

State of NC QRadar Workshop

Threat Hunting, Advanced Analytics,
Augmented Intelligence, and Automated Response



Michael Melore, CISSP

IBM Cyber Security Advisor



@MichaelMelore

October 2017

A tremendous amount of security knowledge is created for human consumption **but most of it is untapped**

Traditional
Security Data

- Security events and alerts
- User and network activity
- Logs and configuration data
- Threat and vulnerability feeds

Human Generated
Knowledge



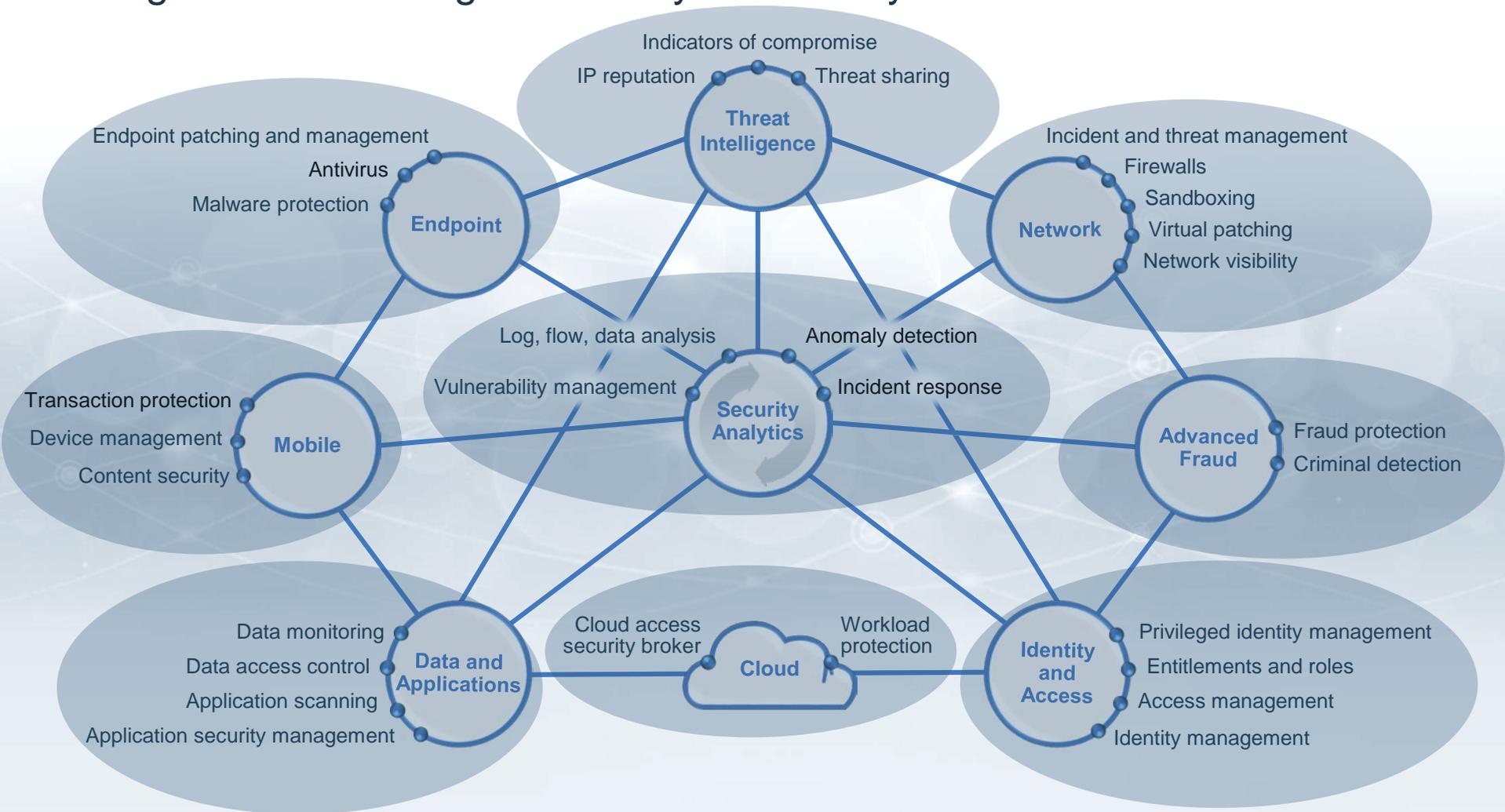
A universe of security knowledge Dark to your defenses

Typical organizations leverage only 8% of this content*

Examples include:

- Research documents
- Industry publications
- Forensic information
- Threat intelligence commentary
- Conference presentations
- Analyst reports
- Webpages
- Wikis
- Blogs
- News sources
- Newsletters
- Tweets

Integrated and intelligent security immune system



Today's challenges

Escalating Attacks

Designer Malware

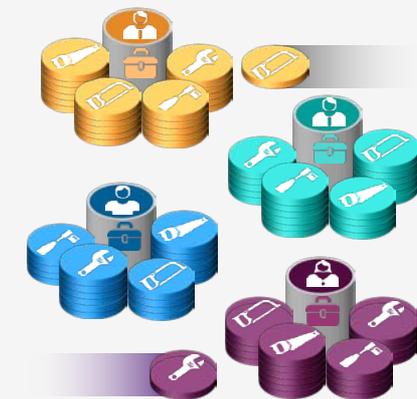
Spear Phishing

Persistence

Backdoors

- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

Increasing Complexity



- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

Resource Constraints



ITSecurityJobs.com

Sorry, no applicants found

- Struggling security teams
- Too much data with limited manpower and skills to manage it all
- Managing and monitoring increasing compliance demands

Workflow



Advanced Analytics



DETECT



Cognitive



ENRICH



Threat Hunting



INVESTIGATE



ORCHESTRATE



What is Needed to Conduct Threat Hunting

Known
Indicators



SOC & SIEM



Foundational
Data

Anomaly
Detection



Intelligence Analysis Tools



Organization +
Discovery

QRadar: An integrated, unified architecture in a single web-based console

Log Management

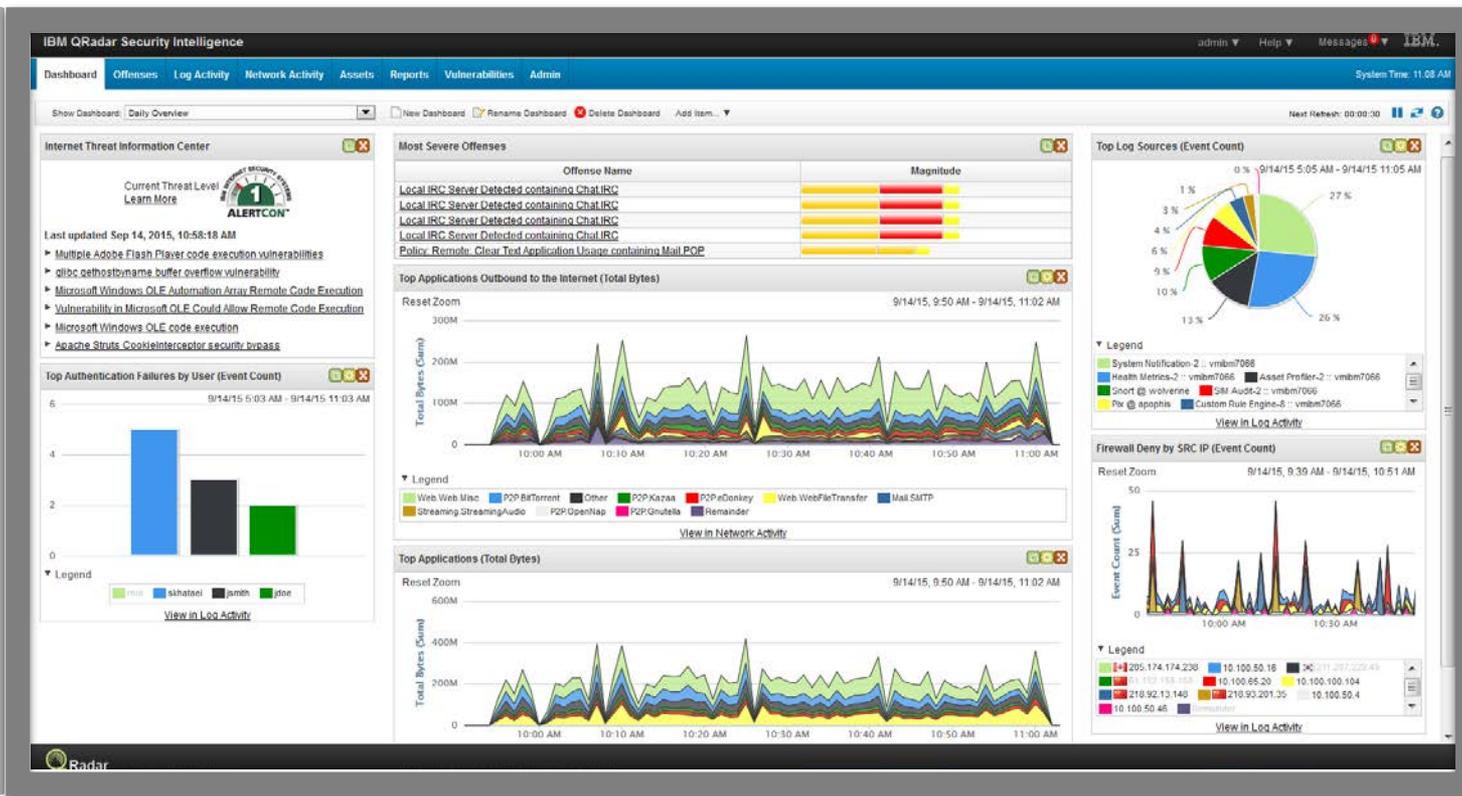
Security Intelligence and Sense Analytics

Network Activity Monitoring

Vulnerability and Risk Management

Network Forensics

Incident Response



QRadar: Watson Advisor

The screenshot displays the IBM QRadar Security Intelligence interface. At the top, there is a navigation bar with various menu items: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, User Analytics, and Watson. The main content area is titled "Incident Overview" and includes a sub-header "Hour graph for Jan 17th". To the right of the graph, there are three key metrics: Open Incidents (4), Average Magnitude (2.8), and Today's Incidents (0). Below the graph is a table of incidents with columns for Status, ID, Description, Source, Type, and Date.

Status	ID	Description	Source	Type	Date
	240	TCP_HIT preceded by System Infected: Ransomware Activity	192.168.0.119	Source IP	2017.01.20
	244	TCP_HIT preceded by TCP_MISS preceded by System Infected: Ransomware Activity preceded by Web Attack: Suspicious Executable File Download preceded by Informational Email Message	lance.springwell	Username	2017.01.20
	243	virus_found-unknown_action preceded by TCP_HIT preceded by Logon attempt using explicit credentials preceded by WebVPN user vpnuser has been authenticated.	tom_wilson	Username	2017.01.20
	237	TCP_HIT preceded by System Infected: Backdoor DarkMoon Activity preceded by Web Attack: Suspicious Executable File Download	192.168.0.235	Source IP	2017.01.20

QRadar: Watson Advisor

The screenshot shows the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', 'User Analytics', and 'Watson'. The main content area displays an 'Incident Overview' for 'Incident 244' with the title 'TCP_HIT preceded by TCP_MISS'. A 'Watson Insights' popup is overlaid on the incident details, providing the following analysis:

Watson Insights [Explore Insights](#)

 "From this offense, QRadar Advisor has analyzed **52 observables**. Reasoning over the offense discovered **13 new indicators** that were not part of the offense. A total of 37 data points have been found to be linked with the offense. Ten of all of the indicators are known to be related with suspicious activity, nine of them have been observed actively in this offense. From the newly found indicators, one has ties to suspicious activity. In particular, nine files and one URL have been found, which are known to be suspicious or malicious. It is believed that the following one **threat actor is related to this offense: "cozyduke"** "

Watson Insights [Explore Insights](#)

 "From this offense, QRadar Advisor has analyzed 52 observables. Reasoning over the offense discovered 13 new indicators that were not part of the offense. A total of 37 data points have been found to be linked with the offense. Ten of all of the indicators are known to be related with suspicious activity, nine of them have been observed actively in this offense. From the newly found indicators, one has ties to suspicious activity. In particular, nine files and one URL have been found, which are known to be suspicious or malicious. It is believed that the following one threat actor is related to this offense: "cozyduke". "

QRadar: Watson Advisor

The screenshot displays the IBM QRadar Security Intelligence dashboard. The main navigation bar includes: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, User Analytics, and Watson. The current view is 'Incident Overview' for 'Incident 244'. The incident title is 'TCP_HIT preceded by TCP_MISS preceded by System Infected: Ransomware Activity preceded by Web'. The interface is split into two main sections: a background 'Incident Overview' and a foreground 'Watson Insights' panel.

Incident Overview (Background):

- Hour graph for Jan 17th (8 PM to 9 PM)
- Table of incidents:

Status	ID	Description
	240	TCP_HIT preceded by System Infected: Ransomware Activity
	244	TCP_HIT preceded by TCP_MISS preceded by System Infected: Ransomware Activity preceded by Web Attack: Suspicious Executable File Download
	243	virus_found-unknown_action preceded by TCP_HIT preceded by Logon attempt using explicit credentials preceded by WebVPN user vptuser has been authenticated.
	237	TCP_HIT preceded by System Infected: Backdoor DarkMoon Activity preceded by Web Attack: Suspicious Executable File Download

Watson Insights Panel (Foreground):

- Incident 244: TCP_HIT preceded by TCP_MISS preceded by System Infected: Ransomware Activity preceded by Web
- Overview | Watson
- Summary Metrics:
 - AV Signature: 9
 - Filename: 15
 - Url: 3
 - Ip Address: 4
- Watson Insights: QRadar Advisor's analysis of 52 observables from this offense has finished. As part of the reasoning process 13 new indicators were discovered. A total of 37 data points have been found to be linked with the offense. Ten of all of the indicators are known to be related with suspicious activity, nine of them have been observed actively in this offense. From the newly found indicators, one has ties to suspicious activity. In particular, nine files and one URL have been found, which are known to be suspicious or malicious. It is believed that the following one threat actor is related to this offense: "cozyduke".
- Supporting Details:
 - Filename (29%)
 - Reputation (19%)
 - Hash (17%)

QRadar: Watson Advisor – Patient 0

ge.com/security/demos/watson/rsa/CozyDuke_QRadar/

record webex

Skytap IBM Security Enablem... W3 OTR National Box GoToMeeting Webex Meetings QRadar Demo Resilient Demo IBM X-Force Verse SalesConnect vSphere Q

IBM QRadar Security Intelligence admin Help Messages IBM. System Time: 6:21 PM

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

Analyzer < Back

Offense 244

Type: Username
Last Update: January 20, 2017
Assigned to:
Magnitude: 2

Observables >

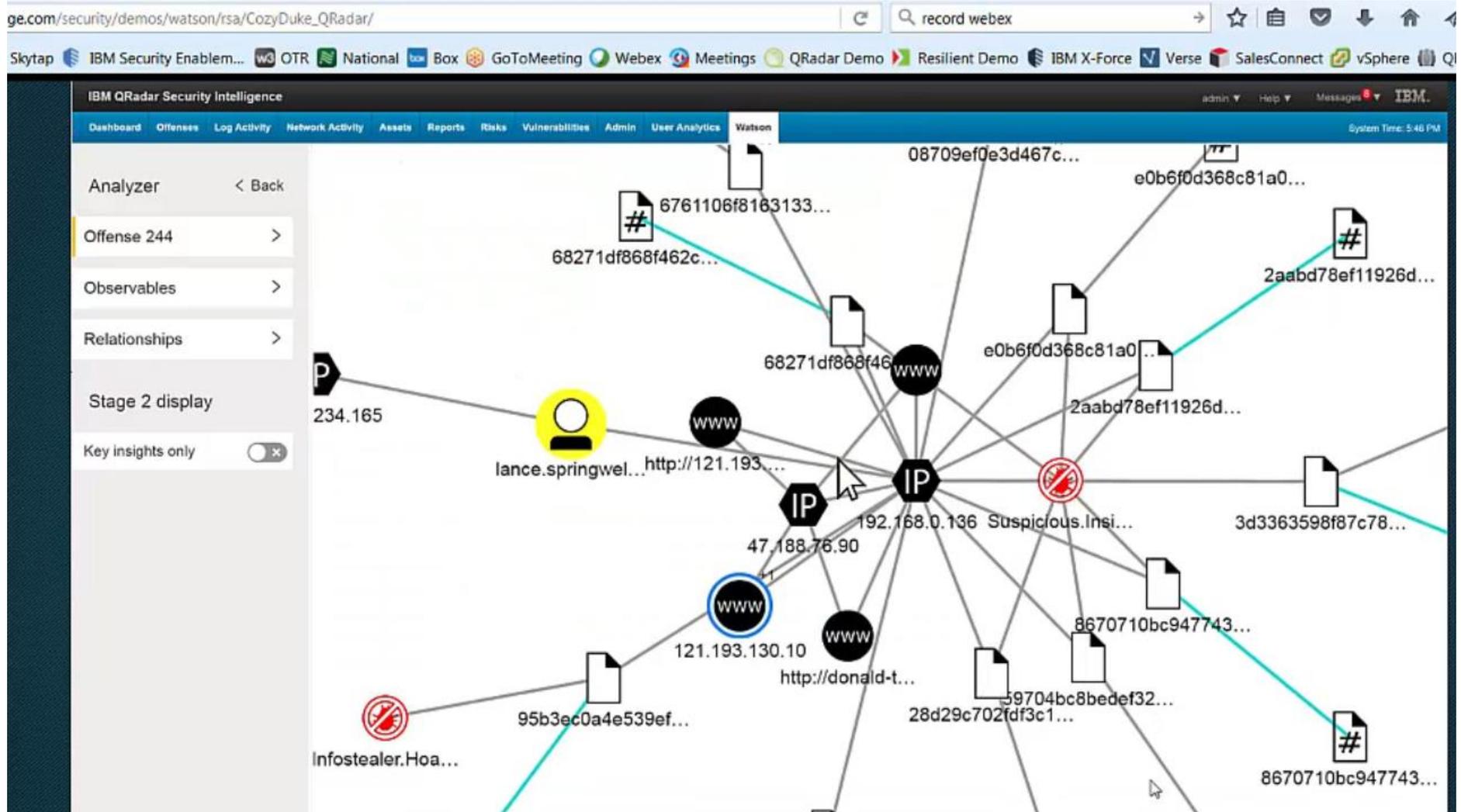
Relationships >

Stage 2 display

Key insights only

The network graph displays a central node, likely an IP address, highlighted in yellow. This central node is connected to numerous other nodes, which include IP addresses and usernames. The connections are represented by lines, and some nodes have associated icons (e.g., a document icon for a file or a person icon for a user). The graph illustrates the relationships between these entities, showing a complex web of connections. A mouse cursor is visible over the central node, indicating it is being interacted with.

QRadar: Watson Advisor – Patient 0



QRadar: Watson Advisor – Threat References

The screenshot displays the IBM QRadar Security Intelligence interface. The top navigation bar includes tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, User Analytics, and Watson. The main content area is divided into three sections:

- Analyzer (Left):** Shows details for Offense 244, including Type: Username, Last Update: January 20, 2017, Assigned to, and Magnitude: 2. It also has sections for Observables, Relationships, Stage 2 display, and a toggle for Key insights only.
- Threat Actor (Right):** A panel titled 'Threat Actor cozyduke' with tabs for Overview and References. The References tab is active, showing a warning: 'ATTENTION: URLs could be malicious and may not be safe to open.' Below this, two references are listed:
 - 52% <https://securelist.com/blog/research/69731/the-cozyduke-ap/>
 - 71% <https://securelist.com/blog/research/69731/the-cozyduke-ap/>
- Network Graph (Center):** A central visualization showing relationships between various entities. A central red circle labeled 'cozyduke' is connected to a red circle labeled 'http://121.193...'. Other nodes include file hashes like '08709ef0e3d467c...', '75bca4f02c63e5...', '6761108f8163133...', and '6781105b163133...', as well as IP addresses like '47.168.76.99' and '192.168.1.1'. A red hat icon is also visible near the 'cozyduke' node.

QRadar: Watson Advisor – Threat Information

The screenshot displays the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Risks', 'Vulnerabilities', 'Admin', 'User Analytics', and 'Watson'. The main content area shows a threat actor analysis for 'cozyduke'. A central diagram illustrates the threat actor's activity, with a red hat icon representing the actor. A callout box highlights two references with associated confidence scores:

- 52% <https://securelist.com/blog/research/69731/the-cozyduke-apt/>
- 71% <https://securelist.com/blog/research/69731/the-cozyduke-apt/>

The interface also shows a sidebar with 'Analyzer' and 'Offense 244' details, including 'Type: Username', 'Last Update: January 20, 2017', and 'Assigned to:'. A 'Key insights only' toggle is visible at the bottom left.

QRadar: Watson Advisor – X-Force Exchange

ge.com/security/demos/watson/rsa/CozyDuke_QRadar/

record webex

Skytap IBM Security Enablem... w3 OTR National Box GoToMeeting Webex Meetings QRadar Demo Resilient Demo IBM X-Force Verse SalesConnect vSphere QI

The screenshot displays the IBM QRadar Security Intelligence interface. On the left, a navigation pane includes sections for 'Analyzer', 'Offense 244', 'Observables' (listing AV Signature, Domain, File, Hash, IP, URL, User), 'Relationships', and 'Stage 2 display'. The main area features a network graph with nodes representing various entities like IP addresses (e.g., 10.64.2.30, 149.56.234.165, 6761106f8163133...), domains (e.g., lance.springwel...), and malware (e.g., Trojan.Win32.Co..., Infostealer.Hoa...). A detailed panel on the right shows the 'Overview' and 'References' for the selected IP 149.56.234.165. Below this, an 'X-Force Exchange Report' is displayed with a score of 1 and a reason related to a Regional Internet Registry location mapping in Canada.

Relevance	Toxicity	Offense Count	Last Seen	Event/Flow Count
1.0	0.0	1	January 20, 2017	3

X-Force Exchange Report

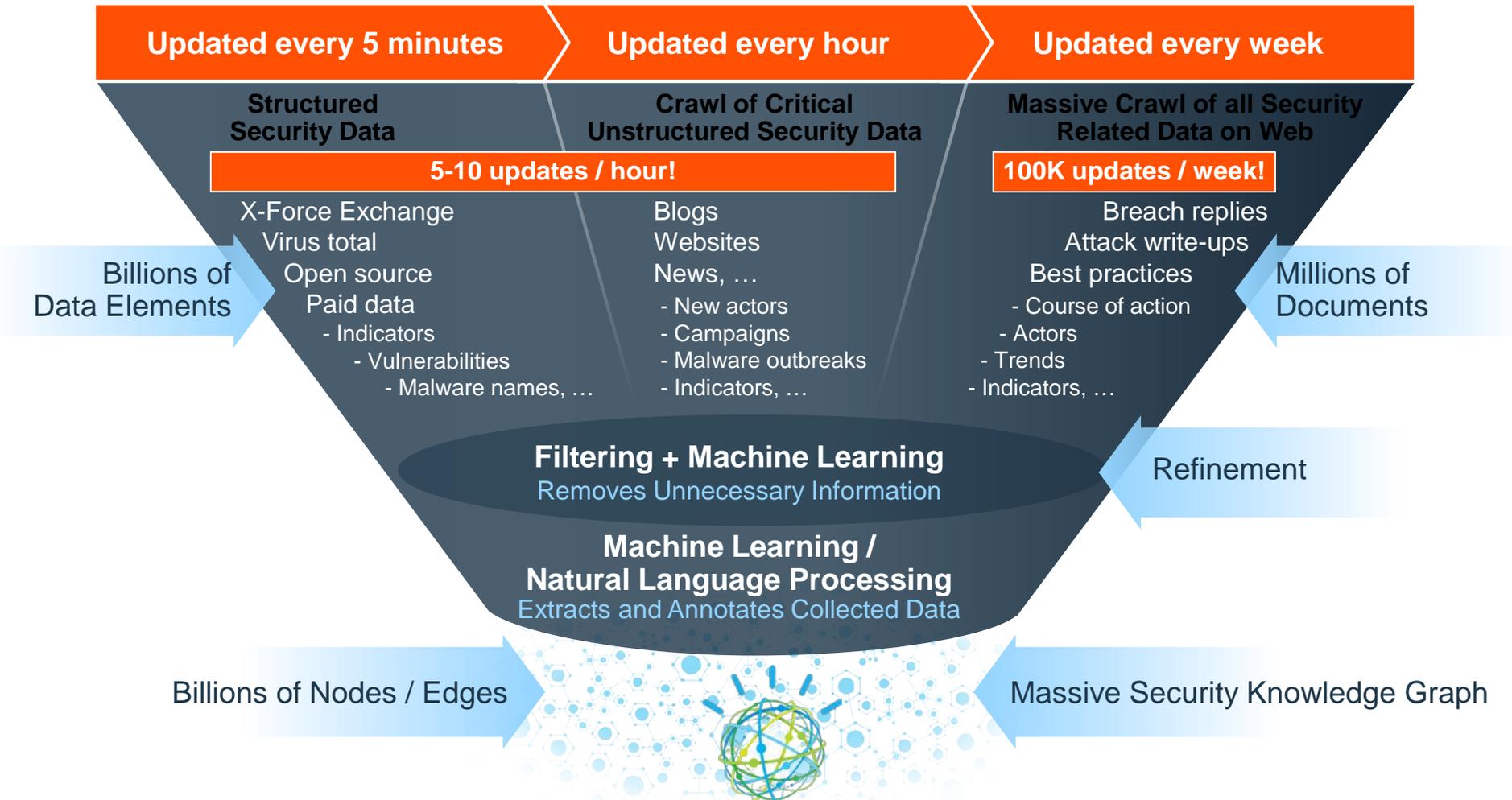
Score	1
Reason	Regional Internet Registry
Description	One of the five RIRs announced a (new) location mapping of the IP.
Country	Canada
Categories	

QRadar: Watson Advisor – Quick Filters

The screenshot displays the IBM QRadar Security Intelligence interface. The top navigation bar includes the URL `ge.com/security/demos/watson/rsa/CozyDuke_QRadar/` and various application icons. The main interface is divided into a left sidebar and a central workspace. The sidebar contains sections for 'Analyzer', 'Offense 244', 'Observables', 'Relationships', 'Stage 2 display', and 'Key insights only'. The 'Observables' section is expanded, showing a list of filter categories and their counts. The central workspace displays a network graph with nodes representing different types of observables and their relationships. A red circle with a slash is overlaid on one of the nodes, indicating a filter application.

Observable Type	Count
AV Signature	6
Domain	2
File	11
Hash	11
IP	4
URL	2
User	1

Building the Foundation of Cognitive Security





Build deep understanding of threats targeting your business through cyber analysis

IBM i2 Enterprise Insight Analysis

Find, fix, and secure endpoints

Prevent advanced network attacks

Use analytics to discover and eliminate threats

Hunt for and investigate threats

Coordinate response activity

Understand the latest threat actors

Get help from security experts

IT and Non-traditional Information Feeds

- PCAP
- Alerts
- System logs
- SIEM
- SSO / AD
- Vulnerability scans
- HR data
- Reviews
- Behavioral data
- Badge logs
- Access logs
- Account creation

External Information Feeds

- Hacker forums
- Intel vendors
- Threat indicators
- Social media
- Government alerts
- Community info



**HUMAN-LED
CYBER
ANALYSIS**

Focused Monitoring and Threat Mitigation

- Integrated data feeds
- Enterprise awareness
- Compliance monitoring
- Threat discovery
- Risk management
- Enable decisions



Key Differentiators of i2 vs. Other IBM Security Products



For Advanced Users
Tier 3, Threat Hunters

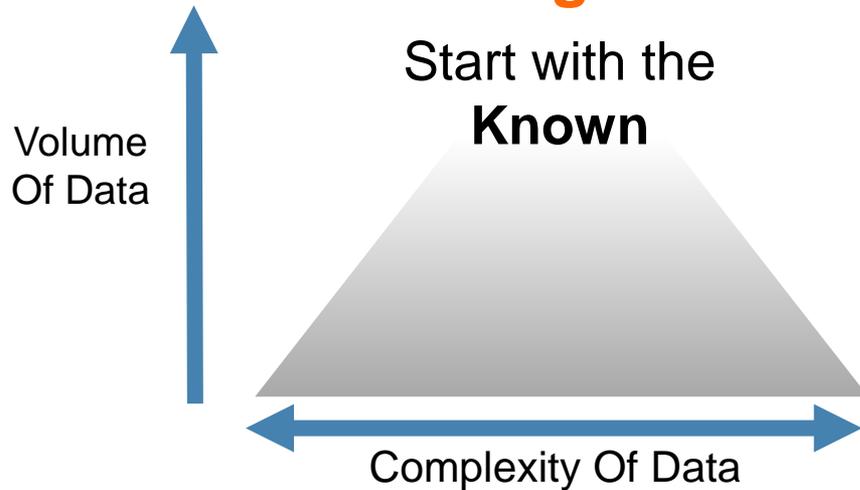


We Do Investigations
Human in the Loop

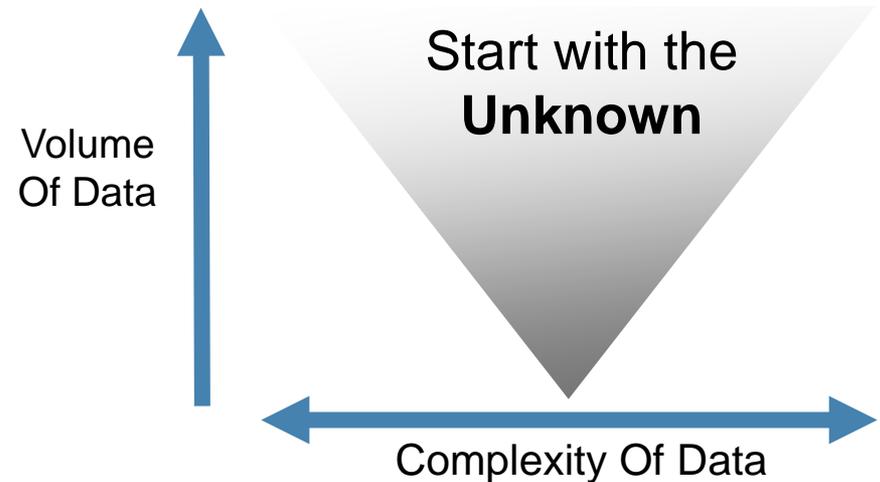


Non-Cyber Datasets
Physical, HR, Dark Web

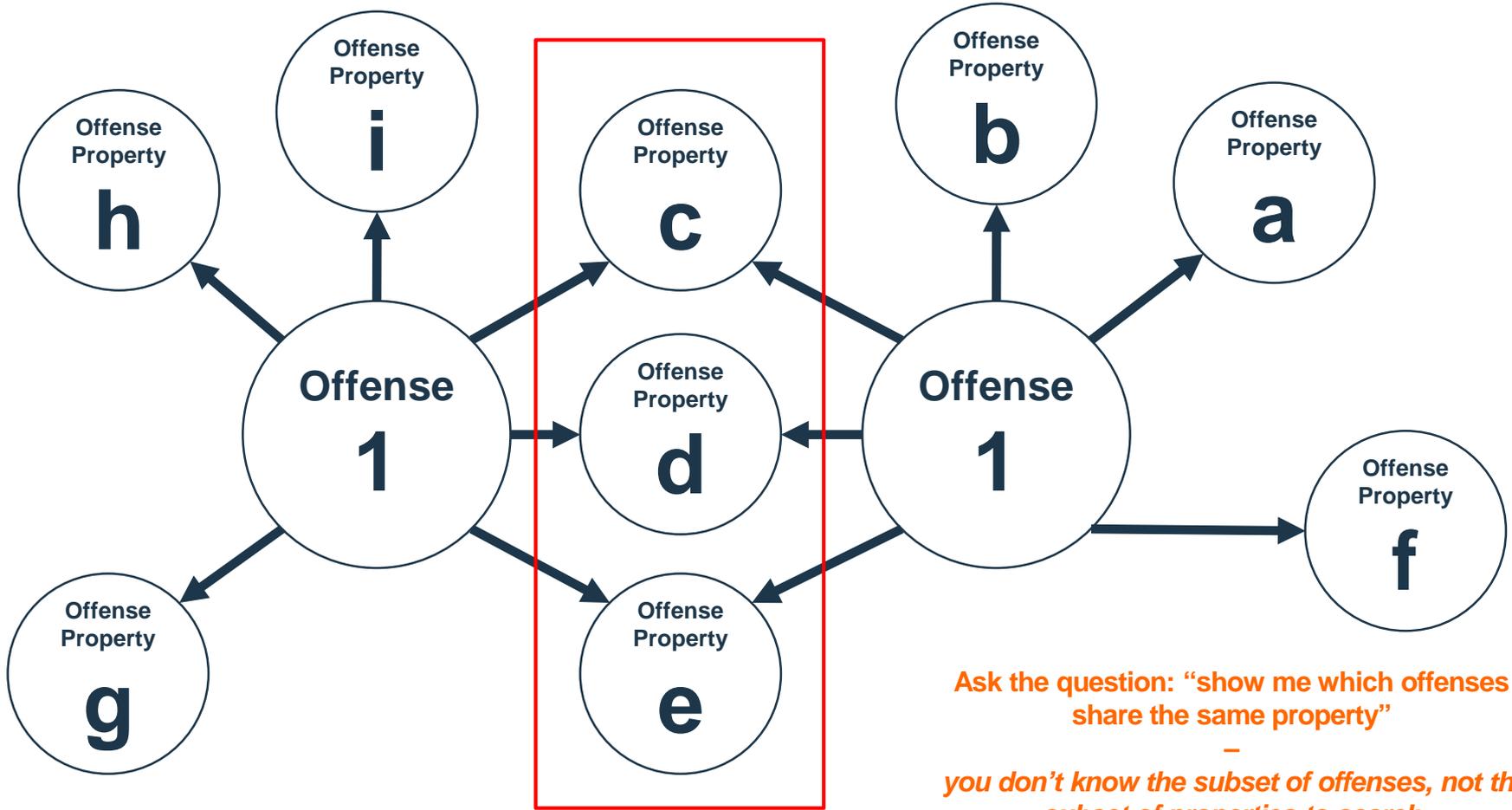
Investigations

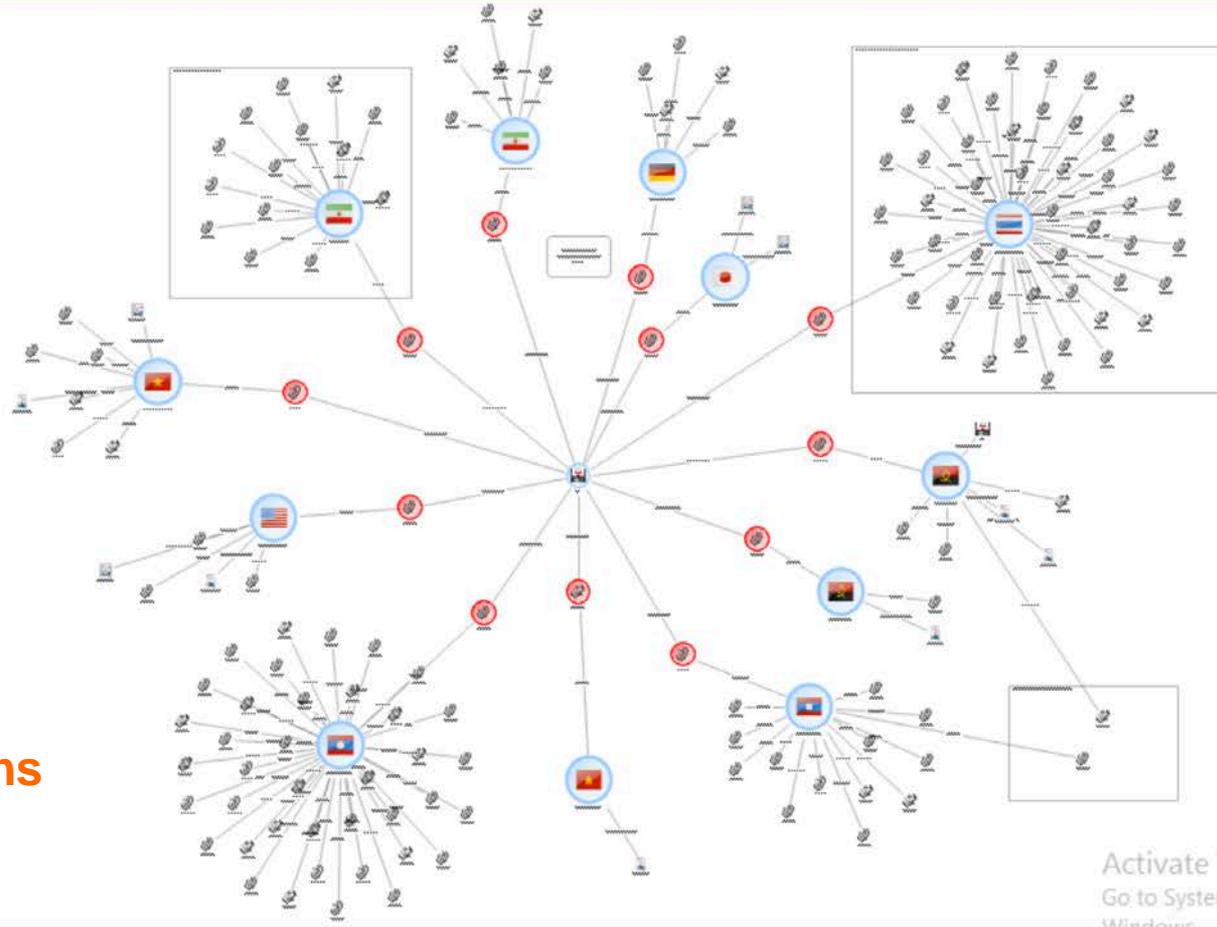


Hunting



What is an Unknown Unknown Search





Investigations

Activate Windows
Go to System in Control Panel to activate Windows.

Hide Selected, Hide Unselected, Show and Hide, Show and Hide Items

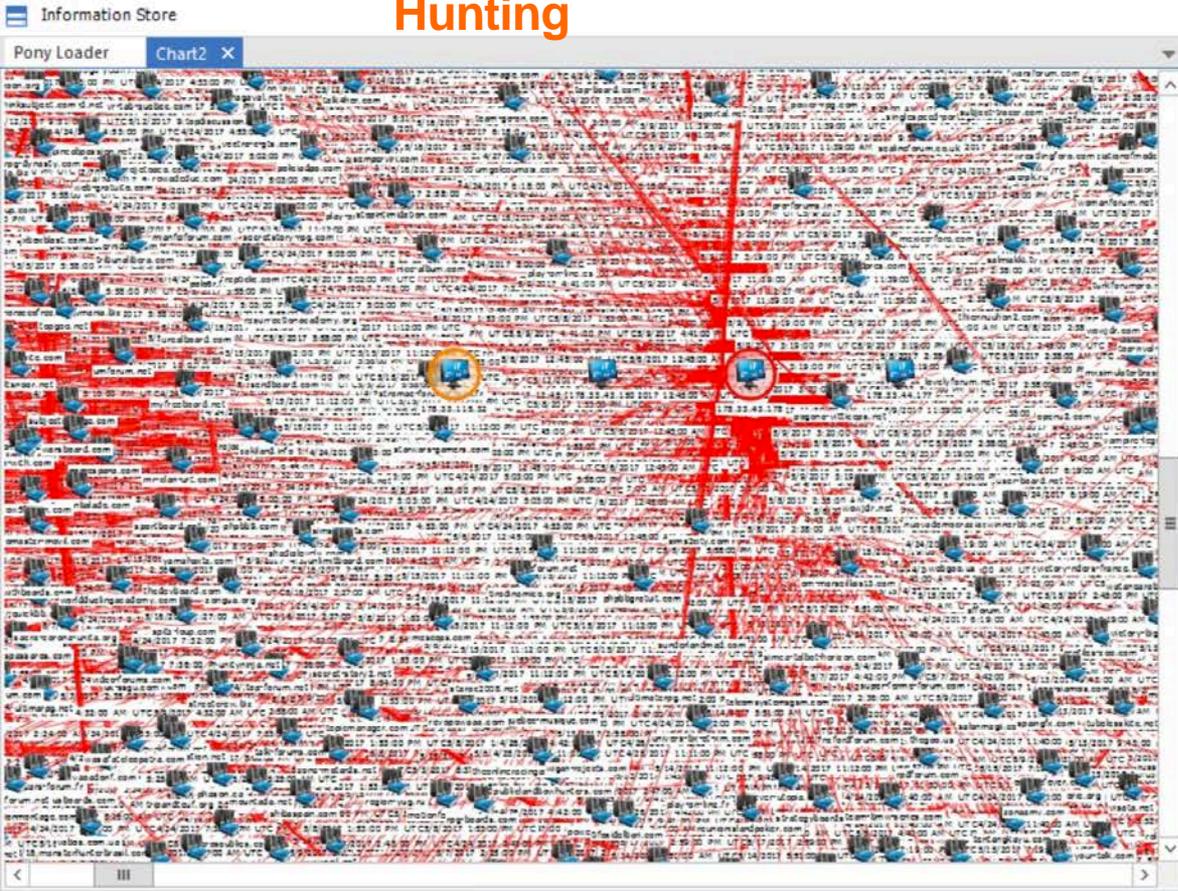
Reveal, Show All, Fit to Window, Fit Selection to Window

Zoom In, Zoom Out, Actual Size, Drag Chart, Zoom and Pan

Fit Height to Window, Zoom to Area, Overview Pane, Show

Page Boundaries, Gridlines, Time Bar, Infotips, More Panes, View Multiple, Split, New Window, Full Screen

Hunting



Charting scheme: Charting Scheme 1

List Most Connected

Counts Values

The number of links or number of connected items are counted

- Most links
- Most inbound
- Connections with the most links
- Most connected entities
- Most outbound

Restrict Show: 50 250 500

Entities with the most links

Entity	Count
178.33.43.178	14571
178.33.115.32	4927
178.33.44.177	4914
178.33.43.150	4863
141.101.115.96	405
151.101.192.194	286
151.101.128.194	286
151.101.64.194	286
realbb.net	212
vampire-legend.net	208
wikiotics.com	185

Update Copy x

50%

Highlight Colors... Set Line Width Highlight Top 8 Undo Highlighting

The Collaborative Endpoint Security and Management Platform

IBM BigFix

IT SECURITY



IT OPERATIONS

IBM BigFix

FIND IT. FIX IT. SECURE IT... **FAST**



Detect	Compliance	Lifecycle	Inventory	Patch
Detect and respond to malicious activity	Continuous policy enforcement and reporting	Software patching, distribution and provisioning	Audit authorized and unauthorized software	Automated patching with high first pass success
<ul style="list-style-type: none"> Asset discovery Detect Investigate Response Query Patch management Software distribution 	<ul style="list-style-type: none"> Query Patch management Security configuration management Vulnerability assessment Compliance analytics Third-party anti-virus management Self quarantine Add-on: PCI DSS 	<ul style="list-style-type: none"> Asset discovery Patch management Software distribution Query Advance patching Remote control OS deployment Power management Sequenced Task Automation 	<ul style="list-style-type: none"> Software / hardware inventory Software usage reporting Software catalogue correlation ISO 19770 software tagging 	<ul style="list-style-type: none"> OS patching Third-party application patching Offline patching

Resilient's unique value

- **Resilient integrates with all existing security systems create a single hub for IR transforming organizations' security posture.**
- Aligns people, process, and technology across the organization
- Enables security teams to automate and orchestrate their IR processes
- Ensures IR processes are consistent, intelligent, and configured to teams' specific needs



Resilient Playbooks

nt x

scidents/2109?tab=81fccb8-abc7-45fd-b7e9-2e494e7be849

resilient Dashboards ▾ List Incidents New Incident My Tasks Simulations Search

Jose Bravo
Bravo IBM ▾

QRadar ID 258 - Massive file open - a possible Ransomware

Actions ▾

Summary

ID 2109
Phase Engage
Severity —
Executive In... Unknown
Date Created 04/11/2017
Date Occur... 04/11/2017
Date Discov... 04/11/2017
Data Compr... Unknown
Incident Type **Ransomware**

People

Created By **Jose Bravo**
Owner **CSIRT**
Members *There are no members.*

Related Incidents

No related incidents.

Attachments

Description

999 events in 2 categories: a Massive file open occurred - a possible Ransomware

Tasks Details QRadar Details Artifacts Breach Notes Members Attachments Stats Timeline

Tasks

0% Complete Filter: All ▾ Selected ▾ Add Task

Task Name	Owner	Due Date	Flags	Actions
Engage				▾
<input checked="" type="checkbox"/> Identify assets affected by ransomware attack			🗨️ 👤	⋮
Detect/Analyze				▾
<input checked="" type="checkbox"/> Identify ransomware variant			🗨️ 👤	⋮
Respond				▾
<input checked="" type="checkbox"/> Isolate affected systems and user accounts from network			🗨️ 👤	⋮
<input checked="" type="checkbox"/> Isolate backup media from network			🗨️ 👤	⋮
<input type="checkbox"/> Block IP addresses & URLs	Unassigned ▾	🕒 No due date	🗨️ 👤	⋮

Instructions

Conduct forensic analysis on memory images, disk images, log files, and other relevant data sources. Identify command & control IP addresses or URLs. If applicable, detonate suspected ransomware executables in a sandbox.

Maintenance of data integrity for future legal or law enforcement use may be a consideration. In addition, identifying the initial source of the



Gain integrated, real-time threat intelligence

IBM X-Force Exchange

Find, fix, and secure endpoints

Prevent advanced network attacks

Use analytics to discover and eliminate threats

Coordinate response activity

Understand the latest threat actors

Get help from security experts



**Crowd-sourced information sharing
based on 700+TB of threat intelligence**
<https://exchange.xforce.ibmcloud.com>



Gain integrated, real-time threat intelligence

IBM X-Force Exchange – Tailored Dashboards

Dashboard

Recent IBM X-Force Advisories

- Dridex v4 - Major version upgrade released**
malware Feb 28, 2017
 - Spear Phishing Attacks Preceding Shamoon Malware Breakouts**
Feb 19, 2017
 - Aggressive SQL Injection Attack**
incident Jan 31, 2017
 - Aggressive SQL Injection Activity**
incident Jan 24, 2017
 - OnePlus 3 'fastboot oem selinux permissive' Vulnerability**
vulnerability Jan 11, 2017
 - Attacking Nexus 6 & 6P Custom Bootmodes**
vulnerability Jan 5, 2017
 - Google Android Synaptics Touchscreen Heap Overflows**
vulnerability Dec 13, 2016
- [view more](#)

Groups



Start working with groups.
Using groups makes it easy to share and collaborate around Collections.
Create a group, add members, and share Collections.

[Create a Group](#)

Malicious IP addresses in the last hour

1,346

Command and Control	4
Spam	1,088
Malware	11
Scanning	175

Recommended Collections

- Known Hostile Actors**
threat-actor, exploit-kit, vulnera... Mar 8, 2017
- Phishing & Spam**
x-force, spam, phishing Mar 7, 2017
- GootKit: Ongoing Research Collection**
x-force, gootkit, botnet, cybercr... Mar 1, 2017
- TrickBot Ongoing Collection**
x-force, trickbot, cybercrime, ... Mar 1, 2017

Most Recent Public Collections

- XFTAS Daily Threat Assessment for March 07, 2017**
xftas Mar 8, 2017
 - Phishing URLs Promoted In Spam Mails**
x-force, phishing, spam Mar 8, 2017
 - XFTAS Daily Threat Assessment for March 02, 2017**
xftas Mar 8, 2017
 - XFTAS Daily Threat Assessment for March 01, 2017**
xftas Mar 8, 2017
- [view more](#)

Latest Vulnerabilities

- WordPress Press This function cross-site request forgery**
Consequences: Gain Access
 - WordPress audio playlist function cross-site scripting**
Consequences: Cross-Site Scripting
 - iCloudCenter Daily Deals Script deal.php SQL injection**
Consequences: Data Manipulation
 - Western Digital My Cloud file upload**
Consequences: Gain Access
 - Western Digital My Cloud OS command execution**
Consequences: Gain Access
 - Western Digital My Cloud cross-site request forgery**
Consequences: Gain Access
 - Western Digital My Cloud username buffer overflow**
Consequences: Gain Access
- [view more](#)

My Collections

You did not create any Collections yet.

Shared with me

No Collections are shared with you yet.

Security Intelligence Blog

- Information Overload — Now What?**
By Ian S. Thomas Mar 8, 2017
- Connecting to the Future With Cognitive Security**
By David Jarvis Mar 8, 2017
- Hybrid Cloud Adoption: The Logical Next Step Toward Innovati...**
By Vikalp Nagori Mar 8, 2017

Featured from App Exchange



QRadar Advisor With Watson

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

Botnet Distribution - proxyback



Affected Countries 71
Trend **Peak** Mar 6, 2017

Find, fix, and secure endpoints

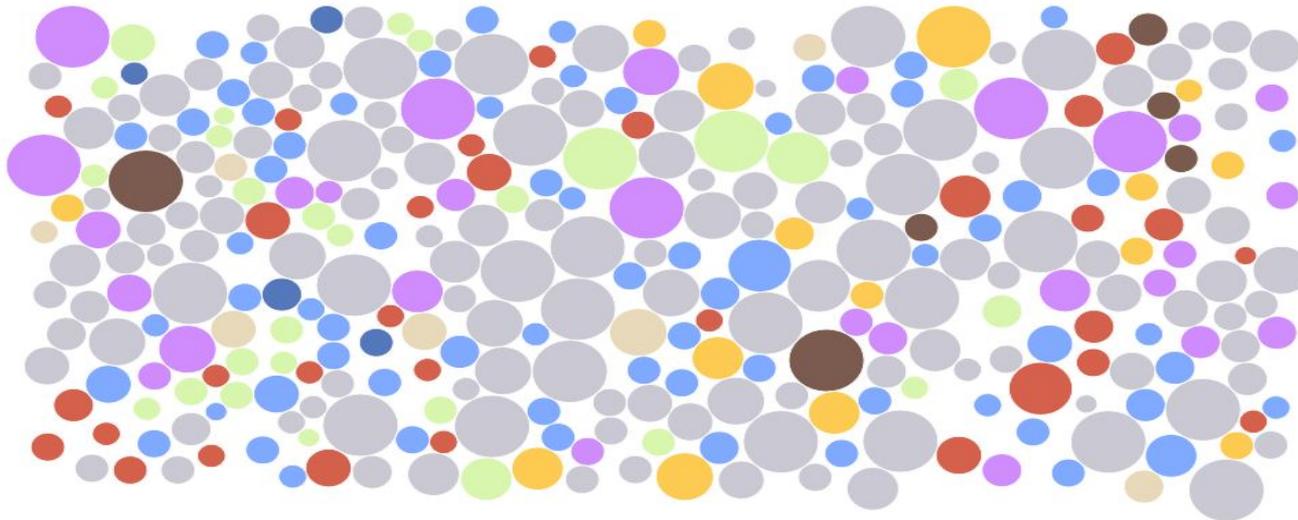
Prevent advanced network attacks

Use analytics to discover and eliminate threats

Coordinate response activity

Understand the latest threat actors

Get help from security experts



Security Incidents < 2016

Displaying **322** incidents
Jan 4, 2016 to Dec 31, 2016.

Each circle represents a target of a security incident such as a data leak or denial of service attack.

Click or hover over circles to see more information. Change the year view by clicking the arrows next to the year above.

Data is a sampling of notable incidents for each year and not a full representation of all incidents.

Learn More:
 Read the 2016 Cost of a Data Breach Study from Ponemon Institute

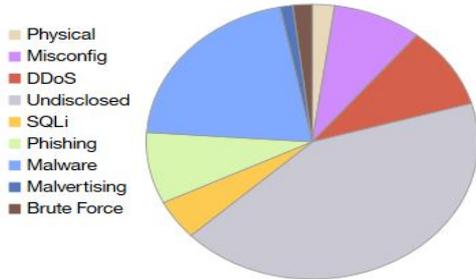
Size of circle estimates relative impact of incident in terms of cost to business.

⌚ ⌚⌚ ⌚⌚⌚

Jan 16 Feb 16 Mar 16 Apr 16 May 16 Jun 16 Jul 16 Aug 16 Sep 16 Oct 16 Nov 16 Dec 16 Jan 17

Attack Types (reset)

Click to view incidents for a specific attack type.



Industries (reset)

Click below to view incidents from a specific industry.

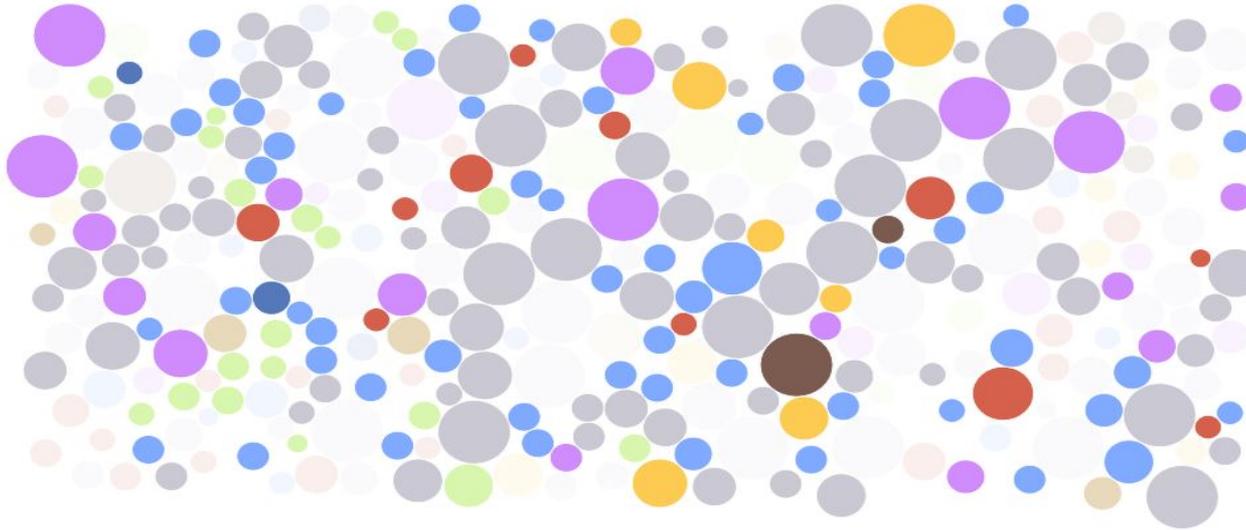


Target Geography (reset)

Size of flag indicates higher volume. Click to view incidents for that geography.



https:exchange.xforce.ibmcloud.com - US



Security Incidents < 2016

Displaying **322** incidents
Jan 4, 2016 to Dec 31, 2016.

Featuring **200** incidents from:
Geography: United States
 (show all incidents)

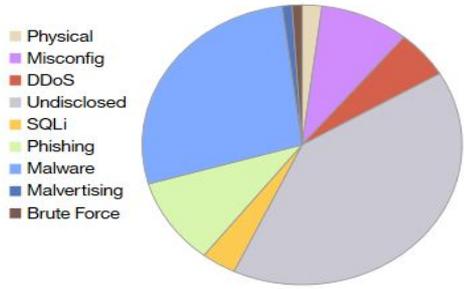
Learn More:
 Read the 2016 Cost of a Data Breach Study from Ponemon Institute

Size of circle estimates relative impact of incident in terms of cost to business.

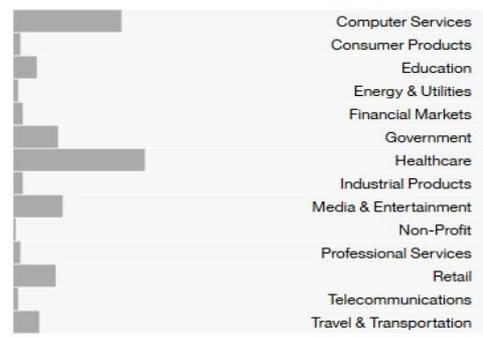
●
●●
●●●
●●●●

Jan 16 Feb 16 Mar 16 Apr 16 May 16 Jun 16 Jul 16 Aug 16 Sep 16 Oct 16 Nov 16 Dec 16 Jan 17

Attack Types (reset)
 Click to view incidents for a specific attack type.



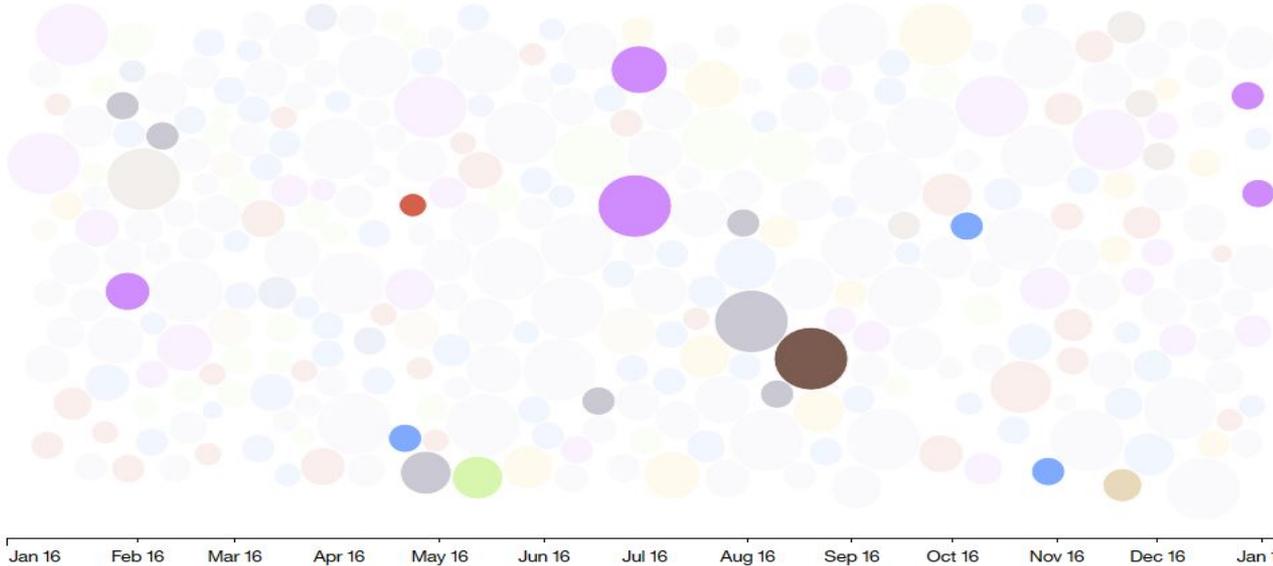
Industries (reset)
 Click below to view incidents from a specific industry.



Target Geography (reset)
 Size of flag indicates higher volume. Click to view incidents for that geography.



https:exchange.xforce.ibmcloud.com – US Government



Security Incidents < 2016

Displaying **322** incidents
Jan 4, 2016 to Dec 31, 2016.

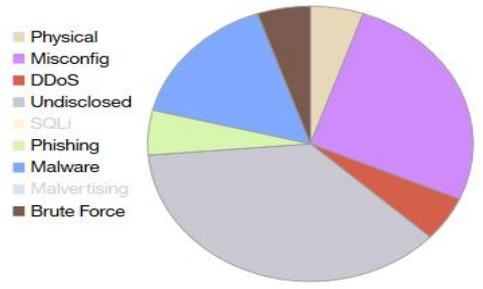
Featuring **19** incidents from:

Industry: Government
Geography: United States
 (show all incidents)

Learn More:
 About how attackers commit extortion by distributed denial of service attacks

Size of circle estimates relative impact of incident in terms of cost to business.

Attack Types (reset)
 Click to view incidents for a specific attack type.



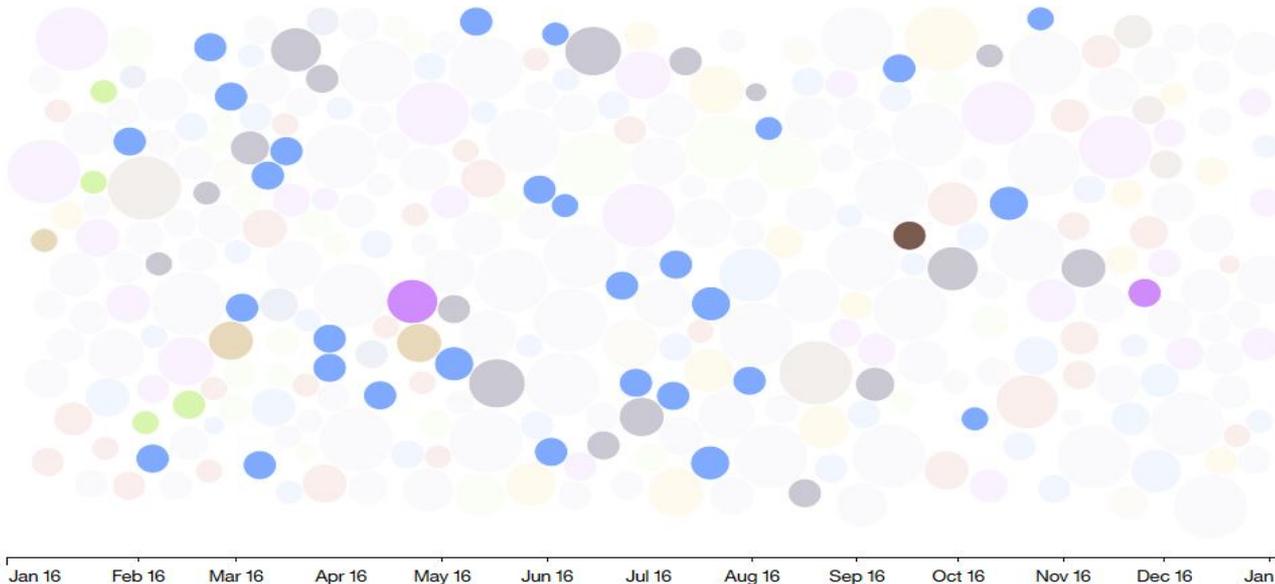
Industries (reset)
 Click below to view incidents from a specific industry.



Target Geography (reset)
 Size of flag indicates higher volume. Click to view incidents for that geography.



https:exchange.xforce.ibmcloud.com – US Healthcare



Security Incidents < 2016

Displaying **322** incidents
Jan 4, 2016 to Dec 31, 2016.

Featuring **56** incidents from:

Industry: Healthcare
Geography: United States
(show all incidents)

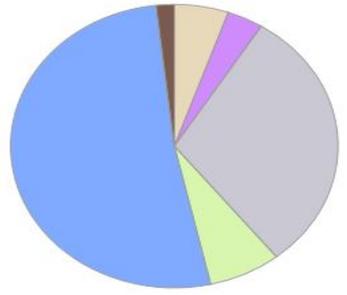
Learn More:
Read the 2016 Cost of a Data Breach Study from Ponemon Institute

Size of circle estimates relative impact of incident in terms of cost to business.

\$ \$ \$ \$\$\$

Attack Types (reset)
Click to view incidents for a specific attack type.

- Physical
- Misconfig
- DDoS
- Undisclosed
- SQLi
- Phishing
- Malware
- Malvertising
- Brute Force



Industries (reset)
Click below to view incidents from a specific industry.

- Computer Services
- Consumer Products
- Education
- Energy & Utilities
- Financial Markets
- Government
- Healthcare**
- Industrial Products
- Media & Entertainment
- Non-Profit
- Professional Services
- Retail

Target Geography (reset)
Size of flag indicates higher volume. Click to view incidents for that geography.



https:exchange.xforce.ibmcloud.com – US Education



Security Incidents < 2016

Displaying **322** incidents
Jan 4, 2016 to Dec 31, 2016.

Featuring **10** incidents from:
Industry: Education
Geography: United States
 (show all incidents)

Learn More:
 Read the 2016 Cost of a Data Breach Study from Ponemon Institute

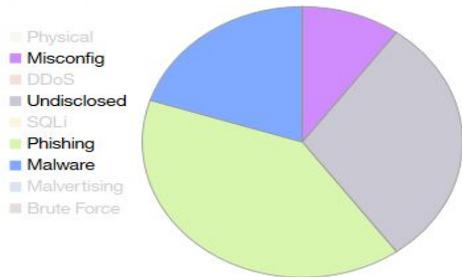
Size of circle estimates relative impact of incident in terms of cost to business.

\$ \$\$ \$\$\$

Jan 16 Feb 16 Mar 16 Apr 16 May 16 Jun 16 Jul 16 Aug 16 Sep 16 Oct 16 Nov 16 Dec 16 Jan 17

Attack Types (reset)

Click to view incidents for a specific attack type.



Industries (reset)

Click below to view incidents from a specific industry.

- Computer Services
- Consumer Products
- Education**
- Energy & Utilities
- Financial Markets
- Government
- Healthcare
- Industrial Products
- Media & Entertainment
- Non-Profit
- Professional Services
- Retail
- Telecommunications
- Travel & Transportation

Target Geography (reset)

Size of flag indicates higher volume. Click to view incidents for that geography.



State of NC QRadar Workshop

Threat Hunting, Advanced Analytics,
Augmented Intelligence, and Automated Response


Michael Melore, CISSP

IBM Cyber Security Advisor



@MichaelMelore

October 2017