IBM Security

Let’s Talk About Threat Intelligence

IBM SECURITY SUPPORT OPEN MIC #20

Slides and additional dial in numbers: **http://ibm.biz/openmic20**

January 26, 2017

IBM

Panelists

- Jason Keirstead – QRadar Architecture Team
- Rory Bray – QRadar Security Architect
- Dwight Spencer – Principal Solutions Architect
- Adam Frank – Principal Solutions Architect
- Peter Szczepankiewicz - QRadar Offering Manager
- Jonathan Pechta – Support Technical Writer / Support Content Lead

Special Guests

- Eric Newman – RiskIQ
- Hugh Docherty - PhishMe
- Steve Ginty - RiskIQ

Announcements

QRadar 7.3 – Coming soon & what you need to know in advance

- Controlled rollout is now in progress for QRadar 7.3.
- This upgrade will be an ISO file that must be installed on each appliance (no patch all)
- Due to the size of the upgrade, it is expected to take slightly longer than previous patches.
- A new requirement of WinCollect 7.2.4 is in place.

QRadar Open Mics – Coming soon

- QRadar Open Mic #21: Vulnerability & Risk Management with QRadar (February 23rd)
- QRadar Open Mic #22: QRadar 7.3 Feature Discussion (Live – March 21st)

QRadar forums

Reminder that we have a new forum at http://ibm.biz/qradarforums.

This is a great place to get questions answered from support, developers, and other QRadar users and administrators.

Threat Intelligence

What is Threat Intelligence? (TI)

- Threat Intelligence is the brother and a component of Security Intelligence, these are the tools, data, and procedures that are relevant to protecting your organization.
- Threat Intelligence includes in-depth curated information about specific threats to help organizations protect themselves from attacks that are new, unknown, or damaging.

Analogy

Think of Threat Intelligence as a Neighborhood Watch program, but for security data. You already have measures and tools in place for protecting your home, but outside data provided by others who have seen risks and incidents you have not can provide critical information to protect you home. The people in your neighborhood watch are the people, vendors, and security community who share data, tools, and techniques.

Vectors

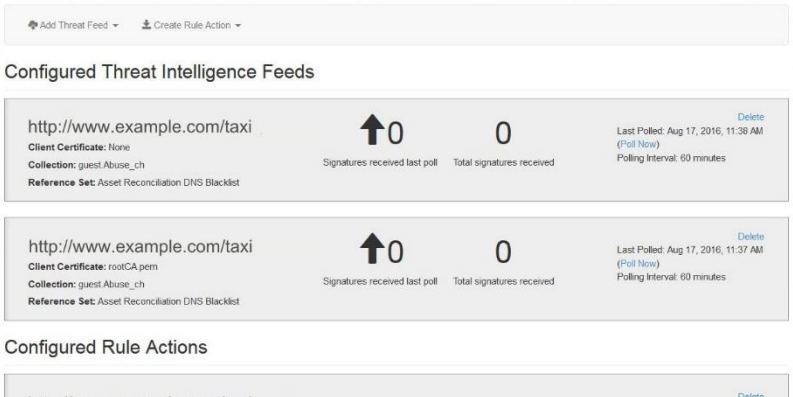
People (phishing), drive by downloads, file infectors, vulnerable applications (CVE), infrastructure issues, legacy software, and more.

How to Bring Threat Intelligence to QRadar

- Threat Intelligence provides users and administrators the power to act on indicators of attacks. With each feed, this data and indicators might be different; however, in QRadar this information all revolves around Reference Data, except for the IBM X-Force IP Reputation Feed enabled via the System Settings in QRadar 7.2.8+.

- QRadar has a “Threat Intelligence” app that leverages STIX/TAXII format feeds to import data in to Reference Sets.

- A number of IBM Partners have created apps that take the guess work out of this process for their feed data.



RISKIQ

QRadar
RiskIQ PassiveTotal for IBM QRadar
Bring the power of RiskIQ PassiveTotal and threat intelligence directly to your...
By RiskIQ, Inc
IBM Validated

QRadar
Threat Intelligence
Stop threats by adding real time threat intelligence feeds to QRadar.
By IBM QRadar
IBM Validated

FireEye

QRadar
FireEye iSight Intelligence
Provide context rich threat intelligence from FireEye to mitigate threats and create...
By FireEye
IBM Validated

THREAT INTELLIGENCE PLATFORM

QRadar
T-Eye App for IBM QRadar
An app that integrates TRIAM's Threat Intelligence Platform with QRadar.
By Trillium Information ...
IBM Validated

resilient an IBM Company
UPDATED

QRadar
IBM Resilient QRadar Integration
Integration between the IBM Resilient Incident Response Platform and IBM QRadar.
By IBM
IBM Validated

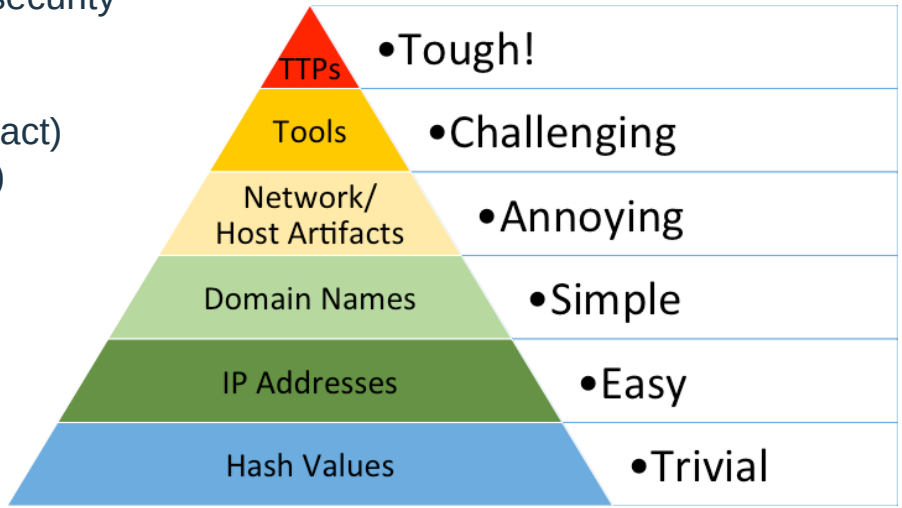
And more, who have not yet released their app, like PhishMe.

Indicators of Compromise Used in Threat Intelligence

An indicator of compromise is any recorded or captured piece of digital evidence from a security incident that can be used to provide information about an intrusion or issue. These indicators provide teams the first concrete targets for your investigation. These are your neighborhood watch fliers. Different threat intelligence feeds might use different indicators, depending on your region, business sector, security requirements.

Other indicators can include data captured by the security intelligence side, such as:

- URLs
- Anomalies (unusual traffic / behavior / first contact)
- Account change events (privileged escalations)
- Former employees
- Regional irregularities
- Mismatched port-application traffic
- Large HTML responses (injections)
- Volume of requests for identical file
- Registry changes
- DNS anomalies



http://detect-respond.blogspot.com

Recommended reading: http://detect-respond.blogspot.com/2014/03/use-of-term-intelligence-at-rsa.html

How to Get Threat Intel Data in to QRadar

A. Adding Threat Intelligence with an IBM Partner App:

1. You must be at QRadar 7.2.6+ or the specified version of QRadar the app has been validated against. In most cases, QRadar support will recommend a minimum of QRadar 7.2.6 Patch 4 for any QRadar systems that leverage apps/extensions.
2. Install the app via the **Admin tab > Extension Management.**

B. If you are adding the IBM X-Force Threat Intelligence Feed:

1. You must be at QRadar 7.2.8 or later.
2. Enable the feed from the **Admin tab > System Settings > Enable X-Force Threat Intelligence Feed> Yes**.

C. Adding a feed using the IBM Threat Intelligence app:

Create an authorized service token, add a proxy server and CA certificates (if required), create reference sets for the data, add your threat feed (STIX/TAXII), create a TAXII Rule Actions.

D. Leverage the QRadar API

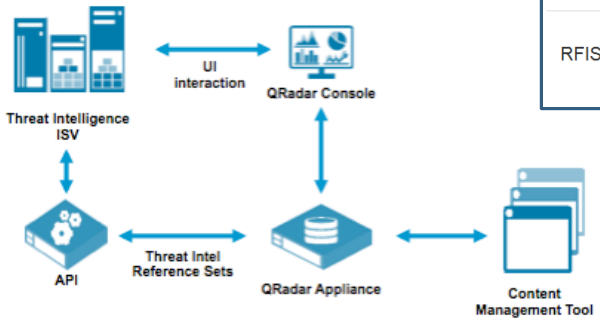
Using the QRadar API, customers can send threat intelligence data to directly update reference sets.

Leveraging a Basic Rule Set for Feed Data (RFISI)

- Partners who work with IBM to create apps are provided a baseline rule set as a content pack. This is available to all users and includes generic rules that can be used with any threat intelligence data. This is the “IBM Security Ready for Security Intelligence Content Pack”, which is available for download from the X-Force App Exchange (https://exchange.xforce.ibmcloud.com/hub/).
- Requires QRadar 7.2.6 Patch 4 or later.
- Includes generic rules that are intended to be modified and exported by vendors. Normal admins can install this to work with or expand on their threat data.

Rules added by the RFISI Threat extension

Rule Name	Description
RFISI: Internal Communication with a Malware URL	This rule adds URLs from content collections to a Malware URLs reference set.
RFISI: Internal Connection to Address Hosting Malware	This rule adds the destination IP address from content collections to a Malware IPs reference set.
RFISI: Internal Connection with Botnet Command and Control	This rule adds the destination IP address from content collections to a Botnet C&C IPs reference set.
RFISI: Internal Hosts Communicating with Anonymizer Host	This rule adds the destination IP address from content collections to an Anonymizer IPs reference set.
RFISI: Mail Server Sending Mail to SPAM Servers	This rule adds the source IP address from content collections to an Spam Senders IPs reference set and compares source IP values to the BB:Mail Servers and a Mail Server IPs reference set.
RFISI: Phishing Email sent to Internal Mail Server	This rule adds the source IP address from content collections to an Phishing Senders IPs reference set and compares source IP values to the BB:Mail Servers and a Mail Server IPs reference set.



Ready for Security Intelligence (RFISI) Rules and Reference Data

- **URL**: https://ibm.biz/rfisi_threat_intel
- **GitHub**: https://github.com/ibm-security-intelligence/data-import/tree/master/rfisi-threat-import

Pre-defined Reference Collections

Each of these sets has a complimentary reference table to hold extended data related to each item in a set. For example, Phishing Senders set will be accompanied by a reference table called Phishing Senders Data.

- **Phishing Senders** - contains IPs of hosts that are known/suspected of sending phishing attempts.
- **Phishing Subjects** - contains subject lines from email campaigns that are known to be phishing attempts
- **Spam Senders** - contains IPs of known spam servers. If the provider doesn't distinguish between phishing and other spam then both go in this set.
- **Malware Senders** - contains IPs of mail hosts known to send malicious emails (virus/malware attachments, html exploits, etc). If the providers doesn't distinguish between these and other spam then all should go to the Spam Senders set.
- **Malware URLs** - contains URLs know to be malware downloads
- **Malware Hostnames** - contains the hosts (or IPs) of servers providing malware downloads. Hostnames are better due to virtual hosting.

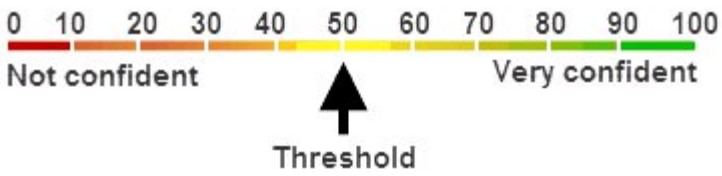
Ready for Security Intelligence (Continued)

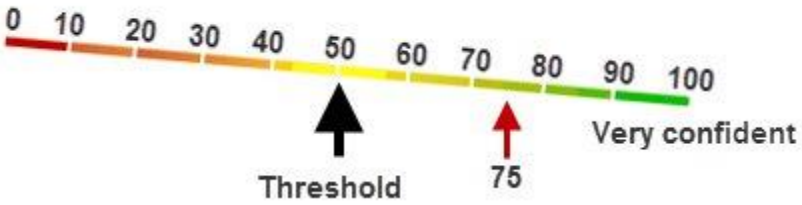
- **Phishing URLs** – contains the URLs associated with phishing emails
- **Malicious URLs** – contains URLs for other exploit types (browser exploits mainly)
- **Botnet IPs** - contains IPs associated with botnet activity. Intended for nodes rather than C&C IPs but if the provider doesn't distinguish between them then both go in this set.
- **Botnet C&C IPs** - contains IPs known to be C&C servers rather than nodes. If the provider does not distinguish between nodes and C&C, then all Ips should go to the Botnet IPs set.
- **Malware IPs** - contains IPs associated with malware post-exploit communications (exfiltration uploads, etc)
- **Anonymizer IPs** - contains IPs of known anonymized services, such as VPN providers, TOR exit nodes and other proxies.
- **Malware Hashes MD5** - contains MD5 sums of malware files
- **Malware Hashes SHA** - contains SHA (SHA-1, SHA-256, etc) sums of malware files
- **Rogue Process Names** - contains process names or executable names for known malware, trojans, etc.

Ready for Security Intelligence (Continued)

Each of these reference tables will have a primary key of the same type and value as the set they compliment. Each reference table also provides the following fields:

- **Provider** - The Threat Intel provider's name so that detection can be attributed to the correct threat integration.
- **Confidence** - A confidence rating between 0 and 100, if applicable. Use 50 if unknown or if translating from high-med-low use a reasonable distribution like 90-50-20.





- **First Seen Date** - The date that the threat provider first observed the indicator.
- **Last Seen Date** - The most recent observation.

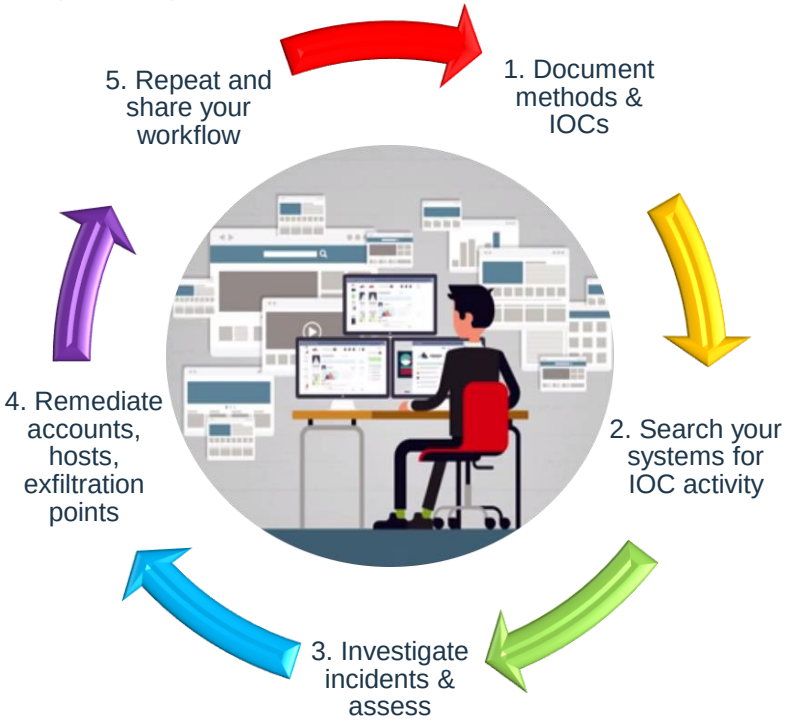
Chat discussion – Your chance to respond to the community…

1. What are some STIX/TAXII feeds that you use in your environment?
   Type in to chat some of the feeds that you find useful or important.
2. How do I judge the quality of my threat intelligence feed?
3. What are quality of Indicators of compromise? Any tips or hints.
4. The best threat intelligence is from inside your own space and analysis. Given a botnet C&C that YOU find, you would naturally go hunt over history. You then can share this data using tools to help others, such as the Malware Information Sharing Platform or the X-Force Exchange.

Investigations, Intelligence, Tools, & Workflow

Identifying the important facts:

1. **How?** (Document / generate reports for everything)
2. **Who?** (Accounts impacted)
3. **What?** (Data or systems involved)
4. **Where?** (Entry & exfiltration points)
5. **Why?** (Weaknesses / required remediation)



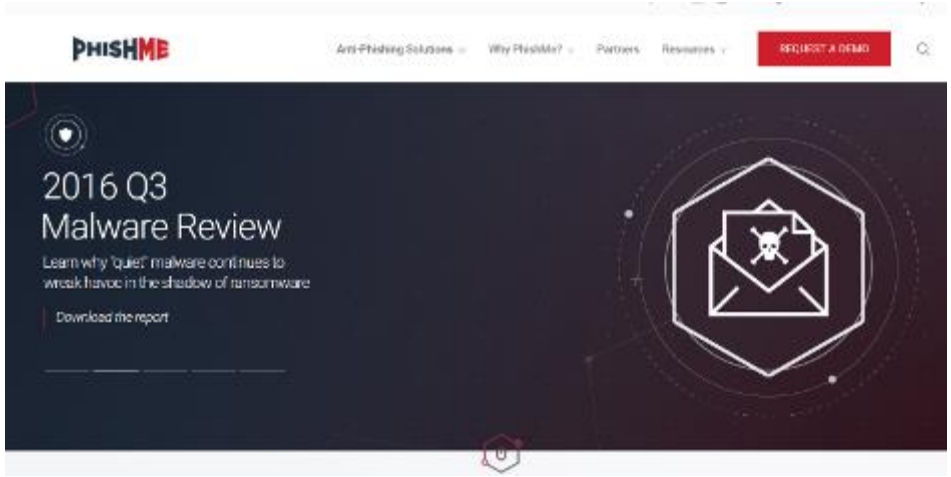
Watson Advisor

A new generation of tools is coming soon with Watson Advisor. Using Cognitive computing to understand massive amounts of data from written to speech. Machine knowledge helps further curate and helps you get the visibility you need to respond swiftly to security incidents when they occur and learning along the way.

Special thanks to our guests

- RiskIQ: https://www.riskiq.com/

- To our panelist from PhishMe: https://phishme.com/



IBM Security

THANK YOU

FOLLOW US ON:

https://www.facebook.com/IBMSecuritySupport

QRadar Forums: https://ibm.biz/qradarforums

youtube/user/ibmsecuritysupport

@askibmsecurity

securityintelligence.com

xforce.ibmcloud.com

IBM