Force Threat Intelligence feed no longer needs to be purchased as a separate subscription in 7.2.8. It is included with the standard license as part of Service & Support. Administrators who previously did not have IP and URL reputation data licensed and want to enable X-Force Threat Intelligence feeds can now enable this feature from the System Settings screen of the Admin tab. Any users who do not upgrade to QRadar 7.2.8 remain on their existing subscription model until they upgrade.



IF X-FORCE WAS RUNNING THE IT DEPARTMENT

IF IBM X-FORCE® WAS RUNNING THE IT DEPARTMENT

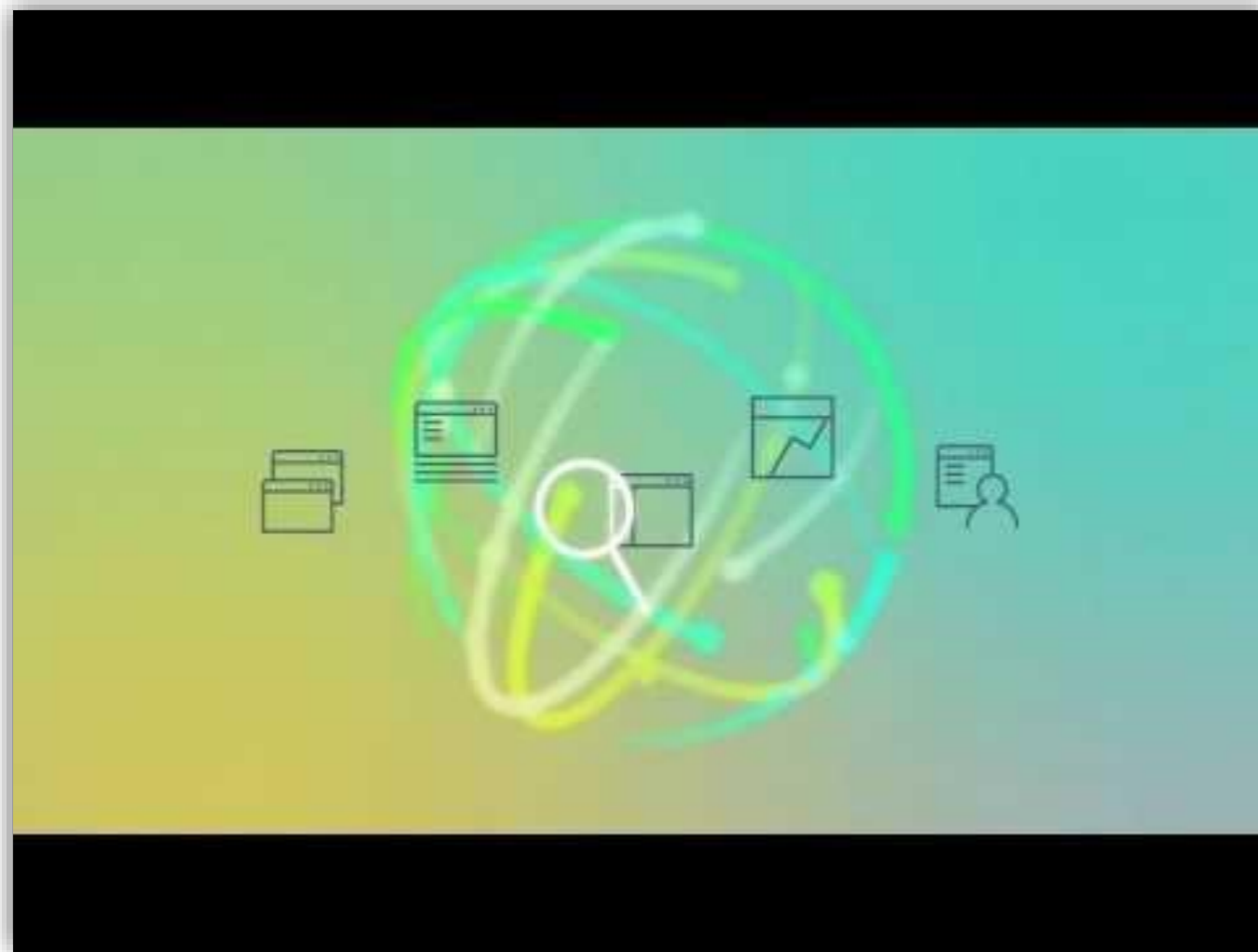
Many readers have asked, if IBM X-Force were running the IT department and saw what happened this year, what would you do? Well, here are ten actions beyond the basics that X-Force would do if we ran the IT department.



Source: IBM X-Force® Research and Development

IBM WATSON?

<http://ibm.co/2n7K001>



IBM Watson YT Channel <http://bit.ly/1IkJTpo>

IBM Security YT Channel <http://bit.ly/1GaLA>

IBM WATSON?

<http://ibm.co/2n7K001>

Buzzwords – machine learning, AI, big data

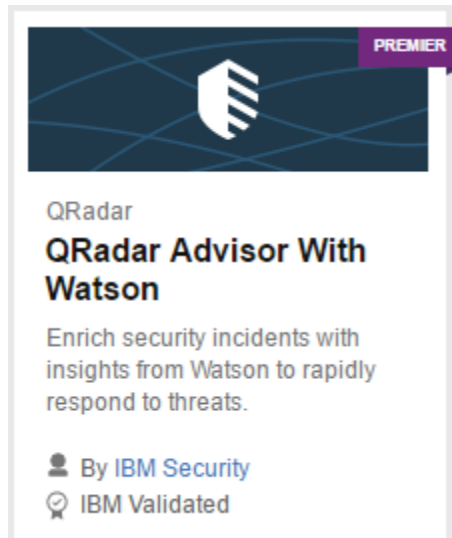
Watson is a question answering (QA) computing system that IBM built to apply advanced natural language processing, information retrieval, knowledge representation, automated reasoning, and machine learning technologies to the field of open domain question answering.

The key difference between QA technology and document search is that document search takes a keyword query and returns a list of documents, ranked in order of relevance to the query (often based on popularity and page ranking), while QA technology takes a question expressed in natural language, seeks to understand it in much greater detail, and returns a precise answer to the question.

According to IBM, "more than 100 different techniques are used to analyze natural language, identify sources, find and generate hypotheses, find and score evidence, and merge and rank hypotheses."

IBM X-FORCE EXCHANGE

<http://bit.ly/1P4mKtu>

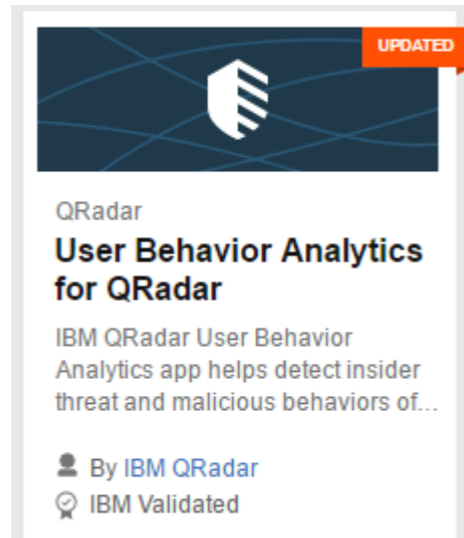


PREMIER

QRadar
QRadar Advisor With Watson

Enrich security incidents with insights from Watson to rapidly respond to threats.

By IBM Security
IBM Validated




UPDATED

QRadar
User Behavior Analytics for QRadar

IBM QRadar User Behavior Analytics app helps detect insider threat and malicious behaviors of...


By IBM QRadar
IBM Validated



QRadar
Qualys App for QRadar

Qualys App for QRadar provides the ability to visualize your network vulnerabilities within IBM QRadar.

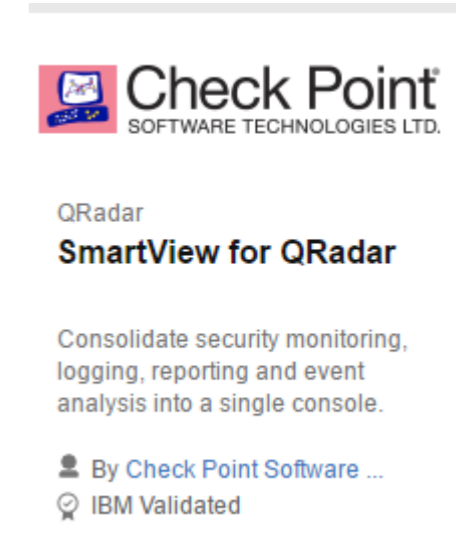
By Qualys
IBM Validated



QRadar
Palo Alto Networks App for QRadar

Reduce, prioritize, and correlate security events and leverage offense workflows to enable...

By Palo Alto Networks
IBM Validated



QRadar
SmartView for QRadar

Consolidate security monitoring, logging, reporting and event analysis into a single console.

By Check Point Software ...
IBM Validated



Mostly for free
Few from IBM itself = supported
Extend features of QRadar
Provide Visualization and more

IBM UBA

<http://bit.ly/1P4mKtu>

IBM QRadar Security Intelligence admin Help Messages 7 IBM System Time: 9:23 AM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin **User Analytics**

Quick insights

Monitored Users
13.9k

Current High Risk Users
251

Sense Events (last hour)
1.3m

Offenses Generated (last hour)
267

System Score (Last 24 Hours)

Risk Category Breakdown (Last Hour) > User Geography

Recent Sense Offenses

Offense # 340 User: Robert Thomas	about 2 hours ago
Event Count: 58 Flow Count: 0 Magnitude: 3	
Offense # 339 User: Joseph James	about 2 hours ago
Event Count: 49 Flow Count: 0 Magnitude: 3	
Offense # 338 User: Eric Jones	about 2 hours ago
Event Count: 47 Flow Count: 0 Magnitude: 3	
Offense # 337 User: William Jackson	about 2 hours ago
Event Count: 59 Flow Count: 0 Magnitude: 3	
Offense # 336 User: David Taylor	about 2 hours ago
Event Count: 46 Flow Count: 0 Magnitude: 3	

Most Risky Users (Overall Score)

Robert Smith	5469	🔴
James Smith	4978	👁️
Michael Smith	4820	👁️
Robert Brown	4722	👁️
John Brown	4636	👁️
James Johnson	4612	👁️
John Johnson	4492	👁️
John Smith	4375	👁️
Michael Johnson	4025	👁️
Robert Williams	3947	👁️

Most Suspicious Users (Window Score)

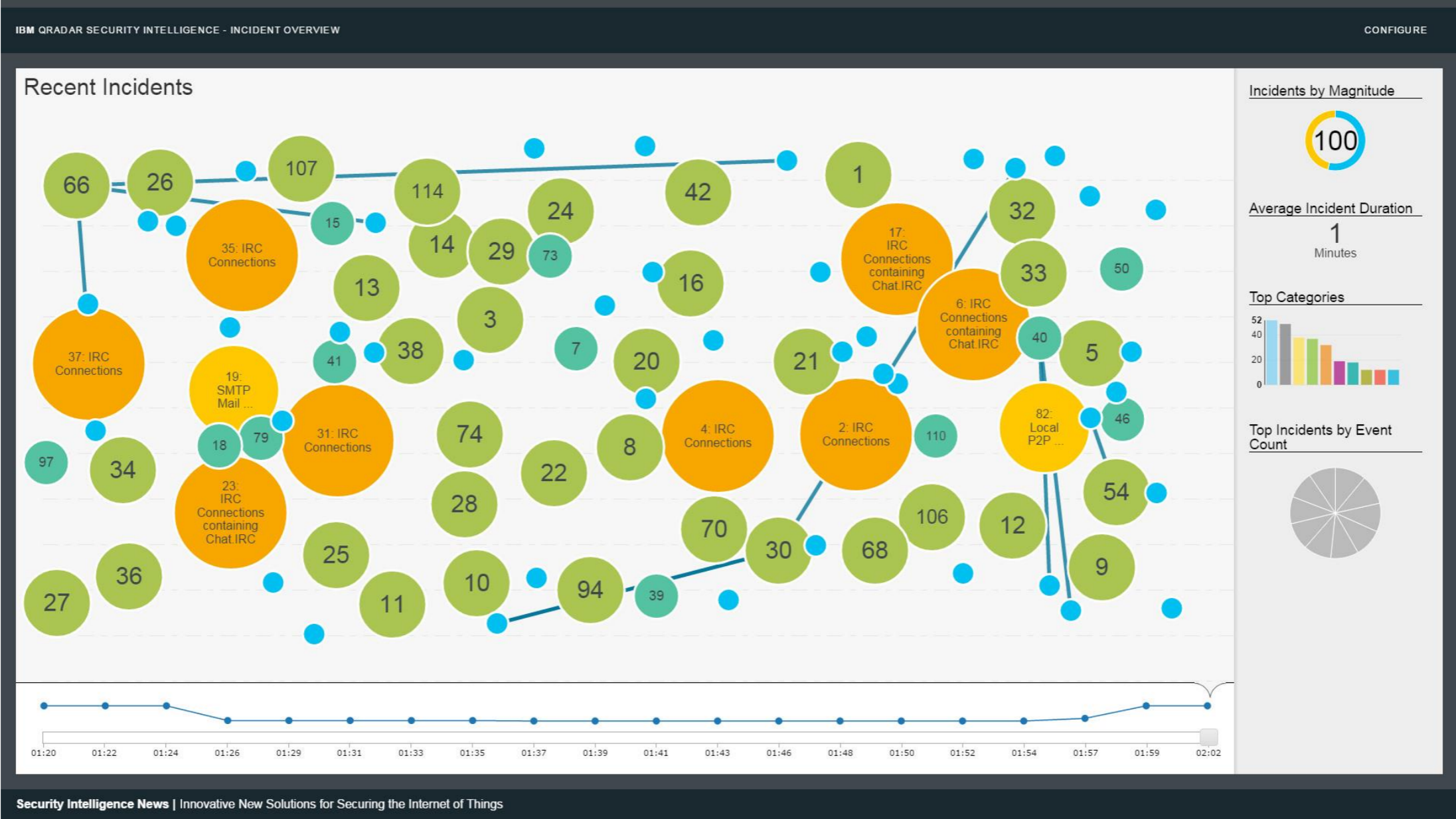
Robert Williams	+335	👁️
James Johnson	+310	👁️
Robert Jones	+300	👁️
John Davis	+275	👁️
James Brown	+265	👁️
John Jackson	+265	👁️
James Jones	+255	👁️
Robert Smith	+255	🔴
William Smith	+245	👁️
William Jones	+245	👁️

Watchlist

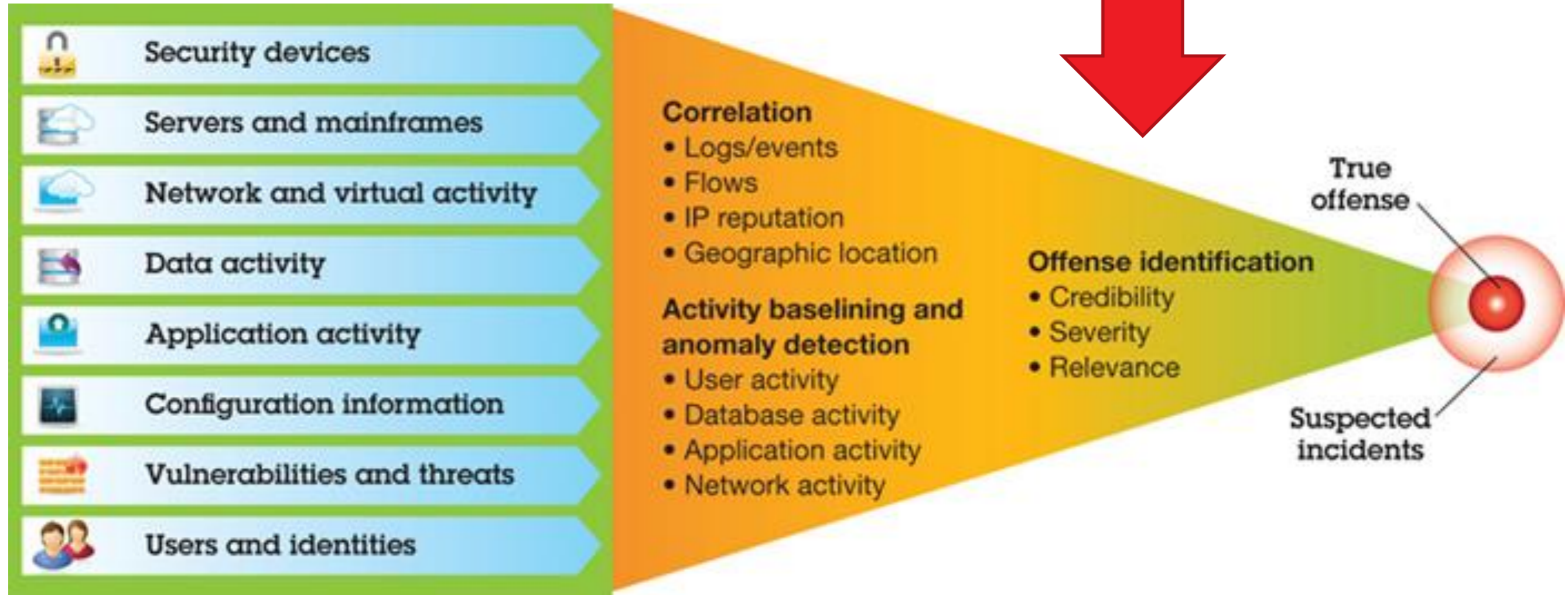
Robert Smith	5.5k	⬇️	⊖
Kenneth Anderson	634.5	⬆️	⊖
Frank Harris	370.5	⬇️	⊖

IBM INCIDENT OVERVIEW

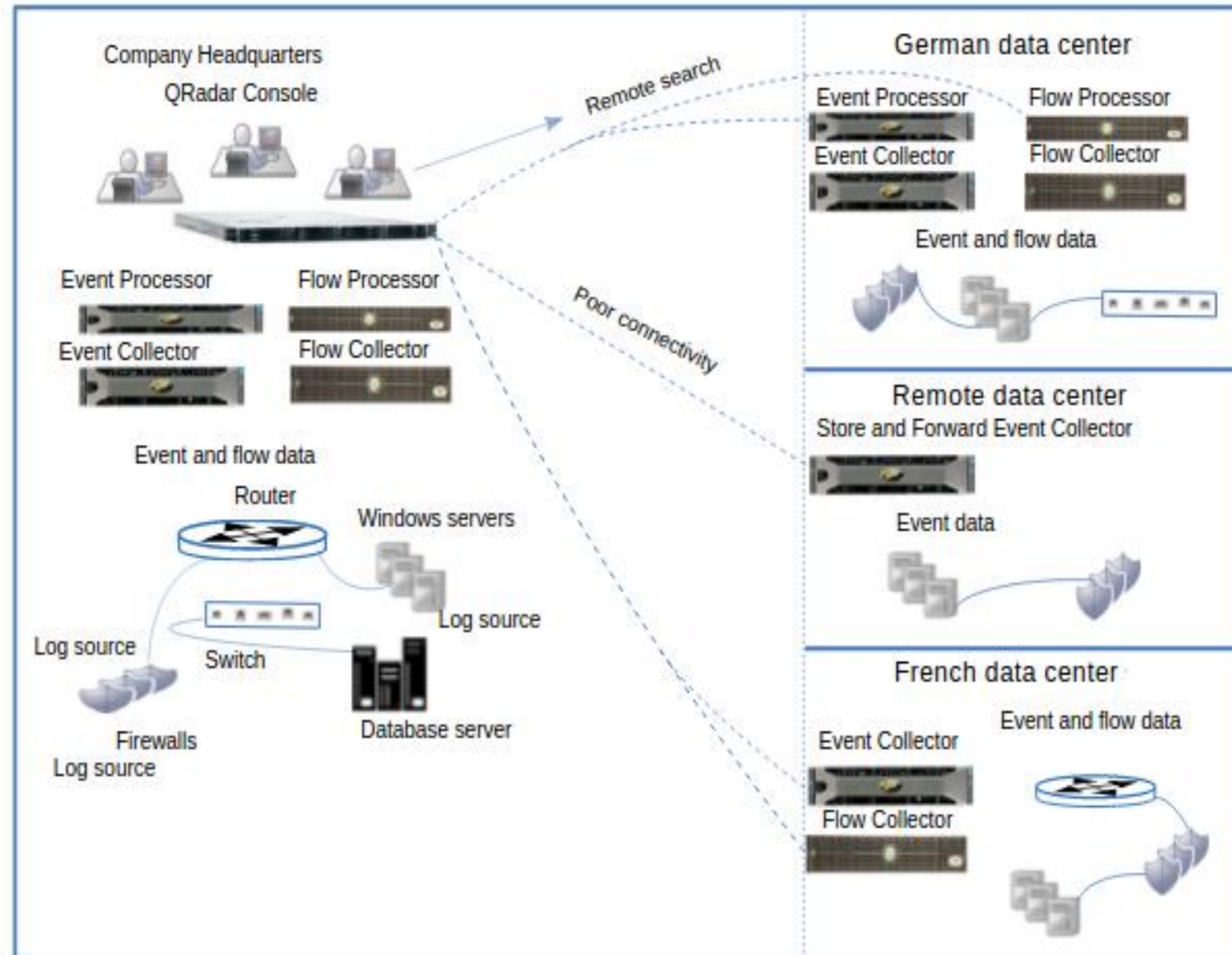
<http://ibm.co/2nKrhuB>



QRADAR HOW IT WORKS?



QRADAR HOW IT WORKS?



QRADAR INPUTS

- **Assets**
 - what, why, how to
- **LogSources / FlowSources**
 - Syslog/NetFlow, Formats, ways to import data to SIEM
 - API
 - DSM – parsers and Manual parsing rules, semi-automatic with GUI DSM Editor
- **Agent or Agentless, that's it's the question**
 - WinCollect, WMI, other
- **Licence model**
 - Limits, buffer for overcommit

QRADAR ASSETS

Sources of asset information

The following sources provide QRadar with asset information:

- **Identity events - Common event sources for identity data:**
 - ✓ Operating system events (Windows, Linux, Mac, UNIX)
 - ✓ DHCP events (routers, switches)
 - ✓ Identity management systems
 - ✓ Authentication events (access points)
 - ✓ Firewalls with VPN services
- **Vulnerability scans – either active scans or scan imports add new assets discovered based on the CIDR ranges defined during the scan.**
- **Importing asset information from the Assets tab (IP, Name, Weight, and description).**
- **DNS lookups**
- **Flow data (bi-directional) provides host profile information for IP address, port information, and applications. Server discovery leverages this information along with scan data to group servers in to building blocks that can be leveraged later on in rules.**

QRADAR SYSLOG EVENT HOW IT LOOK LIKE



Nelogujte bez logiky

Marek Deters (Soitron)

Entrance_System|Information|23.3.2017|8:22:18|UserID:117|

Action:Tourniquet-in|PIN_required:NO|Status:OK

Log name: Security | Logged: 23.3.2017 8:31:36 | An account was successfully **logged on**. | Logon ID: 0x3E7 | Logon Type:

2 | New Logon: Security ID: VIRTUAL\user117 | Linked Logon

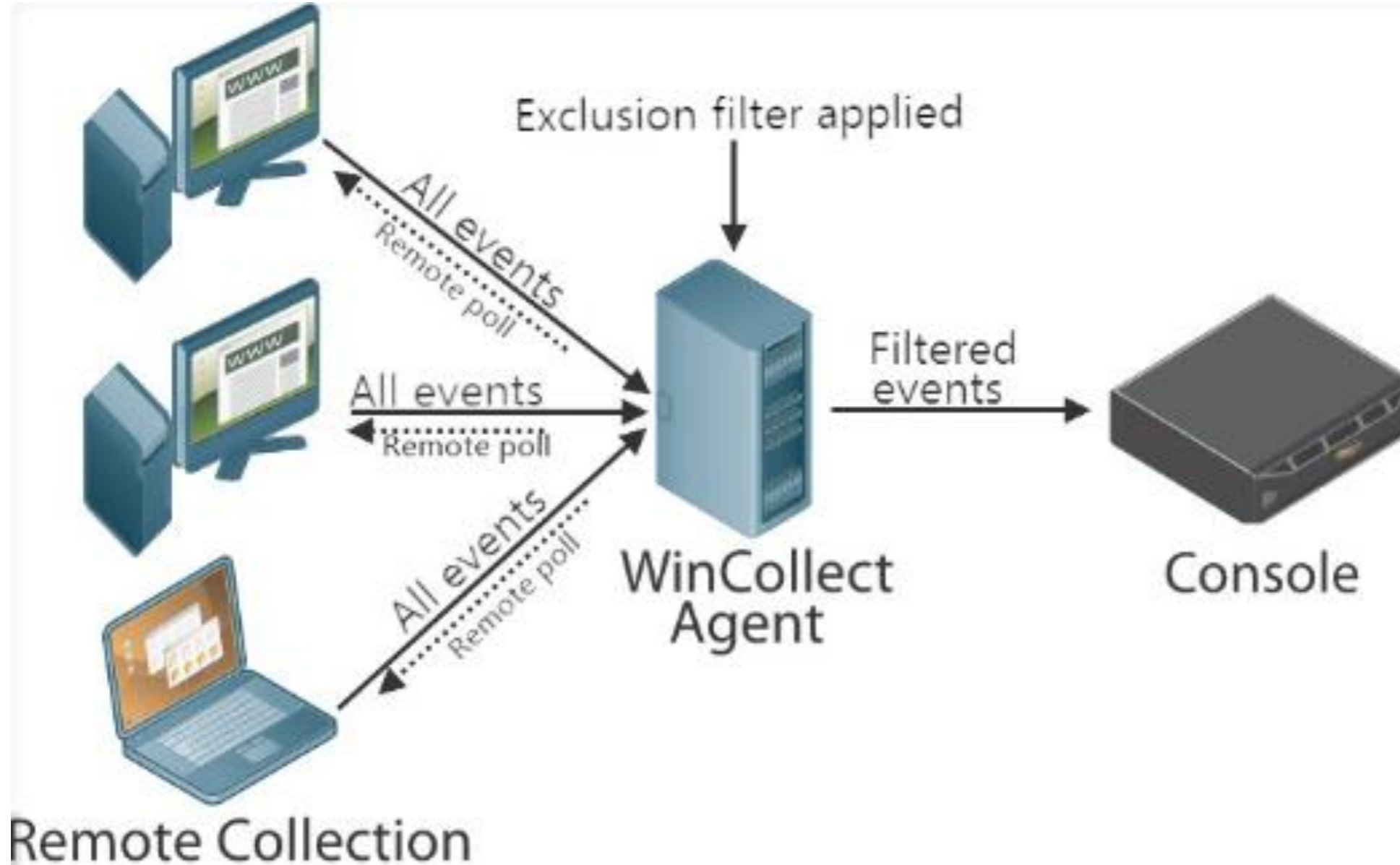
ID: 0x1A605B95 | Workstation Name: DESKTOP117 | Source

Network Address: 127.0.0.1 | Source Port: 0

23.3.2017 9:34:19 %ASA-6-719022: WebVPN user117 has been **authenticated**.

SIEM_ALERT >> **OFFENSE DETECTED**

QRADAR EVENT COLLECTING



WinCollect
WMI
Windows WEF
Linux syslogd
other

QRADAR SYSLOGSOURCES

- Syslog
- JDBC
- JDBC - SiteProtector
- Sophos Enterprise Console - JDBC
- Juniper Networks NSM
- OPSEC/LEA
- SDEE
- SNMPv1
- SNMPv2
- SNMPv3
- Sourcefire Defense Center Estreamer
- Log File
- Microsoft Security Event Log
- Microsoft Security Event Log Custom
- Microsoft Exchange
- Microsoft DHCP
- Microsoft IIS
- EMC VMWare
- SMB Tail
- Oracle Database Listener
- Cisco Network Security Event Logging
- PCAP Syslog Combination Protocol
- Forwarded Protocol
- TLS Syslog Protocol
- Juniper Security Binary Log Collector Protocol
- UDP Multiline Syslog Protocol
- IBM Tivoli Endpoint Manager SOAP Protocol

Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources.

ERROR - Events have not been received from this Log Source in over 720 minutes.

Log Source Name	<input type="text"/>
Log Source Description	<input type="text" value="Palo Alto"/>
Log Source Type	<input type="text" value="Palo Alto PA Series"/>
Protocol Configuration	<input type="text" value="Syslog"/>
Log Source Identifier	<input type="text"/>
Enabled	<input checked="" type="checkbox"/>
Credibility	<input type="text" value="5"/>
Target Event Collector	<input type="text" value="eventcollector0 :: csd32"/>
Coalescing Events	<input checked="" type="checkbox"/>
Incoming Payload Encoding	<input type="text" value="UTF-8"/>
Store Event Payload	<input checked="" type="checkbox"/>
Log Source Extension	<input type="text" value="Select an Extension..."/>
Extension Use Condition	<input type="text" value="Parsing Enhancement"/>

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

- Bulk Imported Log Sources
 - BlueCoat SG test
 - bulklinuxjl
 - gusta-test-bulk
 - TESTBULKEDIT

Save Cancel

QRADAR FLOWSOURCES FORMATS

- NetFlow
- IPFIX
- sFlow
- J-Flow
- PacketeerPacketeer
- Flowlog file
- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

QRADAR API – HTTPS://<CONSOLE IP>/RESTAPI

Integration

Data transfers and sync

Security tokens

list of assets data

Success Responses

HTTP Response	Description
200	The request to retrieve vulnerabilities by asset completed successfully

Error Responses

HTTP Response	Unique Code	Description
420	9101	Invalid search parameters, search cannot be performed

Response Type

MIME Type	Schema
<input checked="" type="checkbox"/> application/json	Warning: No schema available for this response type. Results are not under formal contract.

Parameters

Parameter	Type	Value	Data Type	MIME Type	Schema	Details
savedSearchId	query	<input type="text"/>	String	text/plain	View	Id of saved search
savedSearchName	query	High Risk	String	text/plain	View	Saved search name
filters	query	<input type="text"/>	FilterDTO[]	application/json	View	List of JSON objects for application of bespoke query search dataset filter. Format [{"parameter":"","operator":"","value":""}] e.g. [{"parameter":"IPv4 Address","operator":"Equals","value":"10.100.85.111"}]

[Try it out!](#) [Hide Response](#)

Request URL

https://192.168.254.10:443/restapi/api/qvm/assets?savedSearchName=High+Risk

Request Headers

Version: 1.0
Accept: application/json

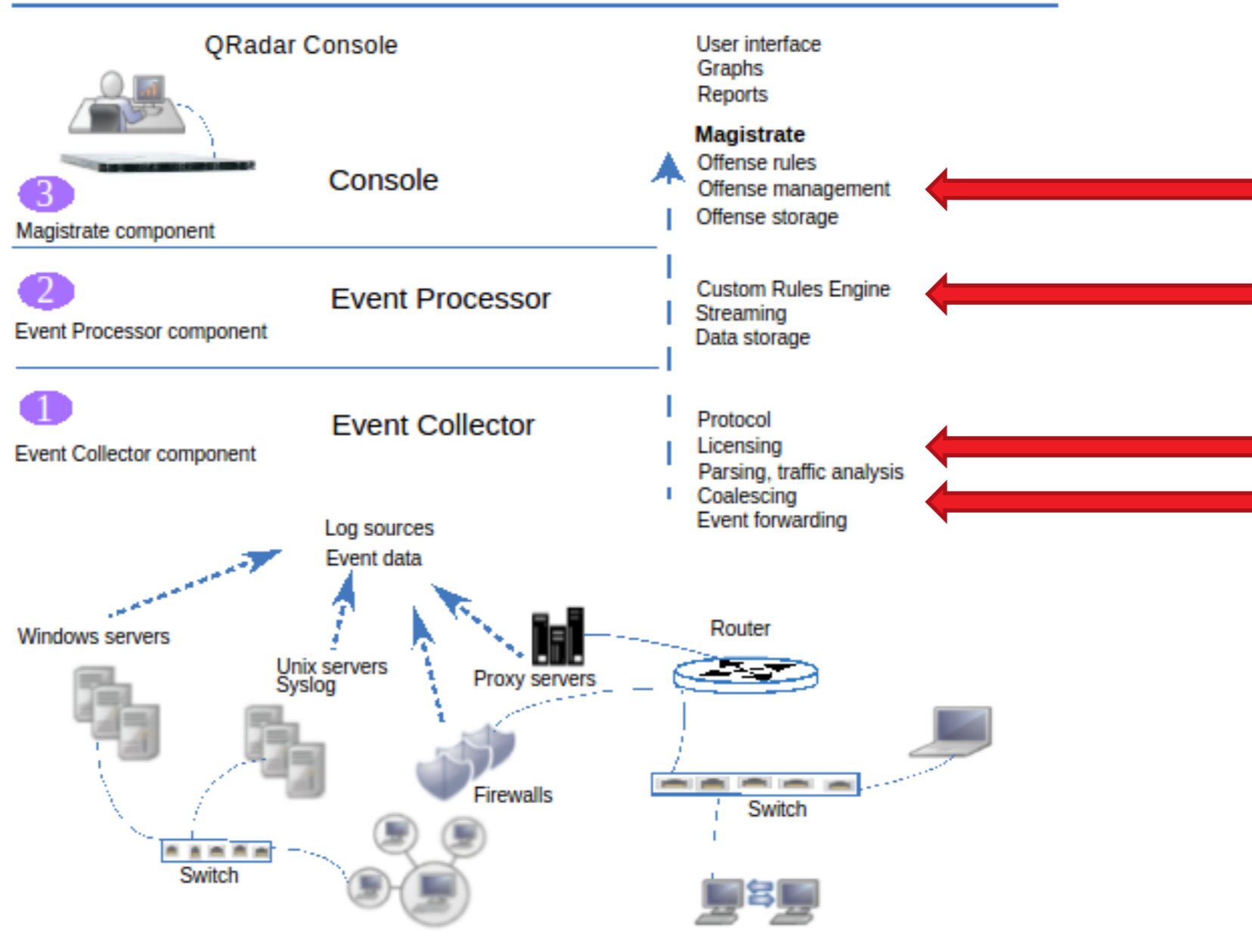
Response Code

QRADAR DSM PARSERS

<http://ibm.co/2ng5qtH>

Cisco	4400 Series Wireless LAN Controller V7.2	Syslog or SNMPv2	All events	Cisco	FireSIGHT Management Center V4.8.0.2 to V6.0.0 (formerly known as Sourcefire Defense Center)	FireSIGHT Management Center	Intrusion events and extra data
Cisco	CallManager V8.x	Syslog	Application events				Correlation events
Cisco	ACS V4.1 and later if directly from ACS V3.x and later if using ALE	Syslog	Failed Access Attempts				Metadata events
Cisco	Aironet V4.x+	Syslog	Cisco Emblem Format				Discovery events
Cisco	ACE Firewall V12.2	Syslog	All events				Host events
Cisco	ASA V7.x and later	Syslog	All events				User events
Cisco	ASA V7.x+	NSEL Protocol	All events				Malware events
Cisco	ASA V7.x+	NSEL Protocol	All events				File events
Cisco	CSA V4.x, V5.x and V6.x	Syslog SNMPv1 SNMPv2	All events	Cisco	Firewall Service Module (FWSM) v2.1+	Syslog	All events
Cisco	CatOS for catalyst systems V7.3+	Syslog	All events	Cisco	Catalyst Switch IOS, 12.2, 12.5+	Syslog	All events
Cisco	Cloud Web Security (CWS)	Amazon AWS S3 REST API	W3C All web usage logs	Cisco	NAC Appliance v4.x +	Syslog	Audit, error, failure, quarantine, and infected events
Cisco	IPS V7.1.10 and later, V7.2.x, V7.3.x	SDEE	All events	Cisco	Nexus v6.x	Syslog	Nexus-OS events
Cisco	IronPort V5.5, V6.5, V7.1, and V7.5	Syslog, Log File Protocol	All events	Cisco	PIX Firewall v5.x, v6.3+	Syslog	Cisco PIX events

QRADAR HOW IT WORKS INTERNALLY?



QRADAR WRITE YOUR OWN RULES 1/4



The screenshot shows the 'Rule Wizard: Rule Test Stack Editor' window. The title bar reads 'Rule Wizard'. Below the title bar, there is a dark header with a red QRadar logo and the text 'Rule Wizard: Rule Test Stack Editor'. The main content area asks 'Which tests do you wish to perform on incoming events?'. Below this question, there is a 'Test Group' dropdown menu currently set to 'All', and an 'Export as Building Block' button to its right. A red arrow points to the 'Test Group' dropdown. Below the dropdown is a search bar labeled 'Type to filter'. A list of test conditions is displayed below the search bar, each preceded by a green checkmark icon. The list includes:

- when the local network is one of the following networks
- when the destination network is one of the following networks
- when the IP protocol is one of the following protocols
- when the Event Payload contains this string
- when the source port is one of the following ports
- when the destination port is one of the following ports
- when the local port is one of the following ports
- when the remote port is one of the following ports
- when the source IP is one of the following IP addresses
- when the destination IP is one of the following IP addresses
- when the local IP is one of the following IP addresses

QRADAR WRITE YOUR OWN RULES 2/4

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Rules that filter logically 1 on events which are detected by the **Local** system

and when the event context is Remote to Local

and when the destination port is one of the following 1433

and when an event matches any of the following Database: Concurrent Logins from Multiple Locations

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

- Anomaly
- Asset Reconciliation Exclusion
- Authentication
- Botnet
- Category Definitions

Notes (Enter your notes about this rule)

<< Back Next >> Finish Cancel Close

QRADAR WRITE YOUR OWN RULES 3/4

Rule Responses

Rule responses are the action that the QRadar appliance takes when all of the rule tests are true.

There are a number of different rule tests that can be leveraged by the user.

Note: The rule responses, such as emails, syslog messages, forwarding events occurs on the processor where the rule becomes true.

Rule Wizard

Rule Wizard: Rule Response

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

- Severity Set to 0
- Credibility Set to 0
- Relevance Set to 0
- Ensure the detected event is part of an offense
- Annotate event
- Drop the detected event

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

- Dispatch New Event
- Email
- Send to Local SysLog
- Send to Forwarding Destinations
- Notify
- Add to a Reference Set
- Add to Reference Data
- Trigger Scan

Response Limiter
 Respond no more than 1 time(s) per 30 minute(s) per Rule

Enable Rule
 Enable this rule if you want it to begin watching events right away.

OUTPUT

QRADAR WRITE YOUR OWN RULES 4/4

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. For example:

Rule (Click on an underlined value to edit it)

Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Contractor VPN after hours on events which are detected by the Local system

- and when an event matches any of the following rules
- and when an event matches any of the following BB:HostDefinition: VPN Assets
- and when the event(s) occur on any of Sunday, Saturday
- and when any of Username are contained in any of External Contractor - AlphaNumeric

QRADAR OUTPUTS

- **Offense**
- Alert
- Action
- Report
- Forward
- Add to **reference set**

QRADAR OFFENSE

Offense 3063 Summary Attacker Targets Categories Annotations Networks Events Flows Rules Actions Print

Magnitude		Relevance	0	Severity	8	Credibility	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan		Event count	1428 events in 3 categories			
Attacker/Src	202.153.48.66		Start	2009-09-29 16:05:01			
Target(s)/Dest	Local (717)		Duration	1m 32s			
Network(s)	Multiple (3)		Assigned to	Not assigned			
Notes	Vulnerability Correlation Use Case Illustration of vulnerability data with IDS alerts An attacker originating from China (202) ... g the Conficker worm exploit (CVE 2008-4250)						

Attacker Summary Details

Magnitude		User	Karen
Description	202.153.48.66	Asset Name	Unknown
Vulnerabilities	0	MAC	Unknown
Location	China	Asset Weight	0

Top 5 Categories Categories

Name	Magnitude	Local Target Count
Buffer Overflow		8
Misc Exploit		3
Network Sweep		716
		1417

Top 5 Local Targets Targets

IP/DNS Name	MAC	Chained	User	MAC	Location	Weight
Windows AD Server	Unknown	No	Unknown	Unknown	main	8
10.101.3.3	Unknown	No	Unknown	Unknown	main	0
10.101.3.4	Unknown	No	Unk		main	0
DC106	Yes	No	Adm		main	10
10.101.3.11	Unknown	No	DC		main	0

Top 10 Events Events

Event Name	Magnitude	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm	Misc Exploit	10.101.3.15	445 09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5	Buffer Overflow	10.101.3.10	445 09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5		10.101.3.15	445 09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar-vm		10.101.3.13	445 09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm		10.101.3.10	445 09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm		10.101.3.15	445 09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm		10.101.3.10	445 09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445 09-29 16:05:01

What was the attack?

Was it successful?

Who was responsible?

Where do I find them?

How valuable are they to the business?

How many targets involved?

Are any of them vulnerable?

Where is all the evidence?

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

