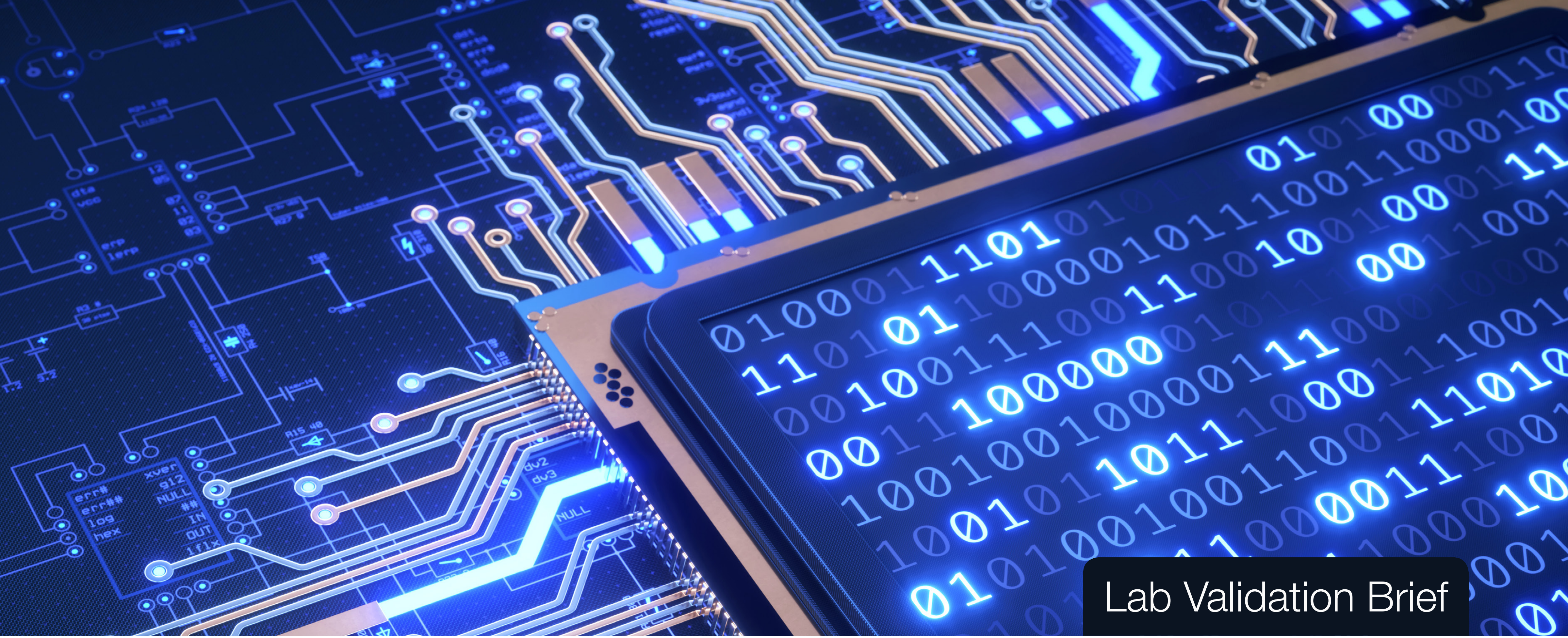


Lab Validation Brief

IBM QRadar 7.3.1 with UBA 3.0

Increasing accuracy. Reducing time to detect.

By Chris Kissel, *Director of Research, IDC Cybersecurity AIRO Team*

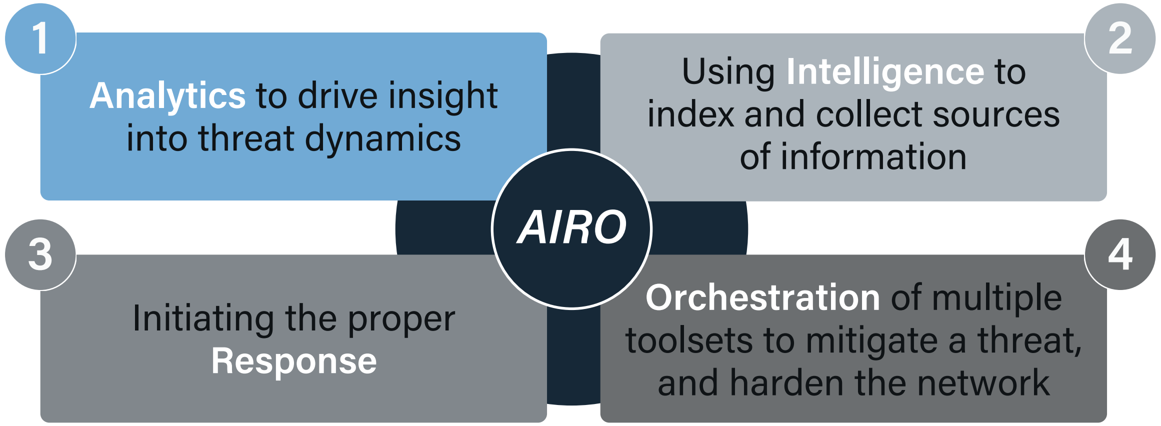
Sponsored by IBM | March 2019

IDC
ANALYZE THE FUTURE

Executive Summary

Validation Brief

IDC validated key features/functionality of IBM QRadar with User Behavior Analytics (UBA) App 3.0 and witnessed platform, detection and investigation features providing security analysts force multipliers for detection and response.


1
Analytics to drive insight into threat dynamics
2
Using **Intelligence** to index and collect sources of information
AIRO
3
Initiating the proper **Response**
4
Orchestration of multiple toolsets to mitigate a threat, and harden the network

Test scenarios:

1. Single, open platform

- » Data integration
- » Data management and scalability
- » Platform extensibility

2. Advanced detection using UBA

- » Instrumenting user activity
- » Applying machine learning
- » Peer group analysis

3. Accelerate investigation

- » Analyst output dashboards & user lists
- » QRadar Advisor with Watson insights
- » Create and refine alerts in such a way that false positives are greatly diminished

IDC Opinion

IDC can validate that IBM QRadar with UBA App is an effective platform in the following areas: threat detection/alert creation, consolidation of security operation processes, open integration of relevant technologies for greater security visibility, change to performance monitoring and workflow, in addition QRadar can initiate the response process. Perhaps as importantly, native to the QRadar platform are analytics that enrich data, harmonize event timelines, and prioritize alerts. The superset of the capabilities is called "offense chaining," and this process greatly reduces false positives and refines the SOC investigatory process.

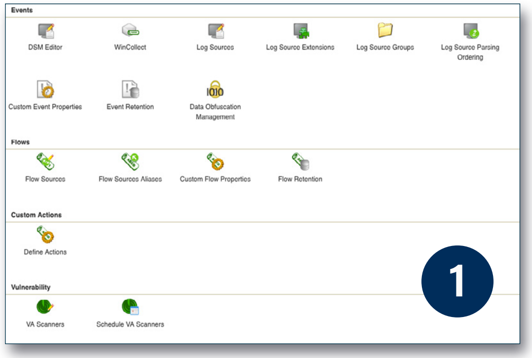
Scenario 1: Single, Open Platform

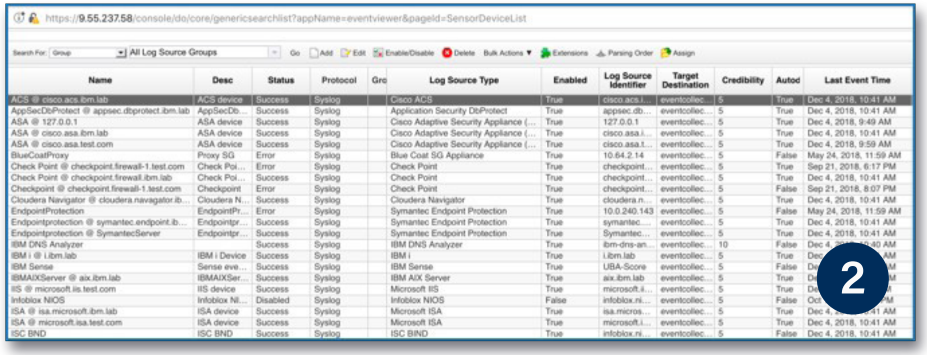
Objective: Demonstrate the purpose and "ease-of-use" of an open and integrated platform

Scenario	**#1 Single, Open Platform**
Validated Features	▪ Data intake (DSM) from endpoint, network, cloud, IAM/AD, application logs ▪ Data archiving and searching ▪ Installation of UBA App via App exchange ▪ Installation of "Advisor with Watson" via App Exchange
Key Findings	▪ Easy to integrate ▪ Obtain enterprise wide visibility ▪ Integrated business context ▪ Time to value ▪ Get more out of investments ("collect once, reuse many times")
Why This Matters	▪ A single platform has many significant advantages: 1. Centralized visibility and data management over multiple security data sources. security data sources. 2. The ability to correlate security data to reduce multiple security alerts, and reduce false positives. 3. A central point for automation and incident response. » Security teams obtain a central view of assets including vulnerabilities, business context and activities. » Security operations grow and need to add functionality such as network traffic analysis, vulnerability management, and user behavior analytics (UBA) to the core system.

Cybersecurity AIRO

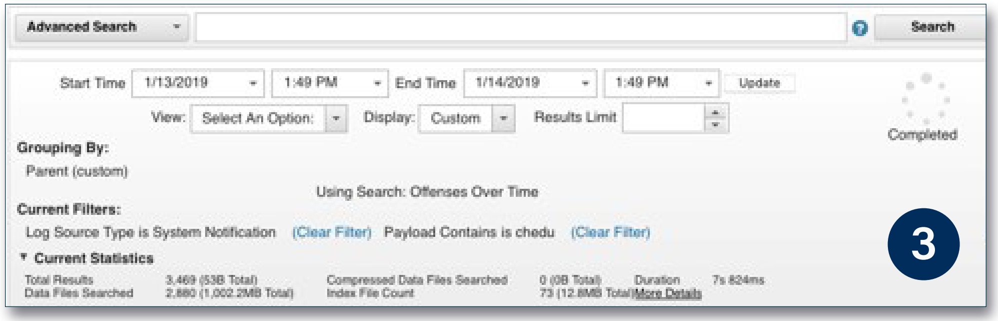
Objective: Additional attestation of key aspects of a single, open platform





https://9.55.237.58/console/do/core/genericsearchlist?appName=eventviewer&pageId=SensorDeviceList

Name	Desc	Status	Protocol	Gro	Log Source Type	Enabled	Log Source Identifier	Target Destination	Credibility	Autod	Last Event Time
ACS @ cisco.acs.ibm.lab	ACS device	Success	Syslog		Cisco ACS	True	cisco.acs.i...	eventcollec...	5	True	Dec 4, 2018, 10:41 AM
AppSecDbProtect @ appsec.dbprotect.ibm.lab	AppSecDb...	Success	Syslog		Application Security DbProtect	True	appsec.db...	eventcollec...	5	True	Dec 4, 2018, 10:41 AM
ASA @ 127.0.0.1	ASA device	Success	Syslog		Cisco Adaptive Security Appliance (...	True	127.0.0.1	eventcollec...	5	True	Dec 4, 2018, 9:49 AM
ASA @ cisco.asa.ibm.lab	ASA device	Success	Syslog		Cisco Adaptive Security Appliance (...	True	cisco.asa.i...	eventcollec...	5	True	Dec 4, 2018, 10:41 AM
ASA @ cisco.asa.test.com	ASA device	Success	Syslog		Cisco Adaptive Security Appliance (...	True	cisco.asa.t...	eventcollec...	5	True	Dec 4, 2018, 9:59 AM
BlueCoatProxy	Proxy SG	Error	Syslog		Blue Coat SG Appliance	True	10.64.2.14	eventcollec...	5	False	May 24, 2018, 11:59 AM
Check Point @ checkpoint.firewall-1.test.com	Check Poi...	Error	Syslog		Check Point	True	checkpoint...	eventcollec...	5	True	Sep 21, 2018, 6:17 PM
Check Point @ checkpoint.firewall.ibm.lab	Check Poi...	Success	Syslog		Check Point	True	checkpoint...	eventcollec...	5	True	Dec 4, 2018, 10:41 AM
Checkpoint @ checkpoint.firewall-1.test.com	Checkpoint	Error	Syslog		Check Point	True	checkpoint...	eventcollec...	5	False	Sep 21, 2018, 8:07 PM
Cloudera Navigator @ cloudera.navagator.ib...	Cloudera N...	Success	Syslog		Cloudera Navigator	True	cloudera.n...	eventcollec...	5	True	Dec 4, 2018, 10:41 AM
EndpointProtection	EndpointPr...	Error	Syslog		Symantec Endpoint Protection	True	10.0.240.143	eventcollec...	5	False	May 24, 2018, 11:59 AM
Endpointprotection @ symantec.endpoint.ib...	Endpointpr...	Success	Syslog		Symantec Endpoint Protection	True	symantec....	eventcollec...	5	True	Dec 4, 2018, 10:41 AM
Endpointprotection @ SymantecServer	Endpointpr...	Success	Syslog		Symantec Endpoint Protection	True	Symantec...	eventcollec...	5	True	Dec 4, 2018, 10:41 AM
IBM DNS Analyzer		Success	Syslog		IBM DNS Analyzer	True	ibm-dns-an...	eventcollec...	10	False	Dec 4, 20 [illegible] 40 AM
IBM i @ i.ibm.lab	IBM i Device	Success	Syslog		IBM i	True	i.ibm.lab	eventcollec...	5	True	Dec [illegible] AM
IBM Sense	Sense eve...	Success	Syslog		IBM Sense	True	UBA-Score	eventcollec...	5	False	De [illegible] M
IBMAIXServer @ aix.ibm.lab	IBMAIXSer...	Success	Syslog		IBM AIX Server	True	aix.ibm.lab	eventcollec...	5	True	De [illegible] M
IIS @ microsoft.iis.test.com	IIS device	Success	Syslog		Microsoft IIS	True	microsoft.i...	eventcollec...	5	True	De [illegible]
Infoblox NIOS	Infoblox NI...	Disabled	Syslog		Infoblox NIOS	False	infoblox.ni...	eventcollec...	5	False	Oct [illegible] PM
ISA @ isa.microsoft.ibm.lab	ISA device	Success	Syslog		Microsoft ISA	True	isa.micros...	eventcollec...	5	True	Dec 4, [illegible] 41 AM
ISA @ microsoft.isa.test.com	ISA device	Success	Syslog		Microsoft ISA	True	microsoft.i...	eventcollec...	5	True	Dec 4, 2018, 10:41 AM
ISC BND	ISC BND	Success	Syslog		ISC BIND	True	infoblox.ni...	eventcollec...	5	False	Dec 4, 2018, 10:41 AM



Start Time 1/13/2019 1:49 PM End Time 1/14/2019 1:49 PM

View: Select An Option: Display: Custom Results Limit

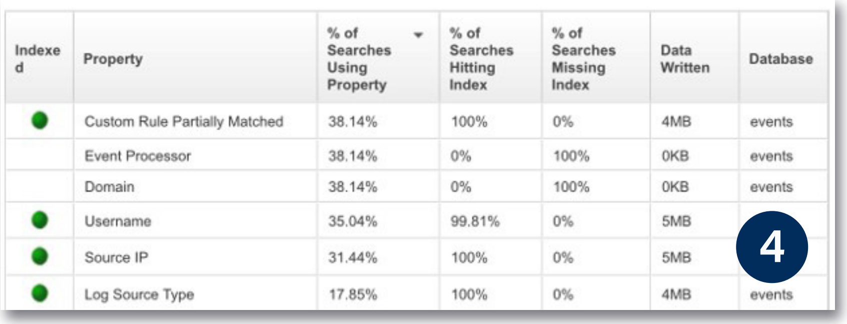
Grouping By:
Parent (custom)

Using Search: Offenses Over Time

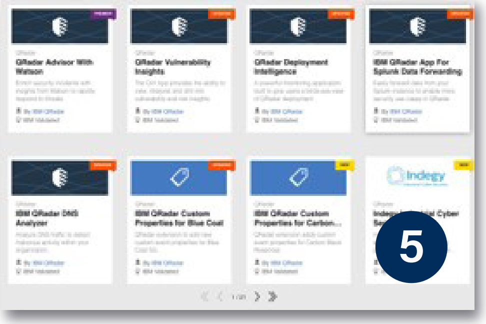
Current Filters:
Log Source Type is System Notification (Clear Filter) Payload Contains is chedu (Clear Filter)

▾ Current Statistics

```
Total Results        3,469 (53B Total)          Compressed Data Files Searched   0 (0B Total)      Duration   7s 824ms
Data Files Searched  2,880 (1,002.2MB Total)    Index File Count                 73 (12.8MB Total) More Details
```



Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	Custom Rule Partially Matched	38.14%	100%	0%	4MB	events
	Event Processor	38.14%	0%	100%	0KB	events
	Domain	38.14%	0%	100%	0KB	events
●	Username	35.04%	99.81%	0%	5MB	
●	Source IP	31.44%	100%	0%	5MB	
●	Log Source Type	17.85%	100%	0%	4MB	events


QRadar Advisor With Watson
QRadar Vulnerability Insights
QRadar Deployment Intelligence
IBM QRadar App For Splunk Data Forwarding
IBM QRadar DNS Analyzer
IBM QRadar Custom Properties for Blue Coat
IBM QRadar Custom Properties for Carbon...
Indegy
1 / 21
5

IDC Inference

1. Centralized IBM QRadar Admin console allows users to configure the system and integrate events, flows and vulnerability data from various data sources. Via the central admin, users can also add additional QRadar apps downloadable from QRadar App Exchange.

2. Log Source Admin: A log source can be any type of network appliance, operating system, database, or security product that generates events. Log sources can be created manually by an administrator or automatically discovered. Each log source contains a device support module (DSM). The DSM software contains the event patterns that are required to identify and parse events for a log source.

3. Users can search for specific events using the Basic or Advanced searching using AQL (Ariel Query Language). The AQL allows the user to build complex WHERE clauses that contain a combination of AND and OR conditions. Look up and include data from reference sets, tables and maps. Look up and include data, such as asset, user, property, and location, from the asset database in a query. Produce customized column headings. Concatenate two or more fields into a single result field. Queries can be saved and shared between users to enable collaboration and faster time to results.

4. Use Index Management to see statistics about how properties are searched and how indexes are used over time. Event and flow indexes will optimize searches. Admins can enable indexes on any event property.

5. IBM App Exchange offers more then 160 apps for download to an IBM QRadar deployment.

Validated – Cybersecurity AIRO

Objective #1 – Single, Open Platform

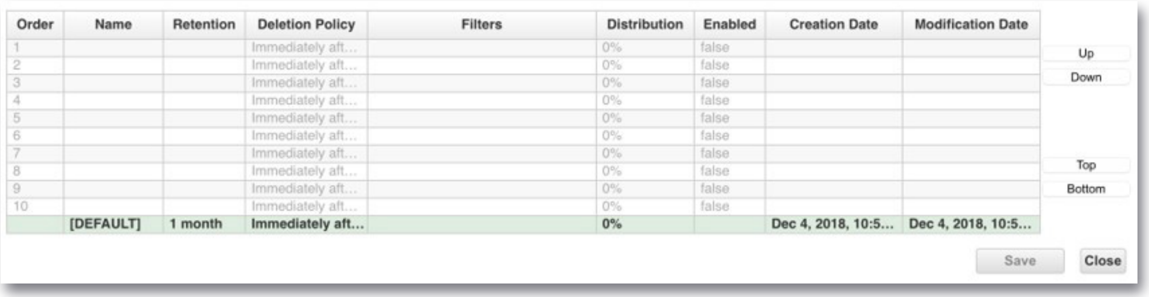
Feature/Validation Summary

IBM was able to demonstrate that IBM QRadar could ingest and identify multiple and disparate log sources (including proxy logs, sensor, and endpoint) for indexing and detection.

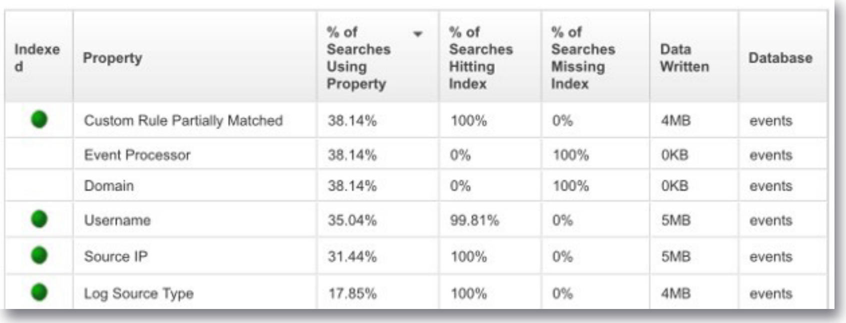
Validation Process

To validate, IBM QRadar executed the following tasks:

- Demonstrated current filter and quick filter.
- At the time of this writing IBM QRadar has support for over 600 different log sources.
- In testing, QRadar was able to take in proxy logs, and through its wizard was able to classify data.
- The retention bucket on the upper right hand side is useful because it enables security teams in various ways:
    - Reduce data overload and archiving costs using retention policies.
    - Retention buckets allow customization of event and flow storage. Multiple retention buckets are processed sequentially from top to bottom. Any events that do not match the retention buckets are automatically placed in the default retention bucket located at the bottom of the list.
    - Data collected can be obfuscated for PII or other privacy policies that may exist.
- An Asset View screen was shown. Importantly, it was able to show CVSS scores as a peer group and as individual assets.
- The Asset View included Vulnerabilities, Services, Windows Services, Packages, Properties, Risk Properties, and Products.
- Rules and Asset Views are correlated meaning that the exact impact of malware can be defined to specific assets.
- Search becomes a trenchant weapon. On the lower right hand side, QRadar demonstrates how searches originate.



Order	Name	Retention	Deletion Policy	Filters	Distribution	Enabled	Creation Date	Modification Date
1			Immediately aft...		0%	false		
2			Immediately aft...		0%	false		
3			Immediately aft...		0%	false		
4			Immediately aft...		0%	false		
5			Immediately aft...		0%	false		
6			Immediately aft...		0%	false		
7			Immediately aft...		0%	false		
8			Immediately aft...		0%	false		
9			Immediately aft...		0%	false		
10			Immediately aft...		0%	false		
	[DEFAULT]	1 month	Immediately aft...		0%		Dec 4, 2018, 10:5...	Dec 4, 2018, 10:5...



Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	Custom Rule Partially Matched	38.14%	100%	0%	4MB	events
	Event Processor	38.14%	0%	100%	0KB	events
	Domain	38.14%	0%	100%	0KB	events
●	Username	35.04%	99.81%	0%	5MB	events
●	Source IP	31.44%	100%	0%	5MB	events
●	Log Source Type	17.85%	100%	0%	4MB	events

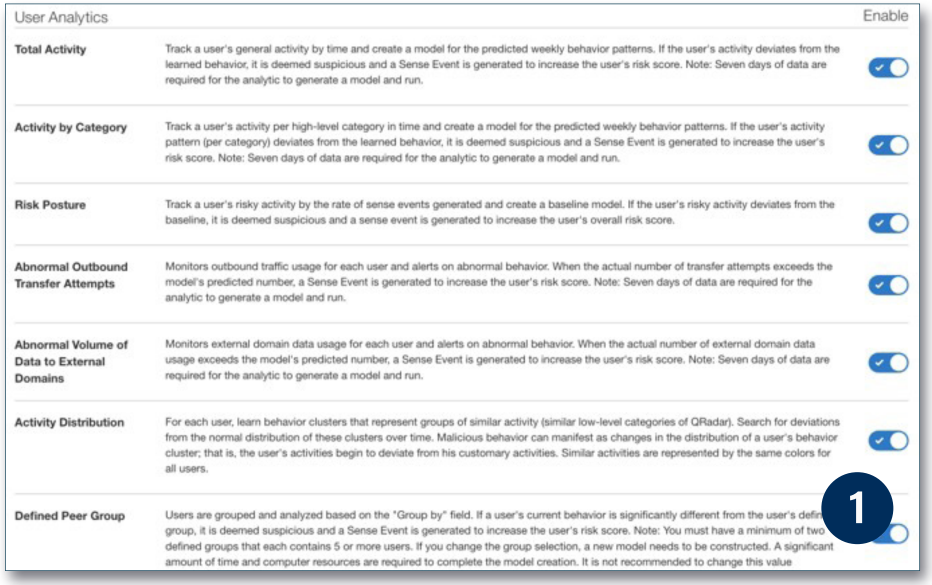
Scenario 2: Advanced Detection (UBA)

Objective: Determine if UBA features in IBM QRadar UBA 3.0 improve threat discovery

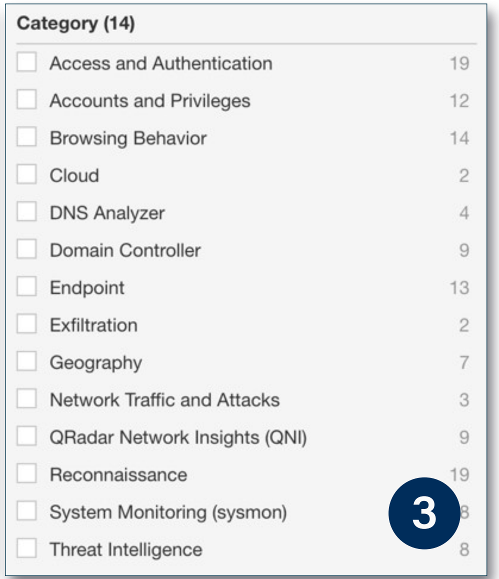
Scenario	**#2 Advanced Detection (UBA)**
Features to Be Tested	▪ Identify user activity ▪ Enable machine learning ▪ Calculate overall user risk score ▪ Build and compare against multiple watchlists
Key Findings	▪ Obtain new insights about a single user ▪ Surface unknown threats using behavioral monitoring ▪ Low operational overhead. Reduce efforts spent on data modeling or content creation (i.e., no need for "data scientist").
Why This Matters	▪ UBA can identify threats (malware) that have already by-passed the network perimeter and need to be acted upon. ▪ Insight about individual users or comparison to peer group activities is an important tool to combat insider threats. ▪ UBA prioritizes users by risk score and provides instant view. ▪ A single "user" has many different identity instances—over firewall logs, access to a cloud-based application, Net flows, etc. UBA aggregates these identities into a single user name. ▪ Machine learning alleviates costs of constantly tuning rules.

Cybersecurity AIRO

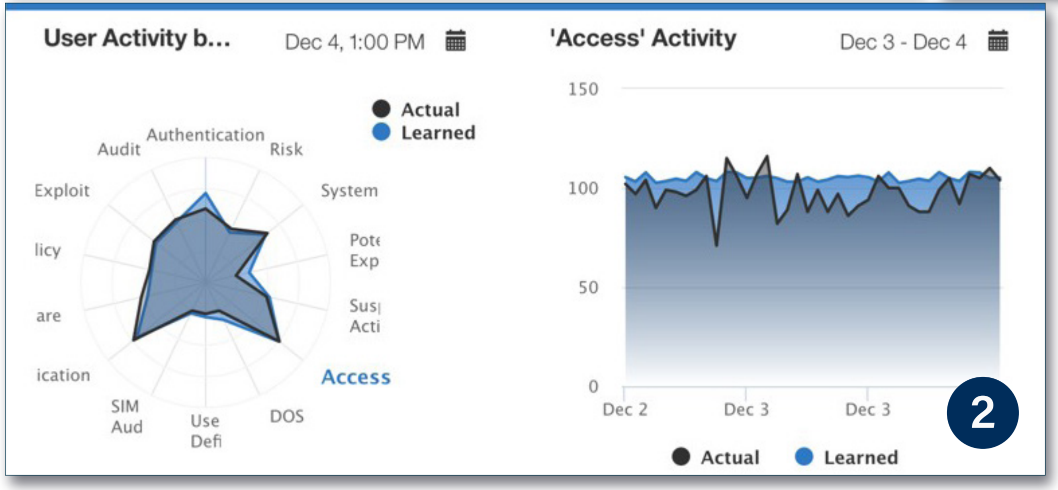
Objective: To see how IBM QRadar implements UBA for addition threat analytics insight and risk prioritization.



User Analytics		Enable
Total Activity	Track a user's general activity by time and create a model for the predicted weekly behavior patterns. If the user's activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.	✓
Activity by Category	Track a user's activity per high-level category in time and create a model for the predicted weekly behavior patterns. If the user's activity pattern (per category) deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.	✓
Risk Posture	Track a user's risky activity by the rate of sense events generated and create a baseline model. If the user's risky activity deviates from the baseline, it is deemed suspicious and a sense event is generated to increase the user's overall risk score.	✓
Abnormal Outbound Transfer Attempts	Monitors outbound traffic usage for each user and alerts on abnormal behavior. When the actual number of transfer attempts exceeds the model's predicted number, a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.	✓
Abnormal Volume of Data to External Domains	Monitors external domain data usage for each user and alerts on abnormal behavior. When the actual number of external domain data usage exceeds the model's predicted number, a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.	✓
Activity Distribution	For each user, learn behavior clusters that represent groups of similar activity (similar low-level categories of QRadar). Search for deviations from the normal distribution of these clusters over time. Malicious behavior can manifest as changes in the distribution of a user's behavior cluster; that is, the user's activities begin to deviate from his customary activities. Similar activities are represented by the same colors for all users.	✓
Defined Peer Group	Users are grouped and analyzed based on the "Group by" field. If a user's current behavior is significantly different from the user's defin group, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value	✓



Category (14)	
□ Access and Authentication	19
□ Accounts and Privileges	12
□ Browsing Behavior	14
□ Cloud	2
□ DNS Analyzer	4
□ Domain Controller	9
□ Endpoint	13
□ Exfiltration	2
□ Geography	7
□ Network Traffic and Attacks	3
□ QRadar Network Insights (QNI)	9
□ Reconnaissance	19
□ System Monitoring (sysmon)	8
□ Threat Intelligence	8



IDC Inference

1. Configured machine learning analytics to display the actual and expected (learned) amount of activity of users throughout the day.
2. The platform validated actual activity against "learned" activity. Also, visualized the actual and expected activity in the UBA view, by activity groups and time.
3. The IBM QRadar UBA app supports use cases based on rules for certain behavioral anomalies. These rules are used to generate data for the UBA app dashboard. Admins can view, filter and tune rules within the UBA app. 139 rules are grouped within these 14 different categories.

Validated – Cybersecurity AIRO

Objective #2 – Advanced Detection (UBA)

Feature/Validation Summary

QRadar does use UBA as an effective tool to monitor individual activity against statistical baselines, individual as well as peer group anomalous behavior, and overall risk scores. Via LDAP integration, the security team can look for infractions by user name. The platform is quickly able to discover outliers within similar business context.

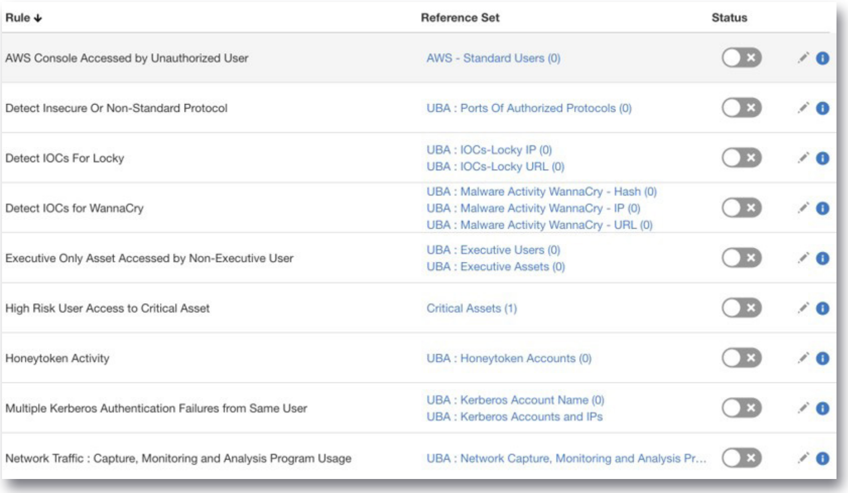
Validation Process

IDC wanted to see multiple vantage points: the type of threat, user names, and a visualization of risk. Additionally, the screen capture on the right shows the types of algorithms that can be deployed:

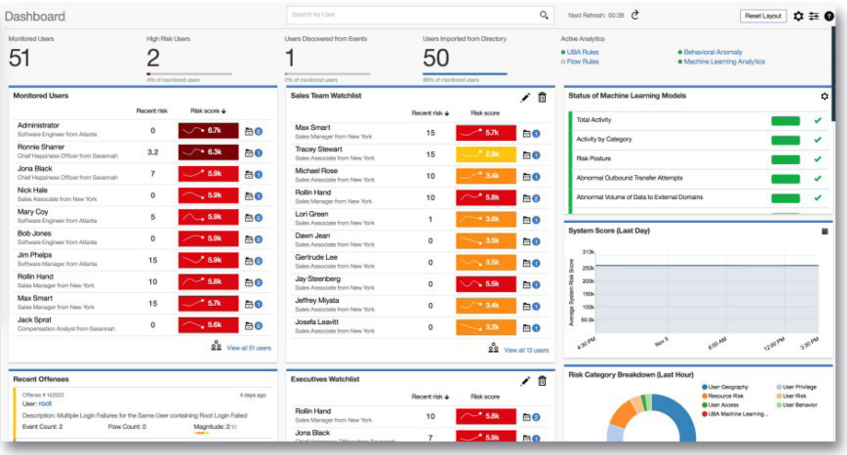
- In the lab demo, we saw quick situational awareness on provisioned and discovered users.
- QRadar could identify assets by user name.
- The UBA feature allowed admin to create watchlists and compare similar users.

To the lower right is a dashboard describing individual risk. Metrics include:

- Monitored Users: Displays the total number of users that the UBA app is actively monitoring.
- High Risk Users: Displays the number of users who are currently exceeding the risk score. The value for determining the risk score is set in the “Risk threshold to trigger offenses” in UBA Settings.
- Users Discovered from Events: Displays the number of users that are discovered from events, excluding imported users.
- Users Imported from Directory: Displays the number of users that were imported from reference tables.
- Active Analytics Status of the active rules content.
- Monitored Users: Displays the top 10 riskiest users by recent risk, risk score, watchlist icon
- System Score: Overall accumulated risk score for all users at a specified point in time.
- Status of Machine Learning Models: Status of the Machine Learning Analytics is visible if the Machine Learning app is installed.



Rule ↓	Reference Set	Status
AWS Console Accessed by Unauthorized User	AWS - Standard Users (0)	✕
Detect Insecure Or Non-Standard Protocol	UBA : Ports Of Authorized Protocols (0)	✕
Detect IOCs For Locky	UBA : IOCs-Locky IP (0) UBA : IOCs-Locky URL (0)	✕
Detect IOCs for WannaCry	UBA : Malware Activity WannaCry - Hash (0) UBA : Malware Activity WannaCry - IP (0) UBA : Malware Activity WannaCry - URL (0)	✕
Executive Only Asset Accessed by Non-Executive User	UBA : Executive Users (0) UBA : Executive Assets (0)	✕
High Risk User Access to Critical Asset	Critical Assets (1)	✕
Honeytoken Activity	UBA : Honeytoken Accounts (0)	✕
Multiple Kerberos Authentication Failures from Same User	UBA : Kerberos Account Name (0) UBA : Kerberos Accounts and IPs	✕
Network Traffic : Capture, Monitoring and Analysis Program Usage	UBA : Network Capture, Monitoring and Analysis Pr...	✕



Dashboard

Search for User

Next Refresh: 00:38

Reset Layout

Monitored Users	High Risk Users	Users Discovered from Events	Users Imported from Directory
51	2	1	50
	4% of monitored users	2% of monitored users	98% of monitored users

Active Analytics
- UBA Rules
- Flow Rules
- Behavioral Anomaly
- Machine Learning Analytics

Monitored Users

	Recent risk	Risk score ↓
Administrator Software Engineer from Atlanta	0	6.7k
Ronnie Sharrer Chief Happiness Officer from Savannah	3.2	6.3k
Jona Black Chief Happiness Officer from Savannah	7	5.9k
Nick Hale Sales Associate from New York	0	5.9k
Mary Coy Software Engineer from Atlanta	5	5.9k
Bob Jones Software Engineer from Atlanta	0	5.9k
Jim Phelps Software Manager from Atlanta	15	5.9k
Rollin Hand Sales Manager from New York	10	5.8k
Max Smart Sales Manager from New York	15	5.7k
Jack Sprat Compensation Analyst from Savannah	0	5.6k

View all 51 users

Sales Team Watchlist

	Recent risk ↓	Risk score
Max Smart Sales Manager from New York	15	5.7k
Tracey Stewart Sales Associate from New York	15	2.9k
Michael Rose Sales Associate from New York	10	3.4k
Rollin Hand Sales Manager from New York	10	5.8k
Lori Green Sales Associate from New York	1	3.6k
Dawn Jean Sales Associate from New York	0	3.5k
Gertrude Lee Sales Associate from New York	0	3.5k
Jay Steenberg Sales Associate from New York	0	5.5k
Jeffrey Miyata Sales Associate from New York	0	3.4k
Josefa Leavitt Sales Associate from New York	0	3.2k

View all 13 users

Status of Machine Learning Models
- Total Activity ✓
- Activity by Category ✓
- Risk Posture ✓
- Abnormal Outbound Transfer Attempts ✓
- Abnormal Volume of Data to External Domains ✓

System Score (Last Day)

Recent Offenses

Offense # 142523 — 4 days ago
User: root
Description: Multiple Login Failures for the Same User containing Root Login Failed
Event Count: 2 Flow Count: 0 Magnitude: 2/10

Executives Watchlist

	Recent risk ↓	Risk score
Rollin Hand Sales Manager from New York	10	5.8k
Jona Black	7	5.9k

Risk Category Breakdown (Last Hour)

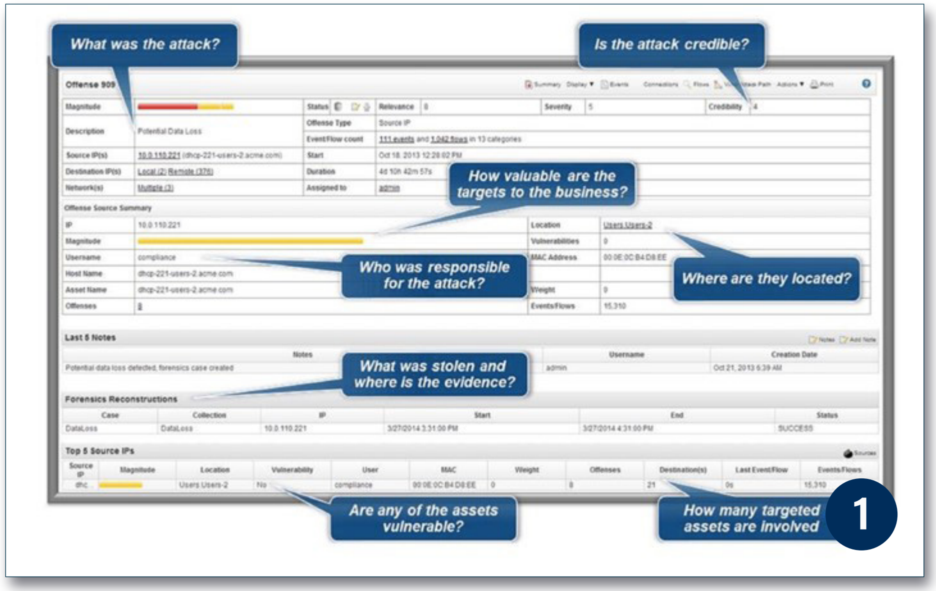
Scenario 3: Accelerate Investigation

Objective: Determine if IBM QRadar UBA 3.0 features act as force multiplier for security analysts

Scenario	**#3 Accelerate Investigation**
Features to Be Tested	▪ Individual user and timeline views ▪ Prioritized alert or offense views ▪ Investigate using IBM QRadar Advisor with Watson
Key Findings	▪ Reduced investigative efforts, time to investigate ▪ Demonstrated consistent depth in investigations ▪ Allowed the analyst to prepare an accurate response (avoid whack-a-mole game)
Why This Matters	▪ In a SOC, the threat investigations process is often very formal. The sub-processes include checking triage, threat intelligence, establishing identity, check for damage to memory, and investigate individual files. ▪ All of this has to be done while determining what the greatest risk to the network, users, and individual assets are. ▪ Understanding risk includes the importance of the machine infected, the veracity of the threat, the history of the threat (the longer malware has been on a network the more dangerous it is generally), and the asset value of the target. ▪ The degree to which ANY of these strings of information can be assembled through automation truncates the incident response cycle and reduces human error.

Cybersecurity AIRO

Objective: Prioritize offense and accelerate investigations by gathering and evaluating all observables, local or via Watson.


What was the attack?
Is the attack credible?
How valuable are the targets to the business?
Who was responsible for the attack?
Where are they located?
What was stolen and where is the evidence?
Are any of the assets vulnerable?
How many targeted assets are involved
1

Offense 909

Magnitude		Status		Relevance	0	Severity	5	Credibility	4
Description	Potential Data Loss	Offense Type	Source IP				
		Event/Flow count	111 events and 1,042 flows in 13 categories				
Source IP(s)	10.0.110.221 (dhcp-221-users-2.acme.com)	Start	Oct 18, 2013 12:28:02 PM				
Destination IP(s)	Local (2) Remote (376)	Duration	4d 10h 42m 57s				
Network(s)	Multiple (3)	Assigned to	admin				

Offense Source Summary

IP	10.0.110.221	Location	Users.Users-2
Magnitude		Vulnerabilities	0
Username	compliance	MAC Address	00:0E:0C:B4:D8:EE
Host Name	dhcp-221-users-2.acme.com		
Asset Name	dhcp-221-users-2.acme.com	Weight	0
Offenses	8	Events/Flows	15,310

Last 5 Notes

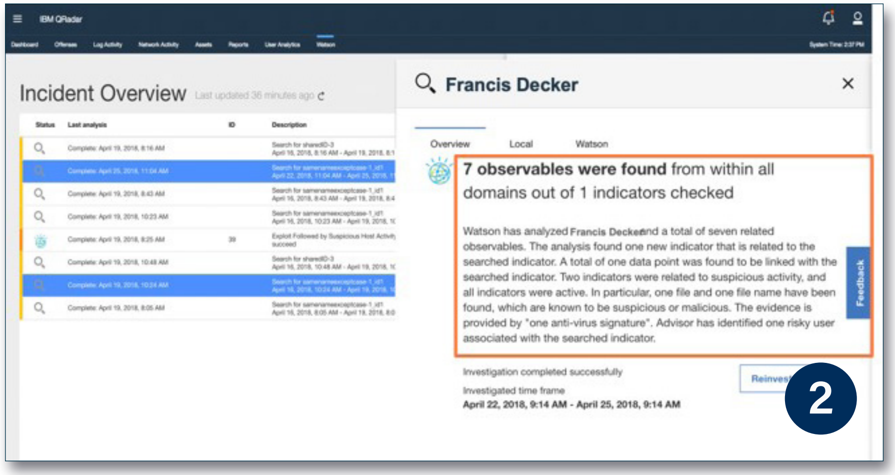
Notes	Username	Creation Date
Potential data loss detected, forensics case created	admin	Oct 21, 2013 6:39 AM

Forensics Reconstructions

Case	Collection	IP	Start	End	Status
DataLoss	DataLoss	10.0.110.221	3/27/2014 3:31:00 PM	3/27/2014 4:31:00 PM	SUCCESS

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
dhc...		Users.Users-2	No	compliance	00:0E:0C:B4:D8:EE	0	8	21	0s	15,310



Incident Overview Last updated 36 minutes ago

Francis Decker

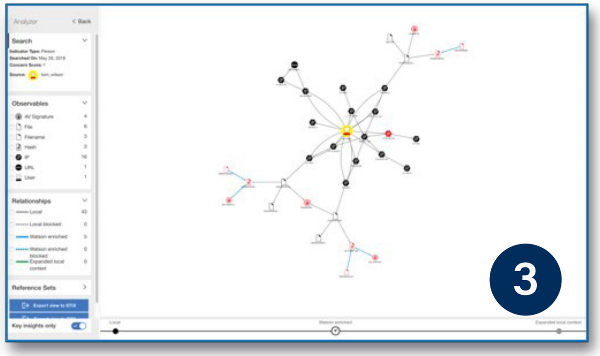
7 observables were found from within all domains out of 1 indicators checked

Watson has analyzed **Francis Decker** and a total of seven related observables. The analysis found one new indicator that is related to the searched indicator. A total of one data point was found to be linked with the searched indicator. Two indicators were related to suspicious activity, and all indicators were active. In particular, one file and one file name have been found, which are known to be suspicious or malicious. The evidence is provided by "one anti-virus signature". Advisor has identified one risky user associated with the searched indicator.

Investigation completed successfully

Investigated time frame

April 22, 2018, 9:14 AM - April 25, 2018, 9:14 AM



IDC Inference

1. The screen capture 1 shows the results of "offense chaining." Toward reducing the MTTR, this correlation condenses by:
   - » Prioritizing offenses (i.e., alerts)
   - » Reduces the number of alerts by auto chaining related events into single offense.
   - » Lets the analyst review details such as related IP addresses, log sources
   - » Take action and assign offense to analyst
2. Mined additional local observables related to this incident. Then was able to find additional related cognitive evidence via Watson to scope the full incident for eradication.
3. The visualization of "Observables," contributes in this way:
   - » Drives consistent investigations by gathering and evaluating all observables, local or via Watson
   - » Prepares accurate response by reviewing all related observables (IP, URL, user)
   - » Export for automated response

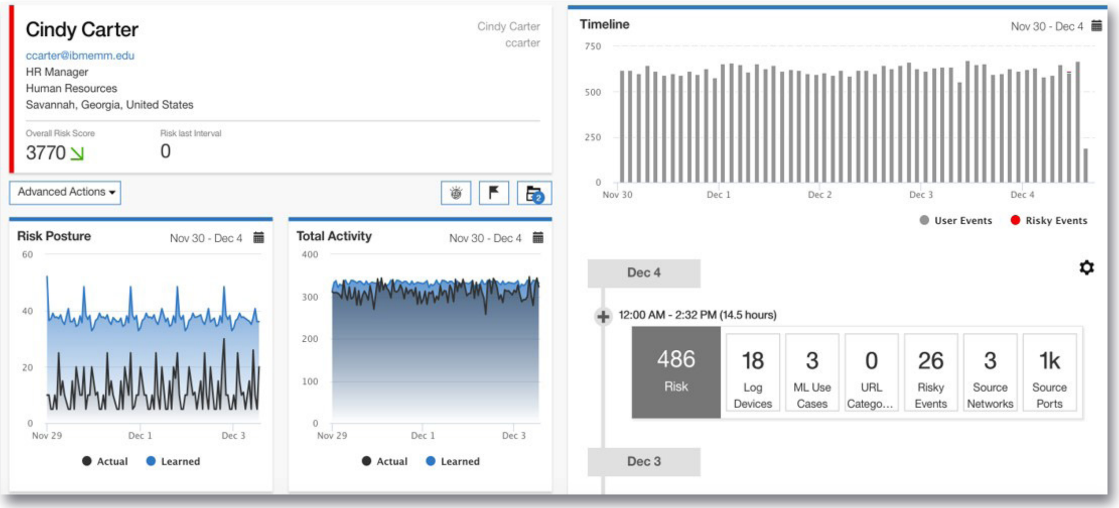
Validated – Cybersecurity AIRO

Objective #2 – Accelerated Investigations

Feature/Validation Summary

On the right hand side an image of a dashboard that illustrates how QRadar calculates risk assessment. Dashboard features showed here include:

- User by name and business group
- Timeline of activities
- Risk posture (both actual and learned)
- Total activity (actual and learned)
- Risk score
- User access (log sources, ML use cases, source ports, etc.



Cindy Carter
ccarter@ibmemm.edu
HR Manager
Human Resources
Savannah, Georgia, United States

Cindy Carter
ccarter

Overall Risk Score: 3770 ↘
Risk last Interval: 0

Dec 4
12:00 AM - 2:32 PM (14.5 hours)

486	18	3	0	26	3	1k
Risk	Log Devices	ML Use Cases	URL Catego…	Risky Events	Source Networks	Source Ports

Dec 3

The presentation of this collected intelligence is no small matter—it saves the analyst a significant amount of time in the triage part of threat investigations.

Validation Process

In the IBM test environment, the forensic investigation of 573 offenses was simulated.

- The user has clicked onto an email which precipitated a PowerShell attack that emanated from a process from a Temp Directory.
- The PowerShell was executed in the background of the Word process in an attempt to obfuscate the malware code it was running.
- The practitioner could reference Sources, Destinations, Log Sources, users, Categories, Annotations, Networks, or Rules to begin the investigation (Rules is usually the logical beginning).

IDC Validation Methodology

This Validation InfoBrief provides a summary of an extensive validation process performed by IDC in collaboration with the supplier's teams. IDC relied on the supplier's equipment, facilities and its configuration to perform this validation. All of the tests were conducted during the presence of one or more IDC analysts.

This InfoBrief is meant to provide a quick set of inferences and insights for IT professionals and business decision makers seeking to perform further due diligence on the capabilities of the product and/or services that have been validated in this InfoBrief. However, the goal of this InfoBrief is not to supply detailed hands-on test plans and validation jobs. It is not meant to replace the evaluation process that most businesses will conduct before making any decision to purchase the product and/or services.

It is for this reason that this InfoBrief is not designed to be an all-inclusive document on all the capabilities of the product, but rather as a concise document that highlights features/functions of products, their relative performance with respect to a traditional environment and the value these features bring to businesses looking to solving certain problems using the evaluated product.

Finally, even though this InfoBrief is a sponsored document, it is not meant to be an IDC endorsement of the product, service or the sponsoring supplier. IDC's opinions are its own and not influenced by the production of this document.

Validation Test Bed

IDC validated the conditions as presented over three Web sessions. The control criteria are defined below. The analyst asked for RegEx and Arial query, packet visibility, and connectivity to the IBM Apps store. The following table provides a summary of the test environment.

Scenario	#1 Single, Open Platform	#2 Advanced Detection (UBA)	#3 Accelerate Investigation
Benefits/User Outcomes	▪ Easy to integrate ▪ Obtain enterprise wide visibility ▪ Integrated business context ▪ Time to value ▪ Get more out of investments ("collect once, reuse many times")	▪ Obtain new identity centric insights ▪ Surface unknown threats ▪ Reduce human effort to create content (there is no need for "data scientist")	▪ Reduce investigative efforts, time to investigate ▪ Get consistent depth in investigations ▪ Prepare for accurate response (avoid whack-a-mole game)
Features to Be Tested	▪ Data intake (DSM) from endpoint, network, cloud, IAM/AD, application logs ▪ Data archiving and searching ▪ UBA install from app exchange ▪ IBM QRadar Advisor with Watson install from app exchange	▪ Surfacing user activity ▪ Machine learning ▪ Calculate overall user risk ▪ Build and compare against peers	▪ User views ▪ Offense/alert views ▪ Connecting the dots via IBM QRadar Advisor with Watson

Notes

- Lab sessions occurred January 25, January 30, and February 4, 2019.
- The sessions occurred remotely over Webex.
- The lab sessions were designed to follow the scenarios as defined on the left.
- The analyst was free to ask questions, propose alternate scenarios, and challenge assumptions.
- Each lab session took roughly one hour.

Conclusion: IBM QRadar 7.3.1 and UBA 3.0 Key Differentiators

Feature Category	Single, open platform • The use of UBA for advanced threat detection • Accelerate investigations
Features	▪ Data intake (DSM) from endpoint, network, cloud, IAM/AD, application logs ▪ Data archiving and searching ▪ UBA deployed to surface user activity ▪ Machine learning implemented to calculate overall user risk ▪ An overall analytics layer that is capable of "offense chaining" (described on the right) ▪ Watson used to consolidate and reconcile external threat intelligence with observable events on the network
Key Differentiators	▪ Data intake from multiple log sources is vitally important. From the standpoint of a holistic cybersecurity posture, proxy logs from cloud service gateways, and endpoints are as important as firewall logs or various NetFlow logs. ▪ Add new functionality (UBA or Advisor with Watson) to QRadar Security Intelligence platform via single administrative interface and app centric workflow. ▪ Multiple ML algorithms quickly determine the degree to which a security incident is anomalous relative to pre-established rules, individual user behavior, and peer group standards. ▪ Perhaps "offense chaining" is a key capability offered on QRadar. What offense linking does is process alerts and connect them to a single entity for prioritization and historical overview. By directly comparing anomalies over multiple log sources, the platform provides practitioners with high fidelity of the incident with multiple vantage points, and the ability to localize where the security alerts emanate. ▪ IBM Watson is used to look at various discovered threat vectors. Watson refers to multiple threat libraries and publicly available threat intelligence to create a more complete description of the threat. ▪ The platform can create an event view of everything that occurred to a specific IP address. ▪ IBM QRadar also offers several protective measures on its platform that were not necessarily covered in the test bed: » Data obfuscation—A practitioner can enable obfuscation fields such as "user name," "credit card number," and "log source." » Even before UBA principles are applied, QRadar has nearly 500 out-of-the-box rules that it can enforce for advanced search.

Essential Guidance - Advice for Buyers

The sessions that IDC conducted with IBM were constructive in the sense that we could validate what IBM claimed it could do on QRadar to our satisfaction. Understand that this happens in a controlled environment (we aren't assuming chicanery, but each network environment is different).

We did not ask for pricing, but the cybersecurity solutions buyer will. Self-evidently, a cybersecurity solution is a great purchase at $1x; and a poor purchase at $10x. The most important thing a buyer can do is get a comprehensive understanding of the licensing agreement (perpetual versus subscription), what its storage arrangements will be, and how the base pricing is established (seats or devices covered/events per second/or egress/ingress points). The buyer should also understand what happens if it exceeds the number of seats purchased. Additionally, the buyer needs to understand what performance issues they may encounter at burst traffic or peak season.

Obviously, a proof of concept (POC) is part of the request for requisition process. Very rarely is a cybersecurity tool booted up into a greenfield environment. A buyer needs to have an understanding of how its security tools will interact with its existing network performance monitoring tools, IT tools, directory services, endpoint protection, and identity and access manger among other platforms and considerations. It is also advised that multiple team members conduct investigations while in the POC to see how the tool drives. Soft values such as customer service, customized script writing to link APIs together, and admin support at the time of installation should be factored in.

IDC concludes that IBM QRadar 7.3.1 with UBA 3.0 is a strong cybersecurity tool that impacts all aspects of a cybersecurity posture including onboarding of machines and end users, pre-established filters, and all phases of incident detection and response. The security operation center (SOC) is often "death by a thousand cuts." The multiple sources of log ingestion help create a single version of truth. Machine learning (ML) applied to advanced detection techniques is translated into a comprehensive risk score. As importantly, ML establishes individual and peer group criterion for anomaly detection which is vital when malware bypasses the perimeter or a network user appears to be authentic because the adversary has highjacked valid credentials. Finally, "offense chaining" largely eliminates the time analysts spend in chasing down alerts. A centralized incident detection and response platform such as QRadar is a state-of-the-art approach as it helps to automate the information gathering needed to determine the effect of malware, fashion the proper response, and recalibrate rules to prevent the next intrusion.