TD SYNNEX

IBM Cloud Pak for Security Specialty Exam Enablement S1000-001

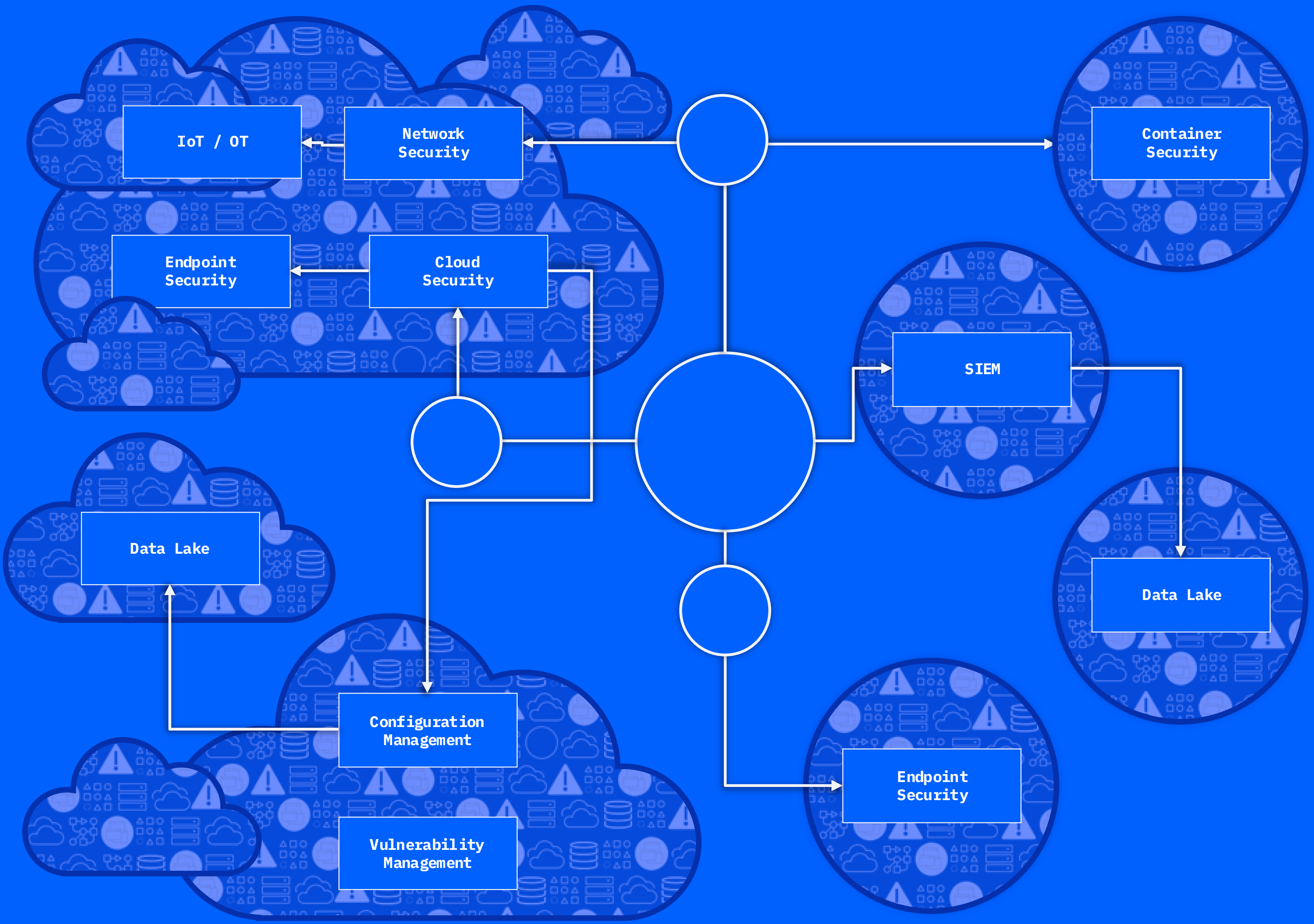
Marshall Hall
Field Solutions Architect

★ Focus Areas Highlighted with Stars

Growing threats, tools and data are inhibiting security operations

SOC analysts need help...

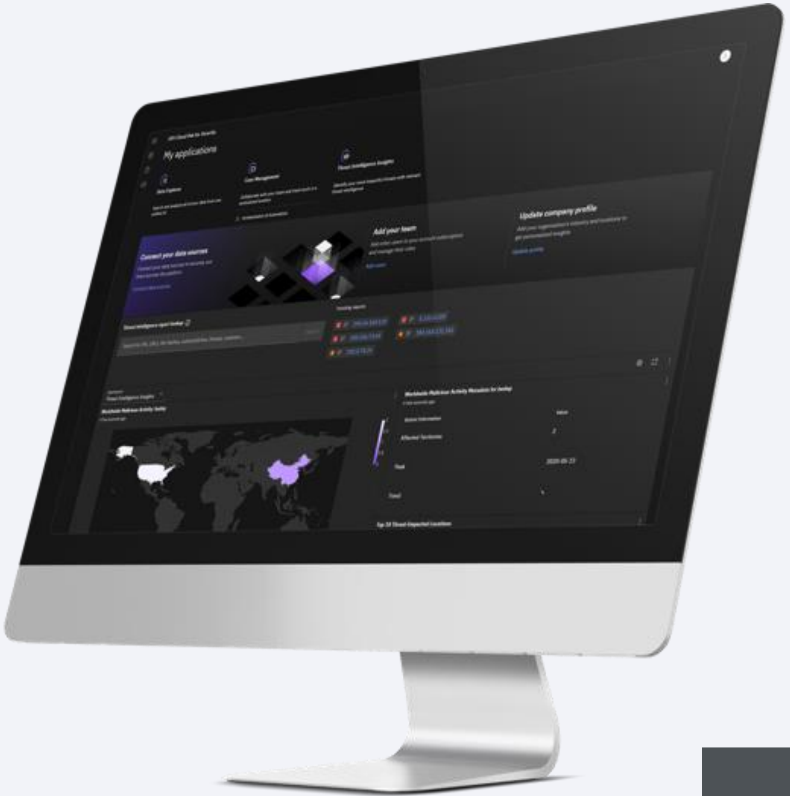
- Prioritizing the increasing amount of events, alerts and intelligence they have
- Quickly navigating multiple tools and data sources to investigate threats
- Reducing manual processes and even more tools to resolve security incidents



IBM Cloud Pak for Security

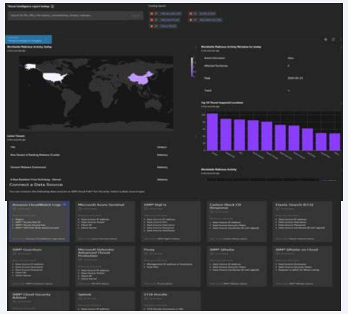
Detect and respond to **threats** with a simple, unified experience

Threat Management



Unified Security Workflows

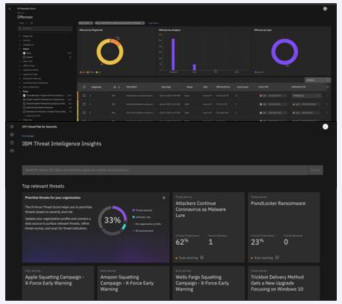
Visibility



Gain unified visibility across the enterprise, security tools and threat intelligence

Dashboards
Unified dashboards and visualizations with reporting

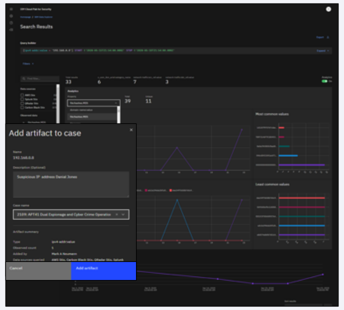
Detection



Detect and unify threats and reduce false positives

Threat Intelligence Insights
Threat intelligence from X-Force and 3rd party sources

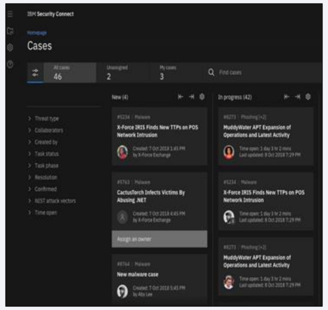
Investigation



Automate investigations with AI and federated searches. Collaborate with integrated case management

Data Explorer
Search and Investigation
across all security systems

Response



Respond faster with automation, play books, and Ansible integration

SOAR
Unified case management integrated with offenses

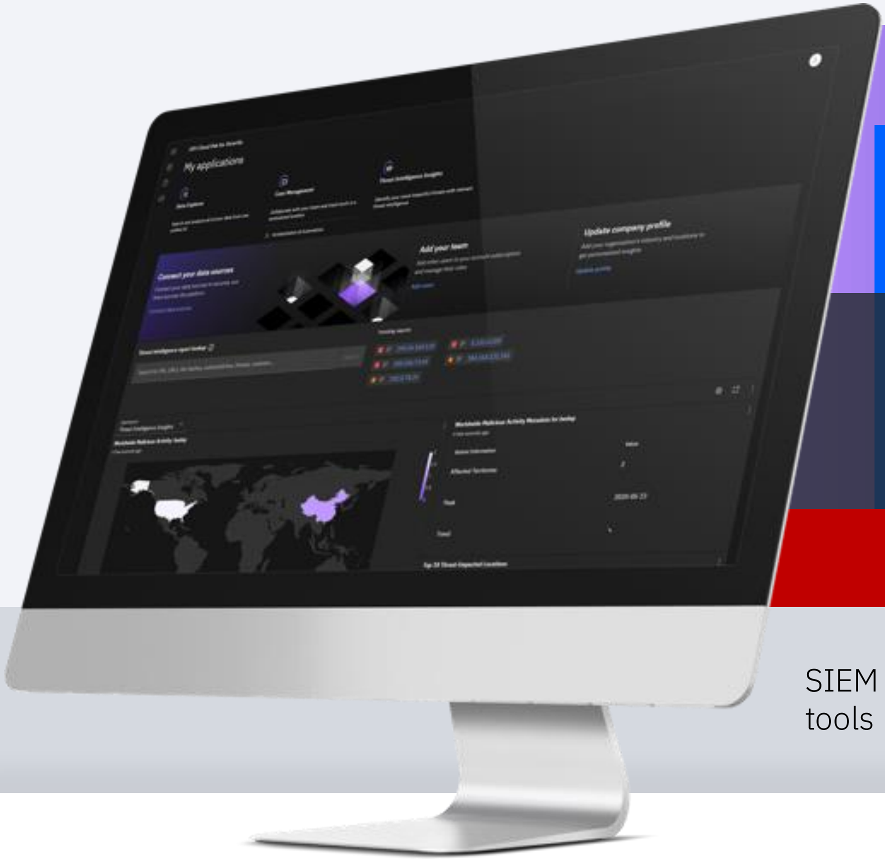
Platform services

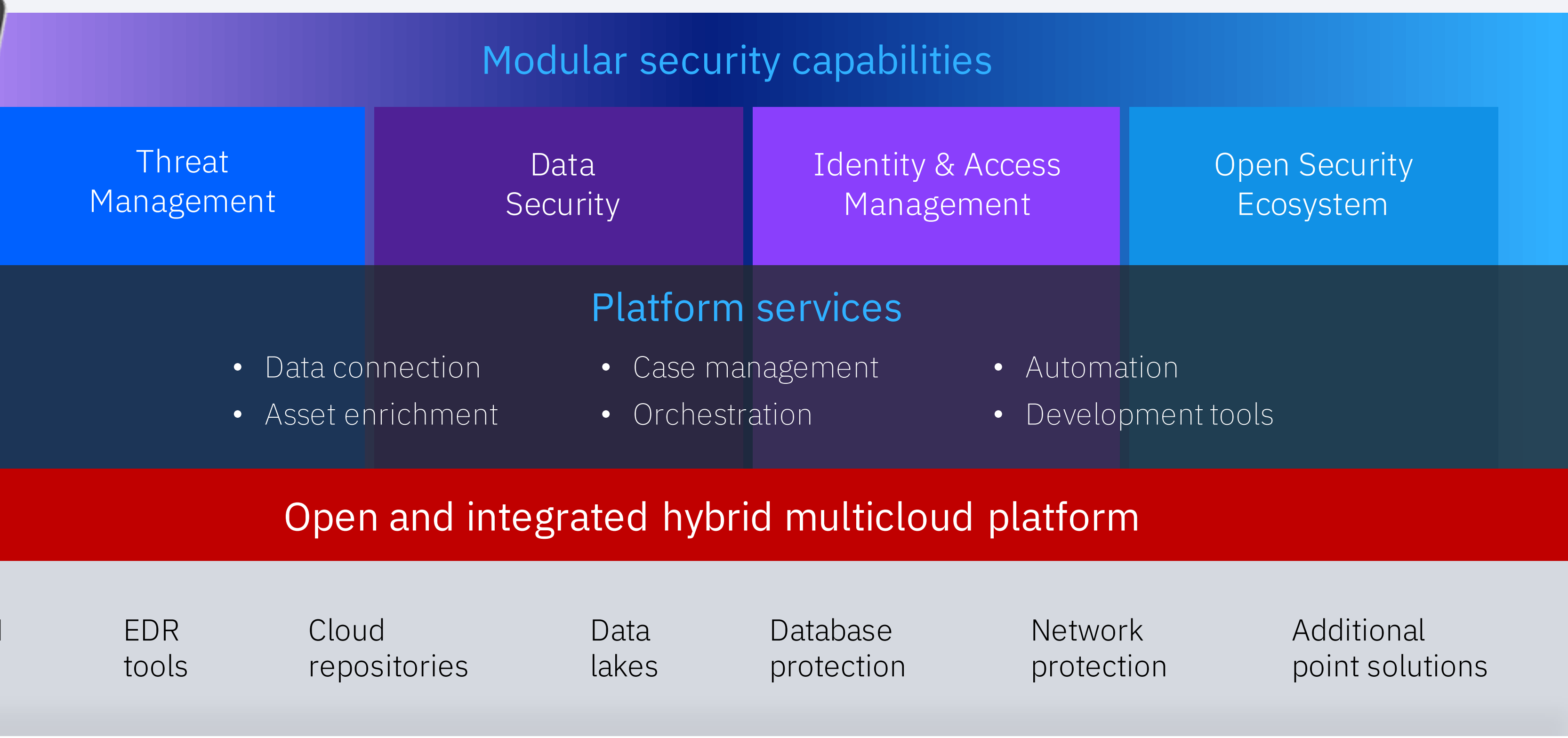
- Data connection
- Asset enrichment
- Case management
- Orchestration
- Automation
- Risk management

Open and integrated hybrid multicloud platform

IBM Cloud Pak for Security

An open multicloud platform to gain security insights, take action faster, and modernize your architecture





Modular security capabilities

- Threat Management
- Data Security
- Identity & Access Management
- Open Security Ecosystem

Platform services

- Data connection
- Asset enrichment
- Case management
- Orchestration
- Automation
- Development tools

Open and integrated hybrid multicloud platform

SIEM tools | EDR tools | Cloud repositories | Data lakes | Database protection | Network protection | Additional point solutions

On premise

Hybrid Cloud

Multicloud

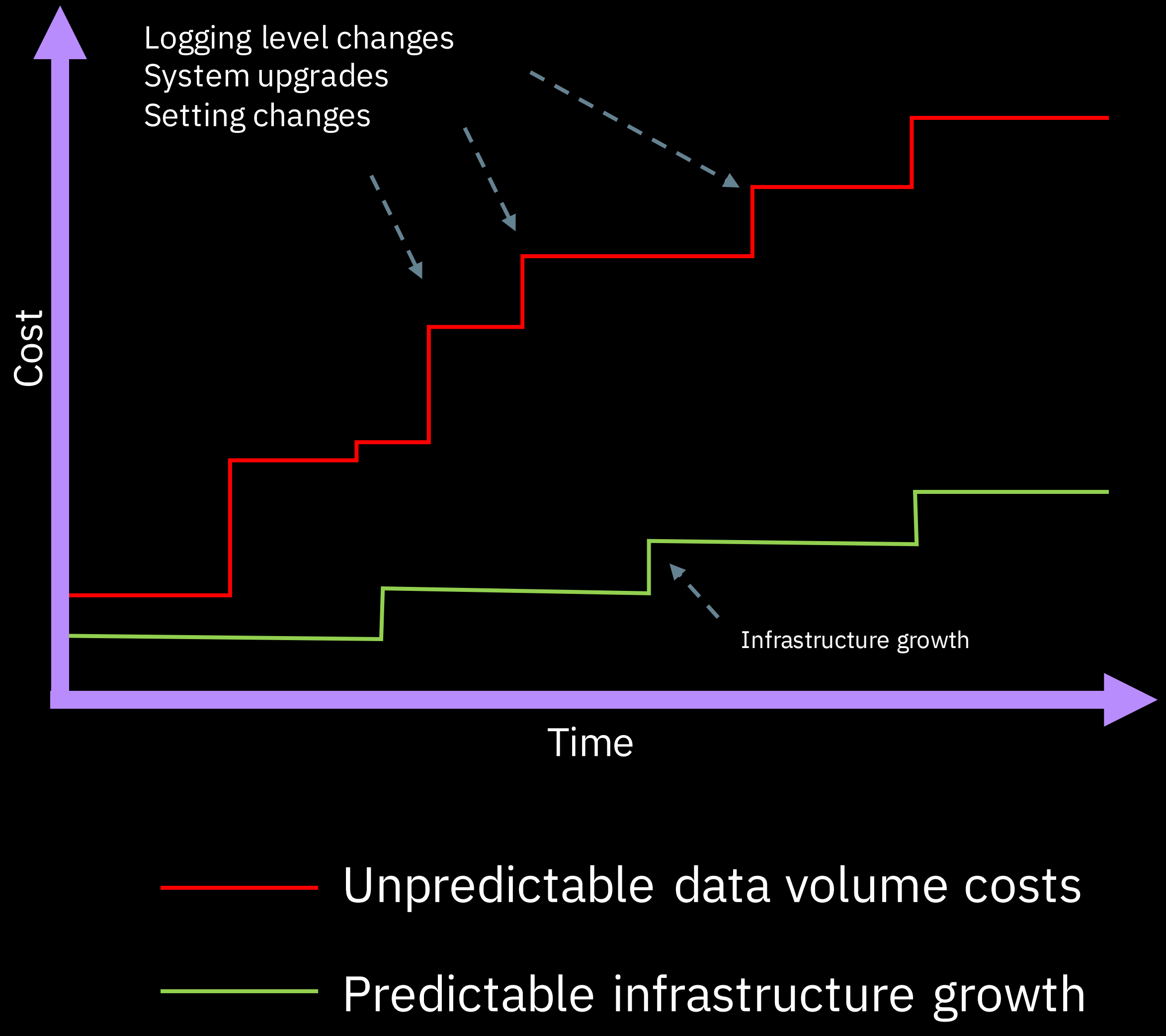
IBM Cloud Pak for Security key benefits

- Simple, predictable pricing model
- Unified analyst workflow
- Open, extensible ecosystem
- Next-generation, cloud native architecture

Simple, predictable pricing model

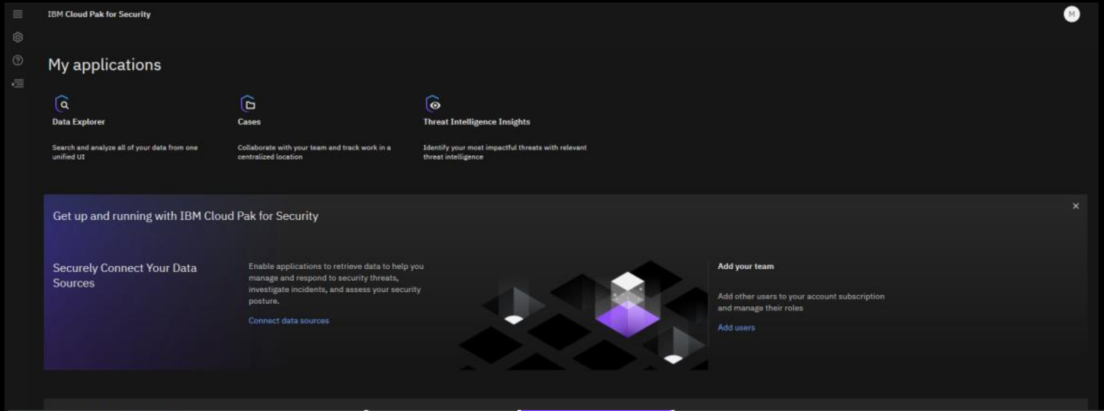
- A predictable, straightforward pricing model that doesn't penalize usage or is based on data volumes

- Cloud Pak for Security pricing model is based around Managed Virtual Servers (MVS) and has no additional charges for data, logs, flows, events actions or users



Unified analyst workflow

- Security teams manage too many tools and cloud platforms with different user workflows and limited automation, creating complexity and slowing down response times
- Cloud Pak for Security provides a modern, streamlined, unified analyst interface to across all their security tools, simplifying user workflows
- Built in Security Automation, Orchestration and Response (SOAR) powered by integration with Ansible removes repetitive manual tasks and leverages an ecosystem of open source connectors and playbooks



IBM Cloud Pak for Security

My applications

Data Explorer

Search and analyze all of your data from one unified UI

Cases

Collaborate with your team and track work in a centralized location

Threat Intelligence Insights

Identify your most impactful threats with relevant threat intelligence

Get up and running with IBM Cloud Pak for Security

Securely Connect Your Data Sources

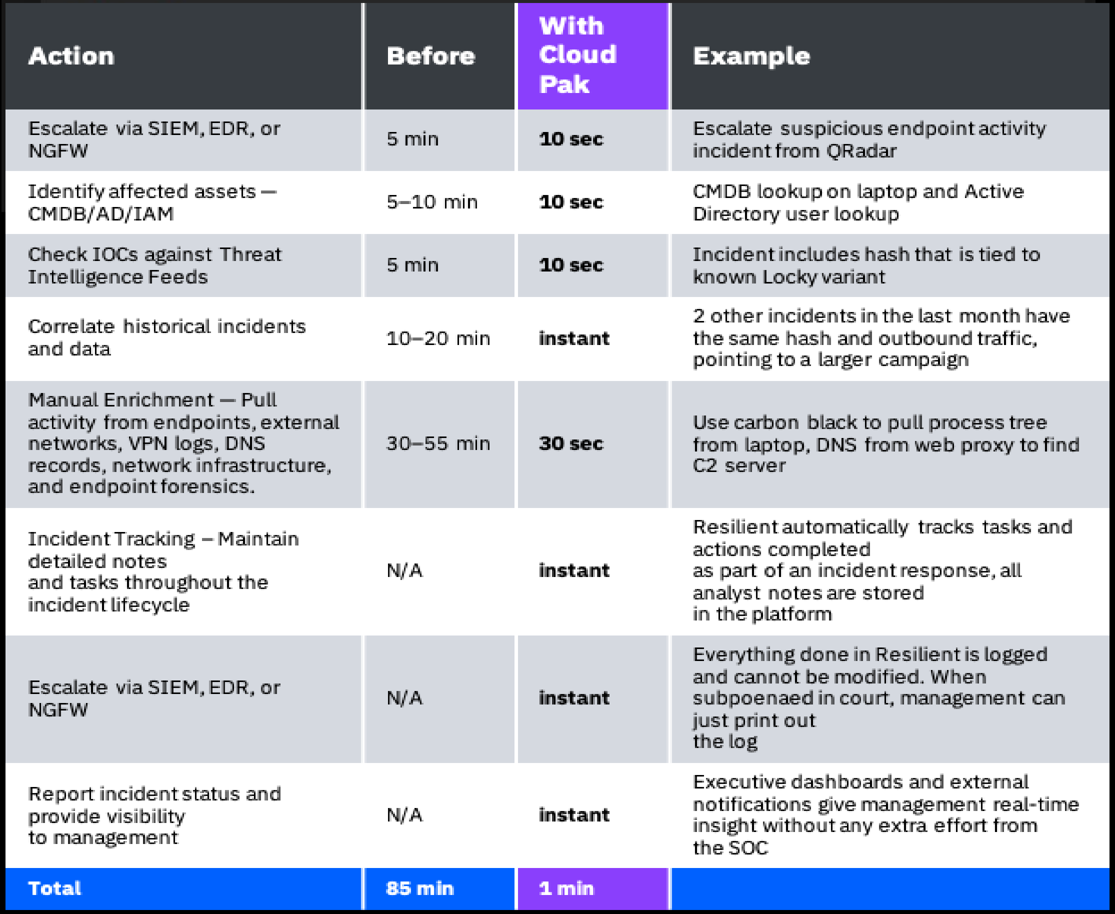
Enable applications to retrieve data to help you manage and respond to security threats, investigate incidents, and assess your security posture.

Connect data sources

Add your team

Add other users to your account subscription and manage their roles

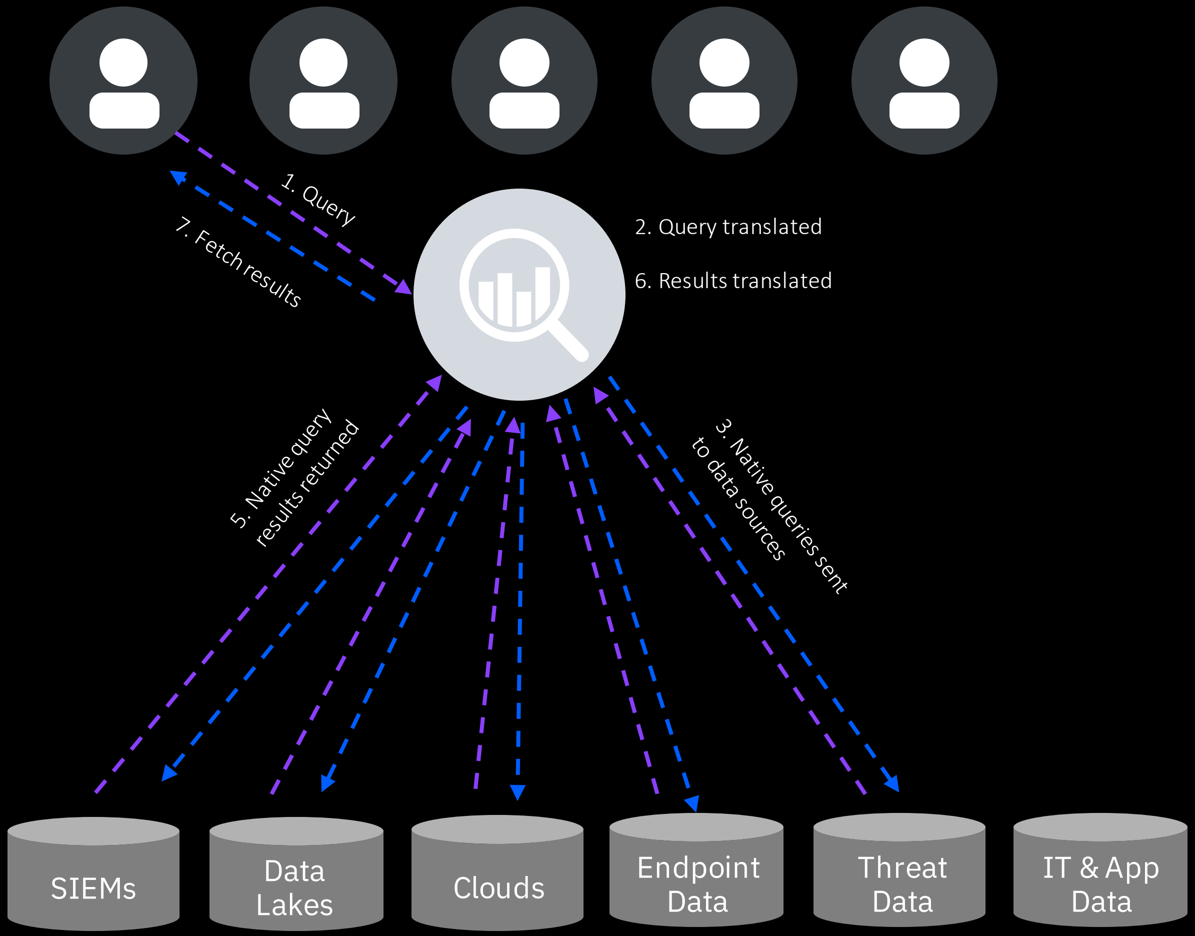
Add users



Action	Before	With Cloud Pak	Example
Escalate via SIEM, EDR, or NGFW	5 min	**10 sec**	Escalate suspicious endpoint activity incident from QRadar
Identify affected assets – CMDB/AD/IAM	5–10 min	**10 sec**	CMDB lookup on laptop and Active Directory user lookup
Check IOCs against Threat Intelligence Feeds	5 min	**10 sec**	Incident includes hash that is tied to known Locky variant
Correlate historical incidents and data	10–20 min	**instant**	2 other incidents in the last month have the same hash and outbound traffic, pointing to a larger campaign
Manual Enrichment – Pull activity from endpoints, external networks, VPN logs, DNS records, network infrastructure, and endpoint forensics.	30–55 min	**30 sec**	Use carbon black to pull process tree from laptop, DNS from web proxy to find C2 server
Incident Tracking – Maintain detailed notes and tasks throughout the incident lifecycle	N/A	**instant**	Resilient automatically tracks tasks and actions completed as part of an incident response, all analyst notes are stored in the platform
Escalate via SIEM, EDR, or NGFW	N/A	**instant**	Everything done in Resilient is logged and cannot be modified. When subpoenaed in court, management can just print out the log
Report incident status and provide visibility to management	N/A	**instant**	Executive dashboards and external notifications give management real-time insight without any extra effort from the SOC
Total	**85 min**	**1 min**	

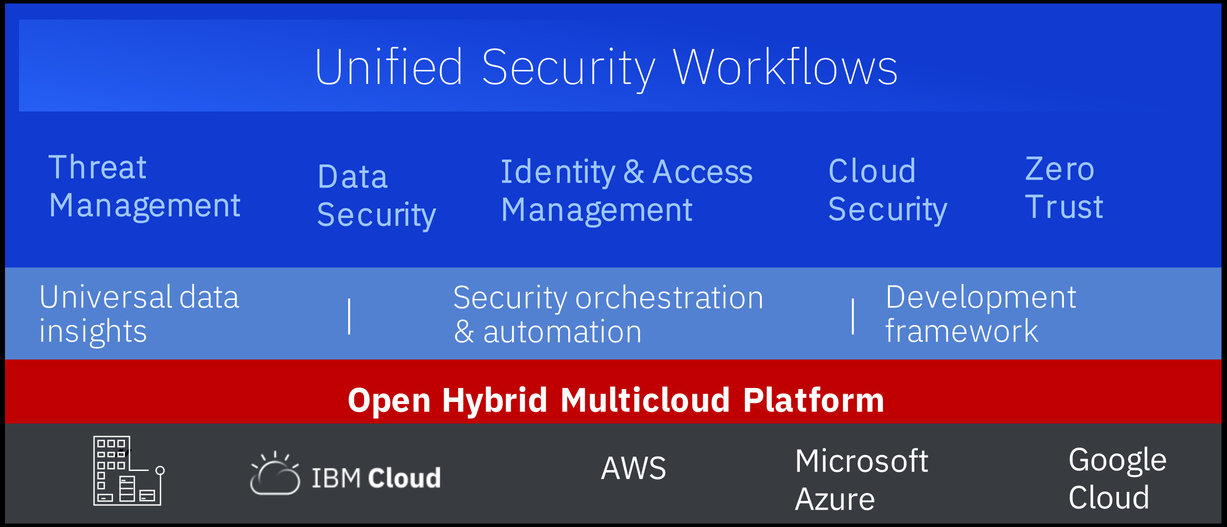
Open, extensible ecosystem

- Organizations need different data sources in their organization with important security data, such as:
  - Cloud services – AWS, Google, Azure with their own integrated security & log management tools (AWS CloudWatch, etc.)
  - Endpoint Detection & Response (EDR), SIEM tools or an existing data lake
- The federated search capabilities in Cloud Pak for Security allow security analysts to search and use this data to hunt or investigate threats without having to move the data itself



Next-gen, cloud native architecture

- Future proof technology investments help in planning a long-term cloud migration strategy
- Cloud Pak for Security is a security platform that will support a hybrid multicloud strategy, with a containerized, microservices deployment model
- The flexible deployment model enables organizations to shift at their own pace

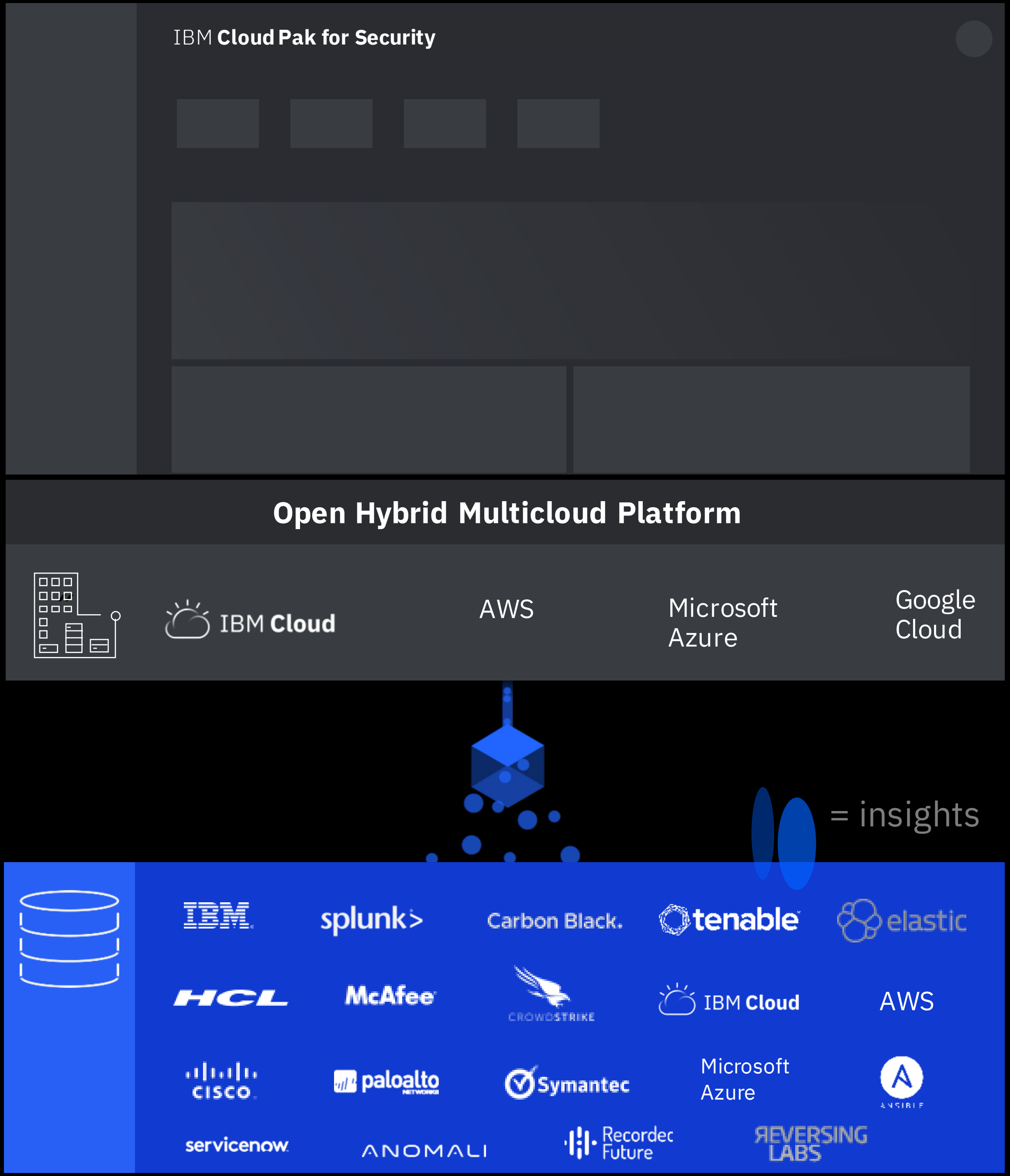


Unified data insights

Get complete insights while leaving your data where it is

Open partner ecosystem

Securely connect third-party security tools within existing security infrastructure



IBM **Cloud Pak for Security**

Open Hybrid Multicloud Platform

IBM **Cloud**

AWS

Microsoft Azure

Google Cloud

= insights

IBM **Cloud**

AWS

Microsoft Azure

Hybrid, multicloud platform

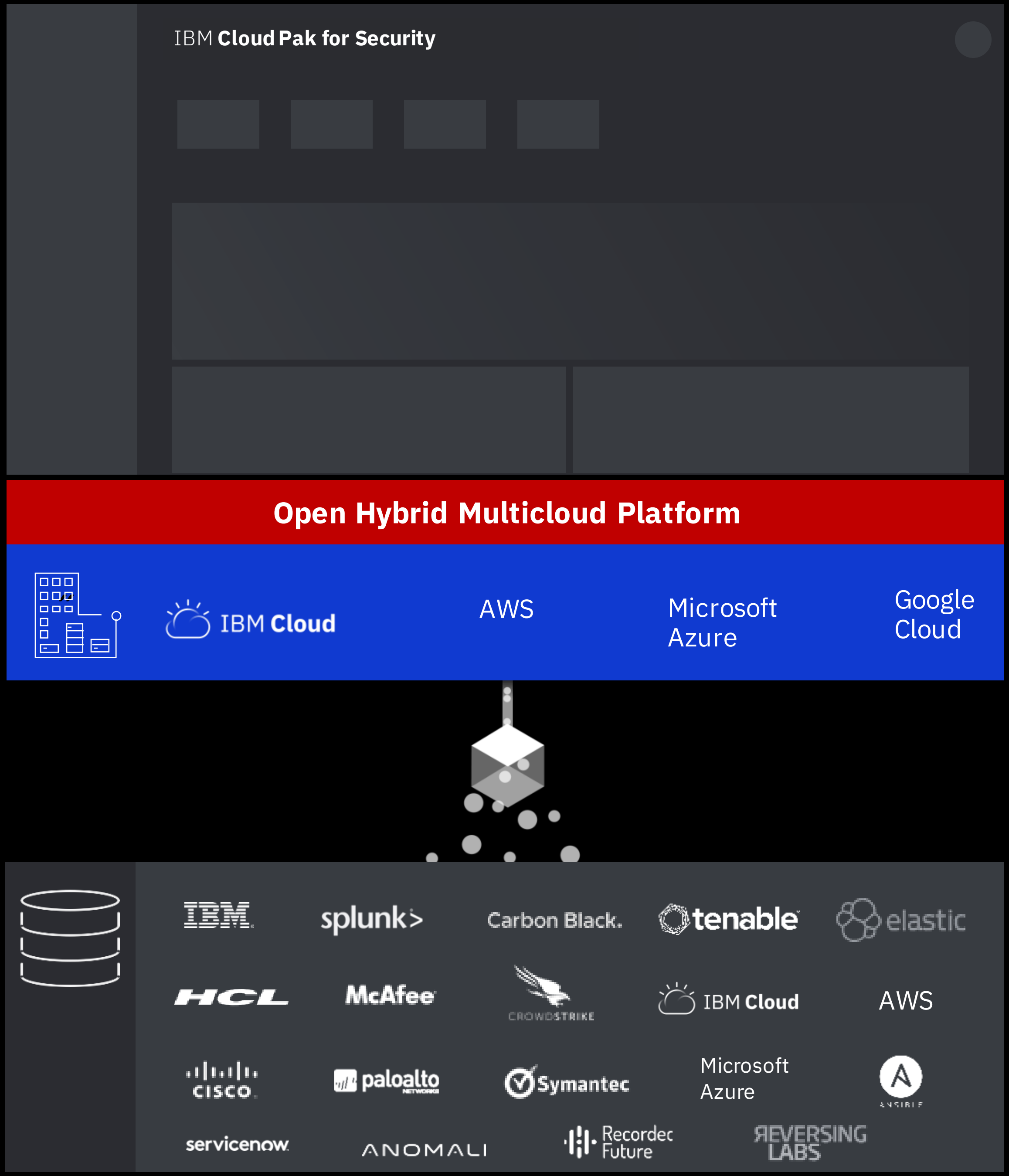
Modern, open architecture for public, private, hybrid clouds, ready to deploy and run anywhere

Unified data insights

Get complete insights while leaving your data where it is

Open partner ecosystem

Securely connect third-party security tools within existing security infrastructure



Unified interface & design system

Work across one unified experience, lower training costs, build apps faster

Outcome-driven solutions

Out-of-the-box ability to address security workflows, anchored by orchestration and automation

Hybrid, multicloud platform

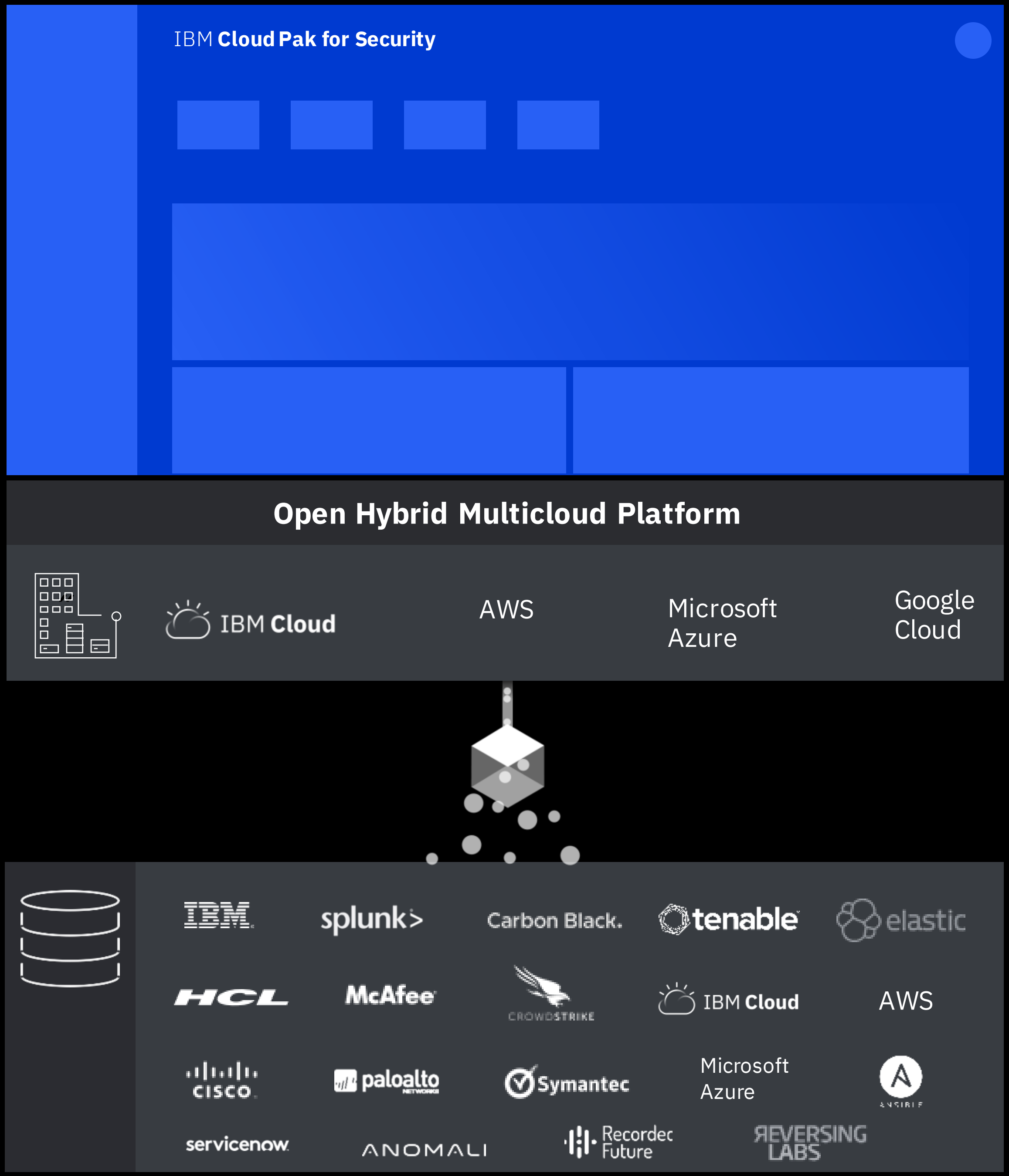
Modern, open architecture for public, private, hybrid clouds, ready to deploy and run anywhere

Unified data insights

Get complete insights while leaving your data where it is

Open partner ecosystem

Securely connect third-party security tools within existing security infrastructure



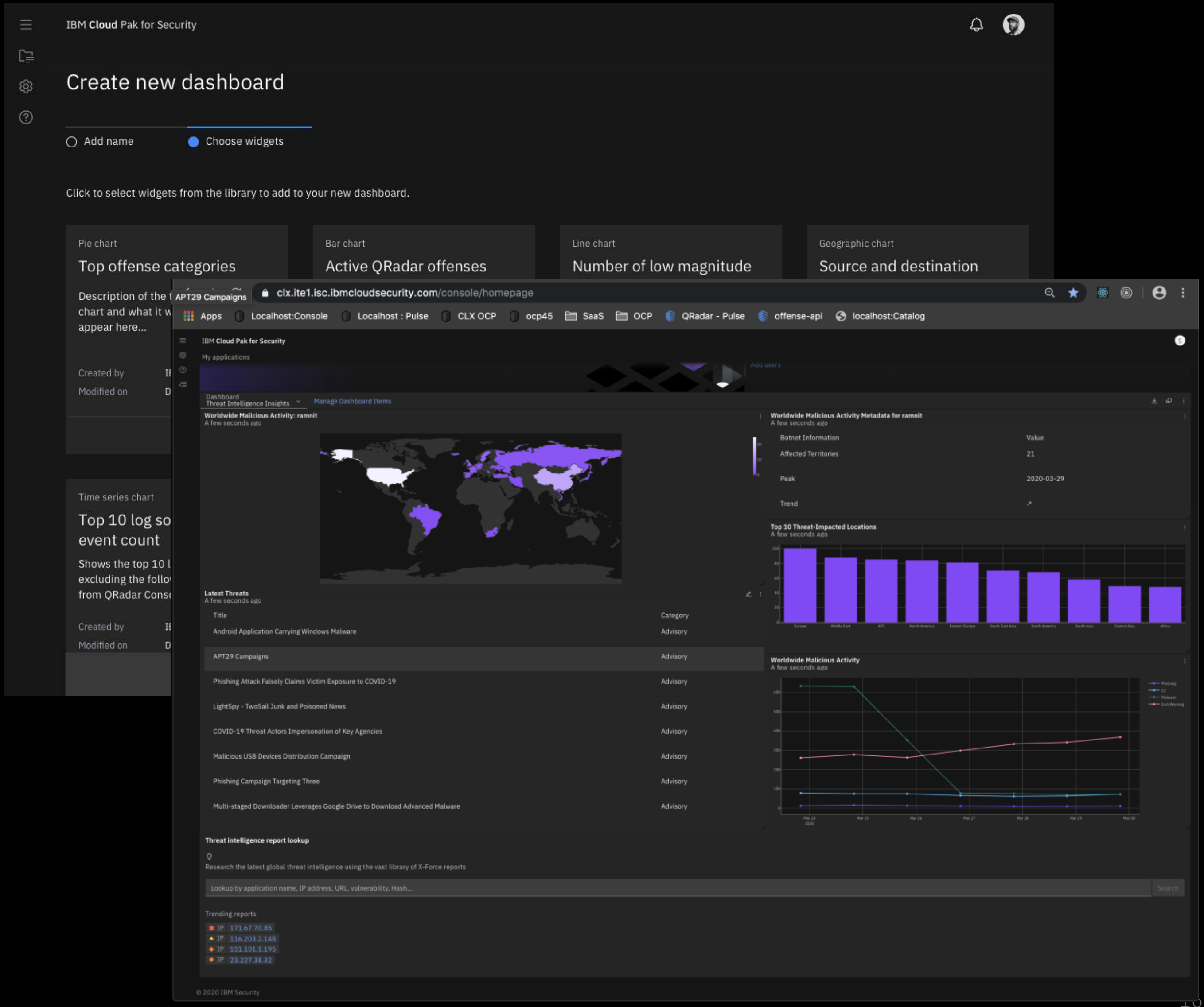
Dashboards

Cybersecurity dashboards for analysts, managers & CISOs

- **Develop various security dashboards based on a common framework**
  Teams can rapidly deliver special-purpose dashboards with information coming from Cloud Pak for Security apps and data services

- **Create custom dashboards from a library of widgets and data sources**
  Analysts can build their own dashboard canvases and fill in with visualizations of their security data

- **Drill into dashboard views for more insights**
  Analysts can drill into high-level dashboard views to get details on specific threats and risks



IBM **Cloud** Pak for Security

Create new dashboard

○ Add name ● Choose widgets

Click to select widgets from the library to add to your new dashboard.

Pie chart
Top offense categories
Description of the chart and what it w… appear here…
Created by I…
Modified on D…

Bar chart
Active QRadar offenses

Line chart
Number of low magnitude

Geographic chart
Source and destination

Time series chart
Top 10 log so… event count
Shows the top 10 l… excluding the follo… from QRadar Cons…
Created by I…
Modified on D…

APT29 Campaigns

clx.ite1.isc.ibmcloudsecurity.com/console/homepage

Apps · Localhost:Console · Localhost : Pulse · CLX OCP · ocp45 · SaaS · OCP · QRadar - Pulse · offense-api · localhost:Catalog

IBM **Cloud Pak for Security**

My applications

Add users

Dashboard
Threat Intelligence Insights

Manage Dashboard Items

Worldwide Malicious Activity: ramnit
A few seconds ago

Worldwide Malicious Activity Metadata for ramnit
A few seconds ago

Botnet Information	Value
Affected Territories	21
Peak	2020-03-29
Trend	↗

Top 10 Threat-Impacted Locations
A few seconds ago

Latest Threats
A few seconds ago

Title	Category
Android Application Carrying Windows Malware	Advisory
APT29 Campaigns	Advisory
Phishing Attack Falsely Claims Victim Exposure to COVID-19	Advisory
LightSpy - TwoSail Junk and Poisoned News	Advisory
COVID-19 Threat Actors Impersonation of Key Agencies	Advisory
Malicious USB Devices Distribution Campaign	Advisory
Phishing Campaign Targeting Three	Advisory
Multi-staged Downloader Leverages Google Drive to Download Advanced Malware	Advisory

Worldwide Malicious Activity
A few seconds ago

Threat intelligence report lookup

Research the latest global threat intelligence using the vast library of X-Force reports

Lookup by application name, IP address, URL, vulnerability, Hash…

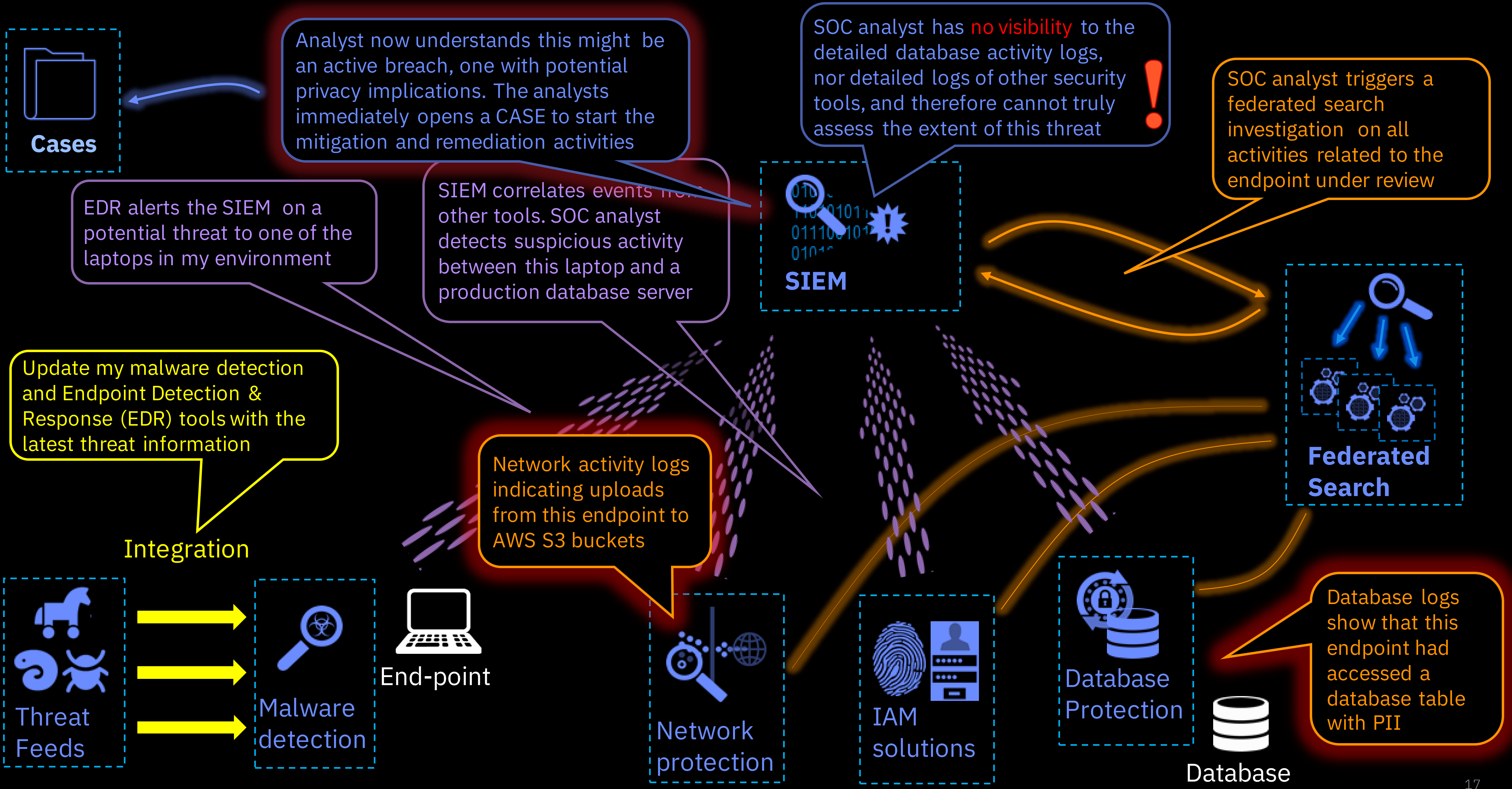
Search

Trending reports

■	IP	171.67.70.85
▲	IP	116.203.2.148
◆	IP	151.101.1.195
◆	IP	23.227.38.32

© 2020 IBM Security

Let’s see how product integration, logs aggregation (SIEM) and federated search work together



Analyst now understands this might be an active breach, one with potential privacy implications. The analysts immediately opens a CASE to start the mitigation and remediation activities

SOC analyst has no visibility to the detailed database activity logs, nor detailed logs of other security tools, and therefore cannot truly assess the extent of this threat

SOC analyst triggers a federated search investigation on all activities related to the endpoint under review

EDR alerts the SIEM on a potential threat to one of the laptops in my environment

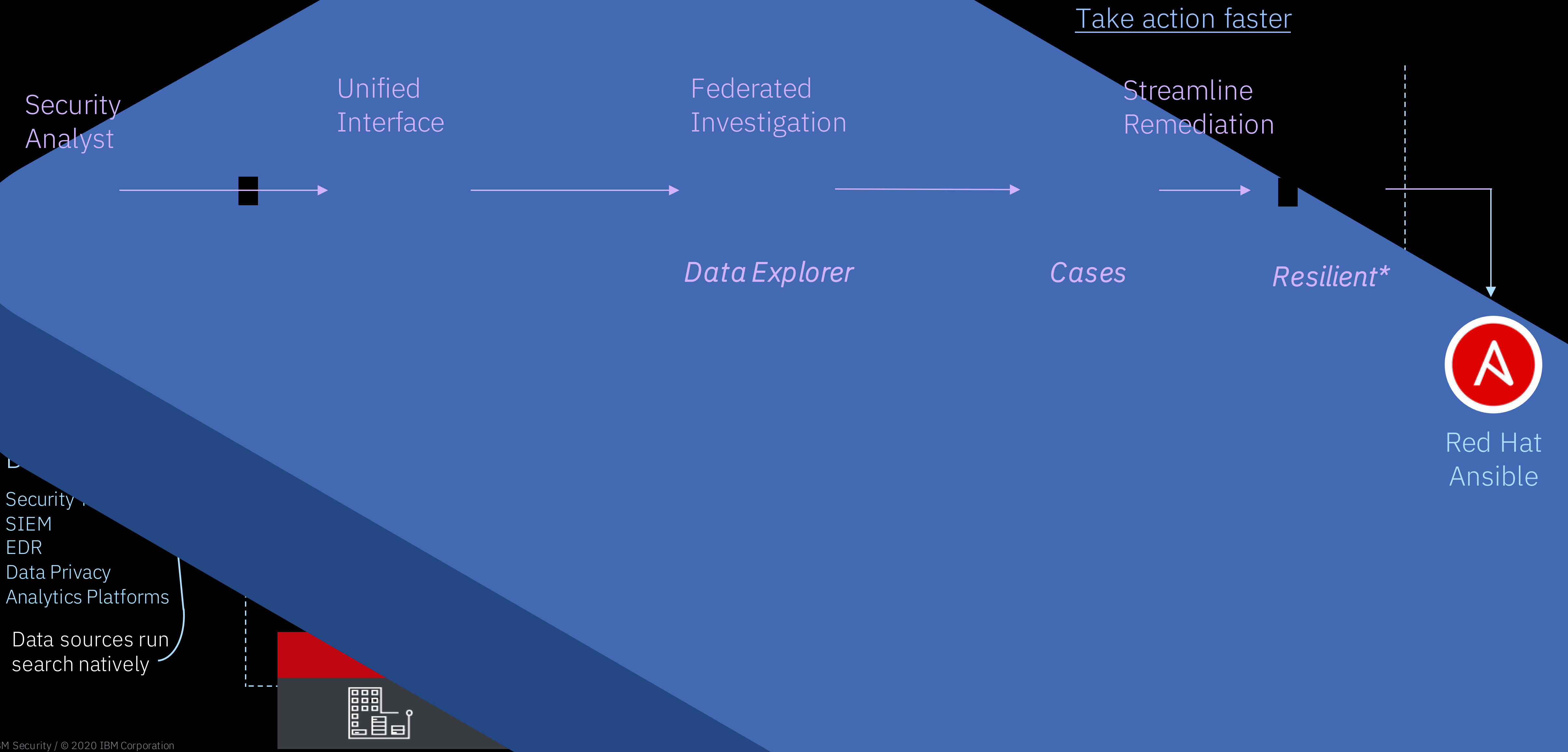
SIEM correlates events from other tools. SOC analyst detects suspicious activity between this laptop and a production database server

Update my malware detection and Endpoint Detection & Response (EDR) tools with the latest threat information

Network activity logs indicating uploads from this endpoint to AWS S3 buckets

Database logs show that this endpoint had accessed a database table with PII

How IBM Cloud Pak f ects data and workflows

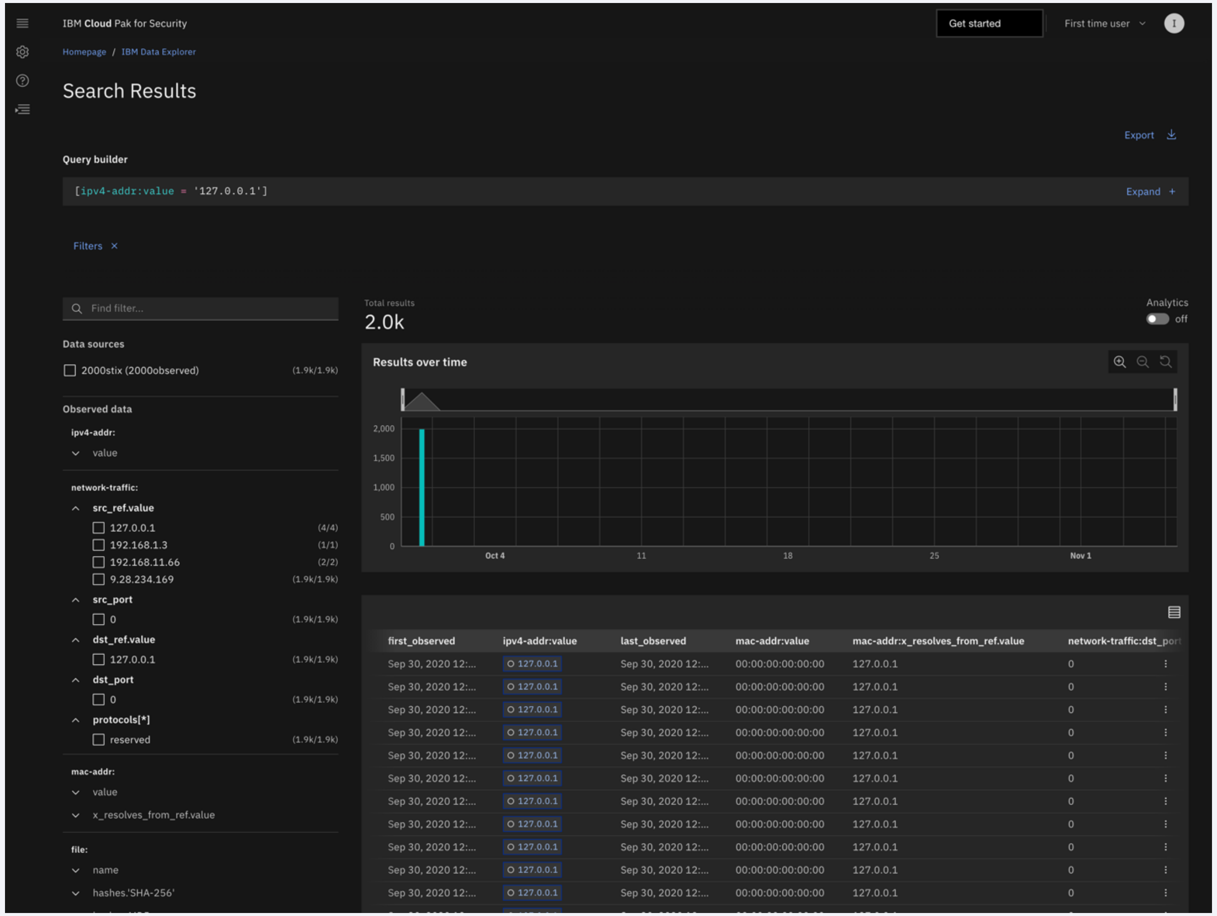


* May 2020

Data Explorer

Federated search & investigation

- **View all critical security data without moving it** using pre-built connectors to cloud and security data sources
- **Single query language (STIX) to investigate** across all data sources for threats, patterns, IOCs, and more
- **Automatically enriched data and attributes** with integrations into threat intelligence and the asset and risk database
- **Statistical insights without querying** provides immediate analysis on least common, most common, and potential outlier values
- **Seamless integration with SOAR cases** to share insights, searches, and findings
- **Expand data sources and capabilities** with SDK or IBM services to create new connectors



Search Results

Query builder

```
[ipv4-addr:value = '127.0.0.1']
```

Total results
2.0k

Data sources

□ 2000stix (2000observed)	(1.9k/1.9k)

Observed data

ipv4-addr:
value

network-traffic:

src_ref.value	
□ 127.0.0.1	(4/4)
□ 192.168.1.3	(1/1)
□ 192.168.11.66	(2/2)
□ 9.28.234.169	(1.9k/1.9k)
src_port	
□ 0	(1.9k/1.9k)
dst_ref.value	
□ 127.0.0.1	(1.9k/1.9k)
dst_port	
□ 0	(1.9k/1.9k)
protocols[*]	
□ reserved	(1.9k/1.9k)

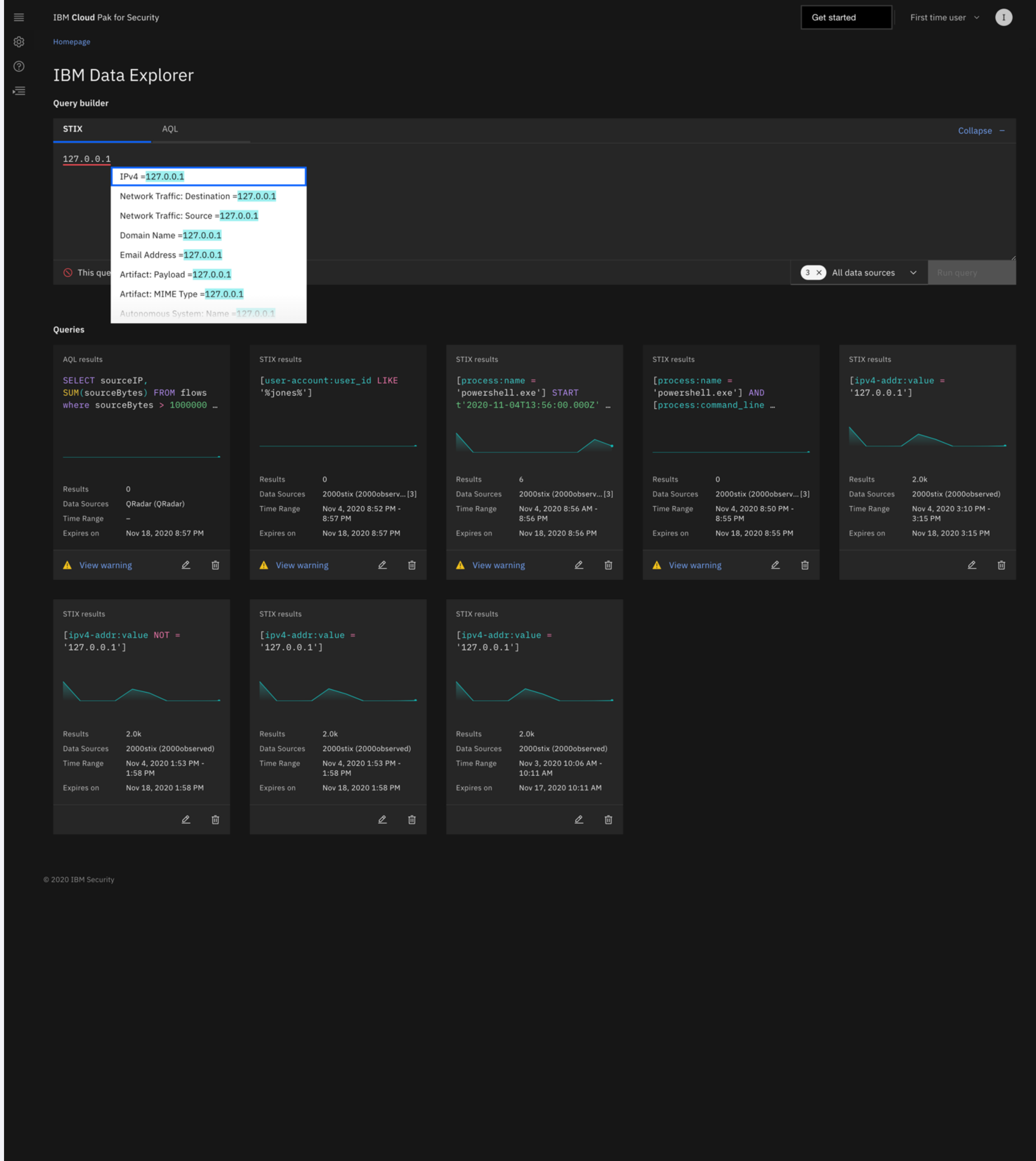
mac-addr:
value
x_resolves_from_ref.value

file:
name
hashes.'SHA-256'

first_observed	ipv4-addr:value	last_observed	mac-addr:value	mac-addr:x_resolves_from_ref.value	network-traffic:dst_port
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0

Querying in Data Explorer

- STIX is an open, standardized language to express cyber threat information – this is what we use to query data sources
- Data Explorer STIX query builder automatically recognizes values (IOC's, observables, etc.) and suggests the proper parameter to build a query
- What you can search for and what gets returned is dependent on each data source and what parameters are mapped
  (For example, a search for process names will return results from Carbon Black but will not return results from QRadar as that property it is not mapped in the QRadar connector)
- Full list of all mapped parameters can be found in the following: https://ibm.ent.box.com/v/supported-stix-attributes
- In CP4S 1.5, AQL search is available for users who have QRadar data sources connected and want an advanced querying capability for only QRadar data sources



IBM Data Explorer

Query builder

```
127.0.0.1
```

- IPv4 =127.0.0.1
- Network Traffic: Destination =127.0.0.1
- Network Traffic: Source =127.0.0.1
- Domain Name =127.0.0.1
- Email Address =127.0.0.1
- Artifact: Payload =127.0.0.1
- Artifact: MIME Type =127.0.0.1
- Autonomous System: Name =127.0.0.1

This que

Queries

AQL results

```
SELECT sourceIP,
SUM(sourceBytes) FROM flows
where sourceBytes > 1000000 …
```

Results 0
Data Sources QRadar (QRadar)
Time Range –
Expires on Nov 18, 2020 8:57 PM
View warning

STIX results

```
[user-account:user_id LIKE
'%jones%']
```

Results 0
Data Sources 2000stix (2000observ... [3]
Time Range Nov 4, 2020 8:52 PM - 8:57 PM
Expires on Nov 18, 2020 8:57 PM
View warning

STIX results

```
[process:name =
'powershell.exe'] START
t'2020-11-04T13:56:00.000Z' …
```

Results 6
Data Sources 2000stix (2000observ... [3]
Time Range Nov 4, 2020 8:56 AM - 8:56 PM
Expires on Nov 18, 2020 8:56 PM
View warning

STIX results

```
[process:name =
'powershell.exe'] AND
[process:command_line …
```

Results 0
Data Sources 2000stix (2000observ... [3]
Time Range Nov 4, 2020 8:50 PM - 8:55 PM
Expires on Nov 18, 2020 8:55 PM
View warning

STIX results

```
[ipv4-addr:value =
'127.0.0.1']
```

Results 2.0k
Data Sources 2000stix (2000observed)
Time Range Nov 4, 2020 3:10 PM - 3:15 PM
Expires on Nov 18, 2020 3:15 PM

STIX results

```
[ipv4-addr:value NOT =
'127.0.0.1']
```

Results 2.0k
Data Sources 2000stix (2000observed)
Time Range Nov 4, 2020 1:53 PM - 1:58 PM
Expires on Nov 18, 2020 1:58 PM

STIX results

```
[ipv4-addr:value =
'127.0.0.1']
```

Results 2.0k
Data Sources 2000stix (2000observed)
Time Range Nov 4, 2020 1:53 PM - 1:58 PM
Expires on Nov 18, 2020 1:58 PM

STIX results

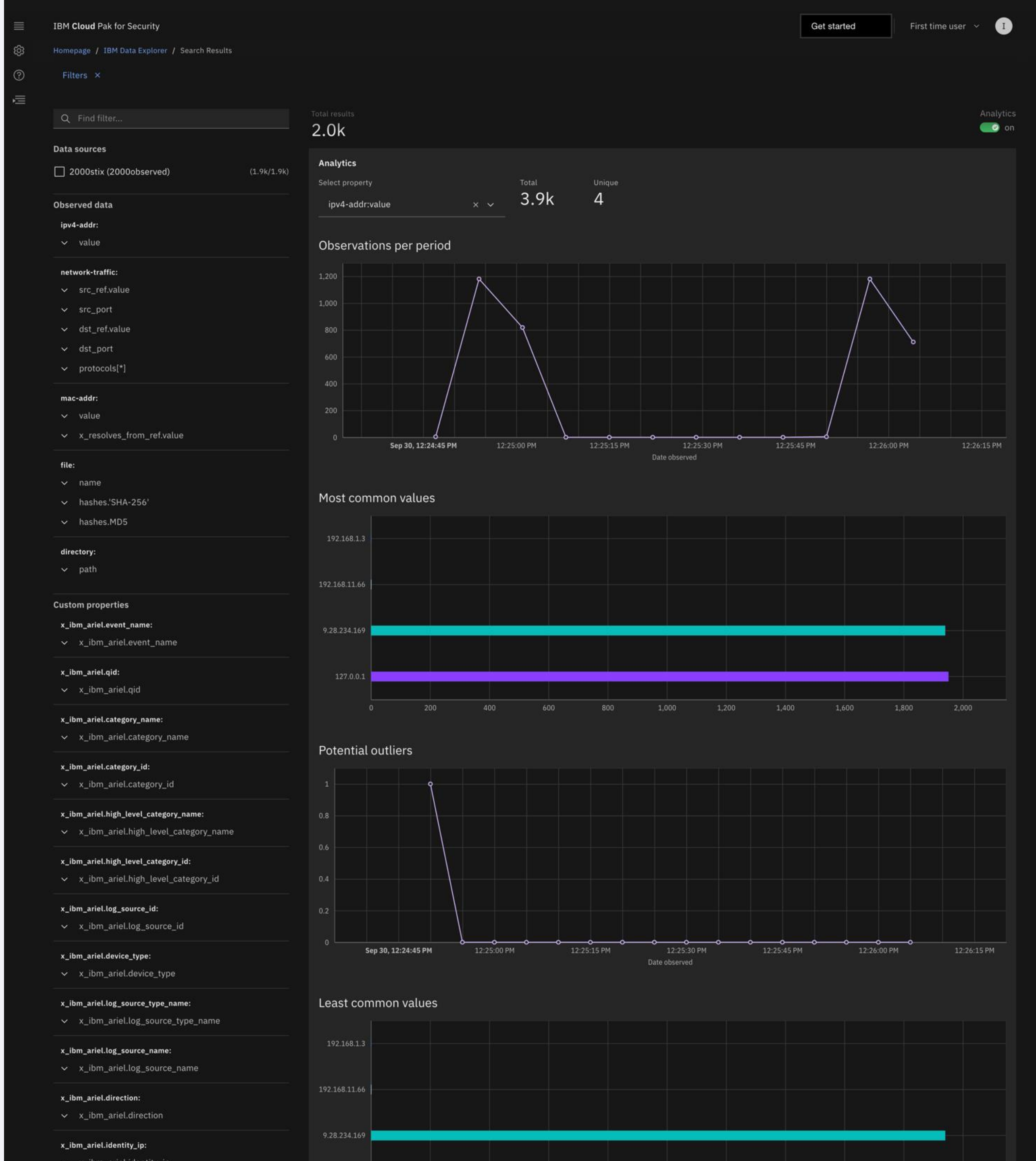
```
[ipv4-addr:value =
'127.0.0.1']
```

Results 2.0k
Data Sources 2000stix (2000observed)
Time Range Nov 3, 2020 10:06 AM - 10:11 AM
Expires on Nov 17, 2020 10:11 AM

© 2020 IBM Security

Results in Data Explorer

- Results can be viewed in either list view or table view. The list view shows all properties for an event in a single row whereas a table view condenses multiple events into multiple rows
- Filters on the left hand side enables users to view all mapped properties and values in the results, see counts of each value, and narrow down the result set without writing additional queries – check the filter to apply IS filter, use the three dot on the right of the filter to apply IS NOT
- Right click on values to bring up a menu that enables you to apply a IS filter, IS NOT filter, copy value, and add to case
- Decorated values (IP’s, Hashes) can be selected to bring information from threat intelligence and connected asset and risk database
- Analytics module (on upper right) opens statistical analysis tables and graphs (least common, most common, potential outliers, values over time)
- Results can be exported into CSV or JSON



IBM Cloud Pak for Security

Homepage / IBM Data Explorer / Search Results

Total results: 2.0k

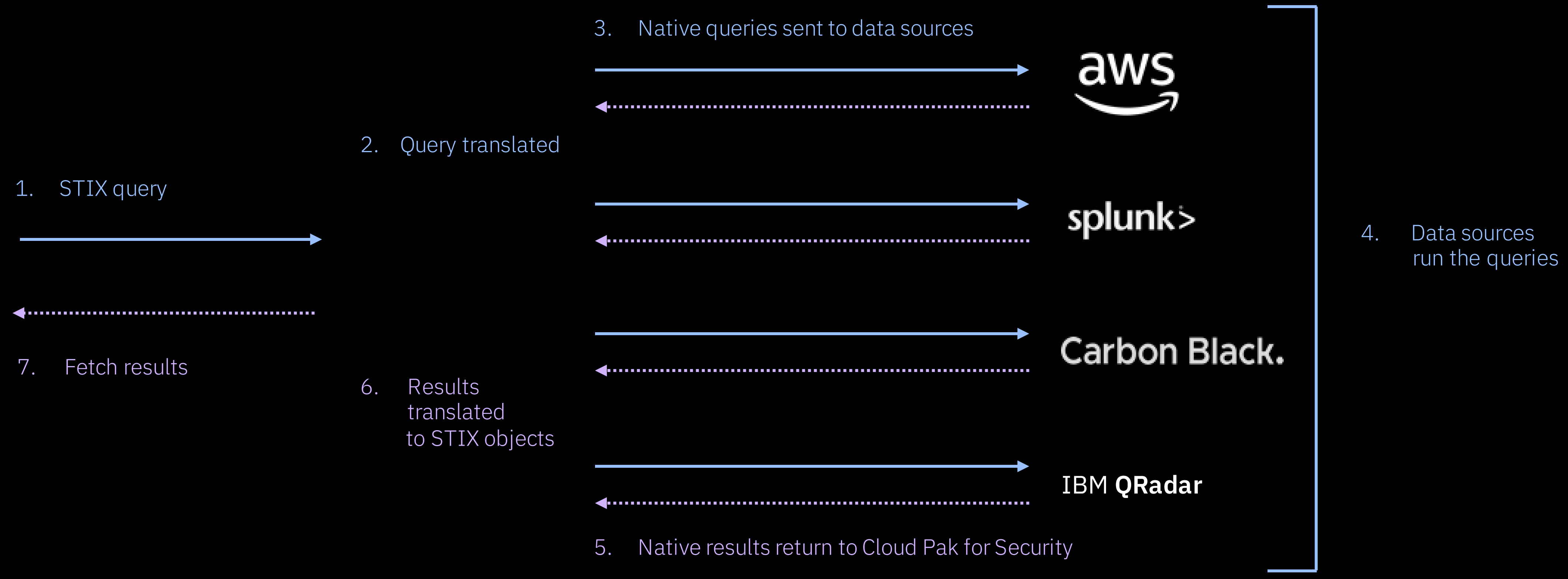
Analytics: on

Select property: ipv4-addr:value

Total: 3.9k

Unique: 4

STIX Shifter – How it works


3. Native queries sent to data sources
2. Query translated
1. STIX query
aws
splunk>
4. Data sources run the queries
Carbon Black.
7. Fetch results
6. Results translated to STIX objects
IBM QRadar
5. Native results return to Cloud Pak for Security

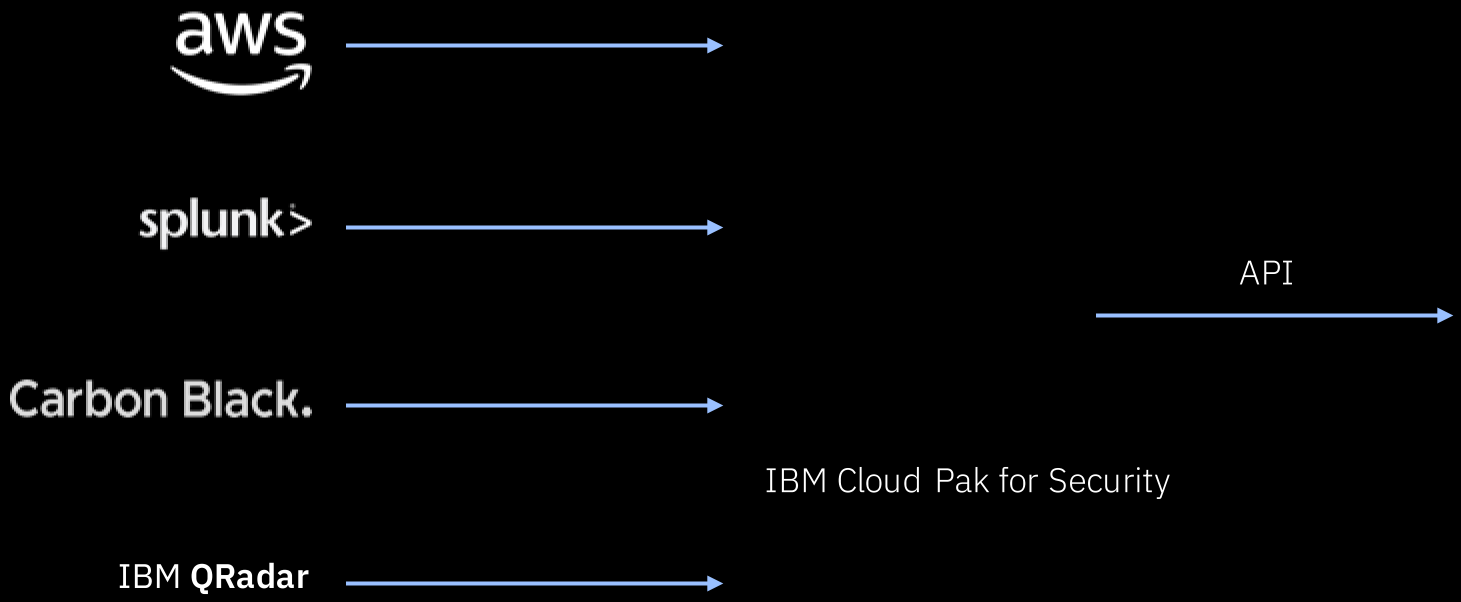
1. Federated query using a STIX pattern
2. Query is translated to the native query language of each of the data sources
3. The converted query is then sent (transmitted) to all data sources
4. Each data source runs its own native query
5. The native query results are then returned from the data source
6. Returned results translated into STIX Objects (basically a JSON structure)
7. The STIX Objects are then stored in the cloud where they are used by other services

Connect Asset Risk (CAR)

Collect and consolidate risk posture across assets, vulnerabilities, and users

Scheduled feed of asset and risk information

Can be a script that runs once a day on each of these data sources



Technical Preview

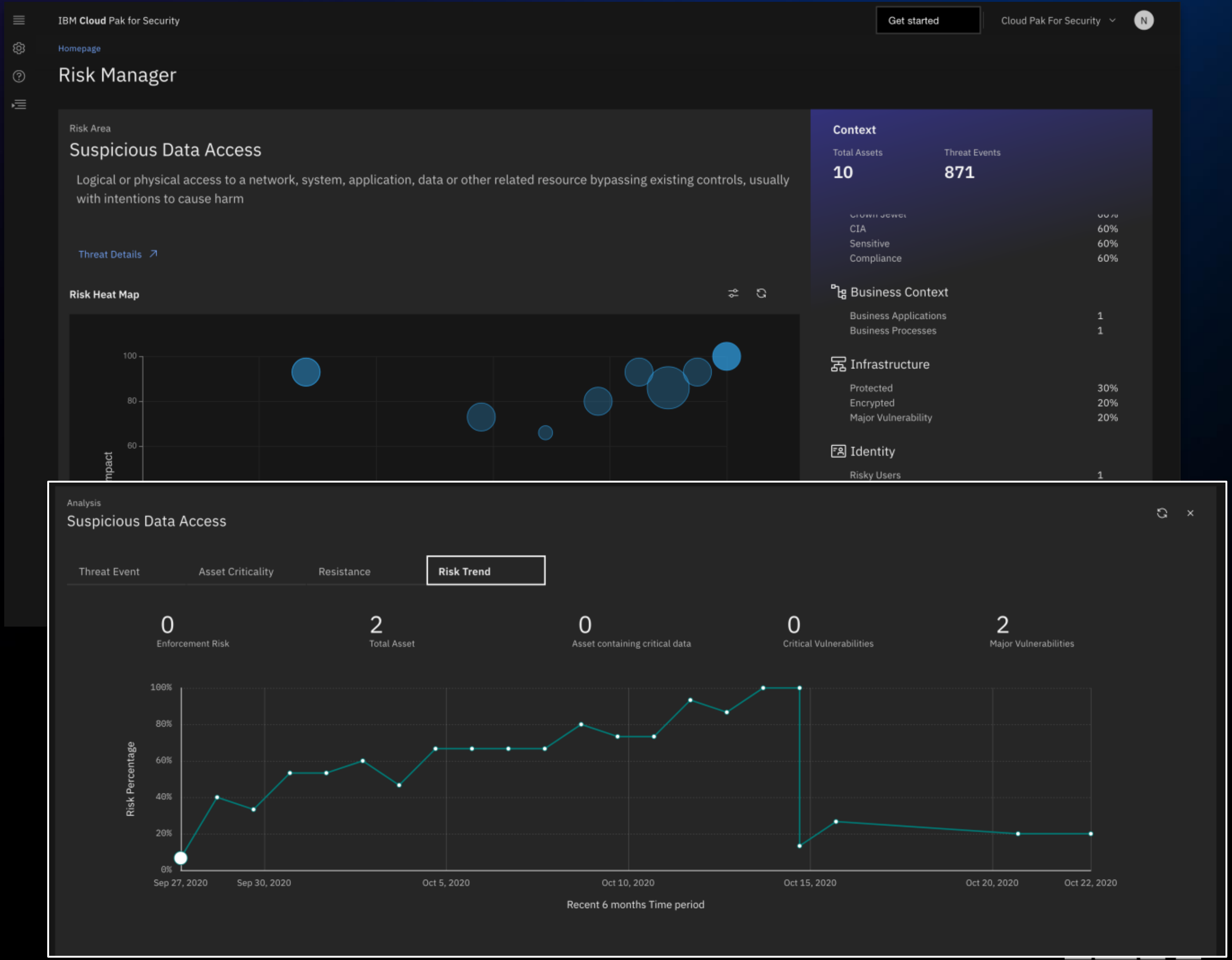
IBM Security Risk Manager for IBM Cloud Pak for Security

Get early visibility into potential security risks by correlating insights across risk vectors and asset criticality

- **Unified view of disparate risk metrics**
  Visualize indicators of consolidated risk from security tools. Investigate impact indicators such as the criticality of the asset to the business or likelihood of a threat event occurring.

- **Common definition of risk**
  Gain clarity into the significance and urgency of your risk areas. The solution's risk scoring engine uses a single definition of risk across sources of vulnerabilities and threats to contextualize risk data.

- **Prioritize remediation management**
  Understand the factors contributing to overall security risk, prioritize and take remedial action to mitigate or reduce identified risk



Risk Manager

Risk Area

Suspicious Data Access

Logical or physical access to a network, system, application, data or other related resource bypassing existing controls, usually with intentions to cause harm

Risk Heat Map

Context

Total Assets 10

Threat Events 871

CIA	60%
Sensitive	60%
Compliance	60%

Business Context

Business Applications	1
Business Processes	1

Infrastructure

Protected	30%
Encrypted	20%
Major Vulnerability	20%

Identity

Risky Users	1

Analysis

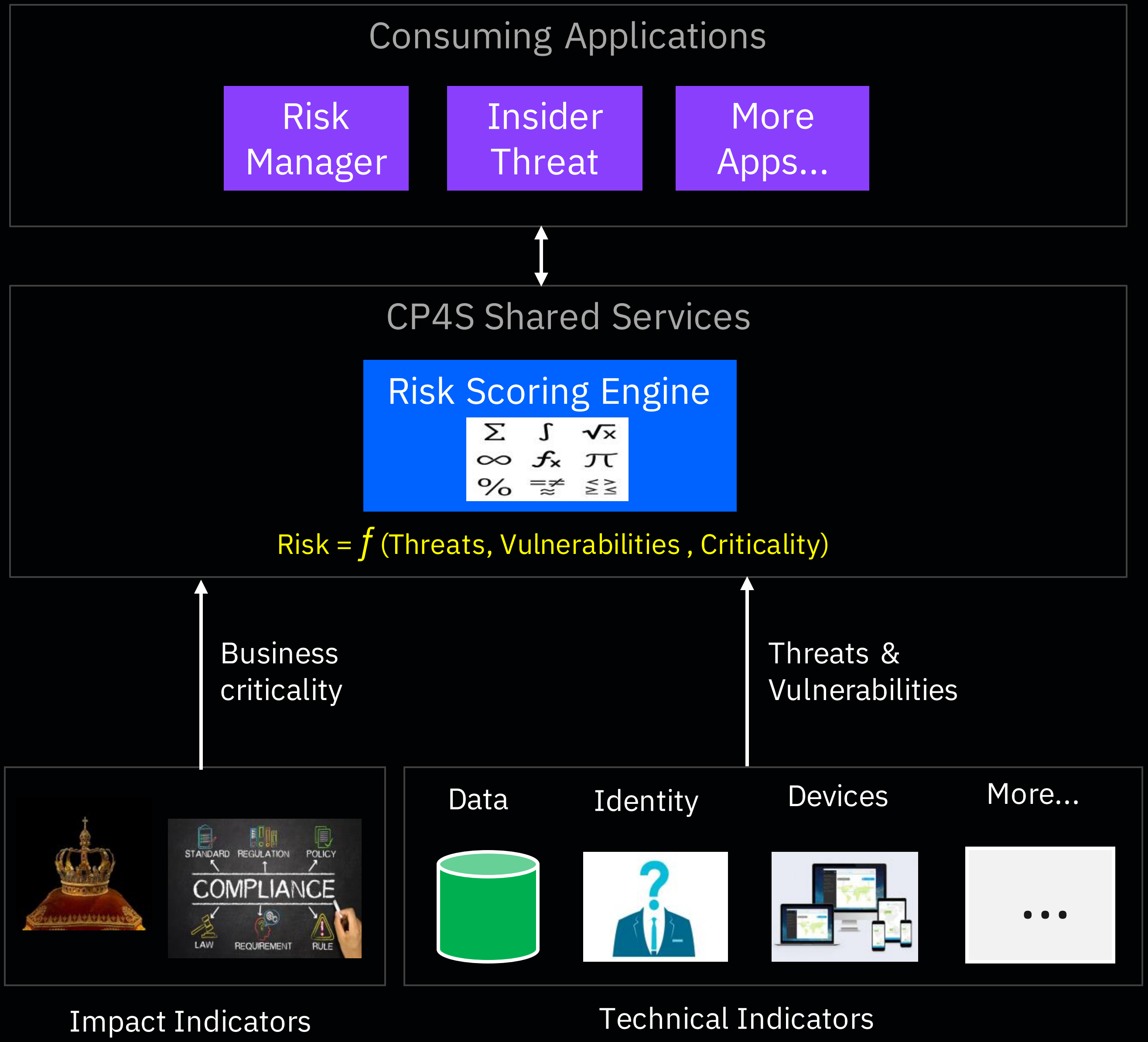
Suspicious Data Access

Enforcement Risk	Total Asset	Asset containing critical data	Critical Vulnerabilities	Major Vulnerabilities
0	2	0	0	2

IBM Security

IBM

Vision for Cross-Domain/Multi-dimensional Risk Engine



Consuming Applications

Risk Manager

Insider Threat

More Apps…

CP4S Shared Services

Risk Scoring Engine

Risk = *ƒ* (Threats, Vulnerabilities , Criticality)

Business criticality

Threats & Vulnerabilities

Data

Identity

Devices

More…

Impact Indicators

Technical Indicators

Objective

Offer a flexible cross-domain and multi-dimensional Risk engine that can be consumed by multiple Apps, Communicating risk uniformly and consistently.

Domain ╲ Dimension	Data	Identity	Devices	More…
Threats	Factors (DBA)	Factors (Risky User)	Factors (Malware)	Factors
Vulnerabilities	Factors (Public privilege)	Factors (access Certification)	Factors (rooted)	Factors
Criticality	Factors (GDPR)	Factors (SoD)	Factors (BYoD)	Factors

Key attributes

- Cross-domain view of risk
- Intra-domain view of risk
- Explainability: how risk score is derived and why did it change over time?
- Adaptability: customize risk to suit own needs such as adding domains, adding dimensions, adding factors and even risk equation parameters

The complexity of threat management

Email

Endpoints

Network

Threat intelligence

Application activity

Vulnerabilities

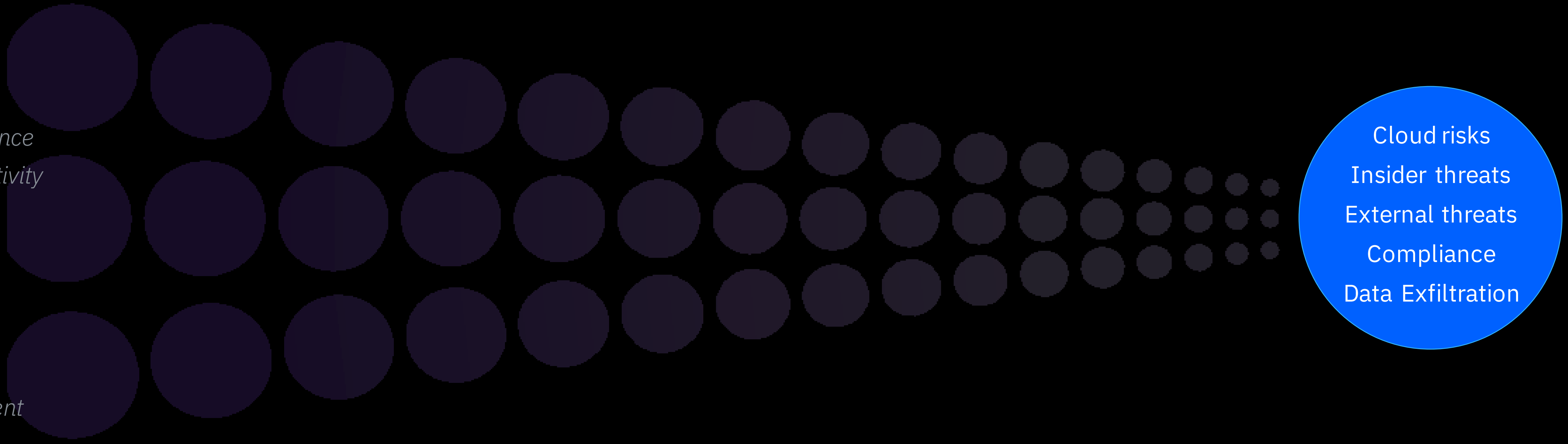
Users

Cloud

Data lake

SIEM

Log management



Cloud risks

Insider threats

External threats

Compliance

Data Exfiltration

SOC analysts need help with...

Visibility

- Normalization
- Categorization
- Enrichment
- Operationalize data at rest
- Network, endpoint, cloud, user and application

Detection

- MITRE ATT&CK®
- Models
- Behavior chaining
- Global threat intelligence

Investigation

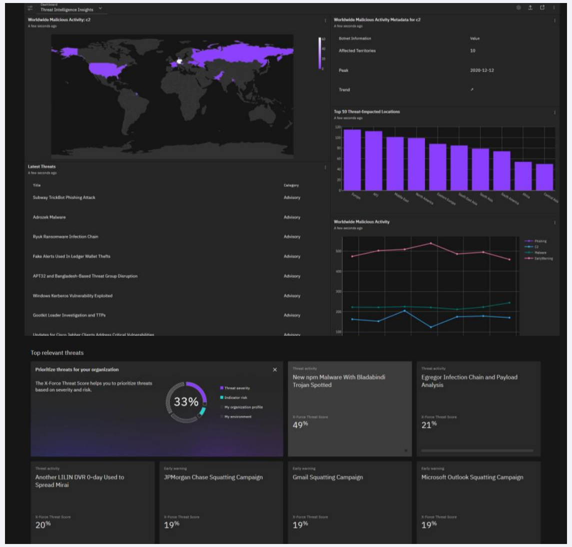
- AI
- Link analysis
- Data mining
- Supervised learning
- Unstructured data analysis
- Federated search

Response

- Dynamic playbooks
- Automation
- Orchestration
- Privacy breach reporting

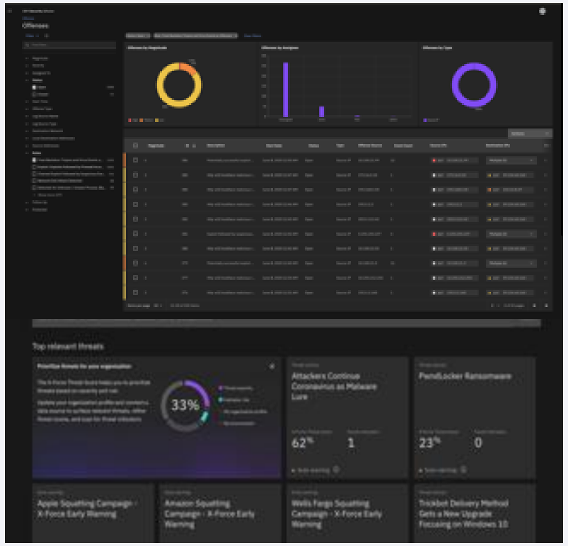
Unifying threat management with IBM Security

Visibility



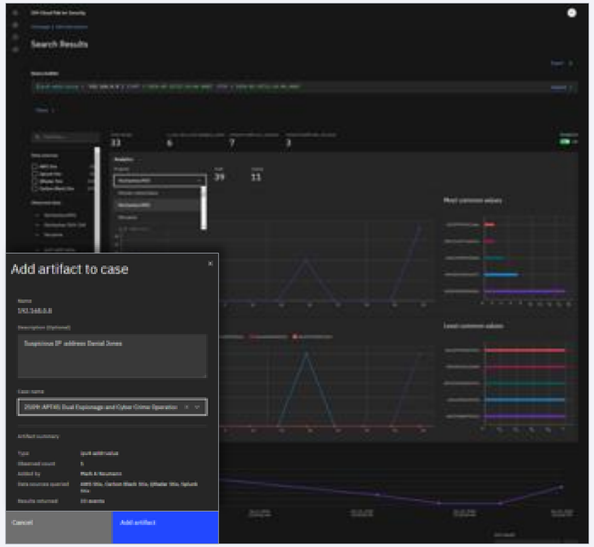
Connect to on-premise and cloud data sources and customize dashboards for comprehensive visibility

Detection



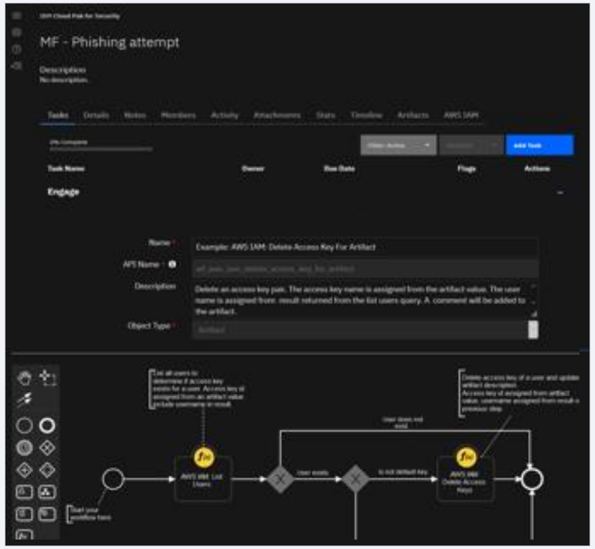
Isolate threats and reduce false positives, to track threats as they progress

Investigation



Run federated searches and collaborate through integrated Case Management, for automatic alert investigation

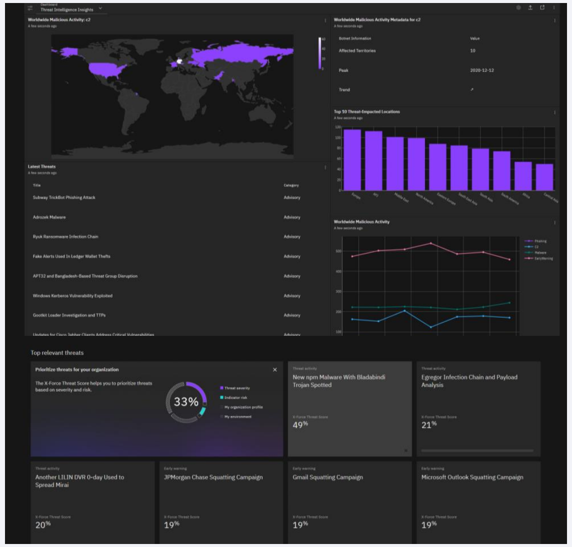
Response



Respond faster with out of the box playbooks, built-in orchestration and automation, including Ansible

Outcomes of threat management solutions

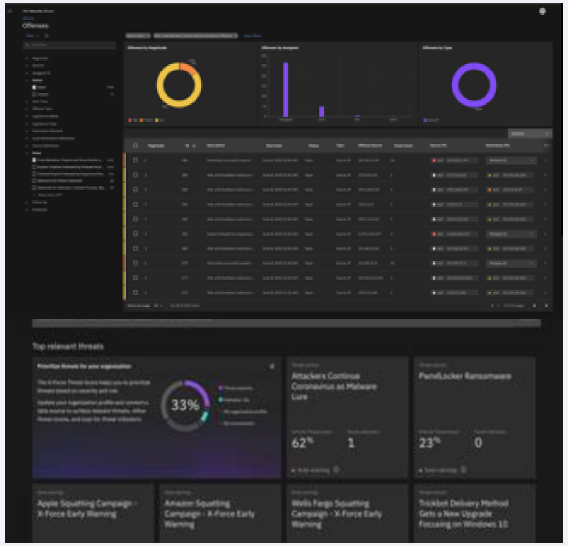
Visibility



600+

validated integrations to reduce risk and MTTD

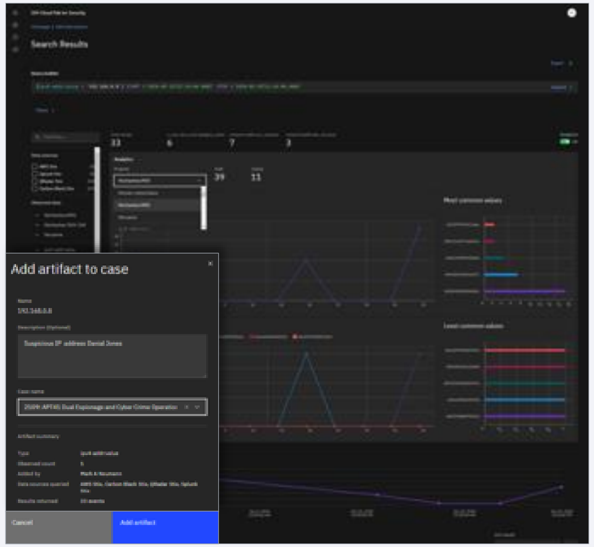
Detection



51%

increase in ability to detect attacks

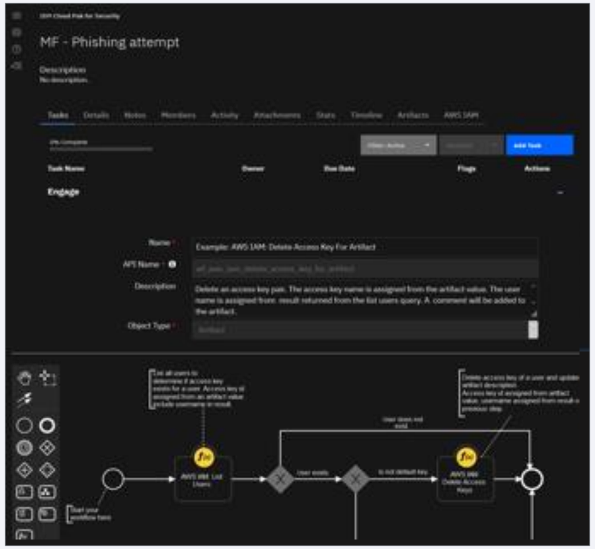
Investigation



60x

improvement in threat investigation time

Response



8x

increase in speed to respond to security incidents

Visibility

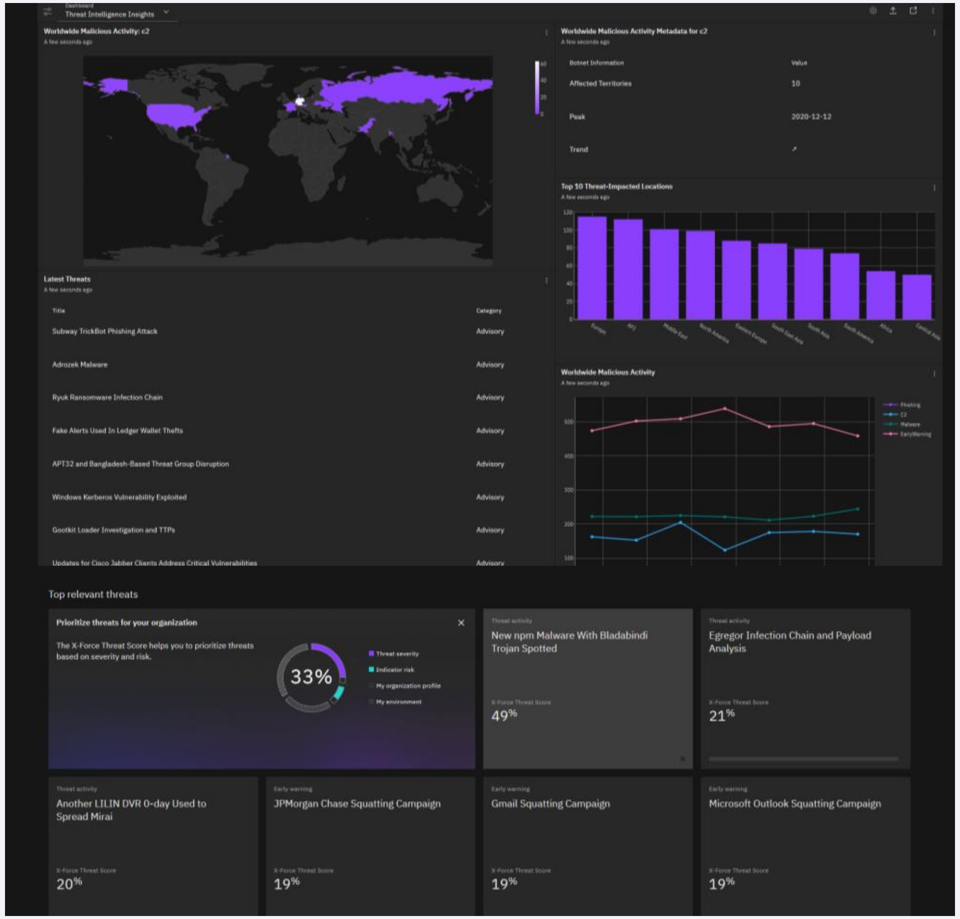
Gain comprehensive visibility into enterprise-wide data

Visibility into cloud usage and risks

Real-time insights into user behavior

Expose threats as they move across the network

Endpoint visibility with Sysmon



Worldwide Malicious Activity Metadata for c2

A few seconds ago

Botnet Information	Value
Affected Territories	10
Peak	2020-12-12
Trend	↗

Latest Threats

A few seconds ago

Title	Category
Subway TrickBot Phishing Attack	Advisory
Adrozek Malware	Advisory
Ryuk Ransomware Infection Chain	Advisory
Fake Alerts Used In Ledger Wallet Thefts	Advisory
APT32 and Bangladesh-Based Threat Group Disruption	Advisory
Windows Kerberos Vulnerability Exploited	Advisory
Gootkit Loader Investigation and TTPs	Advisory
Updates for Cisco Jabber Clients Address Critical Vulnerabilities	Advisory

Top relevant threats

Prioritize threats for your organization

The X-Force Threat Score helps you to prioritize threats based on severity and risk.

33%

- Threat severity
- Indicator risk
- My organization profile
- My environment

Threat activity
New npm Malware With Bladabindi Trojan Spotted
X-Force Threat Score
49%

Threat activity
Egregor Infection Chain and Payload Analysis
X-Force Threat Score
21%

Threat activity
Another LILIN DVR 0-day Used to Spread Mirai
X-Force Threat Score
20%

Early warning
JPMorgan Chase Squatting Campaign
X-Force Threat Score
19%

Early warning
Gmail Squatting Campaign
X-Force Threat Score
19%

Early warning
Microsoft Outlook Squatting Campaign
X-Force Threat Score
19%

> “QRadar drastically reduced the time it took us to connect our 100+hybrid multi-cloud accounts to QRadar. This made it easy to consume both events and network flow traffic from our AWS and other cloud environments.”
>
> Large US-based Insurance Company

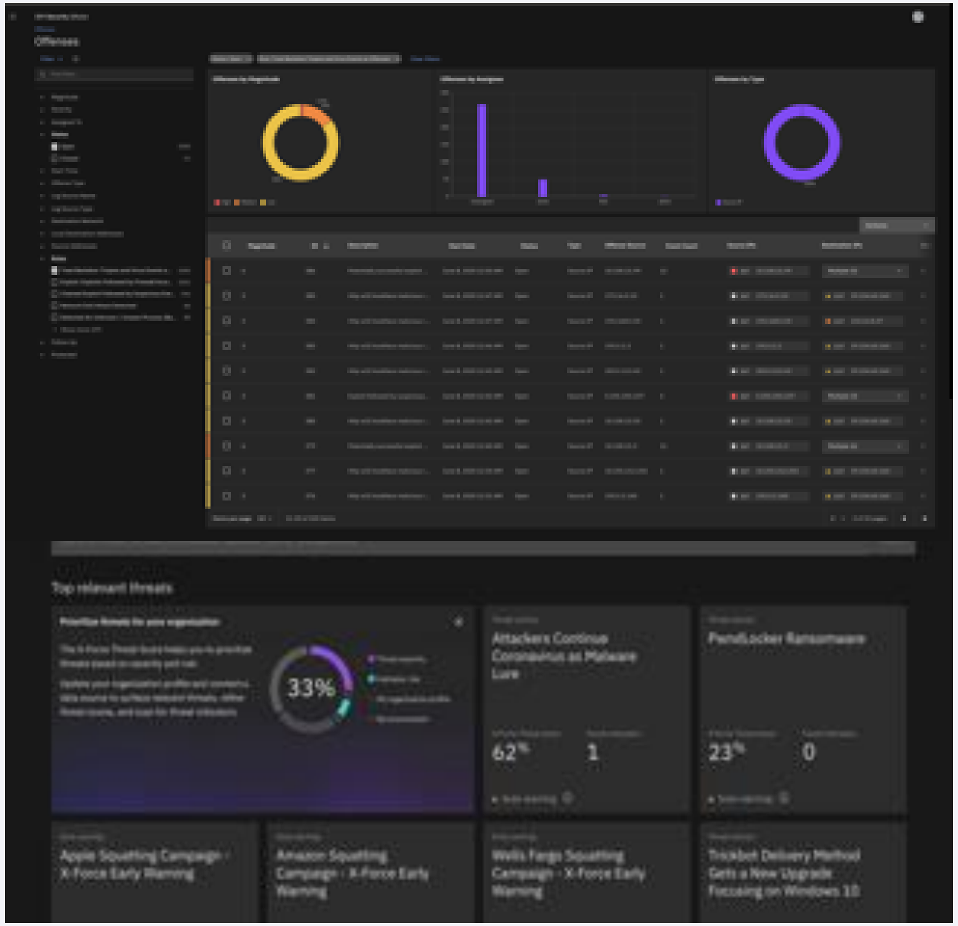
Track threats as they progress, prioritize critical events and investigate potential incidents

Identify known and unknown threats

Real time detection across 100’s of security use cases

Dynamically adjust as attacks unfold

Automatically link multiple malicious behaviors


Offenses
Top relevant threats
33%
Attackers Continue Coronavirus as Malware Lure
62%
1
PwndLocker Ransomware
23%
0
Apple Squatting Campaign - X-Force Early Warning
Amazon Squatting Campaign - X-Force Early Warning
Wells Fargo Squatting Campaign - X-Force Early Warning
Trickbot Delivery Method Gets a New Upgrade Focusing on Windows 10

> “IBM QRadar improves the speed and effectiveness of detecting threats by nearly 75%.”
>
> Forrester

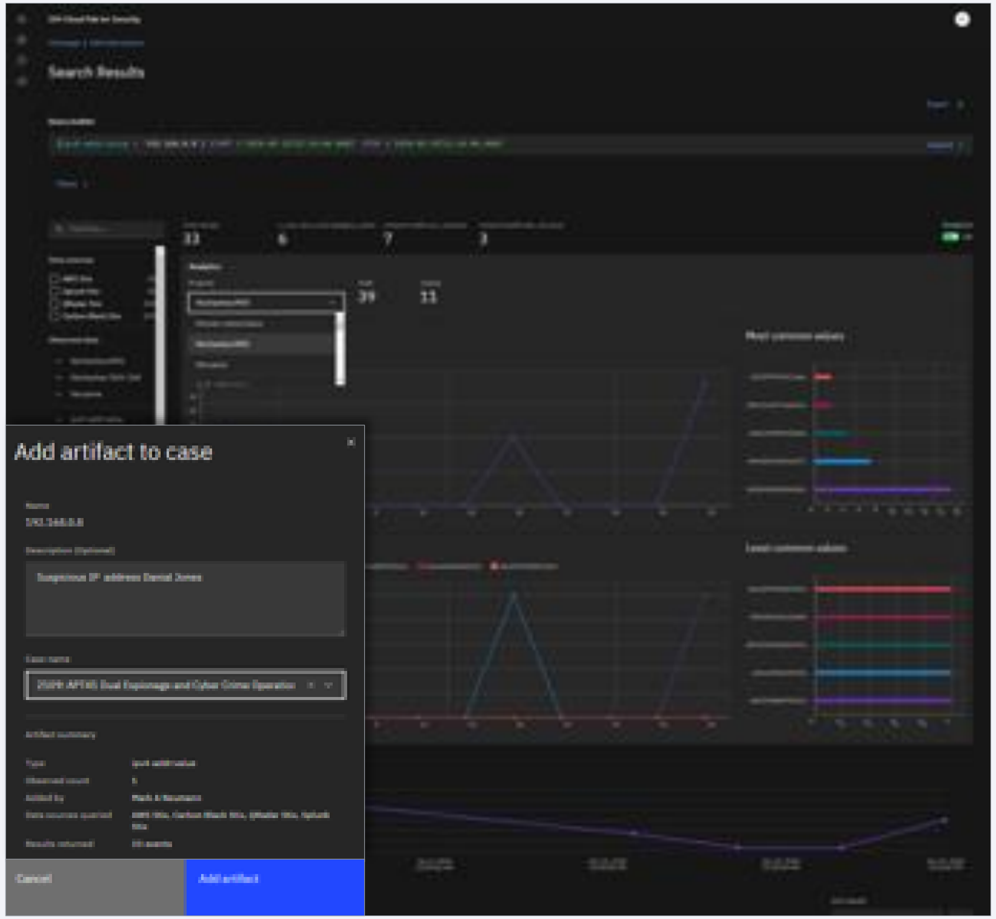
Automated alert investigation driving faster more consistent and accurate responses

Let Watson automatically determine threat priorities

Map investigations to MITRE ATT&CK tactics and techniques

Understand the source and impact of the attack so you can respond effectively

Provide recommendations based on past outcomes in your environment



Name
192.168.0.8

Description (Optional)
Suspicious IP address Daniel Jones

Case name
2019: APT41 Dual Espionage and Cyber Crime Operation

Artifact summary

> “QRadar offers strong support for incident investigation by providing context enrichment from internal and external sources, suggesting next steps based on attacker actions and prioritizing alerts for further action.”
>
> Gartner

Response

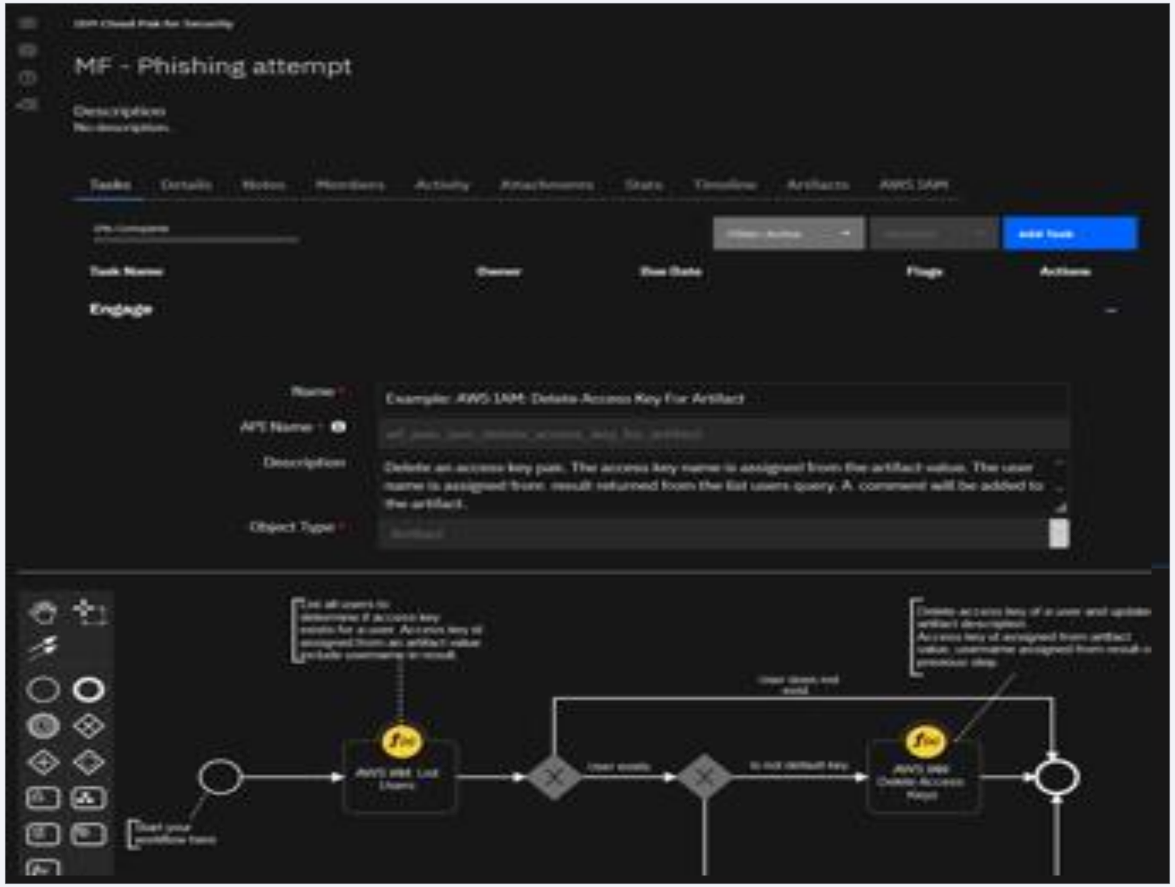
Single hub for SOC operations that allows you to outsmart, outpace and outmaneuver threats

Guided response and case management to help analysts

Align compliance and privacy through breach reporting support

Act fast with automation and orchestration across security and IT Ops tools

Measure results, improve visibility with incident and SOC dashboards



IBM Cloud Pak for Security
Tasks
Details
Notes
Members
Activity
Attachments
Stats
Timeline
Artifacts
AWS IAM
Add Task
Task Name
Owner
Due Date
Flags
Actions

MF - Phishing attempt

Description
No description.

Engage

Name: Example: AWS IAM: Delete Access Key For Artifact

API Name: [illegible]

Description: Delete an access key pair. The access key name is assigned from the artifact value. The user name is assigned from result returned from the list users query. A comment will be added to the artifact.

Object Type: Artifact

List all users to determine if access key exists for a user. Access key is assigned from an artifact value include username in result.
Delete access key of a user and update artifact description.
Access key is assigned from artifact value, username assigned from result of previous step.
User does not exist
User exists
Is not default key
AWS IAM: List Users
AWS IAM: Delete Access Keys
Start your workflow here

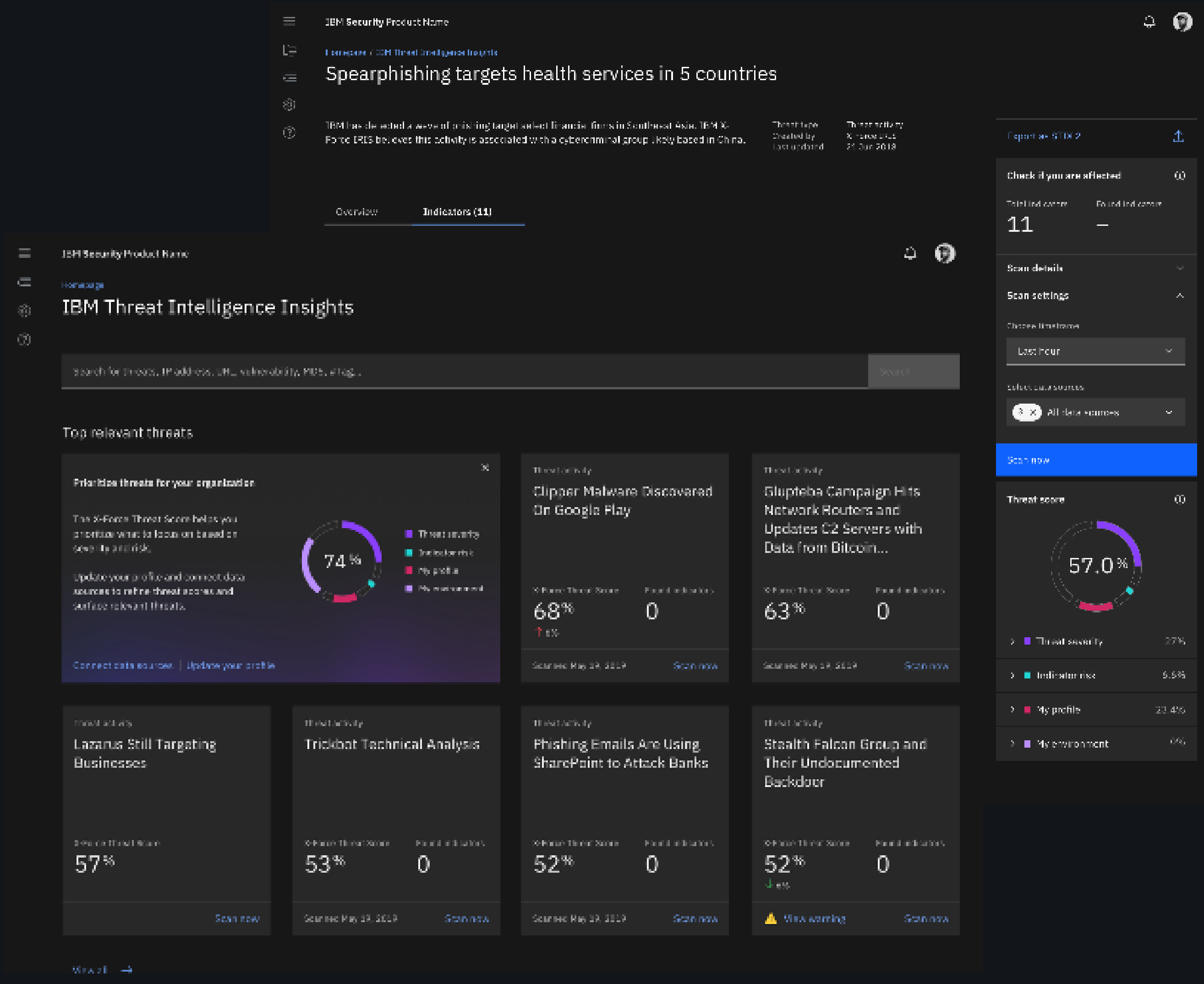
“We refer to the whole IBM ecosystem as a force multiplier; we’ve evolved into an organization with a completely comprehensive and dynamic program around security incident response”

Brian Herr, Chief Security and Privacy Officer, Secure-24

Threat Intelligence Insights

Prioritized, actionable threat intelligence

- **Act upon threat intelligence** with the X-Force Premium Threat Intelligence Reports, which provide contextual information curated by IBM X-Force IRIS team
- **Prioritize threats** with X-Force Threat Score, an adaptive score, calculated based on your relevance, severity, penetration, impact and actual environmental sightings
- **Identify threats active in your environment** with Am I Affected, which runs continuous and automated searches across connected data sources
- **Work from a single console** to investigate threats and indicators of compromise (IOCs) seamlessly across multiple siloed solutions and remediate cyber threats



IBM Security Product Name

Homepage / IBM Threat Intelligence Insights

Spearphishing targets health services in 5 countries

IBM has detected a wave of phishing target select financial firms in Southeast Asia. IBM X-Force IRIS believes this activity is associated with a cybercriminal group likely based in China.

Threat type: Threat activity
Created by: X-Force IRIS
Last updated: 21 Jun 2019

Overview | Indicators (11)

Export as STIX 2

Check if you are affected
Total indicators: 11
Found indicators: –

Scan details

Scan settings

Choose timeframe: Last hour

Select data sources: All data sources

Scan now

Threat score: 57.0%

Threat severity	27%
Indicator risk	6.6%
My profile	23.4%
My environment	0%

IBM Security Product Name

Homepage

IBM Threat Intelligence Insights

Search for threats, IP address, URL, vulnerability, MD5, string...

Top relavant threats

Prioritize threats for your organization

The X-Force Threat Score helps you prioritize what to focus on based on severity and risk.

Update your profile and connect data sources to refine threat scores and surface relevant threats.

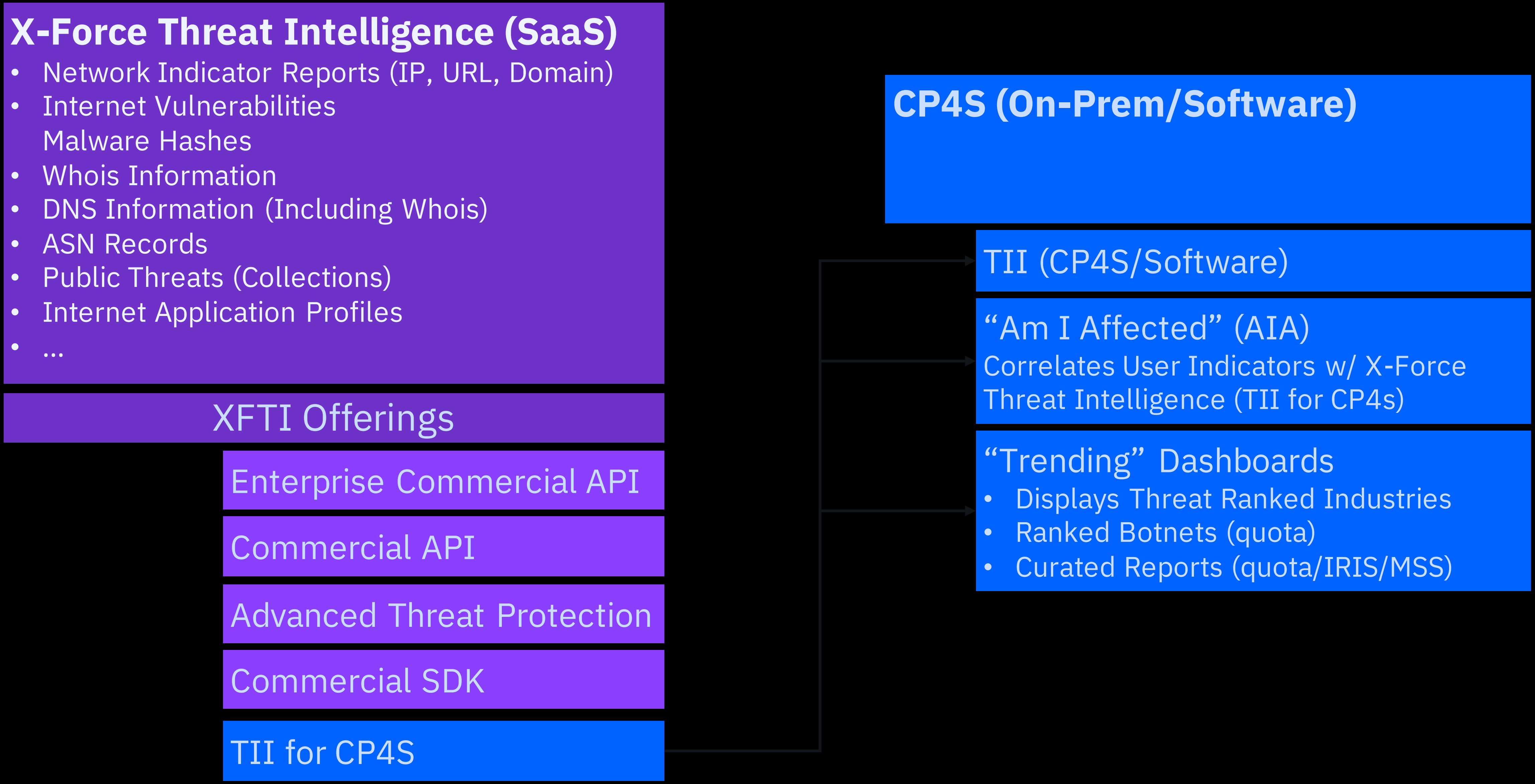
74%: Threat severity, Indicator risk, My profile, My environment

Connect data sources | Update your profile

Threat activity	X-Force Threat Score	Found indicators	
Clipper Malware Discovered On Google Play	68% ↑ 6%	0	Scanned May 19, 2019 · Scan now
Glupteba Campaign Hits Network Routers and Updates C2 Servers with Data from Bitcoin...	63%	0	Scanned May 19, 2019 · Scan now
Lazarus Still Targeting Businesses	57%		Scan now
Trickbot Technical Analysis	53%	0	Scanned May 19, 2019 · Scan now
Phishing Emails Are Using SharePoint to Attack Banks	52%	0	Scanned May 19, 2019 · Scan now
Stealth Falcon Group and Their Undocumented Backdoor	52% ↓ 6%	0	⚠ View warning · Scan now

View all →

Threat Intelligence Insights for CP4S



X-Force Threat Intelligence (SaaS)

- Network Indicator Reports (IP, URL, Domain)
- Internet Vulnerabilities
  Malware Hashes
- Whois Information
- DNS Information (Including Whois)
- ASN Records
- Public Threats (Collections)
- Internet Application Profiles
- …

XFTI Offerings

Enterprise Commercial API

Commercial API

Advanced Threat Protection

Commercial SDK

TII for CP4S

CP4S (On-Prem/Software)

TII (CP4S/Software)

“Am I Affected” (AIA)
Correlates User Indicators w/ X-Force Threat Intelligence (TII for CP4s)

“Trending” Dashboards

- Displays Threat Ranked Industries
- Ranked Botnets (quota)
- Curated Reports (quota/IRIS/MSS)

CP4S Platform Roles & Threat Intelligence Insights (TII)

Fit-for-Purpose User Management

Platform Roles

Cloud Pak for Security
Administrator
User

Application Roles

Threat Intelligence Insights
Administrator
User

Data Explorer
Administrator
User

Platform Roles: enable CP4S Account Admins to assign users to *platform roles* permitting management and monitoring of CP4S, and to assign Application Admin Role to CP4S users, assigning an Application Admin to Threat Intelligence Insights , who in turn can provide user's access to TII and it's entitlement.

TII Features and Functionality

	TII Core App + Standard package	Advanced package
Am I Affected scanning	Manual ad-hoc scanning	Automatic & Manual ad-hoc scanning
Threats: Threat Intelligence Creator/Editor	✓	✓
Data Explorer and Cases integrations	✓	✓
X-Force Exchange Classic content	✓	✓
X-Force Risk Score	✓	✓
Threat activity (IRIS report)	5 Threat Activity Reports	✓ Unlimited reporting
Malware analysis (IRIS report)	1 Malware Analysis Report	✓ Unlimited reporting
DNS Early warning reports	1 DNS EW Predefined Report	✓ Unlimited reporting
Threat groups (IRIS report)	1 Full IRIS Predefined Report	✓ Unlimited reporting
Industry analysis (IRIS report)	1 Full IRIS Predefined Report	✓ Unlimited reporting

Capabilities to assist with cross-cutting use cases

Data Explorer

- View all critical security data without moving it
- Single query language (STIX)
- Automatically enriched data and attributes
- Statistical insights without querying
- Seamless integration with SOAR cases

SOAR

- Reduce time to respond to and remediate
- Streamline and automate
- Guide and execute investigation and response actions consistently
- Customize and extend dynamic playbooks
- Meet compliance requirements with a Privacy add-on

User Behavior Analytics

- Quickly identify risky users associated to insider threats from within CP4S as part of an end-to-end threat management workflow
- Expose QRadar UBA in CP4S enriching unified threat management workflow in CP4S with insider threat
- Integrated with case management and data explorer

Threat Intelligence Insights

- Gain global threat intelligence
- Prioritize threats for your organization with the X-Force Threat Score
- Identify and act on threats active in your environment with Am I Affected
- Infuse third-party threat intelligence feeds to reuse investment in additional threat intelligence

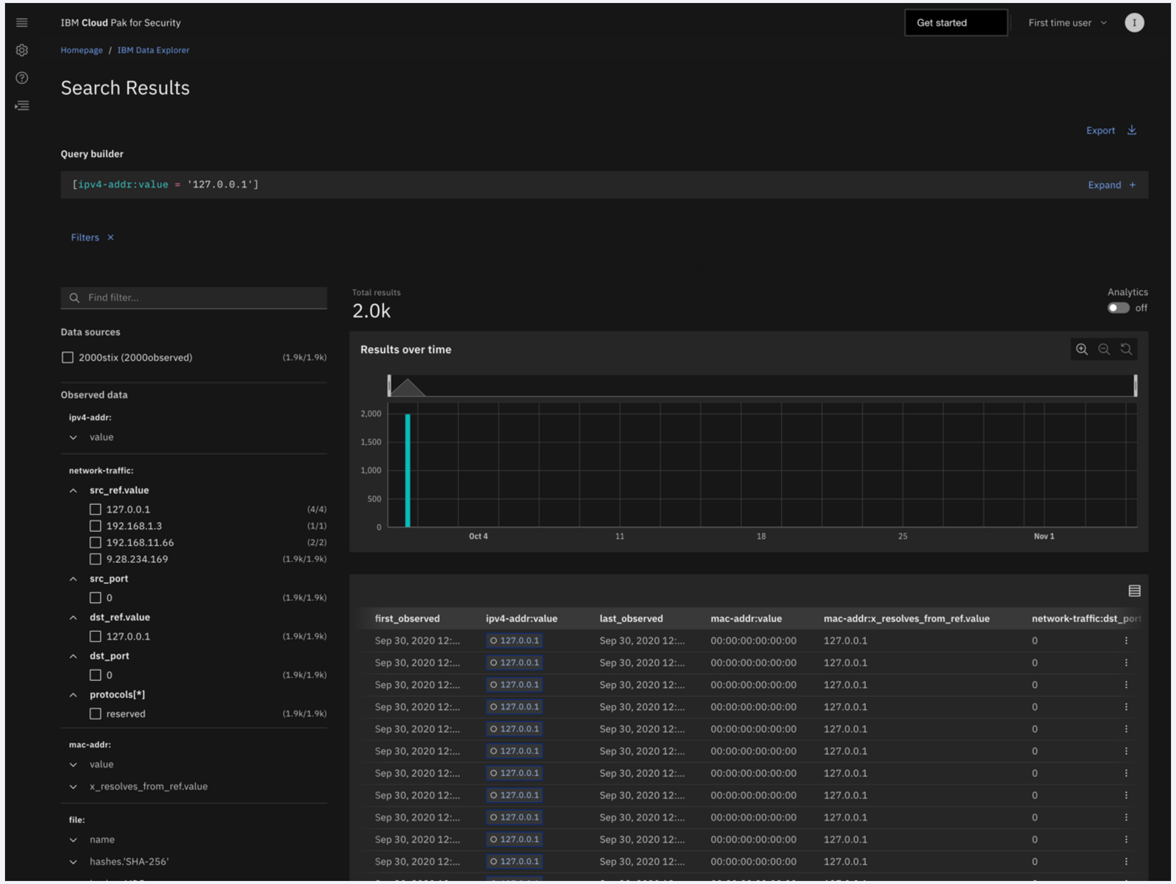
Risk Manager

- An integrated view of risk posture presented in a business-consumable dashboard
- Get early visibility into potential security risks by correlating insights across risk domains
- Visualize what risks have the biggest impact potential
- Quantify and communicate security risk information using common language

Data Explorer

Federated search and investigation

- **View all critical security data without moving it** using pre-built connectors to cloud and security data sources
- **Single query language (STIX) to investigate** across all data sources for threats, patterns, IOCs, and more
- **Automatically enriched data and attributes** with integrations into threat intelligence and the asset and risk database
- **Statistical insights without querying** provides immediate analysis on least common, most common, and potential outlier values
- **Seamless integration with SOAR cases** to share insights, searches, and findings
- **Expand data sources and capabilities** with SDK or IBM services to create new connectors



Search Results

Query builder

```
[ipv4-addr:value = '127.0.0.1']
```

Find filter...

Total results
2.0k

Data sources

□ 2000stix (2000observed) (1.9k/1.9k)

Observed data

ipv4-addr:
value

network-traffic:
src_ref.value
□ 127.0.0.1 (4/4)
□ 192.168.1.3 (1/1)
□ 192.168.11.66 (2/2)
□ 9.28.234.169 (1.9k/1.9k)
src_port
□ 0 (1.9k/1.9k)
dst_ref.value
□ 127.0.0.1 (1.9k/1.9k)
dst_port
□ 0 (1.9k/1.9k)
protocols[*]
□ reserved (1.9k/1.9k)

mac-addr:
value
x_resolves_from_ref.value

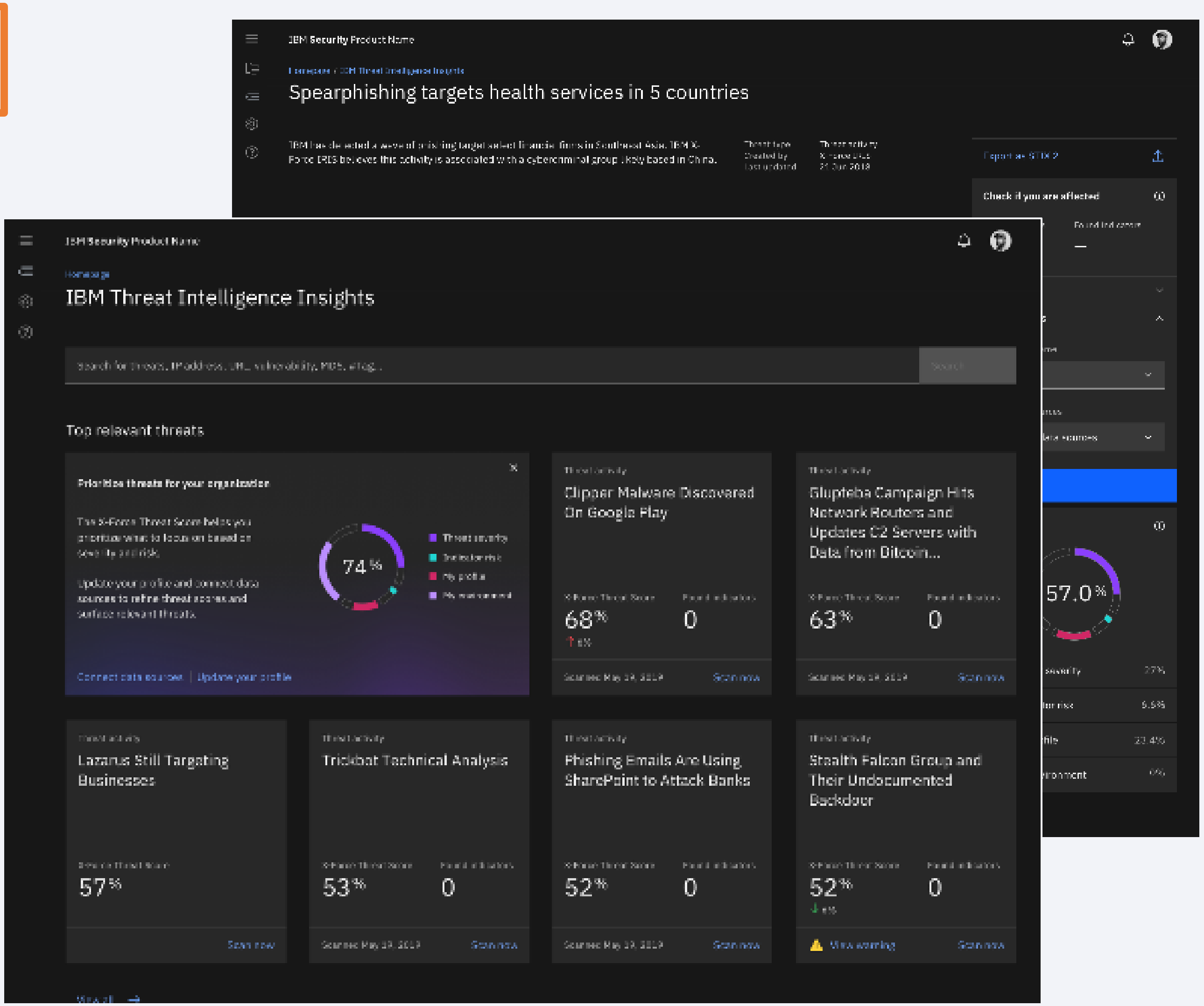
file:
name
hashes.'SHA-256'

first_observed	ipv4-addr:value	last_observed	mac-addr:value	mac-addr:x_resolves_from_ref.value	network-traffic:dst_port
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0
Sep 30, 2020 12:...	127.0.0.1	Sep 30, 2020 12:...	00:00:00:00:00:00	127.0.0.1	0

Threat Intelligence Insights

Prioritized, actionable threat intelligence

- **Gain global threat intelligence** through reports with contextual information curated by the IBM X-Force team
- **Prioritize threats for your organization** with the X-Force Threat Score, an adaptive score, calculated based on your relevance, severity, penetration, impact and actual environmental sightings
- **Identify and act on threats active in your environment** with Am I Affected, which runs continuous and automated searches across connected data sources and automatically creates a case for active threats
- **Infuse third-party threat intelligence feeds** to reuse investment in additional threat intelligence through simple single configuration screen and enrich information throughout the platform in context of an investigation or incident
  - Current pre-built integrations include: AlienVault OTX, Cisco Threatgrid, MaxMind Geolocation, SANS Internet StormCenter and Virustotal



IBM Security Product Name

Spearphishing targets health services in 5 countries

IBM Security Product Name

Homepage

IBM Threat Intelligence Insights

Top relevant threats

Prioritize threats for your organization

The X-Force Threat Score helps you prioritize what to focus on based on severity and risk.

Update your profile and connect data sources to refine threat scores and surface relevant threats.

Connect data sources | Update your profile

Clipper Malware Discovered On Google Play — X-Force Threat Score 68% — Found indicators 0

Glupteba Campaign Hits Network Routers and Updates C2 Servers with Data from Bitcoin... — X-Force Threat Score 63% — Found indicators 0

Lazarus Still Targeting Businesses — 57%

Trickbot Technical Analysis — 53% — 0

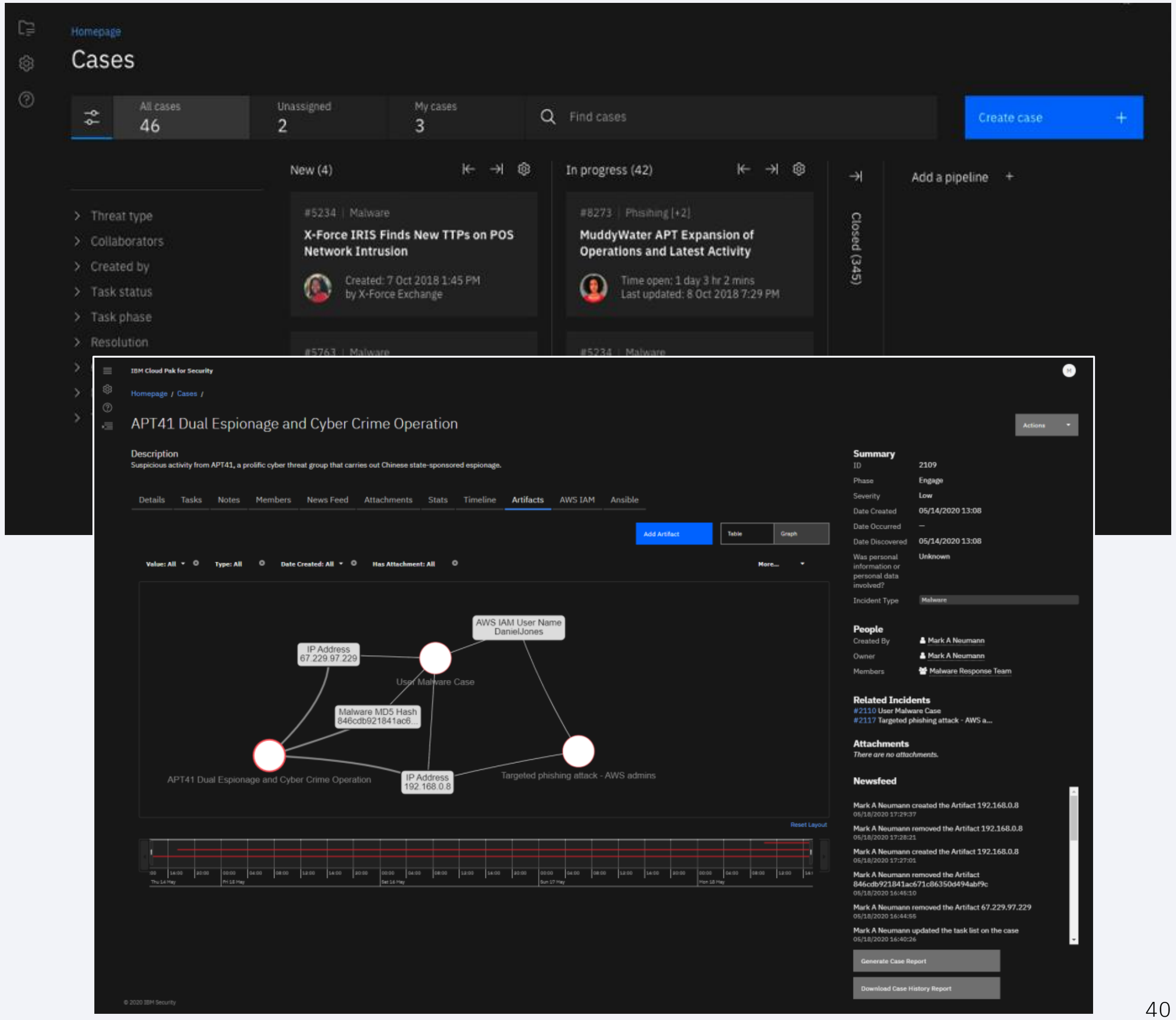
Phishing Emails Are Using SharePoint to Attack Banks — 52% — 0

Stealth Falcon Group and Their Undocumented Backdoor — 52% — 0

Case Management

Orchestration, automation, and response

- **Reduce time to respond to and remediate** complex cyber threats by automating incident response processes
- **Streamline and automate** manual and repetitive tasks such as IOC enrichment and easily identify leverage points used by attackers, track IOCs over time and classify attributes
- **Guide and execute investigation and response actions consistently** with robust case management and tasks, leveraging visual process techniques from lean manufacturing*
- **Drive investigations across the organization** via simple point and click deployment of 160+ third-party integrations
- **Customize and extend dynamic playbooks** through visual workflow editor
- **Meet compliance regulatory requirements** with a Privacy add-on*



#5234 | Malware
X-Force IRIS Finds New TTPs on POS Network Intrusion
Created: 7 Oct 2018 1:45 PM by X-Force Exchange

#8273 | Phisihng [+2]
MuddyWater APT Expansion of Operations and Latest Activity
Time open: 1 day 3 hr 2 mins
Last updated: 8 Oct 2018 7:29 PM

#5763 | Malware

#5234 | Malware

APT41 Dual Espionage and Cyber Crime Operation

Description
Suspicious activity from APT41, a prolific cyber threat group that carries out Chinese state-sponsored espionage.

Summary

ID	2109
Phase	Engage
Severity	Low
Date Created	05/14/2020 13:08
Date Occurred	—
Date Discovered	05/14/2020 13:08
Was personal information or personal data involved?	Unknown
Incident Type	Malware

People

Created By	Mark A Neumann
Owner	Mark A Neumann
Members	Malware Response Team

Related Incidents
#2110 User Malware Case
#2117 Targeted phishing attack - AWS a...

Attachments
There are no attachments.

Newsfeed

Mark A Neumann created the Artifact 192.168.0.8
05/18/2020 17:29:37

Mark A Neumann removed the Artifact 192.168.0.8
05/18/2020 17:28:21

Mark A Neumann created the Artifact 192.168.0.8
05/18/2020 17:27:01

Mark A Neumann removed the Artifact 846cdb921841ac671c86350d494abf9c
05/18/2020 16:46:10

Mark A Neumann removed the Artifact 67.229.97.229
05/18/2020 16:44:55

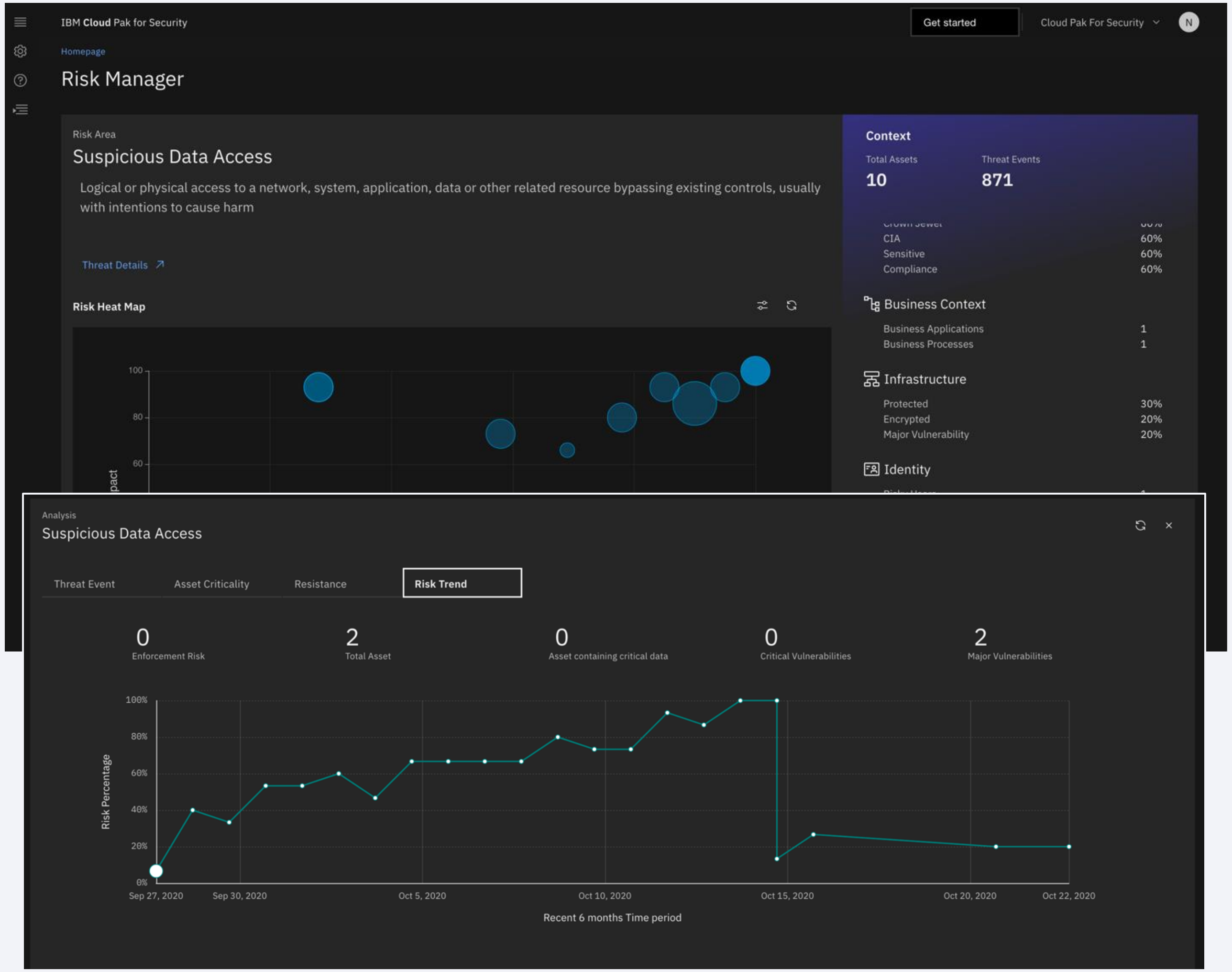
Mark A Neumann updated the task list on the case
05/18/2020 16:40:26

*Upcoming capabilities

Unified risk management

IBM Security Risk Manager (Technical Preview)

- An integrated view of risk posture presented in a business-consumable dashboard
- Get early visibility into potential security risks by correlating insights across risk domains
- Follow a Zero Trust approach to risk mitigation, through solution’s risk context, investigation, remediation and continuous improvement capabilities.
- Visualize what risks have the **biggest impact potential**
- **Quantify** and communicate security risk information using common language
- Understand the factors contributing to security risk, **prioritize** and take action to mitigate or reduce identified risk



Risk Manager

Risk Area

Suspicious Data Access

Logical or physical access to a network, system, application, data or other related resource bypassing existing controls, usually with intentions to cause harm

Context	
Total Assets	10
Threat Events	871
CIA	60%
Sensitive	60%
Compliance	60%
Business Context	
Business Applications	1
Business Processes	1
Infrastructure	
Protected	30%
Encrypted	20%
Major Vulnerability	20%
Identity	

Analysis

Suspicious Data Access

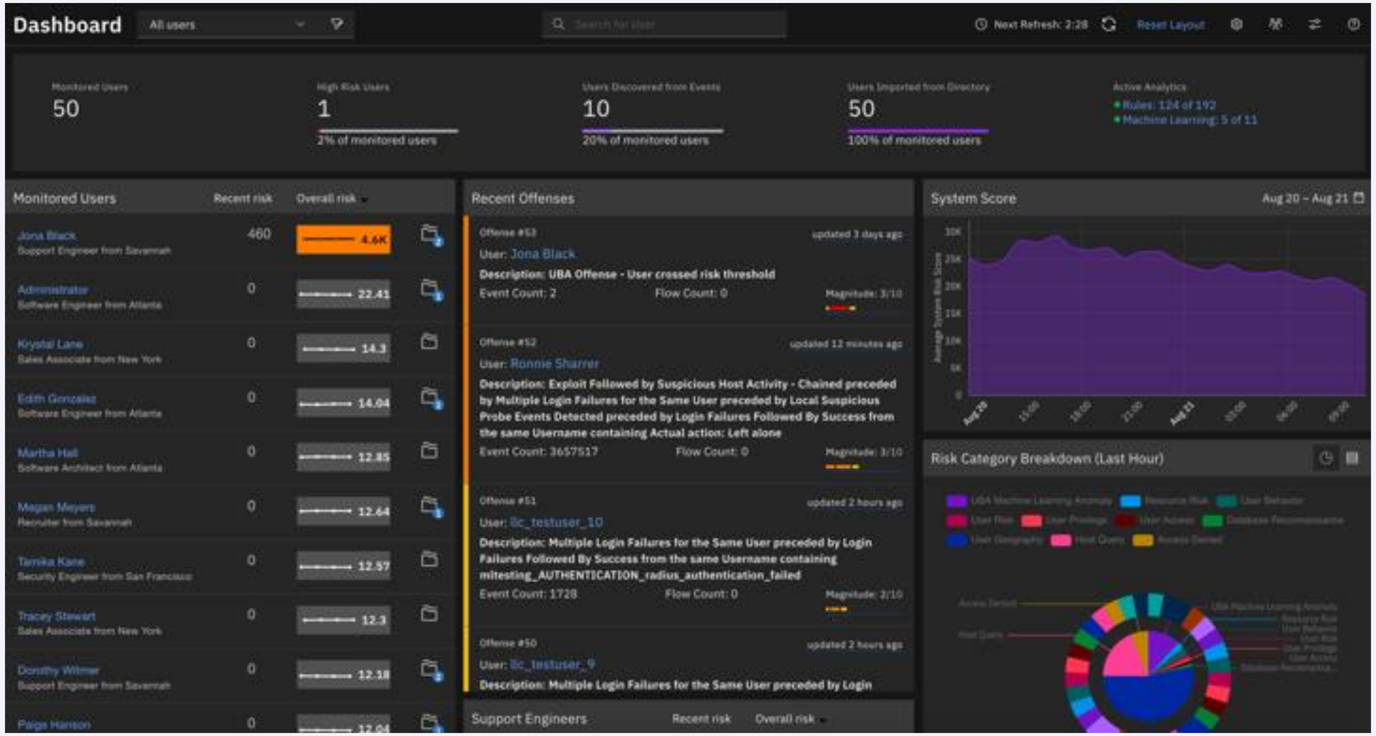
Enforcement Risk	Total Asset	Asset containing critical data	Critical Vulnerabilities	Major Vulnerabilities
0	2	0	0	2

Detecting Insider Threats

IBM Security User Behavior Analytics

230+ out of the box use cases addressing three major insider threat vectors

- Compromised or stolen credentials
- Careless or malicious insiders
- Malware takeover of user accounts or devices



Monitored Users 50

High Risk Users 1 — 2% of monitored users

Users Discovered from Events 10 — 20% of monitored users

Users Imported from Directory 50 — 100% of monitored users

Active Analytics
- Rules: 124 of 192
- Machine Learning: 5 of 11

Monitored Users	Recent risk	Overall risk
Jona Black Support Engineer from Savannah	460	4.6K
Administrator Software Engineer from Atlanta	0	22.41
Krystal Lane Sales Associate from New York	0	14.3
Edith Gonzalez Software Engineer from Atlanta	0	14.04
Martha Hall Software Architect from Atlanta	0	12.85
Megan Meyers Recruiter from Savannah	0	12.64
Tamika Kane Security Engineer from San Francisco	0	12.57
Tracey Stewart Sales Associate from New York	0	12.3
Dorothy Witmer Support Engineer from Savannah	0	12.18
Paige Hanson	0	12.04

Recent Offenses

Offense #53 — updated 3 days ago
User: Jona Black
Description: UBA Offense - User crossed risk threshold
Event Count: 2 Flow Count: 0 Magnitude: 3/10

Offense #52 — updated 12 minutes ago
User: Ronnie Sharrer
Description: Exploit Followed by Suspicious Host Activity - Chained preceded by Multiple Login Failures for the Same User preceded by Local Suspicious Probe Events Detected preceded by Login Failures Followed By Success from the same Username containing Actual action: Left alone
Event Count: 3657517 Flow Count: 0 Magnitude: 3/10

Offense #51 — updated 2 hours ago
User: llc_testuser_10
Description: Multiple Login Failures for the Same User preceded by Login Failures Followed By Success from the same Username containing mltesting_AUTHENTICATION_radius_authentication_failed
Event Count: 1728 Flow Count: 0 Magnitude: 2/10

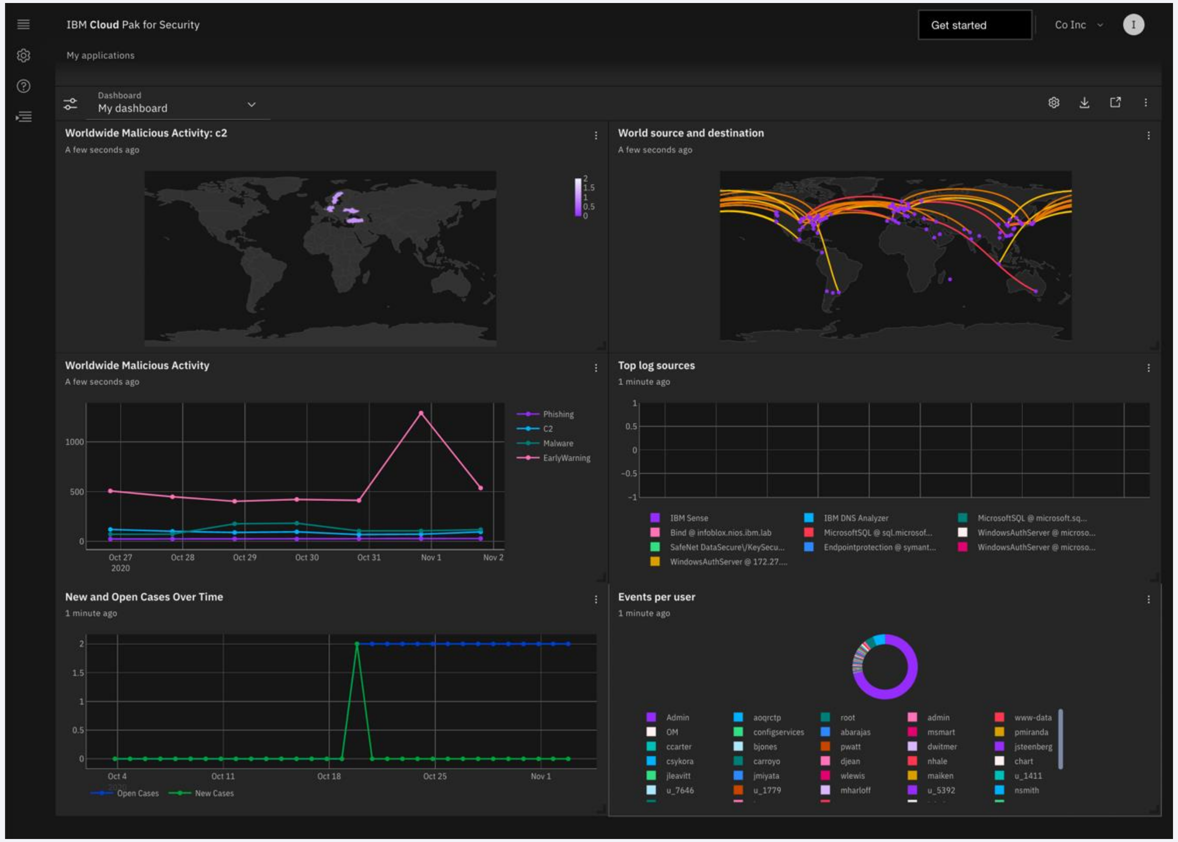
Offense #50 — updated 2 hours ago
User: llc_testuser_9
Description: Multiple Login Failures for the Same User preceded by Login

Support Engineers	Recent risk	Overall risk

Dashboards and analytics

Customized metrics for threats and risks

- **View and customize unified SOC dashboards** with operational metrics from Threat Intelligence, SIEM and SOAR systems
- **Visualize high-level security data for management and drill into details for analysts** by building your own dashboard canvases
- **Understand case management and response efficiency** with SOAR-specific metrics around case type, severity, and time
- **Quickly identify risky users associated with insider threats** by directly accessing QRadar User Behavior Analytics*



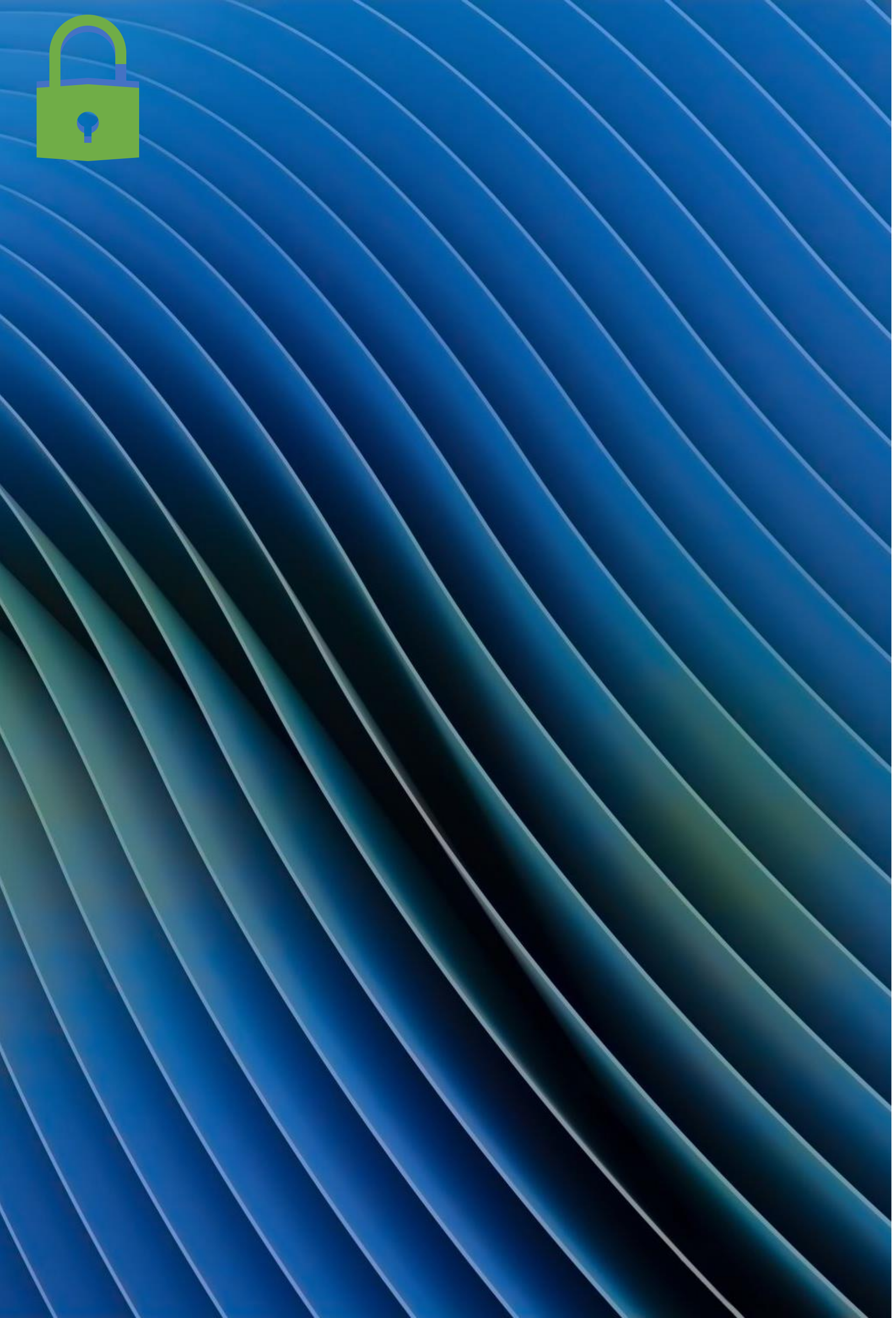
*Upcoming capabilities

IBM Cloud Pak for Security provides connectors for the following data sources:

- IBM Qradar
- IBM Qradar on Cloud
- Splunk Enterprise Security
- Elasticsearch
- Carbon Black CB Response
- BigFix
- Microsoft Defender Advanced Threat Protection
- IBM Security Guardium
- IBM Cloud Security Advisor
- Amazon CloudWatch Logs

<u>Alternate data sources</u>:

- STIX Bundle
- Proxy data source



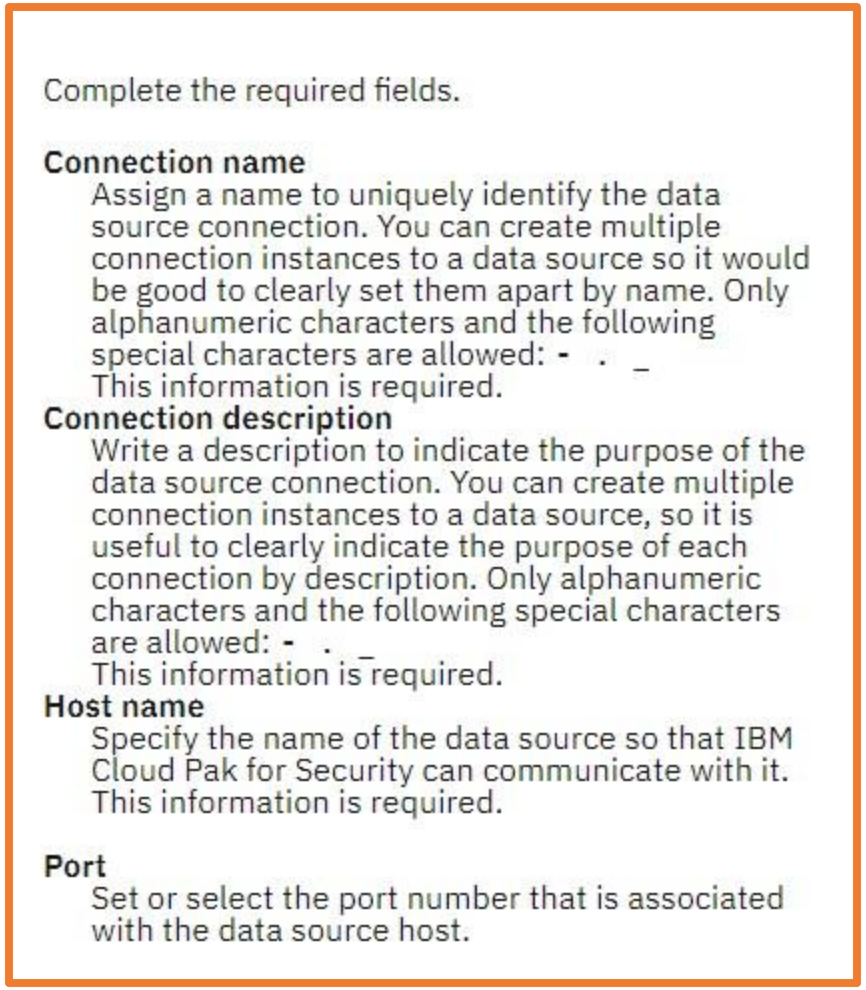
Prerequisites

A USER ACCOUNT WITH ACCESS TO CLOUD PAK FOR SECURITY.

ACCESS CREDENTIALS AND INFORMATION ABOUT THE DATA SOURCE.

Steps to add a **QRadar on Cloud** Connection

1. Log in to IBM Cloud Pak for Security and navigate to data sources.
2. Click add connection and select IBM QRadar on Cloud.
3. Enter a connection name and description.
4. Enter a host name and port (provided by QROC admin).
5. Click the add a configuration link.
6. Add a configuration name and enter the **SEC token** (provided by admin).
7. Click the save button.
8. Confirm the Status on the left pane shows as connected and click done.



Complete the required fields.

Connection name
Assign a name to uniquely identify the data source connection. You can create multiple connection instances to a data source so it would be good to clearly set them apart by name. Only alphanumeric characters and the following special characters are allowed: **-** . _
This information is required.

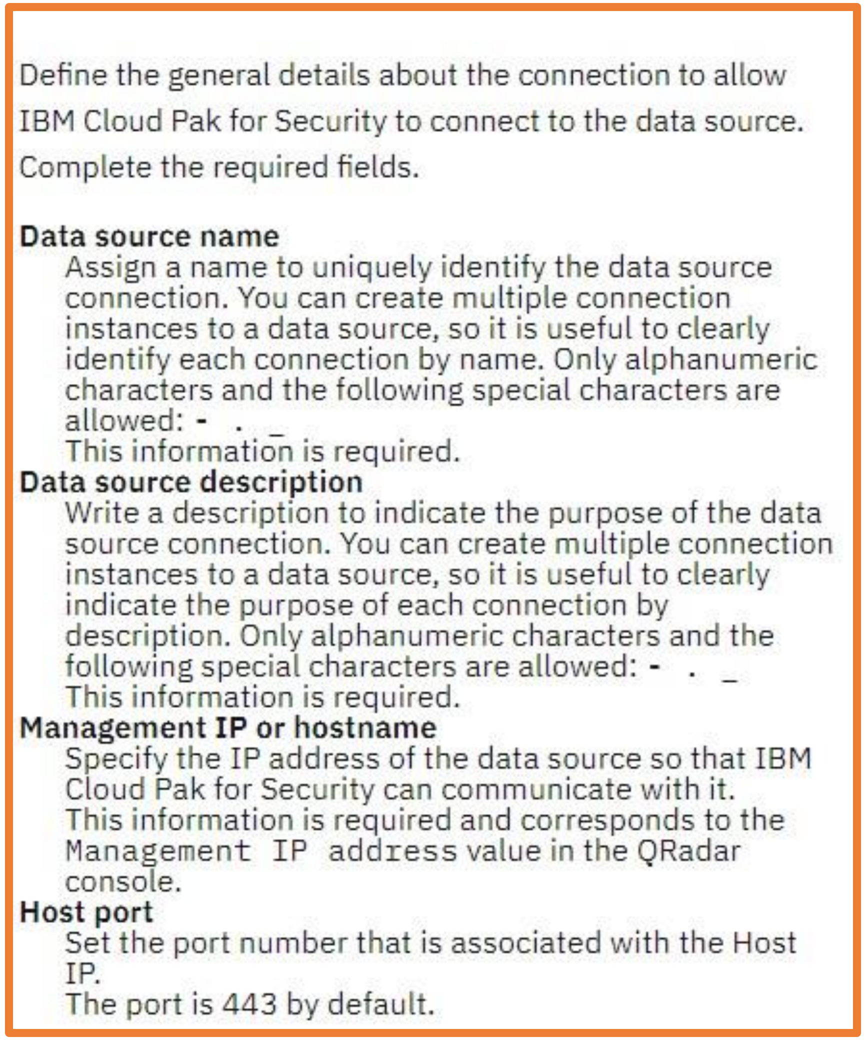
Connection description
Write a description to indicate the purpose of the data source connection. You can create multiple connection instances to a data source, so it is useful to clearly indicate the purpose of each connection by description. Only alphanumeric characters and the following special characters are allowed: **-** . _
This information is required.

Host name
Specify the name of the data source so that IBM Cloud Pak for Security can communicate with it.
This information is required.

Port
Set or select the port number that is associated with the data source host.

Steps to add a **QRadar** Connection

1. Log in to IBM Cloud Pak for Security and navigate to data sources.
2. Click add connection and select IBM QRadar.
3. Enter a connection name and description.
4. Enter the IP or host name and port (provided by QRadar admin).
5. Click the add a configuration link.
6. Add a configuration name and enter the **auth token** (provided by admin).
7. Click the save button.
8. Add the QRadar connection certificate (optional).
9. Confirm the Status on the left pane shows as connected and click done.



Define the general details about the connection to allow IBM Cloud Pak for Security to connect to the data source. Complete the required fields.

Data source name
Assign a name to uniquely identify the data source connection. You can create multiple connection instances to a data source, so it is useful to clearly identify each connection by name. Only alphanumeric characters and the following special characters are allowed: **-** . _
This information is required.

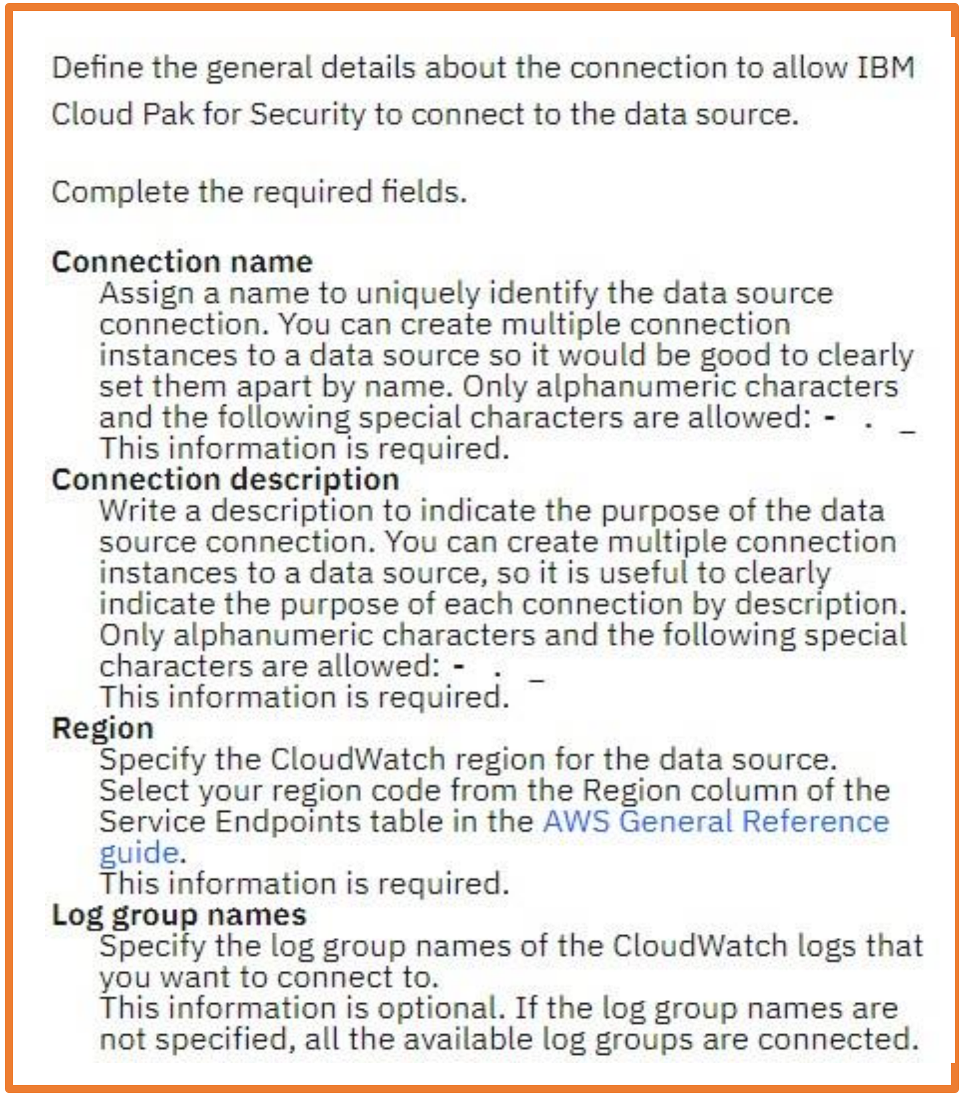
Data source description
Write a description to indicate the purpose of the data source connection. You can create multiple connection instances to a data source, so it is useful to clearly indicate the purpose of each connection by description. Only alphanumeric characters and the following special characters are allowed: **-** . _
This information is required.

Management IP or hostname
Specify the IP address of the data source so that IBM Cloud Pak for Security can communicate with it.
This information is required and corresponds to the `Management IP address` value in the QRadar console.

Host port
Set the port number that is associated with the Host IP.
The port is 443 by default.

Steps to add an **AWS** Connection

1. Log in to IBM Cloud Pak for Security and navigate to data sources.
2. Click add connection and select AWS.
3. Enter a connection name and description.
4. Enter the CloudWatch Region (Required) for the data source and log group names (optional)
5. Click the add a configuration link.
6. Add a configuration name and enter the following:
   a. **AWS Access key id** and **Secret access key**
   b. **AWSAccess key id**, **secret access key**, and **IAM role**.
7. Click the save button.
8. Add the CloudWatch connection certificate (optional).
9. Confirm the Status on the left pane shows as connected and click done.



Define the general details about the connection to allow IBM Cloud Pak for Security to connect to the data source.

Complete the required fields.

Connection name
Assign a name to uniquely identify the data source connection. You can create multiple connection instances to a data source so it would be good to clearly set them apart by name. Only alphanumeric characters and the following special characters are allowed: - . _
This information is required.

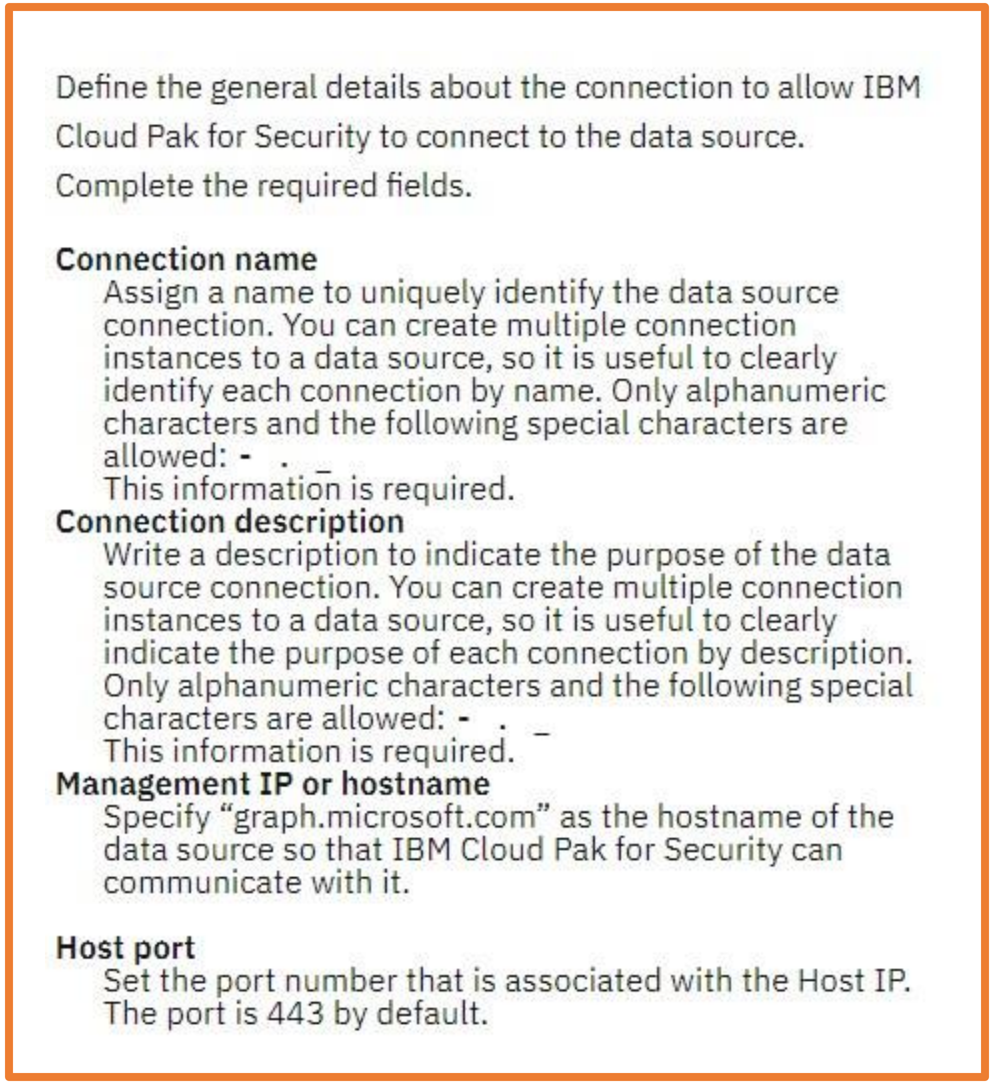
Connection description
Write a description to indicate the purpose of the data source connection. You can create multiple connection instances to a data source, so it is useful to clearly indicate the purpose of each connection by description. Only alphanumeric characters and the following special characters are allowed: - . _
This information is required.

Region
Specify the CloudWatch region for the data source. Select your region code from the Region column of the Service Endpoints table in the AWS General Reference guide.
This information is required.

Log group names
Specify the log group names of the CloudWatch logs that you want to connect to.
This information is optional. If the log group names are not specified, all the available log groups are connected.

Steps to add an **Azure** Connection

1. Log in to IBM Cloud Pak for Security and navigate to data sources.
2. Click add connection and select Microsoft Azure.
3. Enter a connection name and description.
4. Enter the host name (graph.microsoft.com) and port (443).
5. Click the add a configuration link.
6. Add a configuration name and enter the **Tenant**, **Client ID**, and **Secret** to the Microsoft Graph API
7. Click the save button.
8. Confirm the Status on the left pane shows as connected and click done.



Define the general details about the connection to allow IBM Cloud Pak for Security to connect to the data source.

Complete the required fields.

Connection name
Assign a name to uniquely identify the data source connection. You can create multiple connection instances to a data source, so it is useful to clearly identify each connection by name. Only alphanumeric characters and the following special characters are allowed: - . _
This information is required.

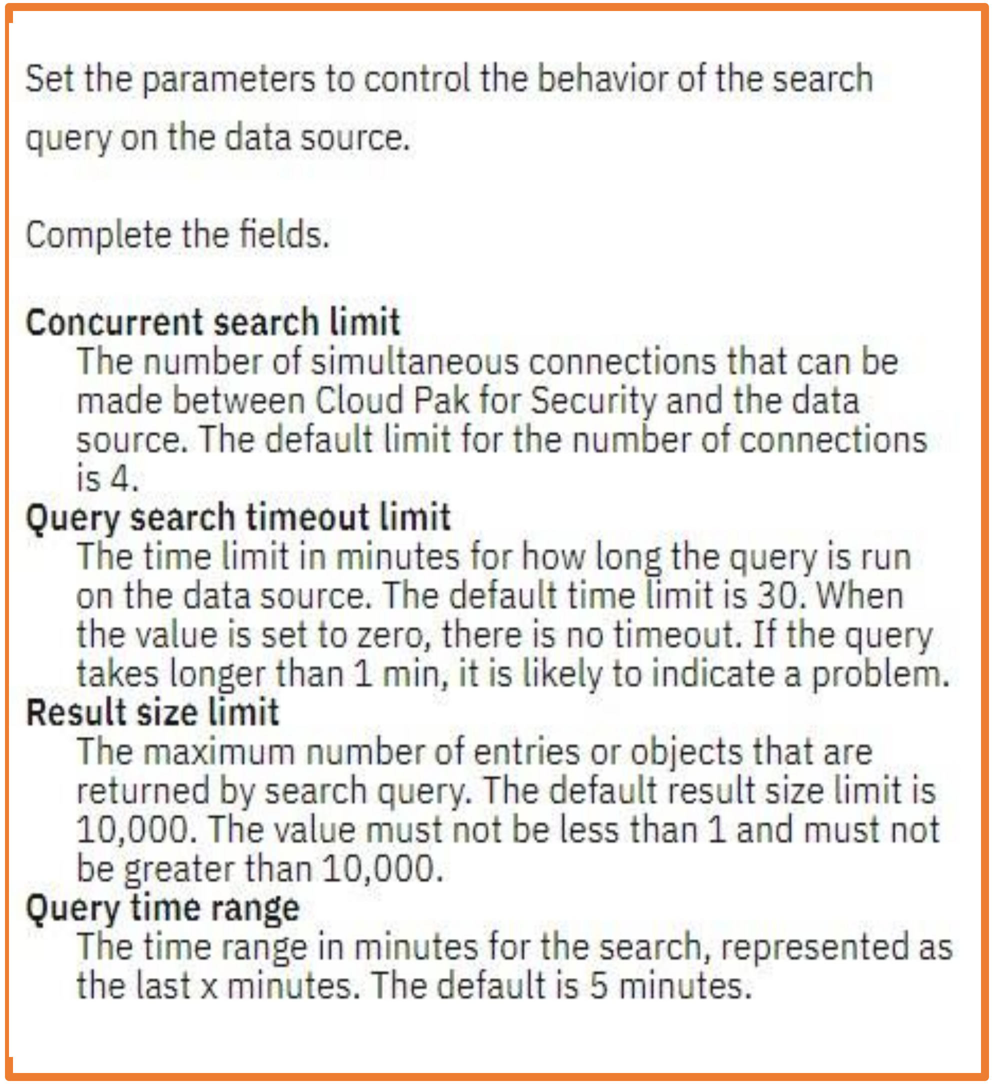
Connection description
Write a description to indicate the purpose of the data source connection. You can create multiple connection instances to a data source, so it is useful to clearly indicate the purpose of each connection by description. Only alphanumeric characters and the following special characters are allowed: - . _
This information is required.

Management IP or hostname
Specify "graph.microsoft.com" as the hostname of the data source so that IBM Cloud Pak for Security can communicate with it.

Host port
Set the port number that is associated with the Host IP. The port is 443 by default.

Data Connection Query Parameters

1. Query parameters are the same for each data source.
2. Used to tune the query behavior by data connection.
3. Default values are recommended to start.
4. Adjust parameters per data source to improve search performance.



Set the parameters to control the behavior of the search query on the data source.

Complete the fields.

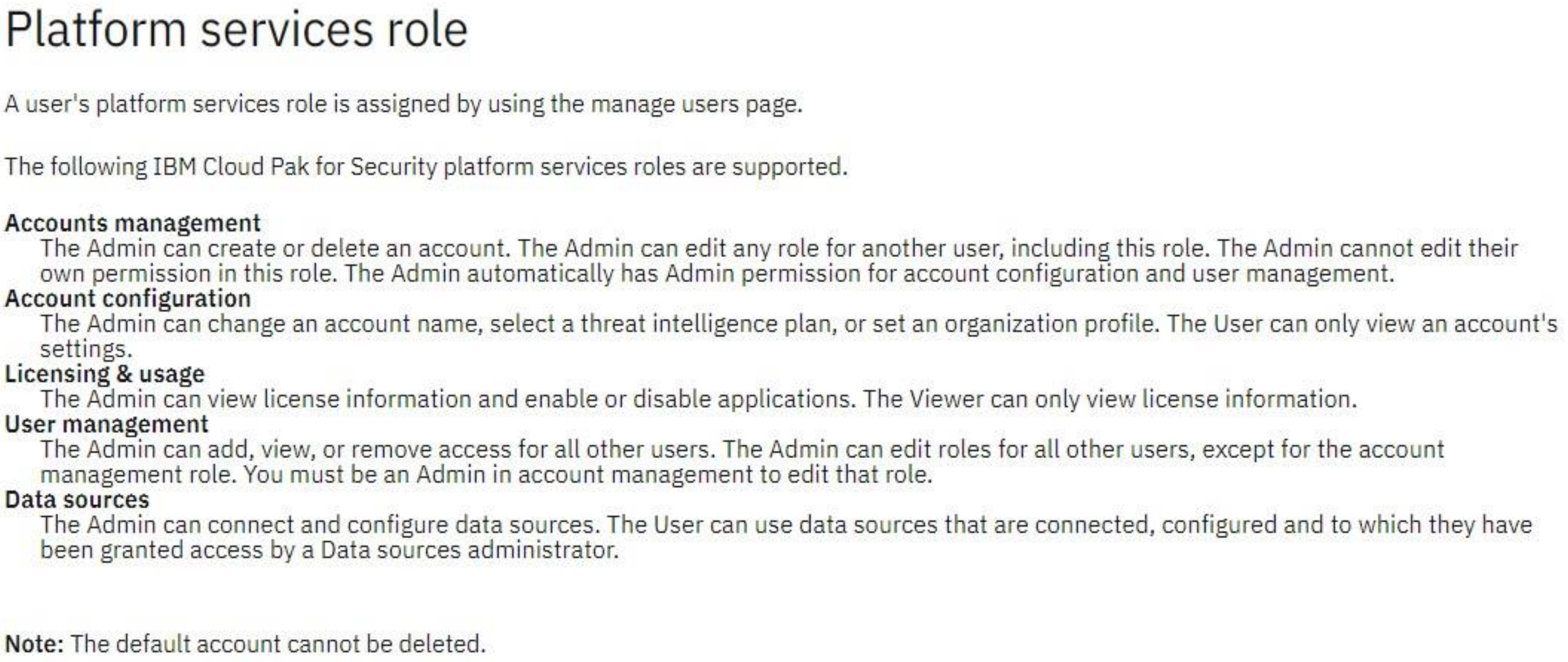
Concurrent search limit
The number of simultaneous connections that can be made between Cloud Pak for Security and the data source. The default limit for the number of connections is 4.

Query search timeout limit
The time limit in minutes for how long the query is run on the data source. The default time limit is 30. When the value is set to zero, there is no timeout. If the query takes longer than 1 min, it is likely to indicate a problem.

Result size limit
The maximum number of entries or objects that are returned by search query. The default result size limit is 10,000. The value must not be less than 1 and must not be greater than 10,000.

Query time range
The time range in minutes for the search, represented as the last x minutes. The default is 5 minutes.

User Permissions



Platform services role

A user's platform services role is assigned by using the manage users page.

The following IBM Cloud Pak for Security platform services roles are supported.

Accounts management
The Admin can create or delete an account. The Admin can edit any role for another user, including this role. The Admin cannot edit their own permission in this role. The Admin automatically has Admin permission for account configuration and user management.

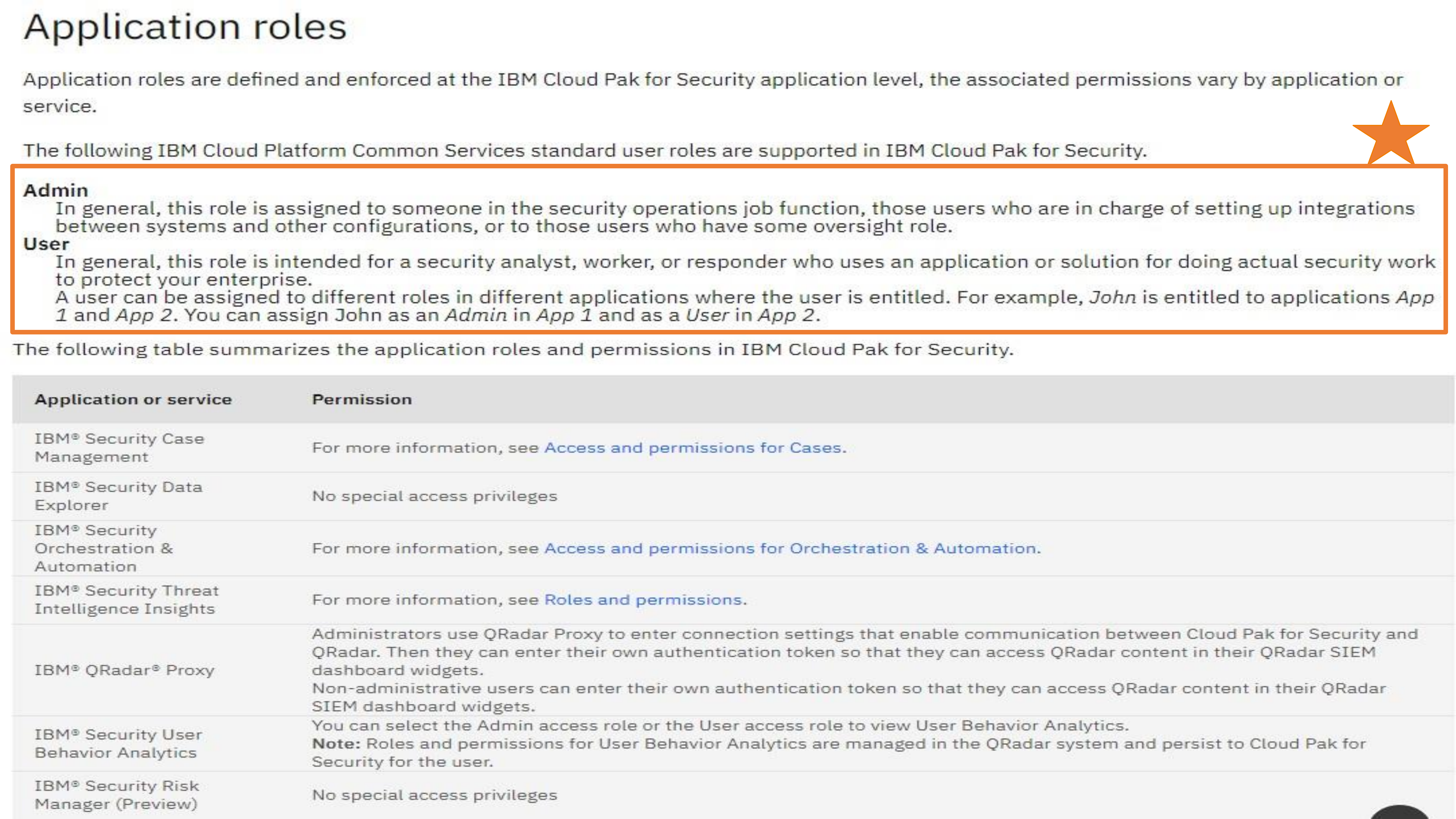
Account configuration
The Admin can change an account name, select a threat intelligence plan, or set an organization profile. The User can only view an account's settings.

Licensing & usage
The Admin can view license information and enable or disable applications. The Viewer can only view license information.

User management
The Admin can add, view, or remove access for all other users. The Admin can edit roles for all other users, except for the account management role. You must be an Admin in account management to edit that role.

Data sources
The Admin can connect and configure data sources. The User can use data sources that are connected, configured and to which they have been granted access by a Data sources administrator.

Note: The default account cannot be deleted.



Application roles

Application roles are defined and enforced at the IBM Cloud Pak for Security application level, the associated permissions vary by application or service.

The following IBM Cloud Platform Common Services standard user roles are supported in IBM Cloud Pak for Security.

Admin

In general, this role is assigned to someone in the security operations job function, those users who are in charge of setting up integrations between systems and other configurations, or to those users who have some oversight role.

User

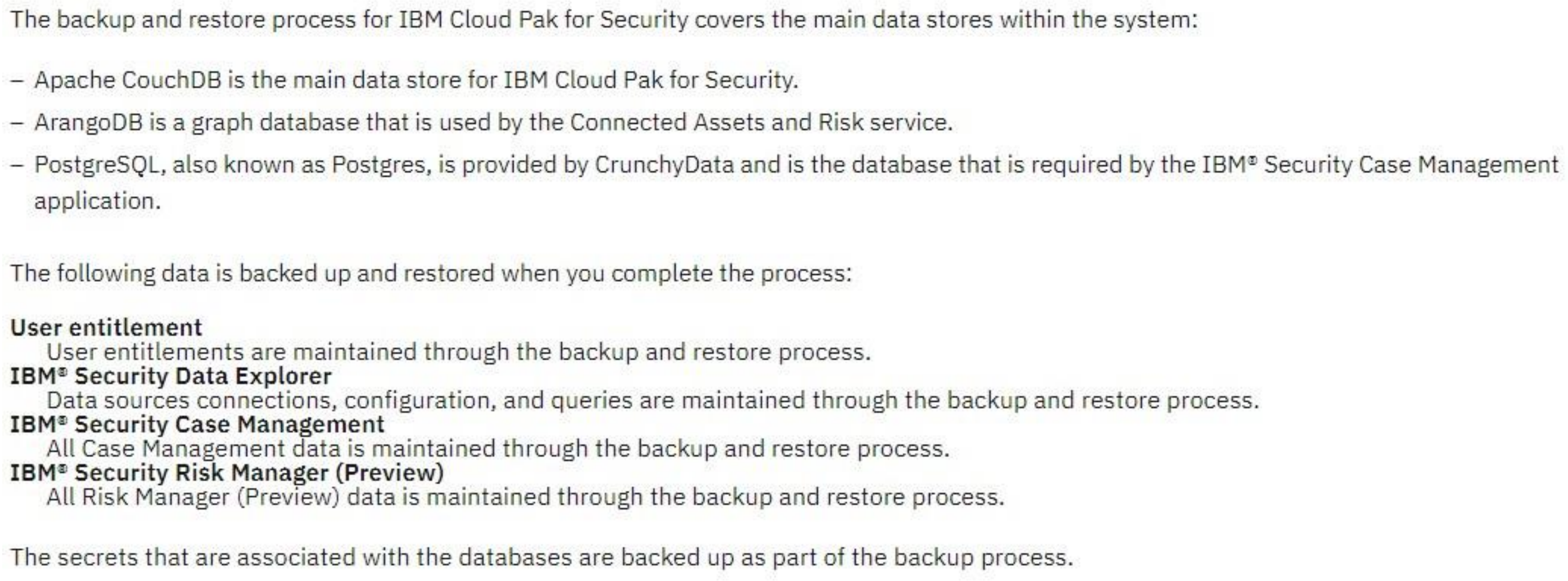
In general, this role is intended for a security analyst, worker, or responder who uses an application or solution for doing actual security work to protect your enterprise.

A user can be assigned to different roles in different applications where the user is entitled. For example, *John* is entitled to applications *App 1* and *App 2*. You can assign John as an *Admin* in *App 1* and as a *User* in *App 2*.

The following table summarizes the application roles and permissions in IBM Cloud Pak for Security.

Application or service	Permission
IBM® Security Case Management	For more information, see Access and permissions for Cases.
IBM® Security Data Explorer	No special access privileges
IBM® Security Orchestration & Automation	For more information, see Access and permissions for Orchestration & Automation.
IBM® Security Threat Intelligence Insights	For more information, see Roles and permissions.
IBM® QRadar® Proxy	Administrators use QRadar Proxy to enter connection settings that enable communication between Cloud Pak for Security and QRadar. Then they can enter their own authentication token so that they can access QRadar content in their QRadar SIEM dashboard widgets. Non-administrative users can enter their own authentication token so that they can access QRadar content in their QRadar SIEM dashboard widgets.
IBM® Security User Behavior Analytics	You can select the Admin access role or the User access role to view User Behavior Analytics. **Note:** Roles and permissions for User Behavior Analytics are managed in the QRadar system and persist to Cloud Pak for Security for the user.
IBM® Security Risk Manager (Preview)	No special access privileges

Backup and Restore



The backup and restore process for IBM Cloud Pak for Security covers the main data stores within the system:

- Apache CouchDB is the main data store for IBM Cloud Pak for Security.
- ArangoDB is a graph database that is used by the Connected Assets and Risk service.
- PostgreSQL, also known as Postgres, is provided by CrunchyData and is the database that is required by the IBM® Security Case Management application.

The following data is backed up and restored when you complete the process:

User entitlement
User entitlements are maintained through the backup and restore process.

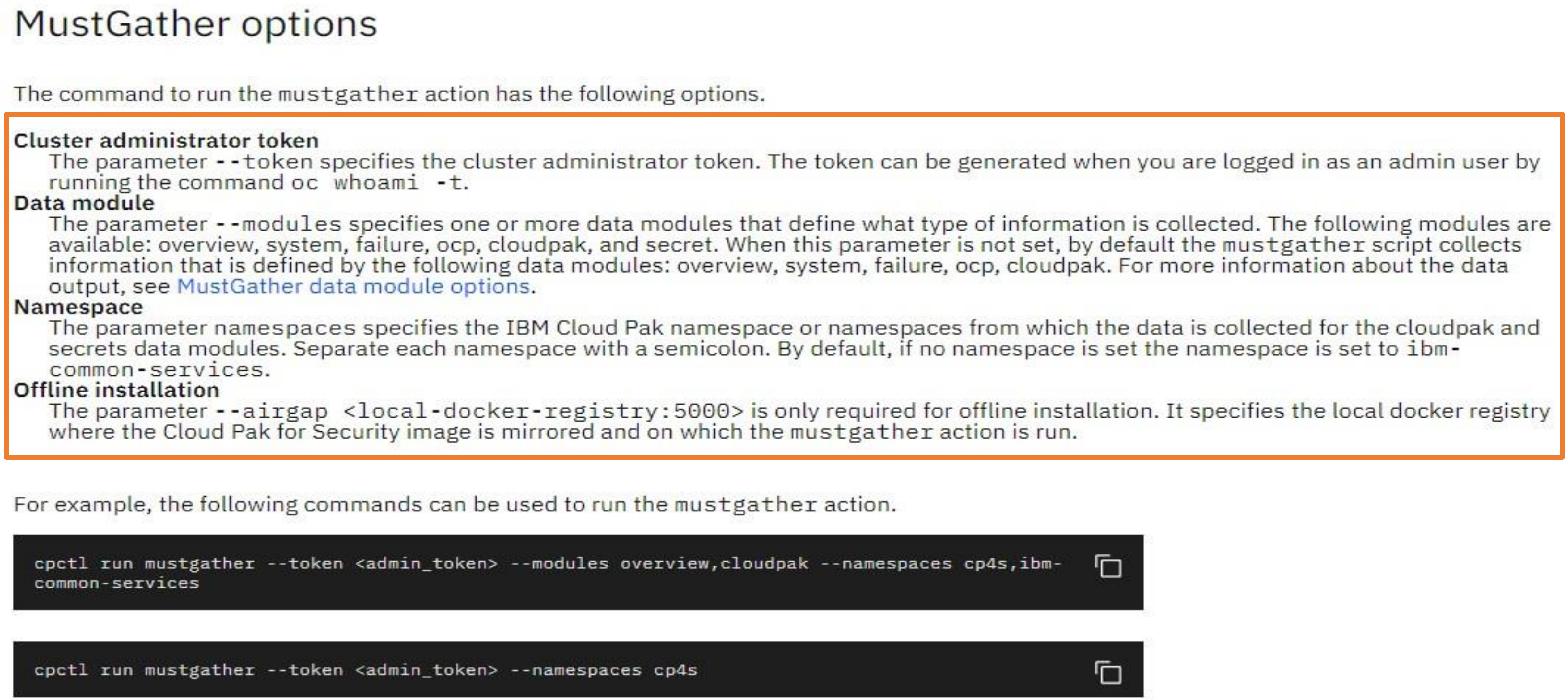
IBM® Security Data Explorer
Data sources connections, configuration, and queries are maintained through the backup and restore process.

IBM® Security Case Management
All Case Management data is maintained through the backup and restore process.

IBM® Security Risk Manager (Preview)
All Risk Manager (Preview) data is maintained through the backup and restore process.

The secrets that are associated with the databases are backed up as part of the backup process.

Troubleshooting



MustGather options

The command to run the mustgather action has the following options.

Cluster administrator token
The parameter --token specifies the cluster administrator token. The token can be generated when you are logged in as an admin user by running the command oc whoami -t.

Data module
The parameter --modules specifies one or more data modules that define what type of information is collected. The following modules are available: overview, system, failure, ocp, cloudpak, and secret. When this parameter is not set, by default the mustgather script collects information that is defined by the following data modules: overview, system, failure, ocp, cloudpak. For more information about the data output, see MustGather data module options.

Namespace
The parameter namespaces specifies the IBM Cloud Pak namespace or namespaces from which the data is collected for the cloudpak and secrets data modules. Separate each namespace with a semicolon. By default, if no namespace is set the namespace is set to ibm-common-services.

Offline installation
The parameter --airgap <local-docker-registry:5000> is only required for offline installation. It specifies the local docker registry where the Cloud Pak for Security image is mirrored and on which the mustgather action is run.

For example, the following commands can be used to run the mustgather action.

```
cpctl run mustgather --token <admin_token> --modules overview,cloudpak --namespaces cp4s,ibm-
common-services
```

```
cpctl run mustgather --token <admin_token> --namespaces cp4s
```

CP4S Hardware Requirements

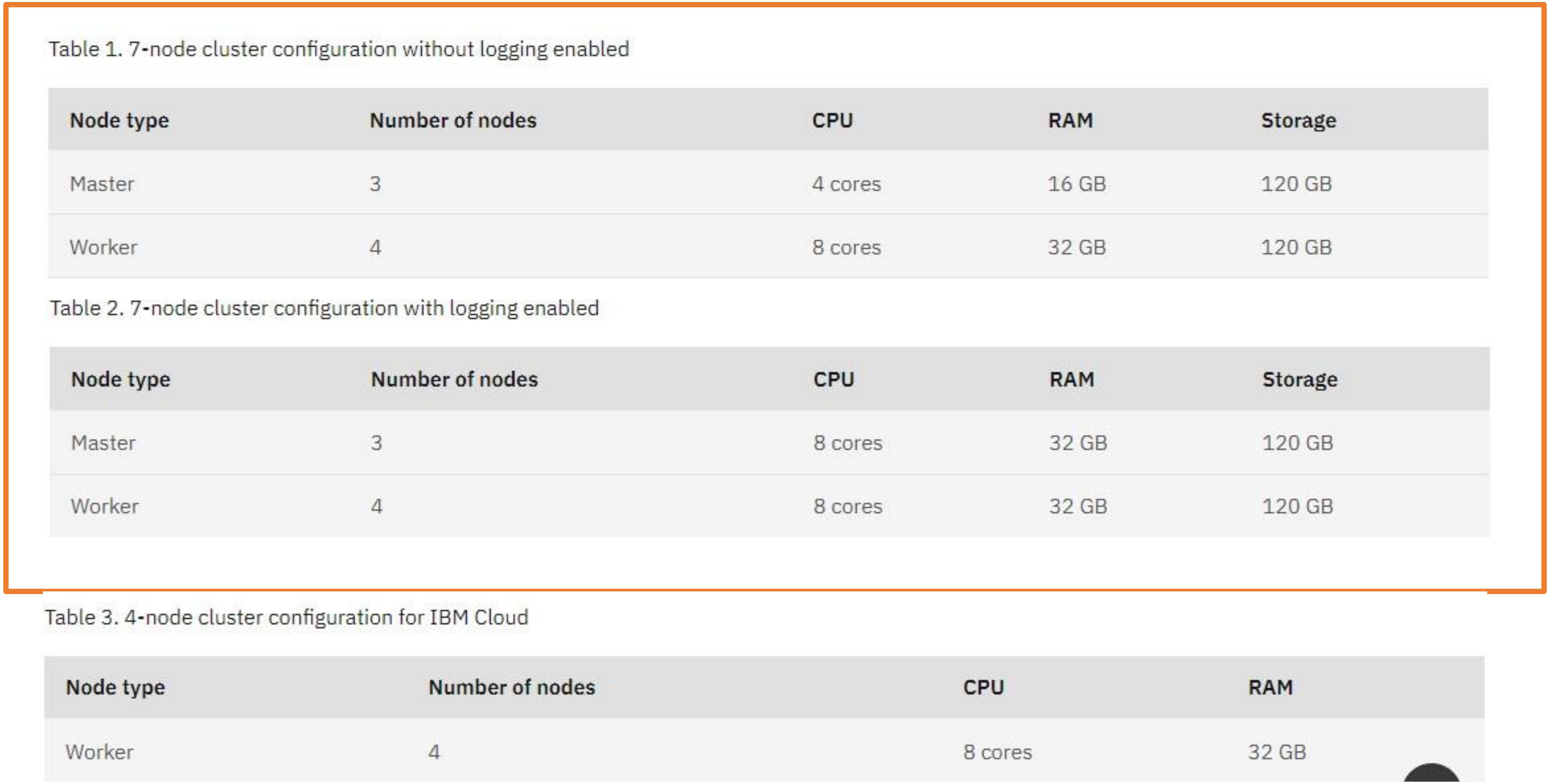


Table 1. 7-node cluster configuration without logging enabled

Node type	Number of nodes	CPU	RAM	Storage
Master	3	4 cores	16 GB	120 GB
Worker	4	8 cores	32 GB	120 GB

Table 2. 7-node cluster configuration with logging enabled

Node type	Number of nodes	CPU	RAM	Storage
Master	3	8 cores	32 GB	120 GB
Worker	4	8 cores	32 GB	120 GB

Table 3. 4-node cluster configuration for IBM Cloud

Node type	Number of nodes	CPU	RAM
Worker	4	8 cores	32 GB

Cloud Pak for Security V1.x Administrator Specialty Exam

- S1000-001: IBM Cloud Pak for Security V1.x Admin Specialty
  - Number of questions: 40
  - Number of questions to pass: 27
  - Time allowed: 90 mins.

- Exam is proctored with Pearson Vue
  - Schedule exam at https://home.pearsonvue.com/ibm
  - Click the View Exams button and search for S1000-001.
  - Select testing option and date/time.
  - Exam is $100 per attempt.

Testing Options:

- Pearson Vue Test Center
- Online at home or office using OnVue.
- https://home.pearsonvue.com/ibm/onvue

Practice Questions

1. What capabilities does Cloud Pak for Security bring together?
    a. EDR
    b. Datalake and UBA
    c. SIEM and Identity
    d. All of the above

2. Which OpenShift configuration would be used when logging is required?
    a. 3 Masters (8 Cores,32 GB Mem) and 4 Workers (8 Cores, 32 GB Mem)
    b. 4 Workers (8 Cores, 32 GB Mem) only
    c. 3 Masters (8 Cores,16 GB Mem) only
    d. 3 Masters (8 Cores,16 GB Mem) and 4 Workers (8 Cores, 32 GB Mem)

3. Which CP4S component consolidates asset and risk data to identify security gaps?
    a. Connect Asset & Risk (CAR) Database
    b. Connect Asset & Risk (CAR) Dataset
    c. Consolidated Asset & Risk (CAR) Database
    d. Asset Risk & Threat (ART) Database

4. Which 3 fields are needed to collect the mustgather? (select 3)
    a. Cpctl tool
    b. Namespace
    c. Modules
    d. Token

5. Which of the following are data query parameters?
   a. Connection name, connection description, hostname, port
   b. Concurrent search limit, SEC Token, result size limit, Secret Key
   c. Tenant ID, connection description, Secret, port
   d. Concurrent search limit, query search timeout, result size limit, query time range

6. What are the required general fields for a Qradar data connection?
   a. Concurrent search limit, query search timeout, result size limit, query time range
   b. Connection name, connection description, hostname, port
   c. Tenant ID, connection description, Secret, port
   d. Concurrent search limit, SEC Token, result size limit, Secret Key

7. What application role can assign access to Threat Intelligence Insights (TII)?
   a. TII Administrator and Data Explorer Administrator
   b. TII User
   c. Data Exploerer User
   d. Platform Role Administrator

8. Asset Data must be configured separately for each connector?
   a. True
   b. False

9. What type of certificate is required for a CP4S installation not on IBM Cloud?

   a. Hypertext Transfer Protocol Secure (HTTPS) Certificate
   b. Public Key infrastructure (PKI) Certificate
   c. Transport Layer Security (TLS) Certificate
   d. Secure Sockets Layer (SSL) Certificate

10. Compete the following statement. 'IBM Cloud Pak for Securit y provides a platform ___ _?

    a. to manage all platforms from anywhere.
    b. to undertake costly m igration projects, complex integrations, and continuously switch between different screens and products.
    c. to help more quickly integrate your existing security tools to generate deeper insights into threats across hybrid, multicloud environments, using an infrastructure-independent common operating environment that runs anywhere.
    d. to move client operations to the cloud piece by piece, with applications and data spread across multiple clouds and on-premise resources.

11. What is inscluded with Threat Intelligence Insight’s standard package?

    a. Access X-Force threat intelligence content with manually and automated threat scanning
    b. Access X-Force threat intelligence premium content and automated threat scann ing
    c. Access X-Force threat intelligence premium content, the ability to manually to scan for threats, and automated threat scanning
    d. Access X-Force threat intelligence content and the ability to manually to scan for threats

- Answers:
  - 1: D
  - 2: A
  - 3: A
  - 4: B,C,D
  - 5: D
  - 6: B
  - 7: A
  - 8: B
  - 9: C
  - 10: C
  - 11: B