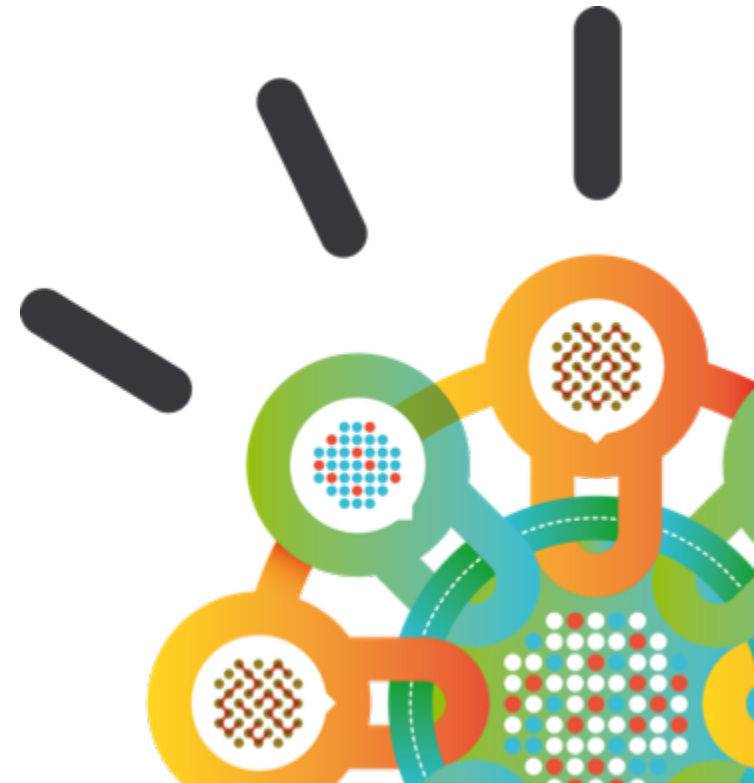




QRadar Security Intelligence

Jason Corbin

Director of Product Management & Strategy



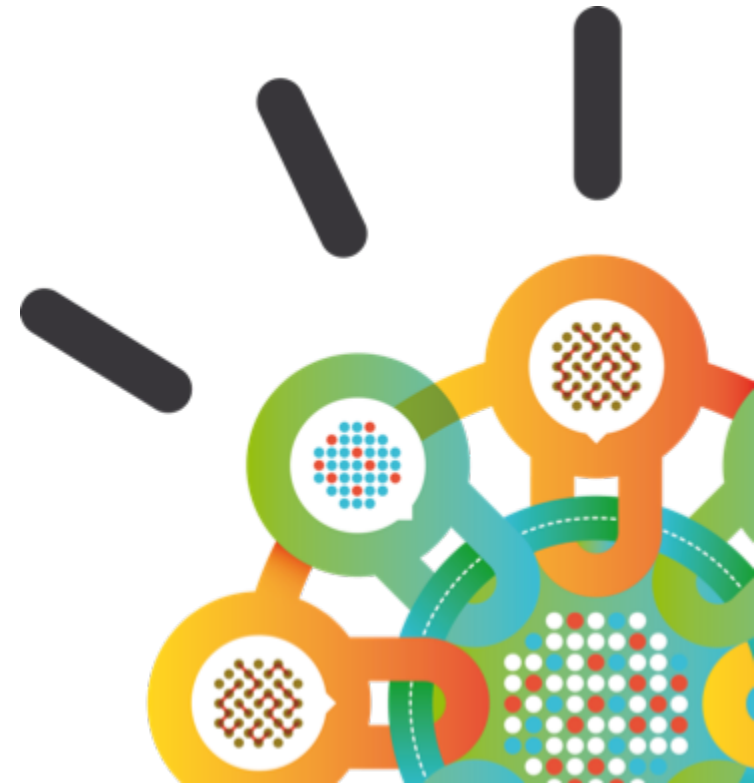
QRadar Overview

Stories From the Road

Vision/Strategy

QRadar as a Platform

If Time Permits



Our Focus



Vulnerability

Pre-Exploit

Exploit

Post-Exploit

Remediation



PREDICTION / PREVENTION PHASE

- Gain visibility over the organization's security posture and identity security gaps
- Detect deviations from the norm that indicate early warnings of APTs
- Prioritize vulnerabilities to optimize remediation processes and close critical exposures before exploit

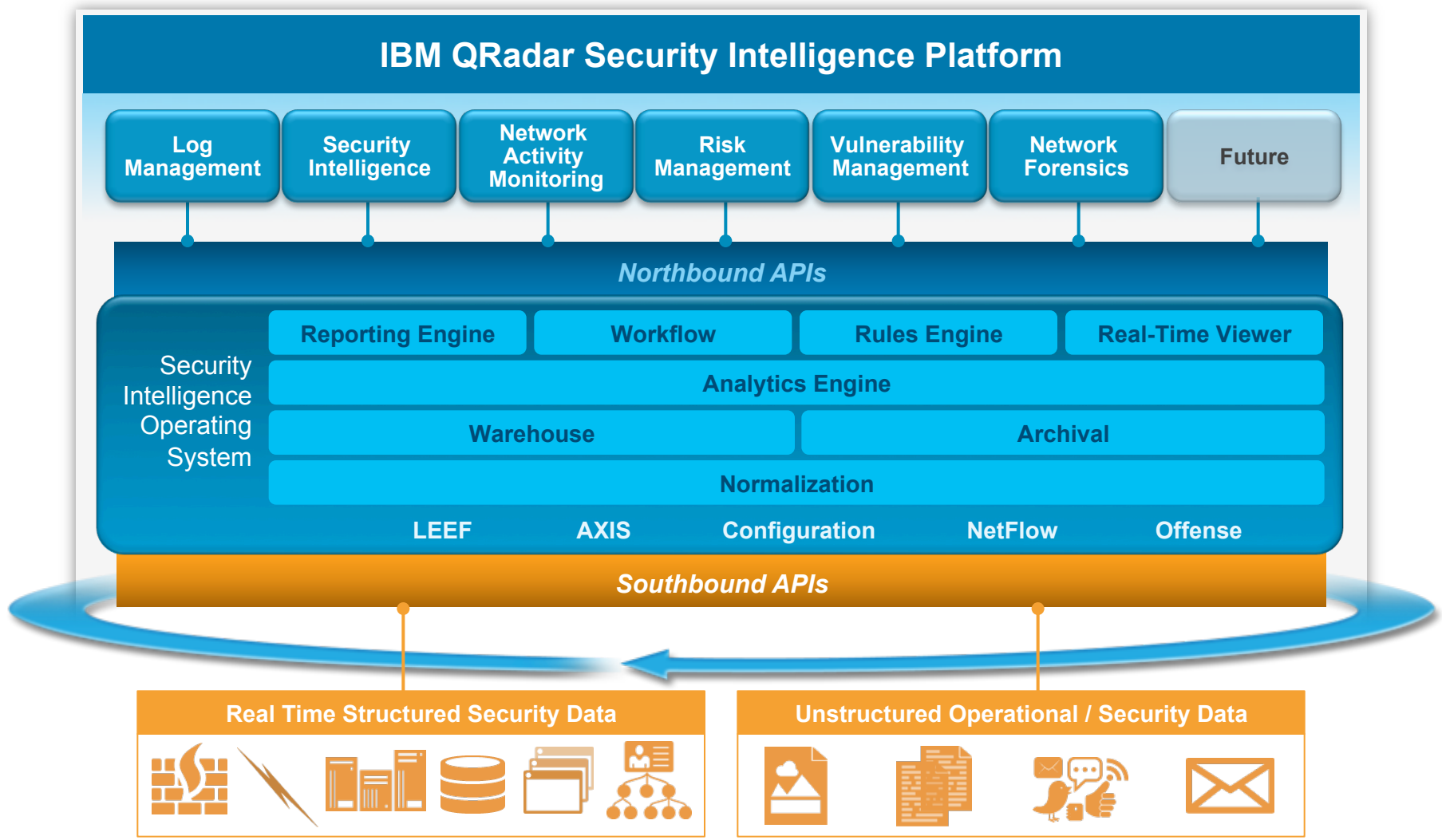
REACTION / REMEDIATION PHASE

- Automatically detect threats with prioritized workflow to quickly analyze impact
- Gather full situational awareness through advanced security analytics
- Perform forensic investigation reducing time to find root-cause; use results to drive faster remediation

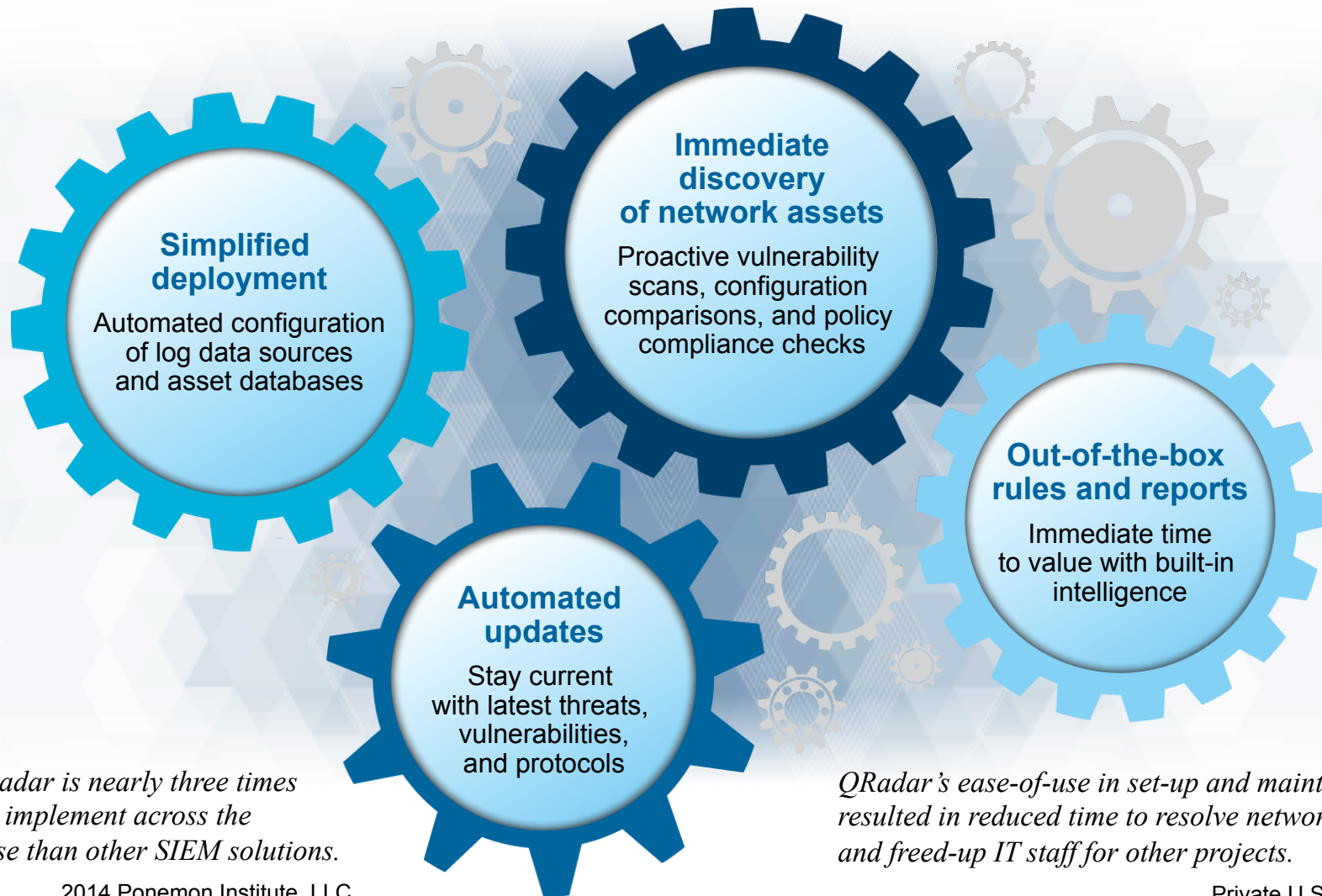
Security Intelligence

The actionable information derived from the analysis of security-relevant data available to an organization

Delivering multiple security capabilities through a purpose-built, extensible platform



Driving simplicity and accelerated time to value



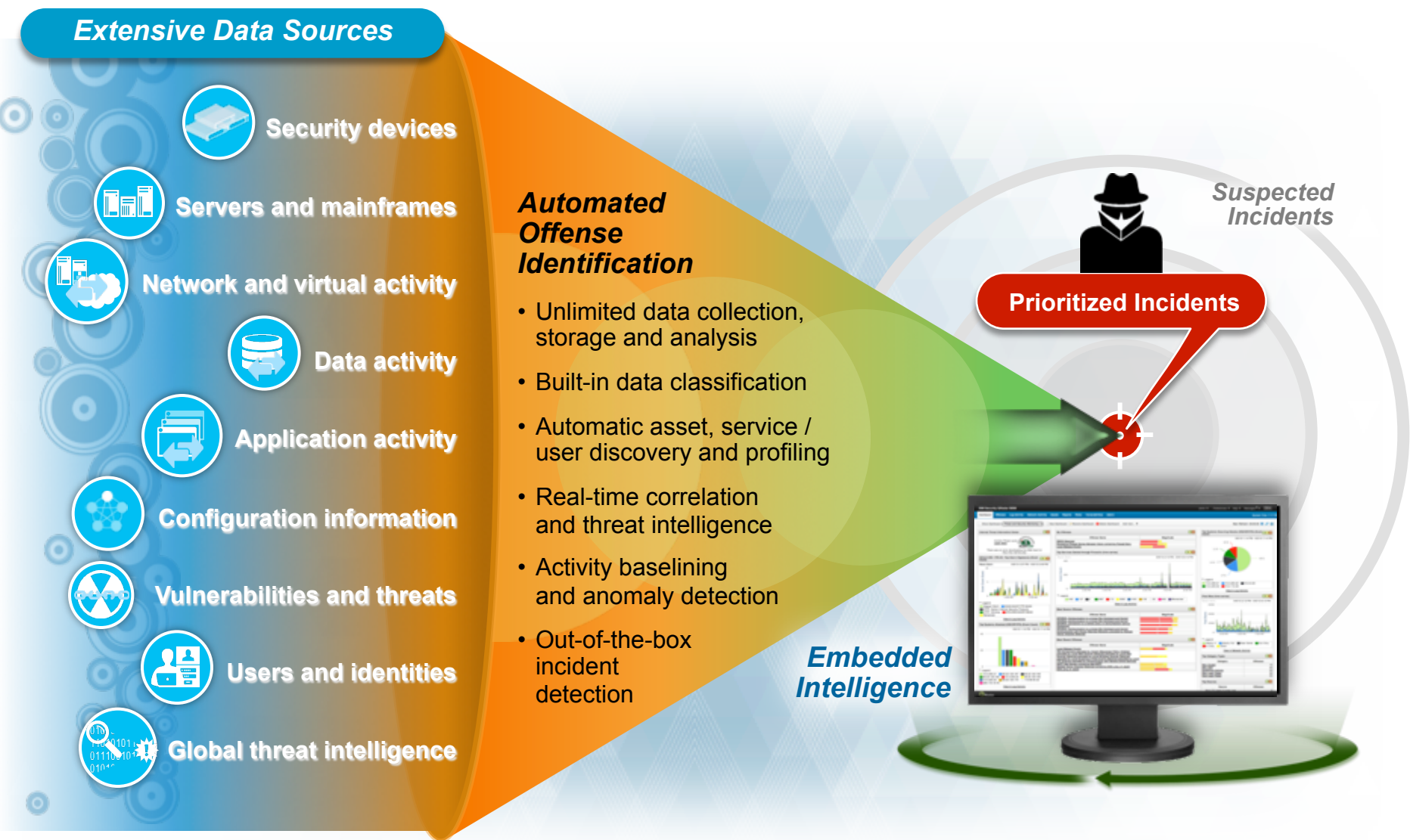
IBM QRadar is nearly three times faster to implement across the enterprise than other SIEM solutions.

2014 Ponemon Institute, LLC
Independent Research Report

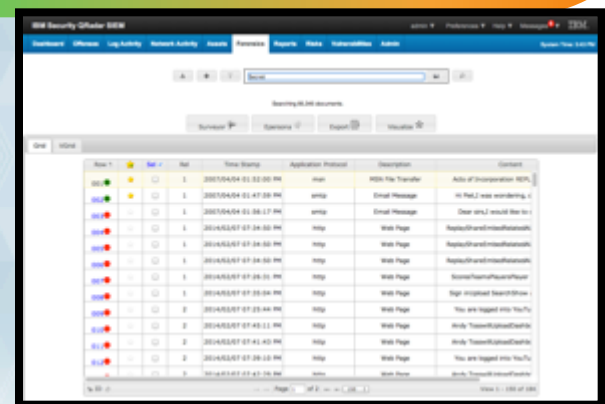
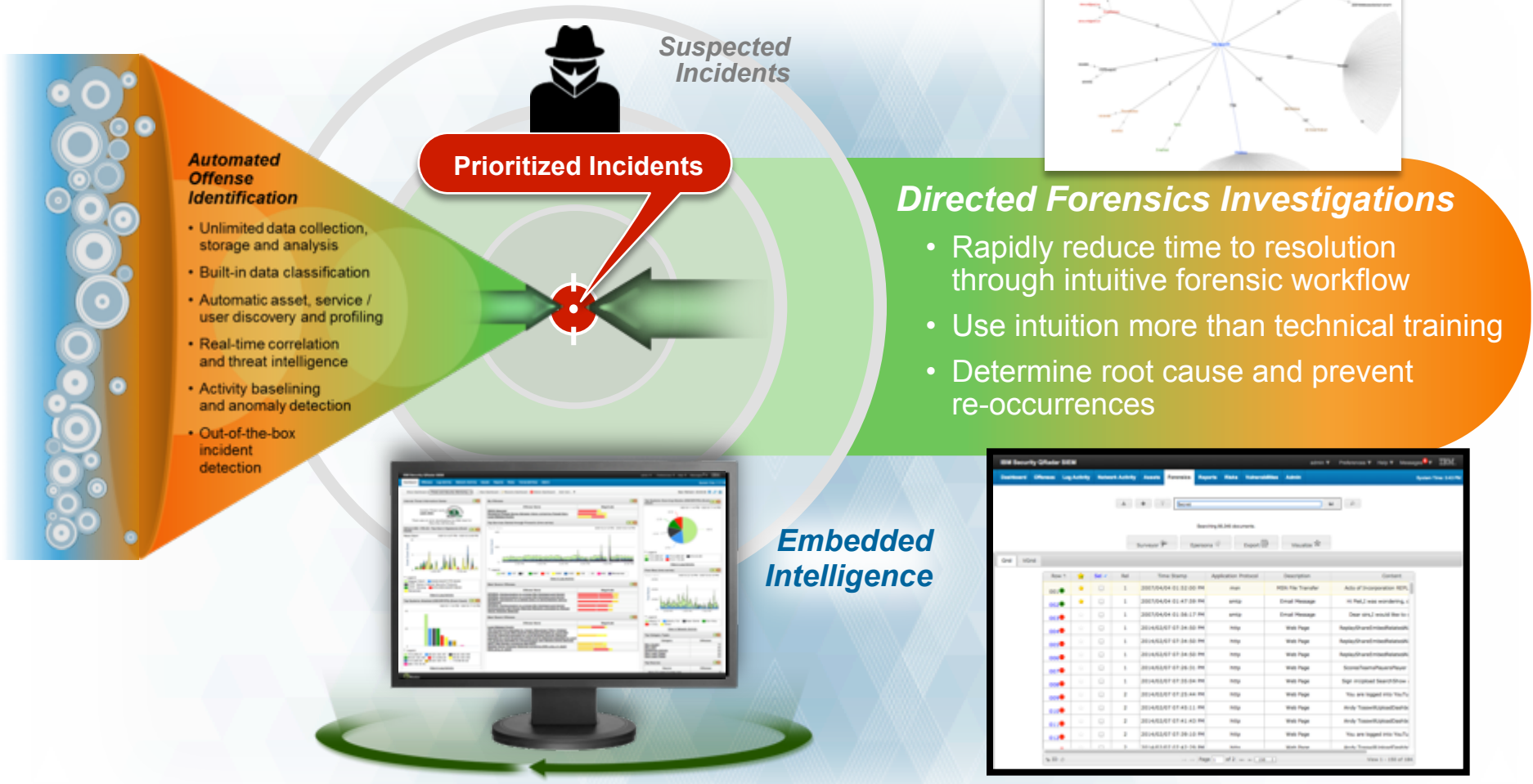
QRadar's ease-of-use in set-up and maintenance resulted in reduced time to resolve network issues and freed-up IT staff for other projects.

Private U.S. University
with large online education community

Turning Massive Amounts of Data into Actionable Insights and Evidence



Extend clarity around incidents with in-depth forensics data

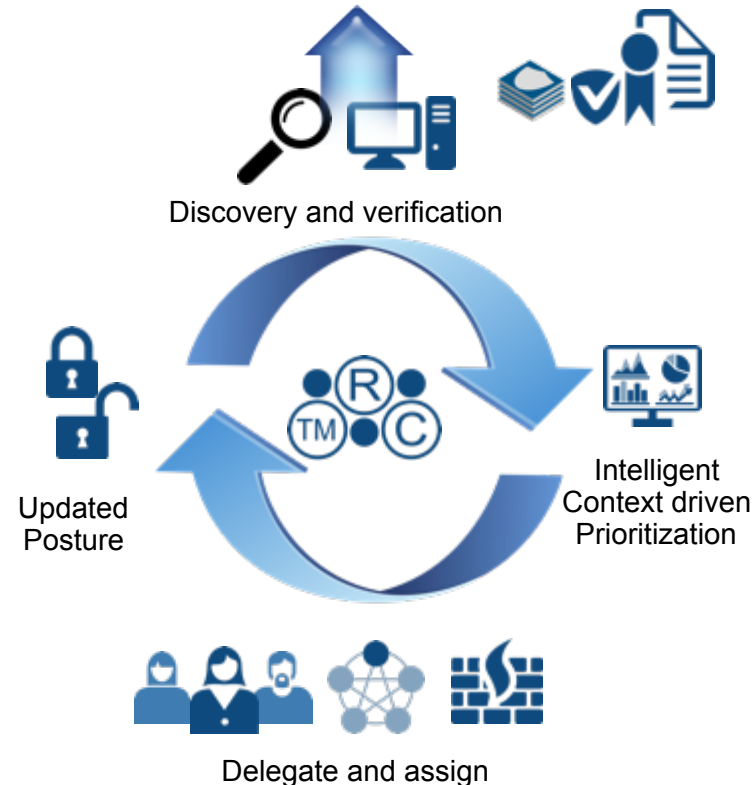


Automated Risk and Vulnerability Management

Discovery and Verification	<ul style="list-style-type: none"> • Uncovers the weaknesses • Endpoints, assets, device configuration • Derived intelligence from the network
Intelligent Context Driven Prioritization	<ul style="list-style-type: none"> • What assets are important ? • Where are the threats ? • Who is talking to who ? • What is blocked and patched already ? • What is out of compliance ?
Automatic Delegation and Assignments	<ul style="list-style-type: none"> • Who needs to take action • What needs to be done <ul style="list-style-type: none"> • Missing patches • Signatures • Configuration changes
Reporting and Alerting	<ul style="list-style-type: none"> • What needs escalation • What is in and out of compliance • Dashboards and reports • APIs

Assets With Open Service Vulnerabilities	Risk Score	Vulnerability	Vulnerability Instances
2	786.40		
3	414.60		
3	126.30		
1	119.50		
1	36.90		
1	14.40		
1	12.20		
1	12.20		
2	11.00		
1	9.60		
1	9.60		

Score: 119.50
 Total count: 21
 High: 2
 Medium: 13
 Low: 6
 Warning: 0



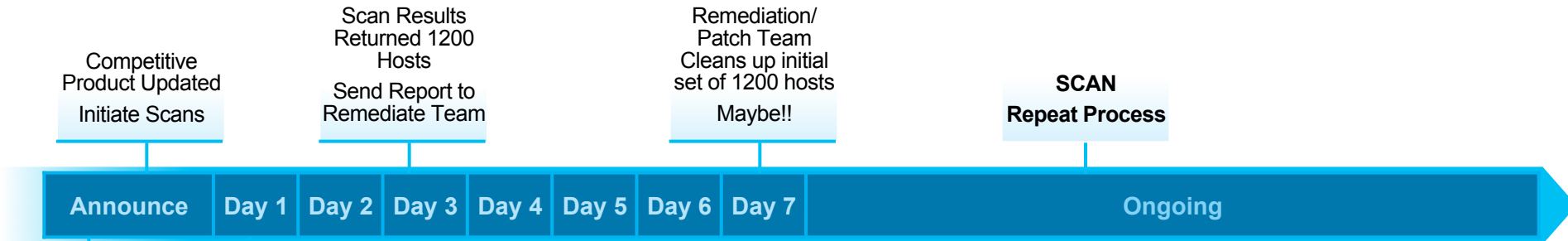


QRadar Stories From The Road

Taking On a Zero Day Vulnerability With Security Intelligence

Microsoft Internet Explorer (IE) zero-day vulnerability (2013-3893)

Other Vendor



QRadar updated with New Vuln Data

Use Qradar to proactively monitor security logs and flows to actively detect exploit

Early Warnings Detects 1200 hosts with vulnerability

50 Most Likely Hosts to be Exploited Patched

QRadar

1. Correlation with Flow Data to determine hosts where this service is active
2. Correlate with X-Force Data to determine hosts communicating with malicious sites/lps
 - a. 1200 down to 50 High Priority Hosts
3. Which ones are exposed to internet



Leveraging the QRadar Portfolio For Shellshock

- Proactively Discover
- Assess Risk
- Continuous Monitoring/Detect Attacks

Discover (QRadar Vulnerability Manager)

- Understand where you are vulnerable
- If you are using 3rd party scans make sure that data is in QRadar
- QRadar has full information on the vulnerability
 - Leverage virtual patching where possible

Vulnerability Details

	Integrity Impact = Complete		
	Availability Impact = Complete		
Vulnerability Impact	Monitoring Failure, Access Control Loss, Reputation Loss		
Description	Bash is a Unix shell for the GNU Project as a free software replacement for the Bourne shell (sh). A ShellShock vulnerability has been discovered in GNU Bash. This vulnerability could allow an attacker to execute arbitrary code.		
Concern	This application is prone to this vulnerability because of an unknown error, allowing an attacker to execute arbitrary code.		
Solution	It is recommended that users contact the vendor for information on how to fix this vulnerability. WORKAROUND: Making use of a web application firewall can help mitigate the exploitability of this vulnerability via the http vector, however Bash will remain vulnerable via other vectors.		
Associated Service			
Virtual Patching :	QID	Device Type	Signature
	5789711	IBM Proventia Network Intrusion Prevention System (IPS)	HTTP_Bash_Shell_Function_Exec
	64759321	Stonesoft Management Center	Generic_UDP-Bash-Shellshock-Code-Injection
	8258287	McAfee IntruShield Network IPS Appliance	HTTP: Apache mod_cgi Bash Environment Variable Code Injection
	20279216	Fortinet FortiGate Security Gateway	Bash.Function.Definitions.Remote.Code.Execution
	2589786	Snort Open Source IDS	ET EXPLOIT Possible CVE-2014-6271 exploit attempt via malicious DHCP ACK
	2589787	Snort Open Source IDS	ET DELETED Possible CVE-2014-6271 exploit attempt via malicious DHCP ACK - option 67
	2589869	Snort Open Source IDS	OS-OTHER Bash CGI environment variable injection attempt
	2589870	Snort Open Source IDS	OS-OTHER Bash CGI environment variable injection attempt
	2589871	Snort Open Source IDS	OS-OTHER Bash CGI environment variable injection attempt
	2589872	Snort Open Source IDS	OS-OTHER Bash CGI environment variable injection attempt
	2589873	Snort Open Source IDS	OS-OTHER Malicious DHCP server bash environment variable injection attempt
	6265075	Juniper Networks Intrusion Detection and Prevention (IDP)	HTTP:CGI:BASH-CODE-INJECTION

Search Save

Manage Vulnerability

Search Parameters

Include Vulnerabilities

Vulnerabilities Displayed

[014-6271 - GNU](#)
[014-3510 - Open](#)
[014-3505 - Open](#)
[014-3506 - Open](#)
[014-3507 - Open](#)
[014-3508 - Open](#)
[014-3509 - Open](#)

00:30

Days Since

Unassigned

45

4

4

4

4

4

Assess Risk (QRadar Risk Manager)

Question Editor - Google Chrome

https://172.16.193.71/console/do/120/srm/editQuestion?dispatch=newQuestion&appName=SRM&pageId=Questionf

What do you want to name this question?
Shellshock vulnerable assets communicating with remote nets and have accepted http traffic

Evaluate On:
Actual Communication

What type of data do you want to return?
Assets

Importance Factor:
5

Time Range:
 Interval Last 7 Days
 Fixed 29/09/2014 00:00 to 29/09/2014 00:00

Which tests do you want to include in your question?

- have accepted communication to any destination
- have accepted communication to destination networks
- have accepted communication to destination IP addresses
- have accepted communication to destination asset building blocks
- have accepted communication to destination asset saved searches
- have accepted communication to destination reference sets
- have accepted communication to destination remote network locations

Find Assets that...

- have accepted communication to destination remote network locations (all)
- and include only the following inbound applications (Web, HttpWeb)
- and are susceptible to vulnerabilities contained in vulnerability saved searches (Shellshock)

This will create single offense with all assets that are accepting web communications from remote locations and are vulnerable. Vulnerability and Patch Reports will automatically prioritize these assets



Proactively Detect Potential Exploits (QRadar SIEM)

Even if you have IPS/IDS, Monitor Web Proxy Logs in Real Time

Rule (Click on an underlined value to edit it)

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

Apply on events which are detected by the system

and when the event(s) were detected by one or more of Web Proxy Logs
 and when the Event Payload contains $\backslash((.*)?)\backslashs*\backslash((.*)?)\backslashs*\backslash;$

Detect with Flow Traffic

Rule (Click on an underlined value to edit it)

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

Apply on flows which are detected by the system

and when the flow context is Remote to Local
 and when a flow matches any of the following BB:HostDefinition: Web Servers, BB:PortDefinition: Web Ports
 and when the remote payload matches the regex $\backslash((.*)?)\backslashs*\backslash((.*)?)\backslashs*\backslash;$

Detecting website spidering and brute force CGI exploits

Rule (Click on an underlined value to edit it)

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

Apply on events which are detected by the system

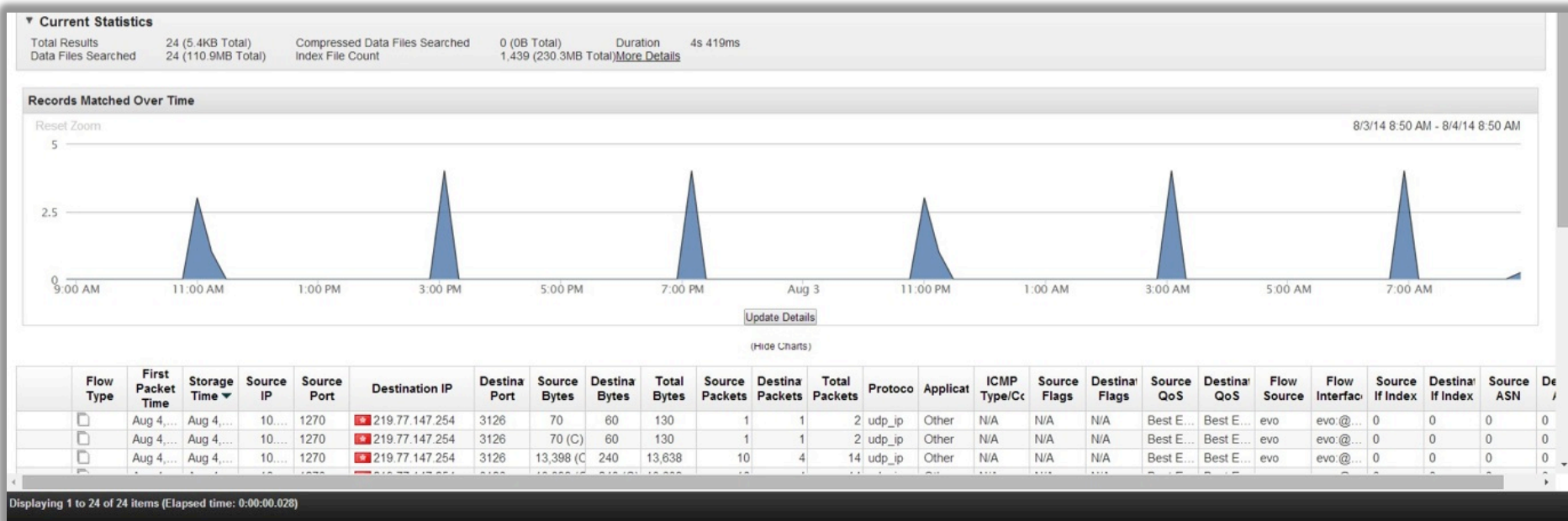
and when the event QID is one of the following (4500022) HTTP 404 - Not Found
 and when at least 100 events are seen with the same Source IP in 1 minutes



Customer Driven Advanced Use Cases

Advanced Search – Identify suspicious long term traffic

- Many threats communicate periodically with command and control over days, weeks and months
- Advanced searching can identify period connections of long period of time
 - E.g. consistent, short, low volume, number of connections per day/week/month between IP addresses, or an IP address and geo
- Generate offense and/or populate a reference set/table (utilizing API)



Advanced Search Mode – Operational Reporting -Account usage reporting

- Different user communities can have variable threat and usage indicators
- Utilize reference data to report on additional user properties, e.g. department, location, Manager etc.

IBM QRadar Security Intelligence admin Help Messages 3 System Time: 10:54 AM

Dashboard Offenses Log Activity Network Activity Assets Reports Vulnerabilities Admin

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


Advanced Search `select username, referencetable('userdata','FullName',username) as Fullname, referencetable('userdata','Location',username) as Location, referencetable('userdata','Manager',username) as Manager, col` Search

Viewing events from Jul 1, 2014, 10:48:00 AM to Jul 1, 2014, 10:53:00 AM View: Select An Option: Display: Default (Normalized) Results Limit

Current Statistics Completed

Top 10 referencetable_userdata_FullName_username:referencetable_userdata_Location_username:referencetable_userdata_Manager_username Results By Customer DB Access Count

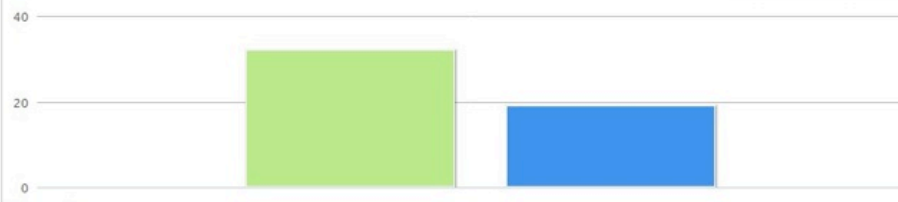
Value to Graph: Customer DB Access Count Chart Type: Pie Chart Display Top: 10



Legend: admin (63%), configservices (37%)

Top 10 referencetable_userdata_FullName_username:referencetable_userdata_Location_username:referencetable_userdata_Manager_username Results By Customer DB Access Count

Value to Graph: Customer DB Access Count Chart Type: Bar Chart Display Top: 10



Legend: admin (32.0), configservices (19.0)

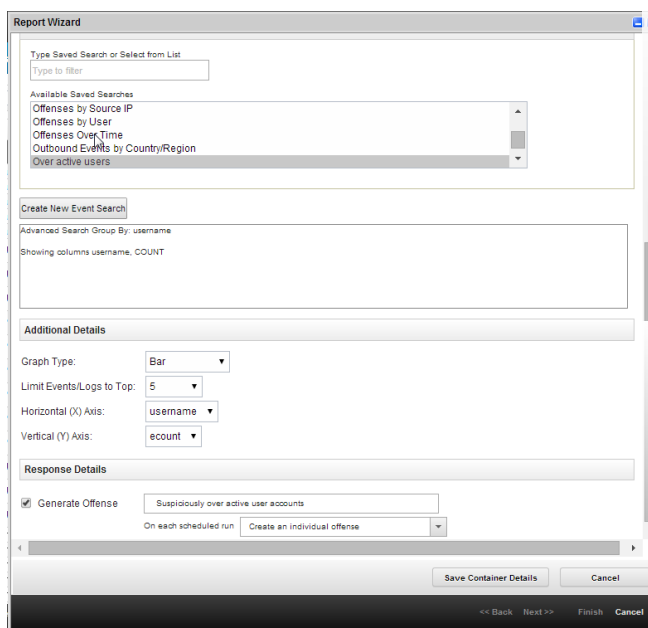
(Hide Charts)

FIRST_username	Fullname	Location	Manager	Customer DB Access Count
admin	Christopher Meenan	Belfast	Jason Corbin	32.0
configservices	Jody Brownell	Fredericton	Mike Cormier	19.0

Displaying 1 to 2 of 2 items (Elapsed time: 0:00:00.127)

Advanced Search – Generate Offenses From Scheduled Analysis

- Provides capability to generate an incident from advanced search as well as real time correlation
- Enables full offense support with drill down to results



Report Wizard

Type Saved Search or Select from List
Type to filter

Available Saved Searches
 Offenses by Source IP
 Offenses by User
 Offenses Over Time
 Outbound Events by Country/Region
 Over active users

Create New Event Search

Advanced Search Group By: username
Showing columns: username, COUNT

Additional Details

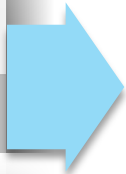
Graph Type: Bar
 Limit Events/Logs to Top: 5
 Horizontal (X) Axis: username
 Vertical (Y) Axis: ecount

Response Details

Generate Offense
 Suspiciously over active user accounts
 On each scheduled run: Create an individual offense

Save Container Details Cancel

<< Back Next >> Finish Cancel



All Offenses > Offense 118 (Summary)

Offense 118 Summary Disp

Magnitude	■■■■	Status	Relevance	1	Severity	2
Description	Suspiciously over active user accounts	Offense Type	Scheduled Search			
		Event/Flow count	1 events and 0 flows in 1 categories			
Source IP(s)	127.0.0.1	Start	Jul 3, 2014, 5:07:43 AM			
Destination IP(s)	127.0.0.1	Duration	0s			
Network(s)	other	Assigned to	Unassigned			

Offense Source Summary

Name	Over active users
Most Recent Results	2644
Creator	admin

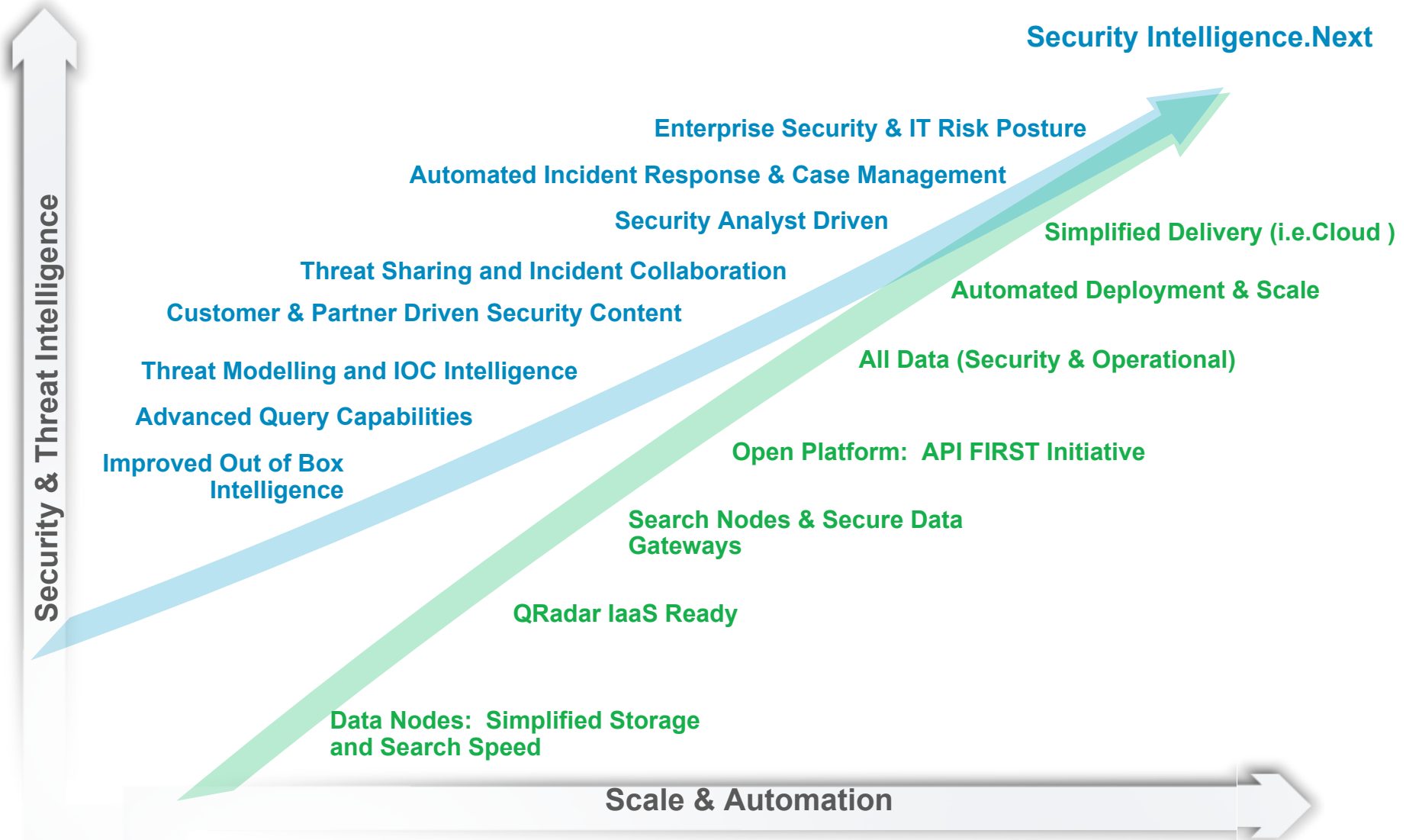


username	
N/A	1.5321769
francois.fagotto@mcgill.ca	63.0
jocelyne.feine@mcgill.ca	45.0
konstantin.speransky@mail.mcgill.ca	29.0
peter.antkowiak@mail.mcgill.ca	1.0
valerie.beaudoin@mail.mcgill.ca	255.0
nihal.thomas	224.0
bronwen.desena@mail.mcgill.ca	65.0
joe	2412.0
adrienne.laube@mail.mcgill.ca	59.0



QRadar Vision

Evolution of Security Intelligence Architecture and Capability

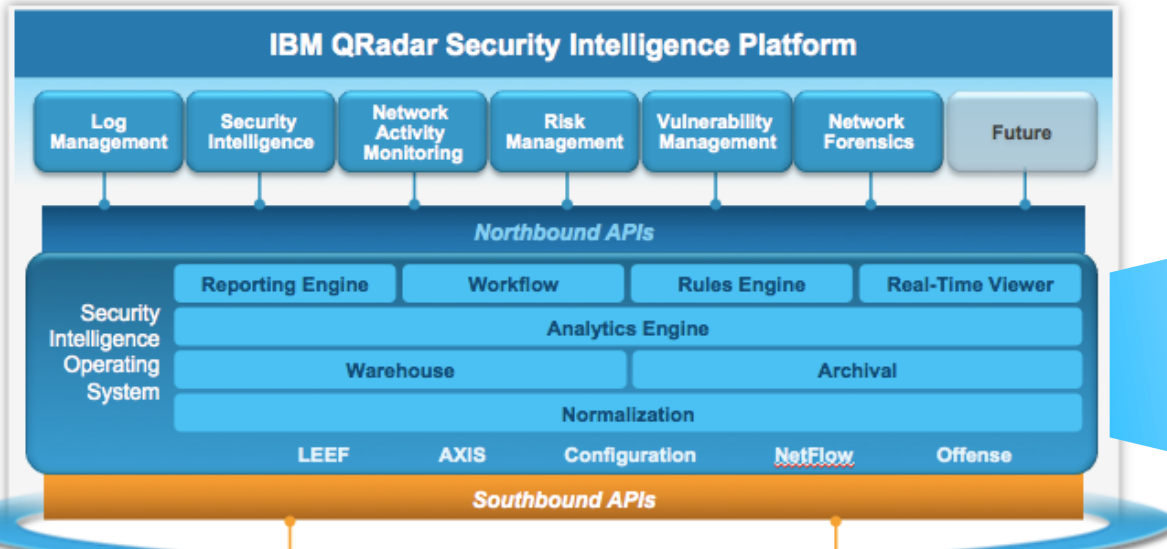




QRadar as a Platform

Example Apps Built on API

Open Architecture – New API, UI Plugins and Console Framework



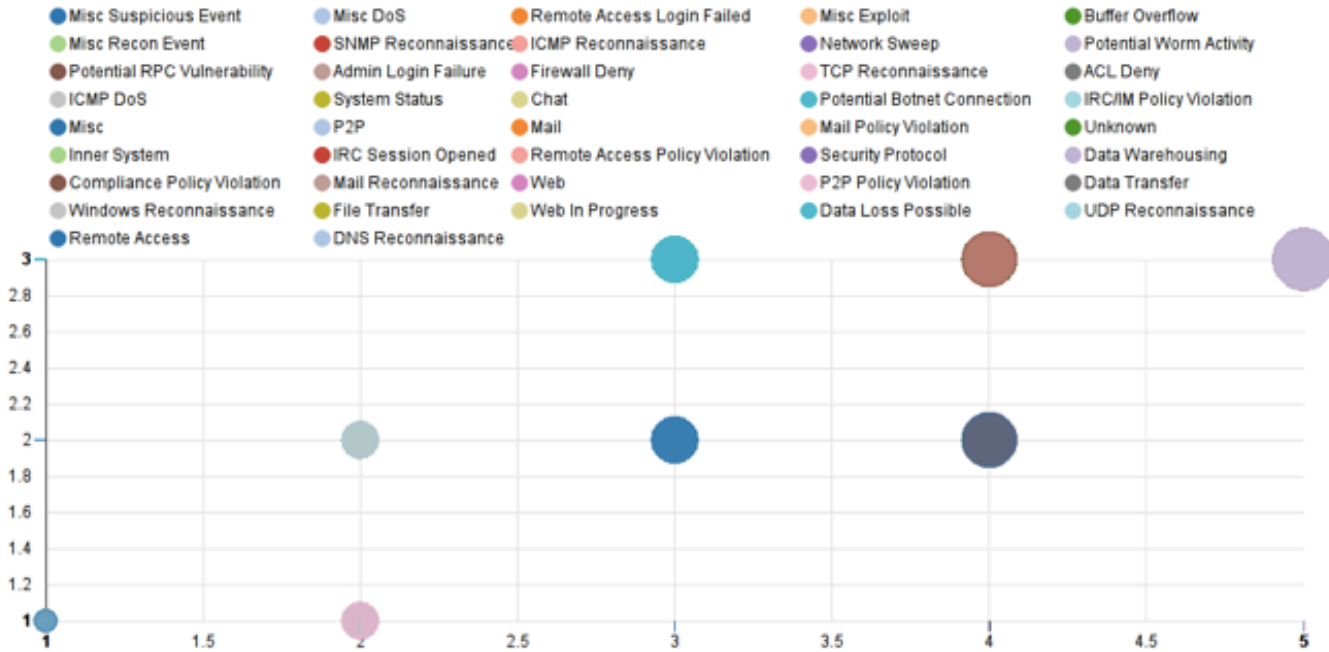
Value

- **New APIs**
 - Data
 - Offenses
 - Configuration/Mgmt
 - Asset Profiles
 - User Interface
- **Simplified Integrations**
- **Improved Customization**
- **Advanced Use Cases**
- **Automation**

* Stretch

Offense/Event+Flow API

Offense Visualizer



Graph Options

X Axis

Magnitude ▾

Y Axis

Credibility ▾

Size

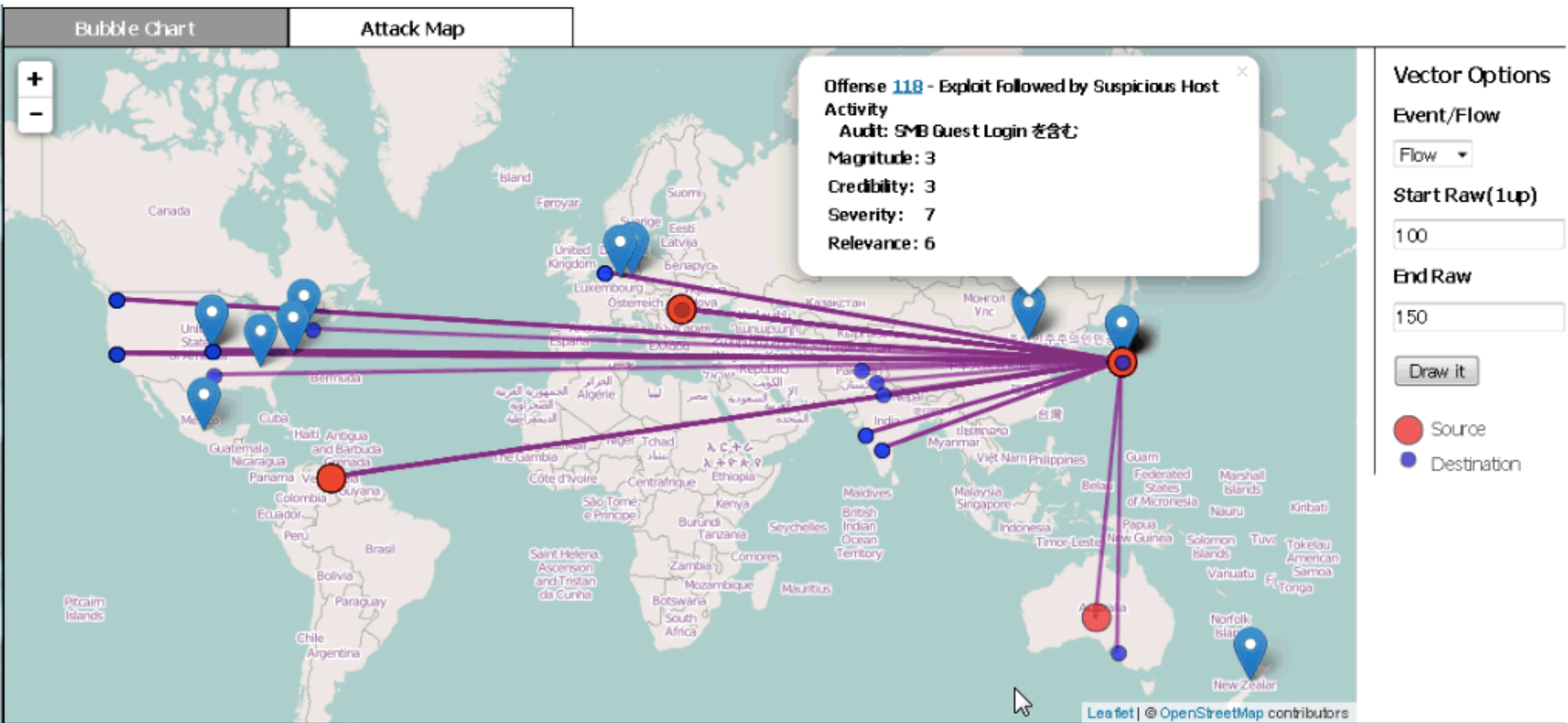
Magnitude ▾

Colorization

Offense Category ▾

- Misc Suspicious Event
- Misc DoS
- Remote Access Login Failed
- Misc Exploit
- Buffer Overflow
- Misc Recon Event
- SNMP Reconnaissance
- ICMP Reconnaissance
- Network Sweep
- Potential Worm Activity
- Potential RPC Vulnerability
- Admin Login Failure
- Firewall Deny
- TCP Reconnaissance
- ACL Deny

Offense/Event+Flow API



Owning The SOC (future example apps)

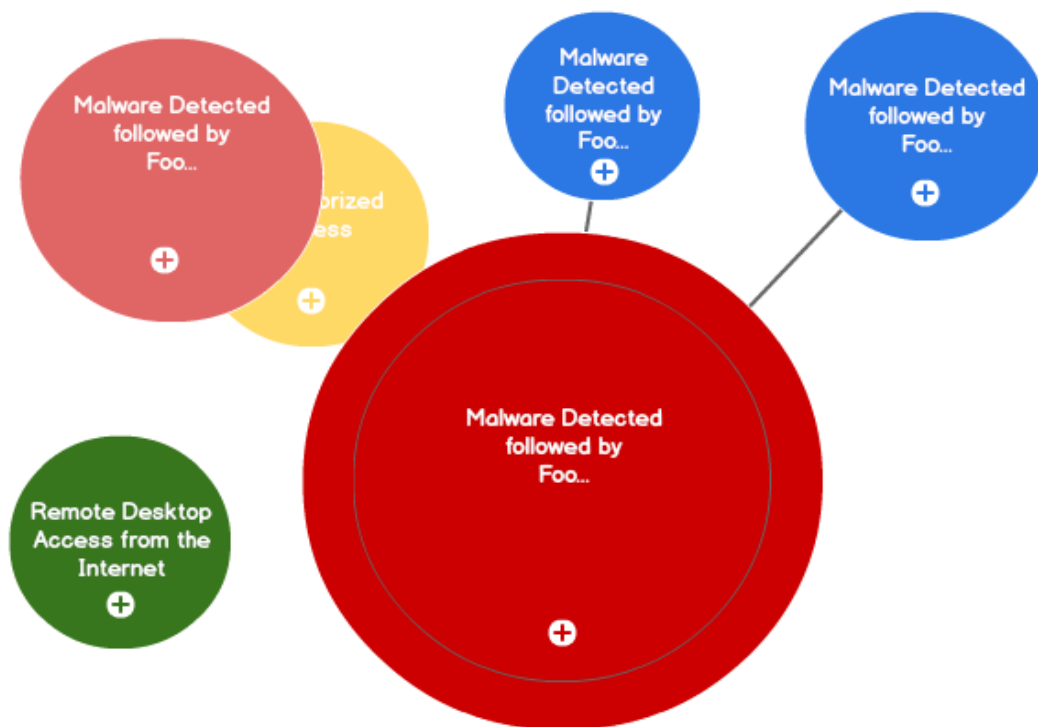
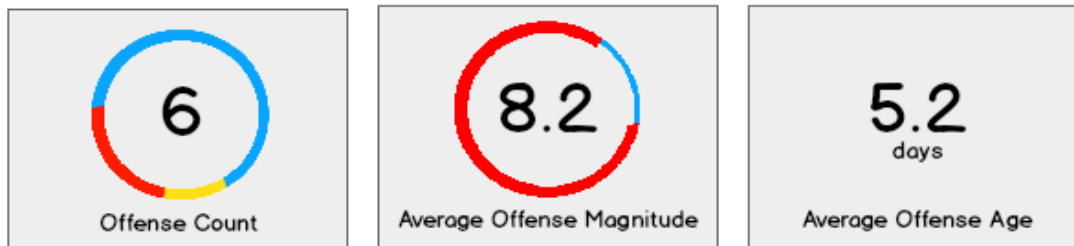
Tracking The Threat

- Understanding the Attack Kill Chain
- Quickly identify severity and overall impact of a threat
- Enable faster response by understanding flow of data.
- Automated Response into the Threat Protection System



IBM QRadar Security Intelligence

Top Offenses



Need to dig further?

- What is the DNA of the Attack?
- Forensic Investigation
- Relationships between IPs involved in this offense based on communications (IPs, ports, etc.).
- Context from other Security Operations solutions

IBM QRadar Security Intelligence

Top Offenses

