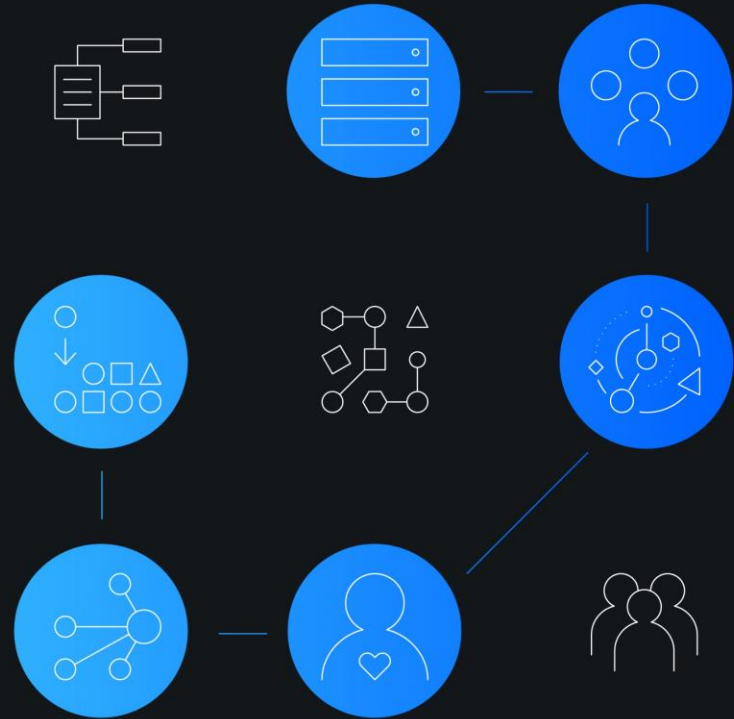


Welcome to

IBM Security Virtual User Group Day



IBM Security Community

8,000 Members Strong and Growing Every Day!

Sign up: <https://community.ibm.com/security>

User Group Day discussion: <https://ibm.biz/qradar-usergroupday> (share feedback, ask questions and continue the conversation after this session!)

Learn: The indispensable site where users come together to discover the latest product resources and insights — straight from the IBM experts.

Network: Connecting new IBM clients, veteran product users and the broader security audience through engagement and education.

Share: Giving YOU a platform to discuss shared challenges and solve business problems together.

IBM Security Community

[Home](#) [Groups](#) [Local Groups](#) [Events](#) [Participate](#) [Resources](#) [All Communities](#)

Learn, Network and Share in the IBM Security User Community

Collaboration is more important than ever before. In this user community of over 8000 members, we work together to tackle the challenges of cybersecurity.

[Join the community](#)

Tuesday 26 May	Guardium Virtual Users Group Monthly meeting for Guardium customers. To receive invitations to the VUG meetings, send an email to leila@us.ibm.com ■ Tue May 26, 2020 12:00 PM - 01:00 PM ET
Wednesday 27 May	Webinar: IT Security in the Post-Corona Threat Landscape It has become clear that the spread of the COVID-19 has also meant a spike in cybercrime. Fraudsters saw a golden opportunity to take advantage of a time when everyone was working from home and was vulnerable. ... ■ Wed May 27, 2020 08:30 AM - 11:15 AM GB
Wednesday 27 May	Virtual Cyber Threat Management PoT Event - May 27-28 As cyber threats (External and Insider), to your organization increase in number and sophistication, you need a balanced data management and threat analytics approach to handle Cyber Threat Management ... ■ Wed May 27, 2020 08:30 AM - Thu May 28, 2020 04:30 PM ET
Wednesday 27 May	Webinar: Identity & Access Management Capabilities to Support Remote Work Webinar Summary With the influx in remote work, your organization needs to ensure that the right people have the right to access the right systems and applications while working from home. Identity ... ■ Wed May 27, 2020 11:00 AM - 12:00 PM ET

Search Discussions

<input type="text" value="Term / Keyword / Phrase"/>			<input type="button" value="Q"/>
1 to 50 of 152 threads (549 total posts)			
<div>Most Recently Updated</div>		<div>50 per page</div>	
Thread Subject	Replies	Last Post	
Default python libraries...	1	19 minutes ago by BEN WILLIAMS Original post by Nathan Getty	
Gadget or Python to send Email	0	11 hours ago by Sean Ebeling	
Auto Close Tasks Based on Field Values	2	13 hours ago by Nick Mumaw	
Generic Email Parsing Script-missing code	1	3 days ago by Nathan Getty Original post by Justin Shoemaker	
Close Incidents with scripts	2	3 days ago by Nathan Getty	

Legal notes and disclaimer

Copyright © 2019 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS document is distributed "AS IS" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice. Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

Other company, product, or service names may be trademarks or service marks of others. A current list of IBM trademarks is available at "Copyright and trademark information" www.ibm.com/legal/copytrade.shtml

The QRadar Threat Management Mission

Enable customers to accurately and efficiently detect and manage threats to help mitigate the risk of data exposure and business disruption.



Provide advanced analytics to accurately detect critical threats against users, networks, systems and applications.



Improve operational efficiency by providing tools to more easily ingest data and better manage the system.



Streamline workflows to help analysts make faster, well-informed escalations, response decisions and actions.



Support customers as they modernize their IT environments and increasingly adopt cloud and containerized environments.

New challenges

Due to recent events employees switching to remote work.

- Increases in overall security incidents due to behavior changes and increased attack surface
- Phishing attack increases
- Visibility of endpoints/servers not connected to VPN
- Abnormal work hours, Different employee locations, web browsing behavior changes
- Increase in SaaS application use and lack of visibility

Typical Remote work behavior

97%

Remote workforce in 2 weeks



Remote Work Force: Tune to the new normal



Utilise Use Case Manager

- Review use cases and their accuracy
- Tune watch lists and logic
- Optimize QRadar network configuration

IBM QRadar Use Case Manager

Tuning

Last updated: 10/09/2019, 14:20:45

Open offenses

Active offenses

Offense creation trend

33

5

Tune your QRadar offenses by analyzing rules that cause the biggest number of offenses

Tune most active rules

QRadar Use Case Manager can help you determine which rules generate the most offenses, and then guide you through the steps to tune them.

Tune based on the CRE event report

The Custom Rules Engine (CRE) event report shows which CRE events were generated most often. It also provides information about the rule activity. You can tune these rules or use the event information from the report to update your QRadar environment.

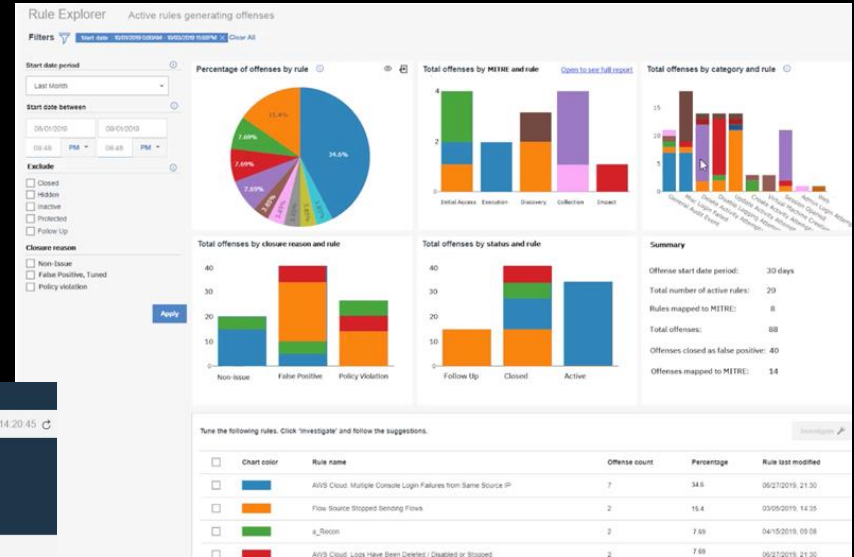
Tune your QRadar offenses by going through the most common configuration steps

Review network hierarchy

Network Hierarchy is used to define which IP addresses and subnets are part of your network. Defining your network hierarchy and keeping it up-to-date is an important step in helping prevent false offenses.

Review building blocks

Rules use information about your servers to determine whether to generate the rule responses. Review and update common rule building blocks to enable QRadar to discover and classify more servers on your network, and prevent false positives.



Remote Work Force: QRadar Best Practice Monitoring and Detection



01

Important Log Data

- Firewall, VPN & Proxy
- Endpoint and EDR Logs
- Email/Spam Filtering Logs
- DNS & DHCP Logs
- Cloud Services and Platforms



02

Collect flow data

- Utilize QNI or QFlow
- Flow collector locations:
 - Third-Party Infrastructure Clouds
 - Inside interface of the VPN Concentrator in the DMZ
 - Entry point of Third-Party Cloud Services



03

Utilize User Behavior Analytics (UBA)

- Update to the current version of UBA
- Update UBA Reference Sets
- Set up “Geo-Safety Use Case”
- Review the following Rule Categories:



04

Utilize the colliding content packs and UBA use case from App Exchange

- ✓ Data Exfiltration
- ✓ Phishing
- ✓ Sysmon and Windows
- ✓ Access and Authentication
- ✓ Accounts and Privileges
- ✓ Cloud
- ✓ Geography
- ✓ Network Traffic and Attack
- ✓ QRadar Network Insights

- Turn on the following User Models

- ✓ Access Activity
- ✓ Authentication Activity
- ✓ Data Downloaded
- ✓ Data uploaded to remote networks
- ✓ Outbound Transfer Attempts

Improving the Analyst Experience

Streamline Offense management in new UI

1H 2020

Streamlined offense investigation

- Understand why an offense was created and its impact (rules contributed, assets involved, network affected) in half the time it takes today

Drill-down information available in 1 click

- Drill into asset details, threat intelligence, payload information and rule details
- Save and export investigation artifacts

The screenshot displays the IBM Security QRadar interface. At the top, there are tabs for 'Offenses by Magnitude', 'Offenses by Assignee', and 'Offenses by Type'. The main panel shows an offense titled 'Detected an Attempt to Dump the Container Token preceded by Container Creating Another Container cont...'. Below this, a 'Search results' section is visible, showing a query builder and a table of results. The table has columns for 'qidname_qid', 'sourceip', and 'username'. The results show several 'API request successful' events from source IP 169.254.3.6, and one 'API request failure' event from source IP 169.254.2.8. On the right side, there are several floating panels: 'Detected an Attempt to Dump the Container Token' (Enabled), 'API request successful' (Low Magnitude), 'Event Overview' (Category, Source IP, Destination IP, Log Source, Log Source Time, Protocol), 'Magnitude' (Relevance, Severity, Credibility), 'Payload', and 'Source and destination information' (Source IP).

qidname_qid	sourceip	username
API request successful	INT 169.254.3.6	admin
API request successful	INT 169.254.3.6	admin
API request successful	INT 169.254.3.6	Resident
API request successful	INT 169.254.3.6	Resident
API request failure	INT 169.254.2.8	admin

Dashboarding

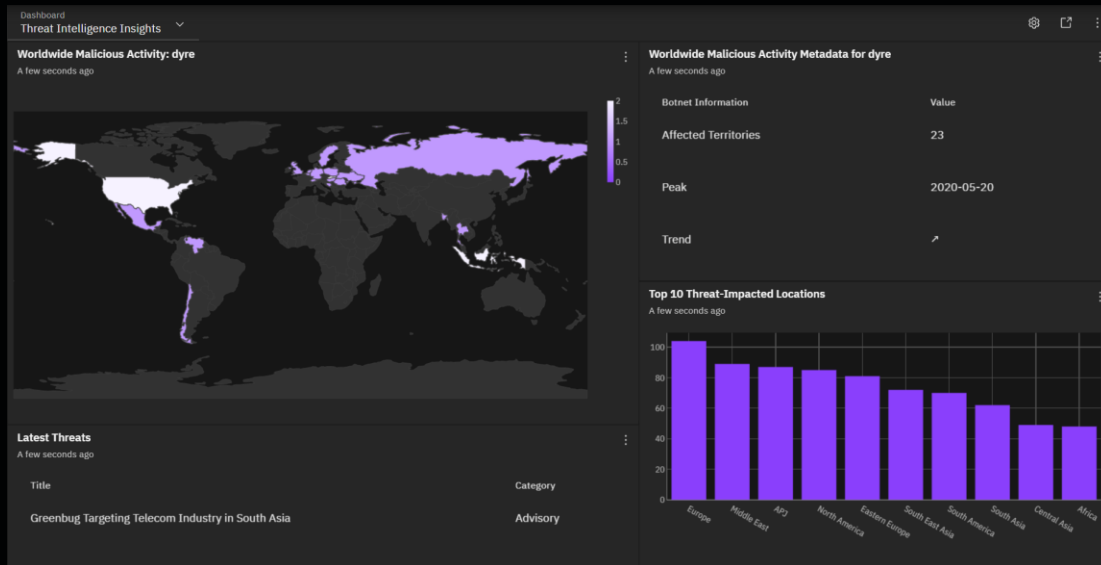
Q4 2019 – 2H 2020

Workflow support with drill down and sharing

- New 'dark mode'
- Drill down from dashboard widgets into QRadar workflows
- Easily share dashboards between users, teams and organizations
- New dashboarding chart types

Greater insights into the environment

- Access Assets and Offenses from Pulse
- Support for all available APIs to enable greater customization of dashboard insights



Increasing visibility and use cases

QRadar Analytics and Response Strategy



Let's look into Cloud

“Over 80% of organizations will use multiple clouds”

1. Continuously collect event and network connection data in real time from cloud to provide continuous end to end visibility
2. Detect threats and malicious behaviors
3. Uncover new and irregular communication patterns and entities



Cloud Security

Q4 2019 – Q2 2020

Just Released

- Microsoft Security Graph API alerts
- IBM Cloud Identity
- Microsoft Cloud Application Security
- Azure Security Center
- Amazon Windows Native Logs
- Google Pub/Sub

Coming Soon

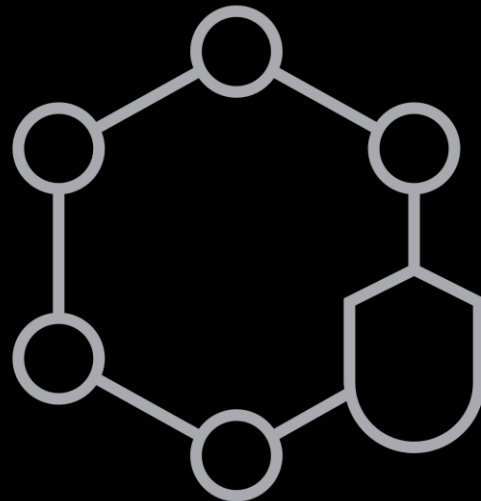
- Azure Windows Native Logs
- Trusteer Fraudulent login detection
- Generic REST API Connector



Let's look into Network

“98% of threats traverse the network”

1. Continuously collect and monitoring network connection meta data in real time, both on premise and in the cloud
2. Detect threats and malicious behaviors
3. Uncover new and irregular communication patterns and entities



Deeper insight into network traffic

2H 2019

New inspectors for greater insight into flow

- New file hashes to correlate against threat intel (SHA256, SHA1, MD5)
- Greater visibility into x.509 certificate attributes, including version, issuer, public key algorithm, etc
- Remote sessions, including RDP and Berkeley r-commands
- JA3 and JA3S fingerprints for insight into applications and systems involved in encrypted sessions

Greater support for cloud environments

- Ingest network data for analysis via AWS VPC Mirroring and Azure vTAP
- VXLAN support to for better domain management
- Software deployment of QNI in cloud environments

Network Traffic Analytics

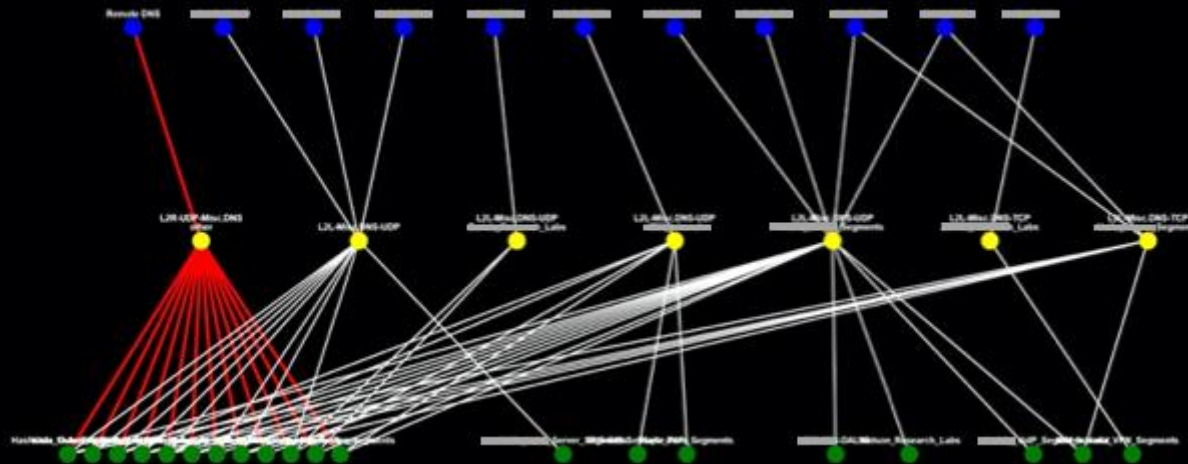
Q4 2020

Dynamically baseline and analyze your network

- Understand what's on your network, and what's normal on your network
- Leverage anomaly detection and real-time visualizations and alerting to detect deviations
- Continuously monitor assets for abnormal changes

Detect threats that are hard to find

- Identify beaconing and C2 activity to detect attackers who already have a foothold
- Detect staging and low & slow data exfiltration
- Detect compromised devices based on behavioral deviations, applications and communication patterns



Let's look into Endpoint

- Monitor and collect telemetry data from endpoints
- Detect threats and anomalous behaviors
- Support threat hunting and investigation activities



Pre-built content to detect threats

Q2-Q4 2020

Endpoint / Servers

- New use cases to detect execution, persistence, evasion and discovery tactics
- New integration support for Sysmon v10

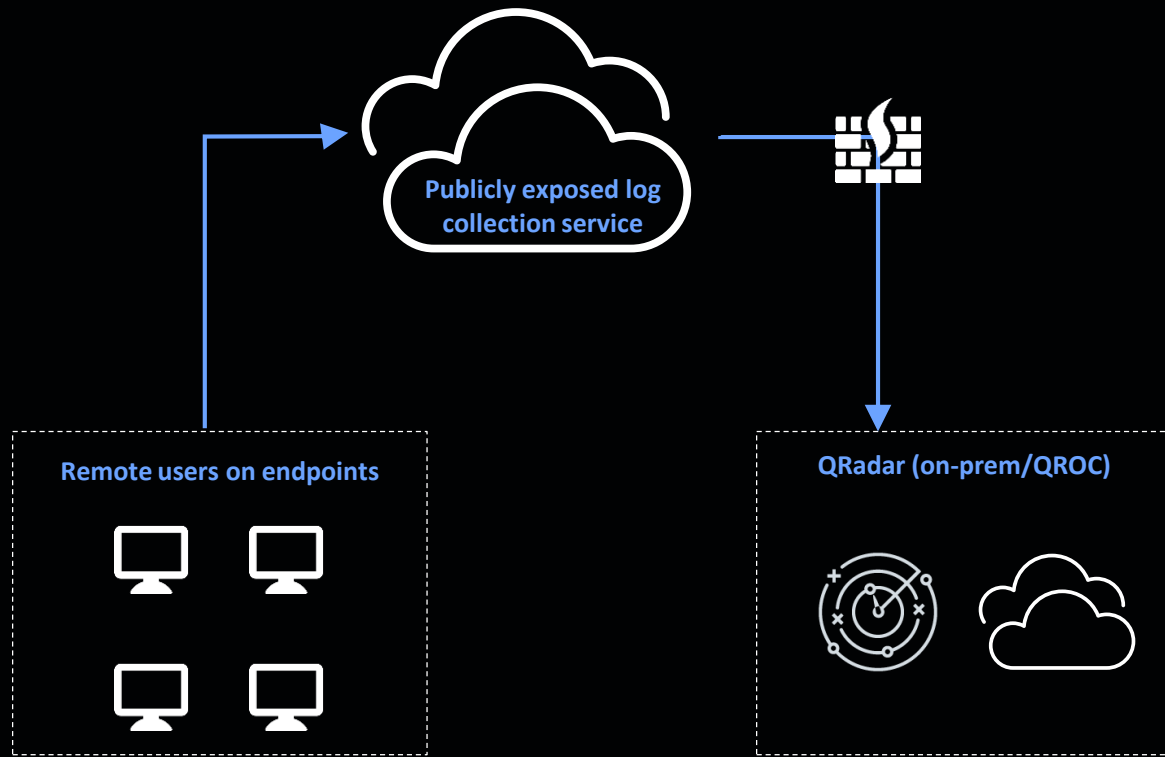
Containers

- Monitor and detect threats to modernized business applications
- New integrations with OSQuery and Kubernetes
- SysFlow Integration



Endpoint visibility for remote workforce use cases

2H 2020



- Rapid and simple insight into endpoint activity
- Visibility with just an internet connection; no VPN needed
- Easily deployed, auto registering agents
- Endpoint threat detection use cases for malware, credential harvesting, DNS threats

Let's look into Users

1. Utilize rules and models to identify out of normal or malicious behaviors that represent risk to organization
2. Continuously aggregate account behaviors over endpoints, network, cloud, apps etc. to identify highest risks
3. Accelerate investigations highlighting key behaviors, actions, and underlying evidence
4. Integrate seamlessly with analyst workflow



User Behavior Analytics Recap

Enable Customizable ML Modeling

- Exposes the powerful SPARK pipelines used in UBA and DNS so users can customize ML analytics without being data scientists
- Apply custom behavior models based on AQL queries

Support New Use Cases

- Abnormal data use indicating potential exfiltration via print, cloud, removable media
- Abnormal browsing, including to religious, government or education sites

Improve ML Performance

- Increase the number of supported users by 15x without adding extra load to the system

The image displays the 'Machine Learning Settings' interface. The top section, 'User Models', shows a list of models with columns for Name, Enabled status, and a three-dot menu. Models listed include Access Activity, Activity Distribution, Aggregated Activity, Authentication Activity, Data Downloaded, Data Uploaded, Defined Peer Group, Learned Peer Group, Outbound Transfer Attempts, Risk Posture, and Suspicious Activity. A 'Create Model' button is visible in the top right.

The 'Create Model' dialog is open, showing the 'Model Definition' tab. It prompts the user to 'Define a new model by choosing a template or by creating your own custom AQL query.' A dropdown menu shows 'Office 365 file activity (create, read, update, delete)'. Below this, the 'Custom AQL query' section explains the query structure and provides a sample query: `LOGSOURCEYPENAME(devicetype) = 'Microsoft Office 365' AND QIDNAME(qid) ILIKE '%File%'`. The 'Property' is set to 'eventcount' and the 'Function' is set to 'SUM'. A 'Validate Query' button is present. The 'Summary' section states: 'This models the SUM of the field eventcount for users each hour. It analyzes only data that matches LOGSOURCEYPENAME(devicetype) = 'Microsoft Office 365' AND QIDNAME(qid) ILIKE '%File%'.' The dialog has 'Cancel' and 'Next' buttons at the bottom.

User Behavior Analytics enhancements

Q1 – Q4 2020

Support for multi-tenanted and multi-domain deployments

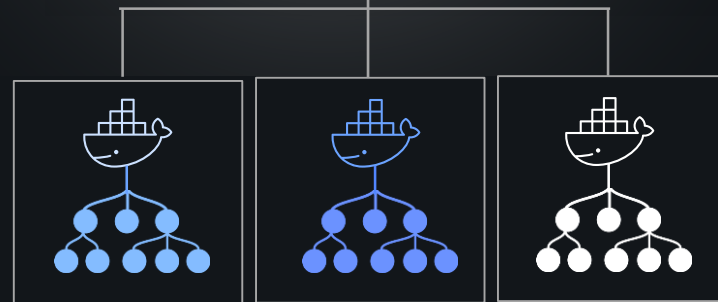
- Enable a segregated instance of UBA per tenant to maintain data privacy
- Support multi-domain awareness and geo-segregation

New use cases for greater insights

- More flexible peer grouping to better understand normal vs anomalous activity
- New asset analytics to bring evolve UBA into UEBA

UI Refresh

- New 'IBM Security Carbon dark theme'
- Streamlined insights
- Integration with new QRadar UI and CP4S



Let's look into Investigations and Threat Hunting

1. Easily access all telemetry data where ever it is (SIEM, EDR, Data Lake, Cloud)
2. Common query language
3. Easily pivot, filter and apply analytics to results to identify anomalies and root cause



Unified Search across multiple data sources

'Virtual data lake' with Data Explorer

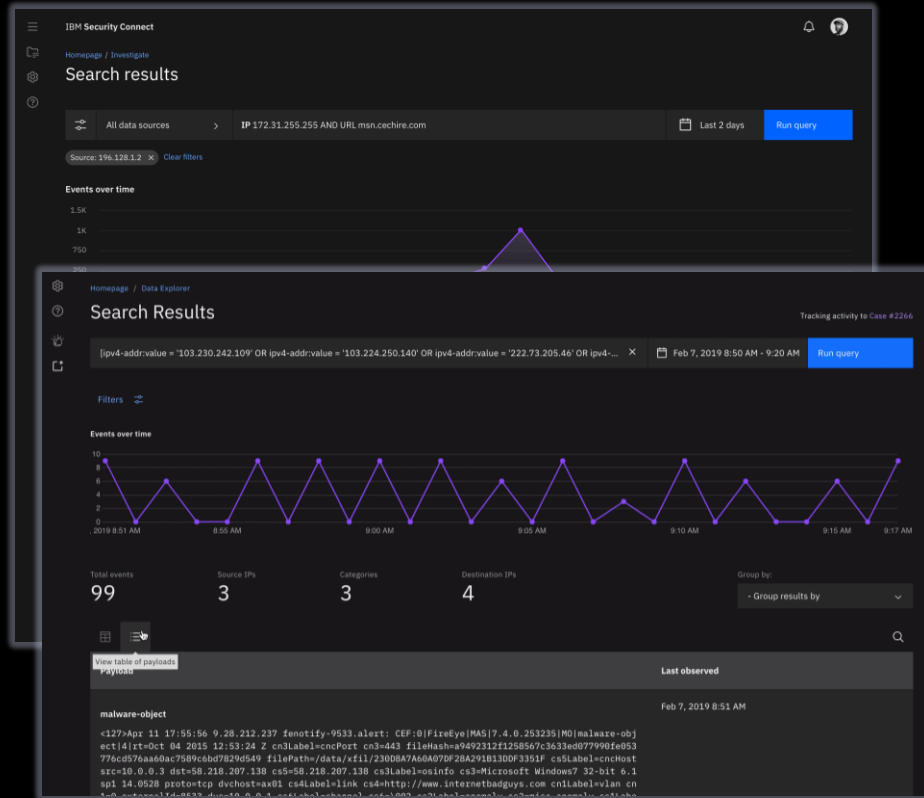
- Leverage data from existing security investments
- Gain complete visibility across disparate security data sources (SIEM, EDR, AV, etc.)

Single UI to search all security data

- Selectively query multiple data sources
- Results can be viewed in table or raw payload
- Easy pivots, group-bys, and quick filters
- Side panel enrichments to provide additional context for data, assets, hashes, etc.

Analytics and Threat Hunting

- Abnormal value identification
- Notebook integration



Let's look into Automated investigations

1. Is this important (high/low)
2. What MITRE tactics and technique have been found
Data mining outside of offence
3. What else going on is this related to
4. Are any high value users or assets involved
5. What malware family threat actors might be the root cause



QRadar Advisor with Watson

Enhanced Investigation Outcome Prediction

- New analytics to improve false positive identification
- Investigation outcomes prediction and recommended next steps

Transparent Investigation and 3rd party Threat Intelligence

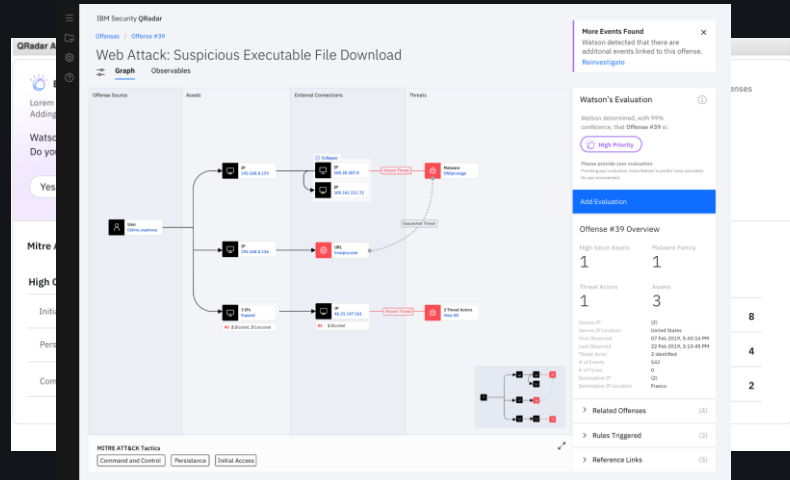
- Utilize existing SOC threat intel feeds in investigations
- Improved attack chain and business context analysis

UI Refresh

- New 'IBM Security Carbon dark theme'
- Integration with new QRadar UI and CP4S

Show users HOW prioritization and root cause was determined

Quickly view all entity status, assets, users, services etc.

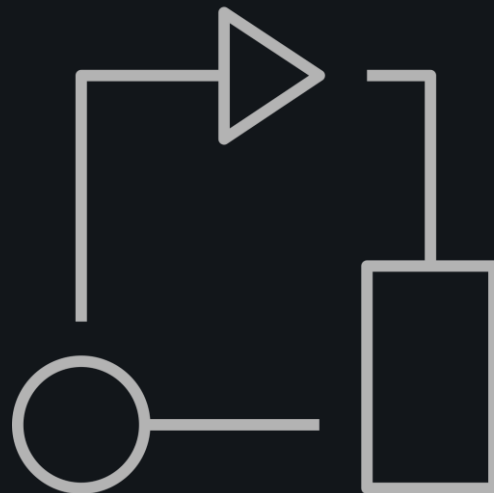


Drill down to underlying evidence and supporting intel and documentation

Filter view by Mitre ATT&CK phase for kill chain diagnosis

Let's look into Response

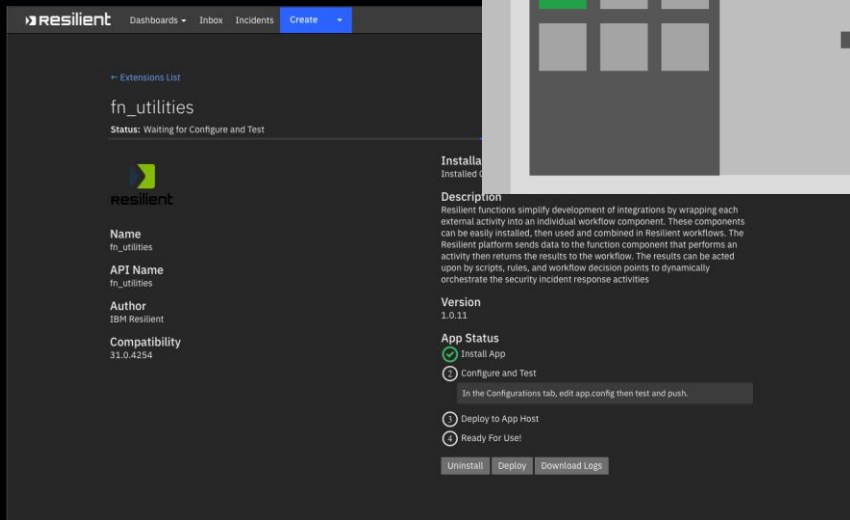
1. Consistency and robust response
2. Act faster with automation
3. Stay compliant
4. Measure and improve



Streamlining and acceleration Automation and Response

Playbook Designer – Q4

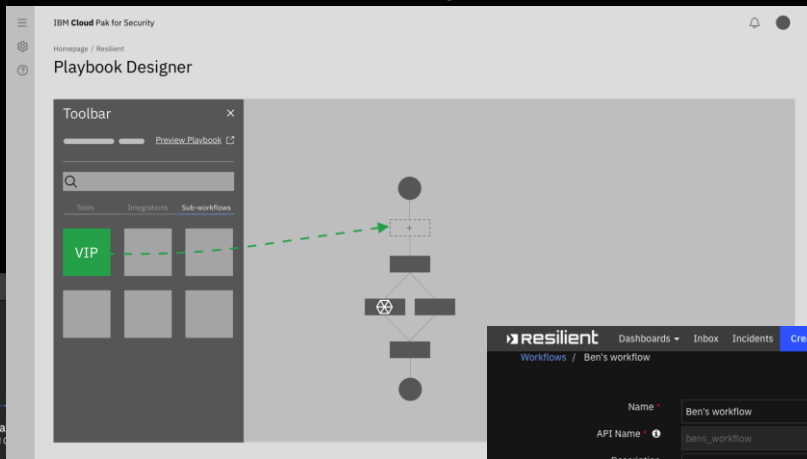
Easy App Install (Q2)



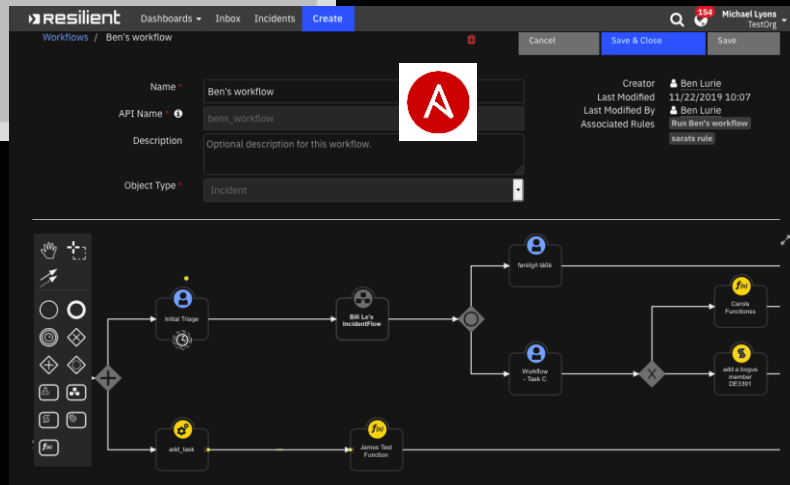
The screenshot shows the Resilient dashboard with the 'fn_utilities' extension installed. The 'Create' button is highlighted in the top navigation bar. The extension details include:

- Name:** fn_utilities
- API Name:** fn_utilities
- Author:** IBM Resilient
- Compatibility:** 31.0.4254

The 'App Status' section shows the app is installed and ready for use, with buttons for 'Uninstall', 'Deploy', and 'Download Logs'.



Deep Ansible Integration – Q4



Improving the Admin Experience

Use Case Manager

Q4 2019 – 1H 2020

Visualize coverage across the MITRE ATT&CK framework

- View your ability to detect tactics and techniques
- Use insights to prioritize the rollout of new use cases and apps
- Get tips on what apps and data sources based on security posture
- New UI Refresh

The screenshot displays the IBM QRadar Use Case Manager interface. A sidebar menu on the left includes options: Main menu, Rules Explorer (selected), Tuning Home, Active Rules, CRE Report, Network Hierarchy, and Host Definitions. The main content area shows the 'Rules Explorer' section with a filter set to 'Rule or Building Block(BB): Rule' and a group of 'Threats'. Below this, a table lists 175 rules, all of which are 'Asset Reconciliation Exclusion' custom rules. The table columns include Rule name, Group, Rule category, Type, Origin, Rule enabled status, Response, Creation date, and Modification date.

Rule name (175)	Group	Rule category	Type	Origin	Rule enabled	Response	Creation date	Modification date
AssetExclusion: Exclude DNS Name By IP	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude DNS Name By MAC Address	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude DNS Name By NetBIOS Name	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude IP By DNS Name	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude IP By MAC Address	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude IP By NetBIOS Name	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude MAC Address By DNS Name	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude MAC Address By IP	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude MAC Address By NetBIOS Name	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019
AssetExclusion: Exclude NetBIOS Name By DNS Name	Asset Reconciliation Exclusion	Custom Rule	EVENT	SYSTEM	On	Add to a Reference Set	01/06/2014	12/05/2019

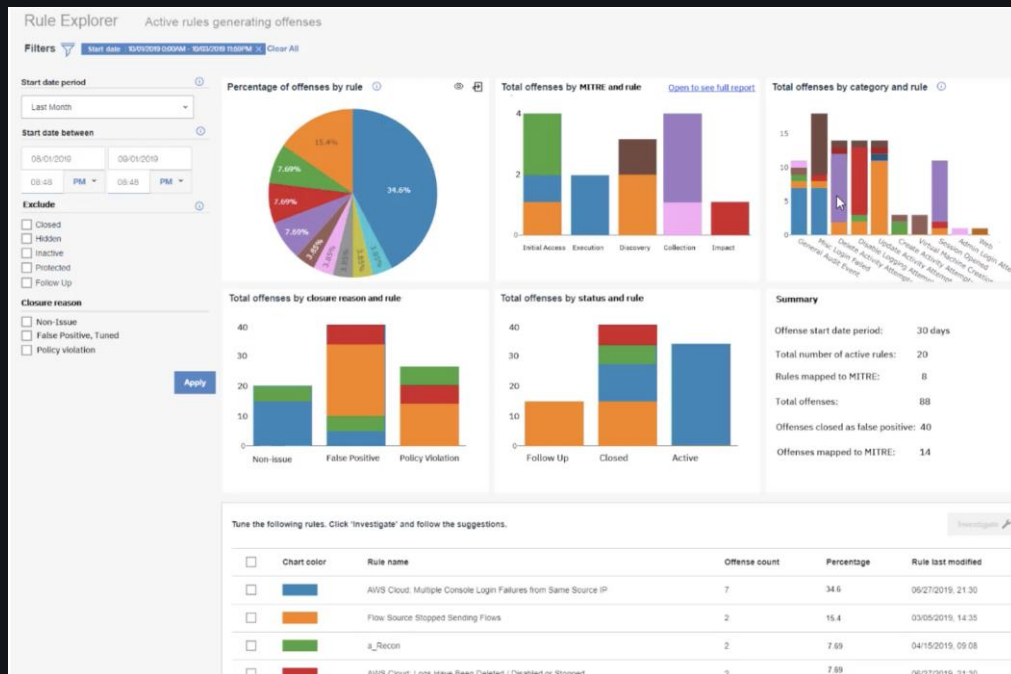
Use Case Manager

1H 2020

New Offense insights by MITRE ATT&CK stage, category and use cases

Gain new insight into offenses

- Add MITRE context better understand your ability to detect threats
- Enhance insights to become content-aware and enable filtering by platform
- Drill down into coverage to see installed and uninstalled use cases



More easily and securely ingest new data sources

Q4 2019 – Q1 2020

Easily onboard structured data sources

- Intuitive UI to enable users configure ingestion and parsing for structured data in Name-Value-Pair (ie. Value Delimiter) or Generic-List format (ex. CSV) format
- Augment support from today, which includes JSON, LEEF, CEF

Easier management of lightweight, one-way log collection

- Disconnected log collection enables uni-directional communication, ideal for highly secure environments and MSSP tenants
- New protocol and DSM support on continuous delivery

Configuration

Property Autodetection Configuration

Enable Property Autodetection
Automatically generates new properties to capture all fields that are present in the events that are received by this Log Source Type. Newly detected properties appear in the Properties tab. ☒

Property Detection Format
Select the structured data format for this Log Source Type's events. **NAME VALUE PAIR**

Delimiter in Name Value Pairs
The delimiter used between each Name and Value

The delimiter used between each Name Value Pair

Enable Properties for use in Rules and Search Indexing
Newly detected properties are made available for use in rules and search indexes. This setting can negatively impact event pipeline performance. You can toggle this setting per property in the Properties tab at any time. ☐

Expression

Expression Type: **NAME VALUE PAIR**

Expression: **(userFirst) (userSecond)**

Value Delimiter: **=**

Delimiter: **|**

Edit

Expression

Expression Type: **GENERIC LIST**

Expression: **(\$2) (\$3)**

Delimiter: **,**

Edit

New support for cloud and multi-tenanted apps

Q1 2020

Run apps in a multi-tenanted environments

- Extend security profiles and data segregation policies to apps
- Centrally manage apps for multiple domains and tenants

More easily manage and monitor the health of apps

- See all apps and content by tenant in one place
- Monitor app health and identify any errors
- Easily start, stop and delete apps as needed

Deploy elastically scalable apps as SaaS

- New Cloud App platform unlocks the power of apps for QRadar on Cloud customers
- Fully managed app infrastructure deploys in just a few click

The screenshot displays the IBM QRadar Assistant web interface. The top navigation bar includes links for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Incident Response (Alpha), and Pre-Validation. The main content area is titled 'Installed Applications' and features a search bar and filter options (Status: All, Failed to Install, Error / Stopped, Running). Below the filters are three tables: 'Installed Applications', 'Installed Content', and 'Custom Applications'. The 'Installed Applications' table lists two items: 'IBM Offender Pre-Validation App' and 'App Authorization Manager'. The 'Installed Content' table lists three items: 'IBM QRadar Content Extension for Microsoft Windows Custom Properties', 'IBM Offender Custom Properties for Check Point', and 'IBM QRadar Custom Properties for Carbon Black Protection'. The 'Custom Applications' table lists one item: 'QRadar Assistant'. An 'Application Details Summary' modal is open, showing details for 'QRadar Pulse - QRadar v7.3.0+'. The modal includes a 'Manage' tab and a 'Details' tab. The 'Details' tab shows the following information: ID: 1053, Name: Pulse - Threat Globe, Version: 1.1.3, Memory: 200 MB, Status: Running. At the bottom of the modal are buttons for 'Cancel', 'Stop', and 'Start'.

ID	Name	Status	Version	Memory	Installed By	Install Date	Options
321	IBM Offender Pre-Validation App	Running	1.0.3	400 MB	admin	Jul 03, 2019	...
2	App Authorization Manager	Running	1.0.13	200 MB	configservice	Aug 26, 2018	...

ID	Name	Status	Version	Memory	Installed By	Install Date	Options
323	IBM QRadar Content Extension for Microsoft Windows Custom Properties	Running	1.0.4	2.5 MB	admin	Jul 03, 2019	...
325	IBM Offender Custom Properties for Check Point	Running	1.0.1	2.5 MB	admin	Jul 03, 2019	...
322	IBM QRadar Custom Properties for Carbon Black Protection	Running	1.0.1	2.5 MB	admin	Jul 03, 2019	...

ID	Name	Status	Version
...	QRadar Assistant	Running	2.3.0

Application Details Summary

QRadar Pulse - QRadar v7.3.0+

By IBM QRadar
IBM Validated
6735 550 MB Required

Manage Details

Pulse - Threat Globe

ID: 1053
Name: Pulse - Threat Globe
Version: 1.1.3
Memory: 200 MB
Status: Running

> pulse_full_name

Cancel Stop Start

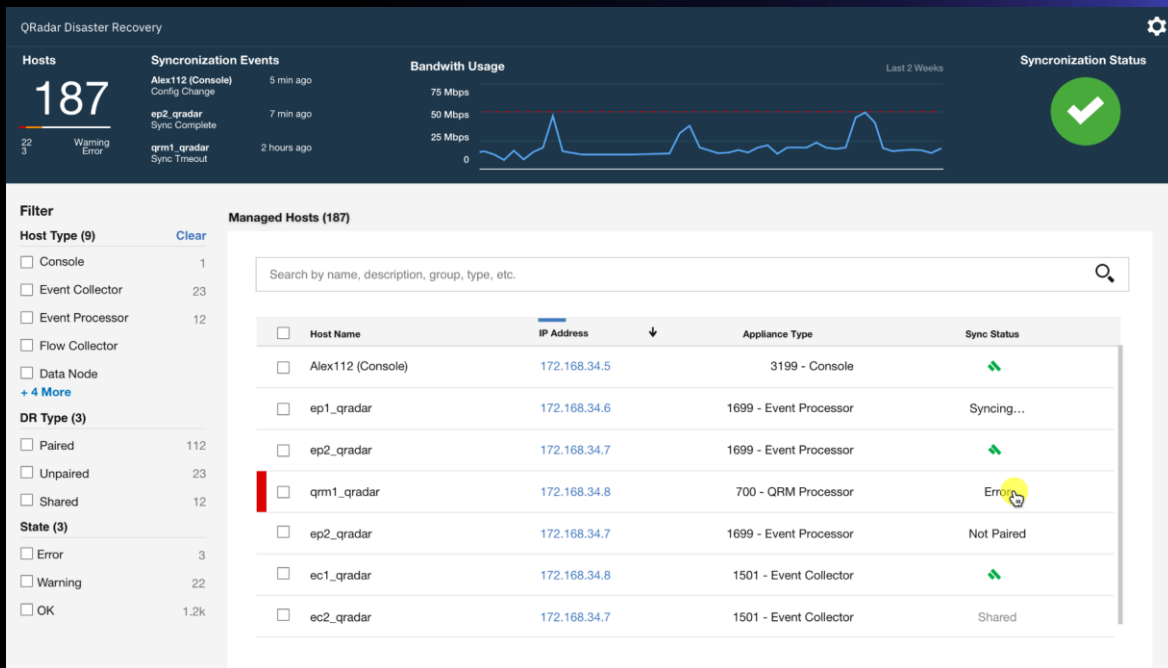
New Enterprise-class Disaster Recovery

Q2 – Q4 2020

Simplified streamlined setup, hot-warm standby

Greater enterprise DR support

- Robust, easy to setup Disaster Recovery with less manual configuration
- Cross datacenter support with 'warm' standby systems
- Automated data and configuration synchronization
- Re-sync of data and collection re-homing on 'fail back'

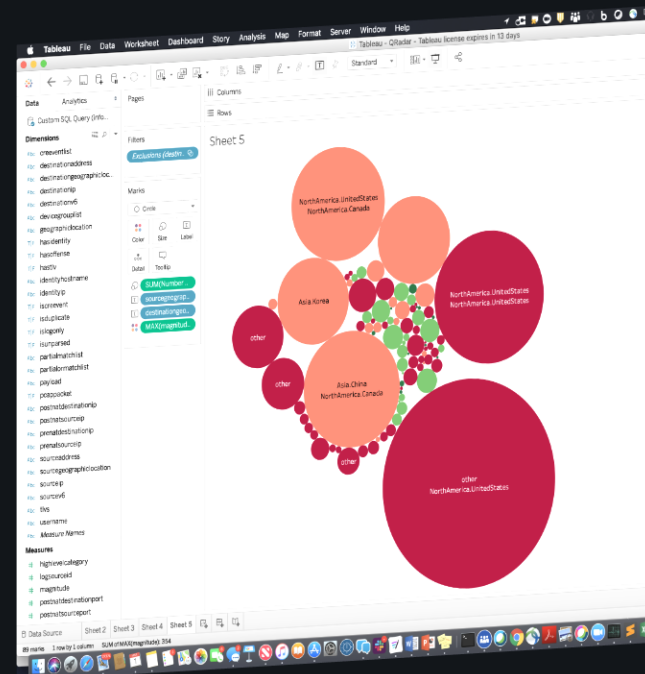


Q2 2020

Mass storage, search and analytics delivered from the cloud for QRoC and On-Prem

Open, Scalable Cloud Data Lake

- Data backup/archive to industry standard S3 storage platforms
- AQL & SQL based query with full ODBC, JDBC support
- Open Big Data format (Apache Parquet) for additional analytics and reporting platforms



By connecting data and augmenting existing investments, SOCs can gain:



Timely, relevant, and actionable threat intelligence



The ability to detect and respond to threats in one place



The ability to check against indicators that aren't stored in their SIEM



A solution that seamlessly works with all of their current tools and products



THANK YOU

FOLLOW US ON:



ibm.com/security



securityintelligence.com



ibm.com/security/community



xforce.ibmcloud.com



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



youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. 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.