No Tricks, Just Treats

Threat Management with

IBM QRadar SIEM

October 27, 2022

Legal notes and disclaimer

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

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

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

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

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

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

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

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

Agenda

QRadar XDR – IBM’s Threat Management Portfolio

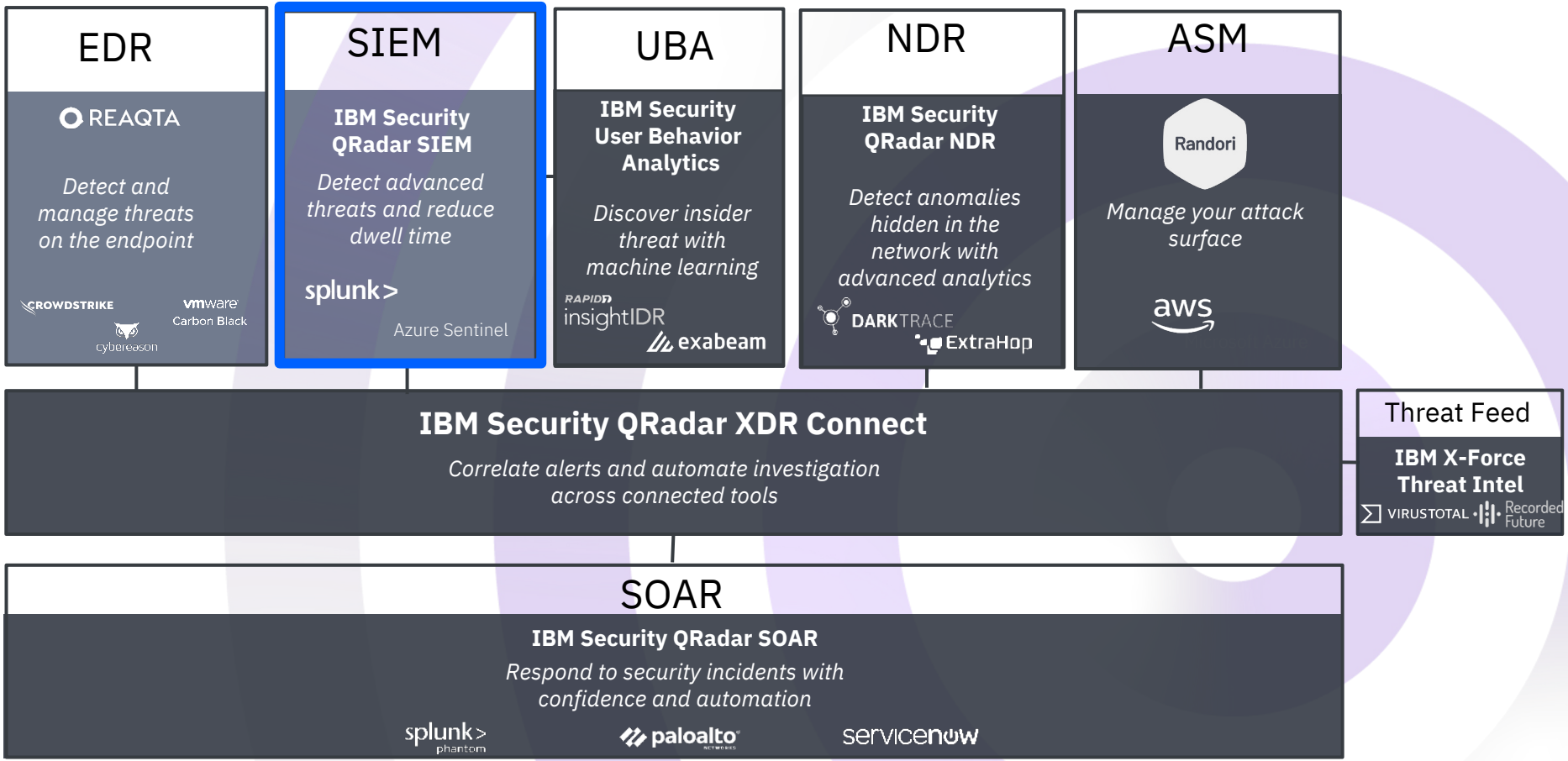
QRadar SIEM Core

- Overview
- New Functionalities

QRadar SIEM *Next-Gen*

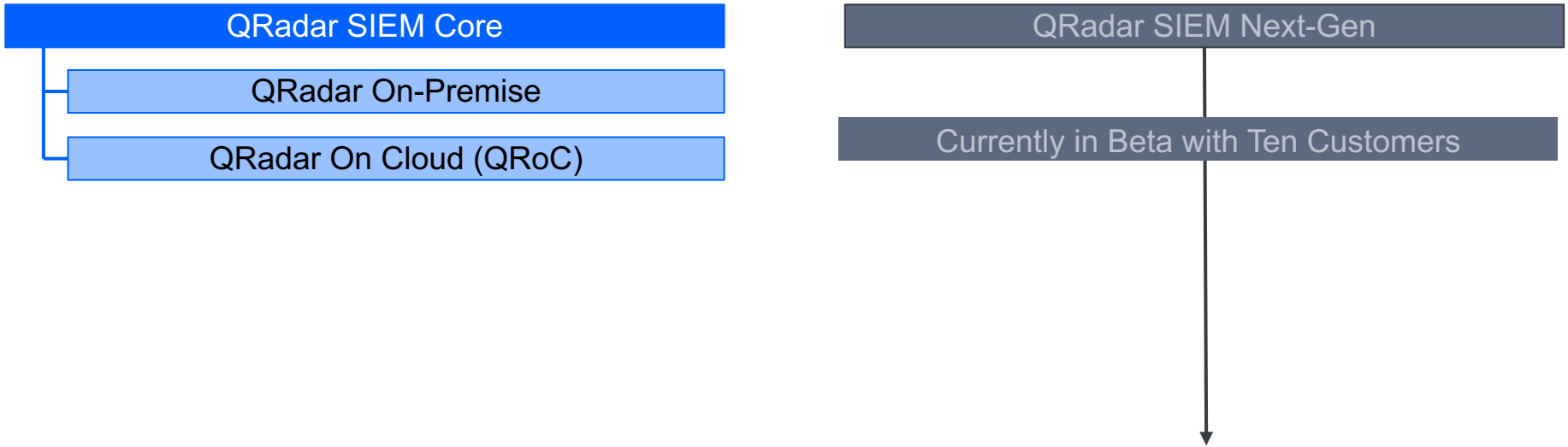
- Sneak Peek

IBM Security QRadar XDR: An open approach



QRadar SIEM *Core*

Overview QRadar SIEM Core



IBM Security QRadar a Leader 13 consecutive times

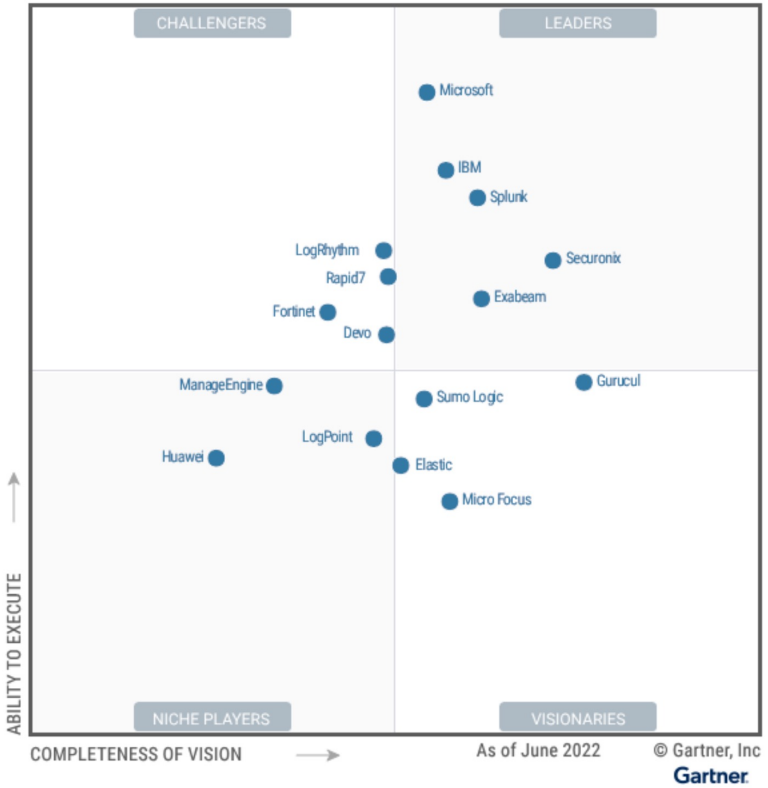
Gartner recognizes IBM QRadar SIEM for strong analytics and customization, our globally dedicated resources, and the breadth of integrations within the IBM Security portfolio.

The 2022 Gartner MQ for SIEM had a strong focus on:

- Endpoint Analytics
- Integration capabilities
- UBA
- Cloud
- Use of Threat Intelligence

Magic Quadrant

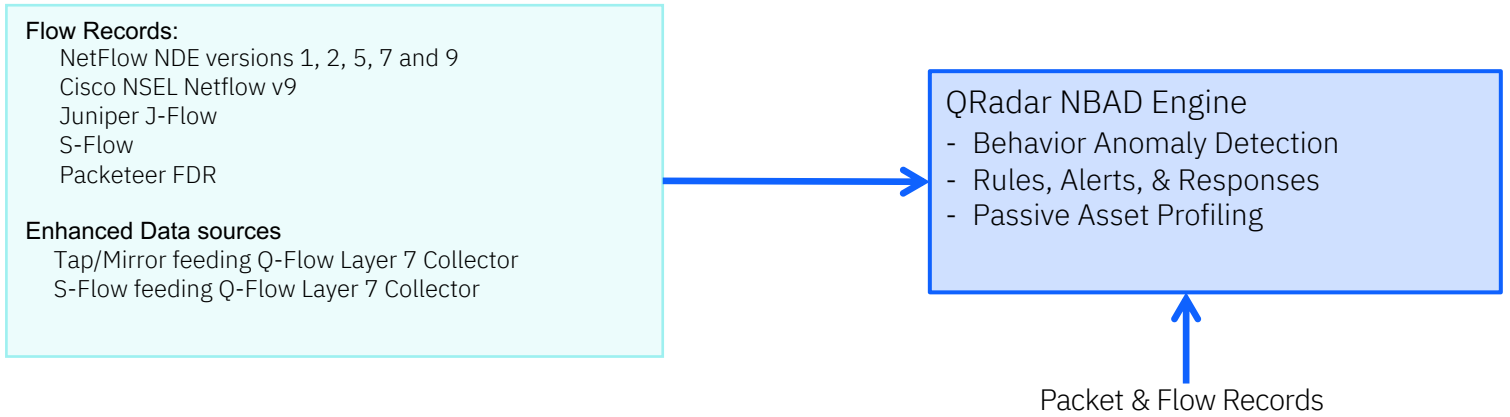
Figure 1: Magic Quadrant for Security Information and Event Management



QRadar SIEM Core Nuts & Bolts

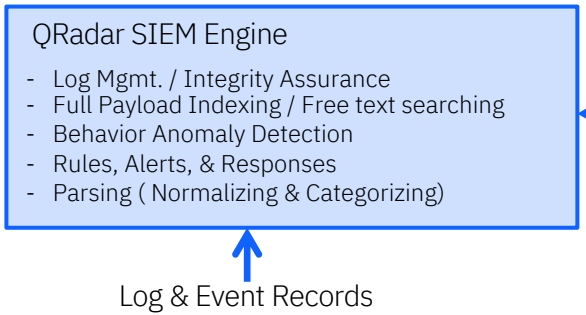
QRadar SIEM Core *Workflow*

Network Behavior



QRadar SIEM Core *Workflow*

Log Events



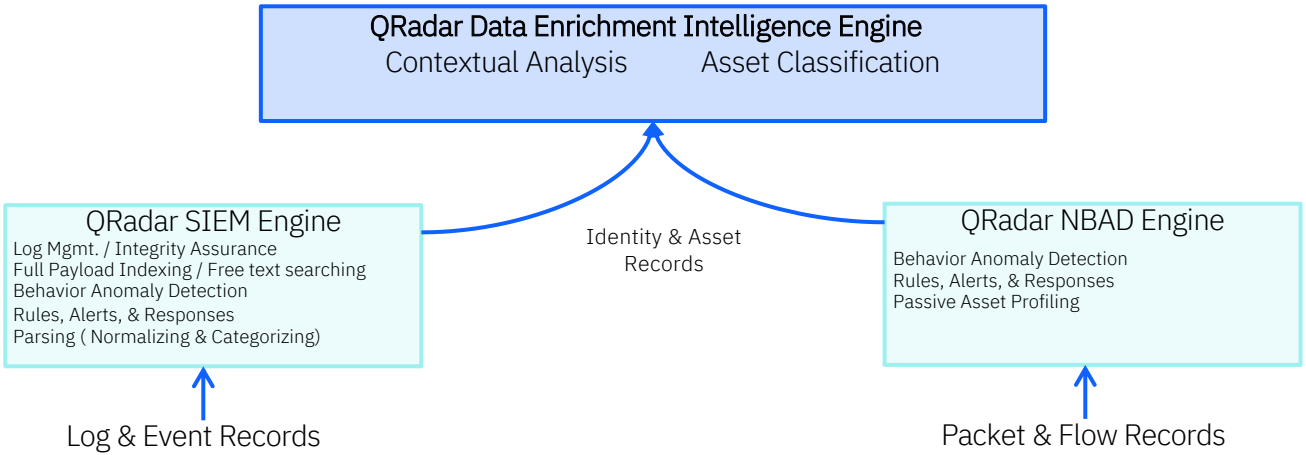
Vendor Agnostic Methods:
- Syslog (TCP, UDP, TLS & Multi-Line)
- JDBC
- OPSEC/LEA
- SDEE
- SNMP v1, 2 & 3
- SMB Tail
- PCAP Syslog Combination Protocol
- Log File protocol - FTP, SCP, SFTP

Vendor Specific Methods:
- Juniper Security Binary Log Collector Protocol
- IBM Tivoli Endpoint Manager SOAP Protocol
- Sourcefire Defense Center Estreamer
- Sophos Enterprise Console
- Juniper Networks NSM
- Oracle Database Listener
- Cisco Network Security Event Logging
- IBM SiteProtector
- EMC VMWare
- MS Office 365
- Azure Event Hub/AD
- Google G Suite
- Amazon Cloudtrail

Microsoft Collection Methods:
- Agentless (WMI)
- Agents (IBM or Open-Source)
- Hybrid (IBM "Proxy" system collects remotely)

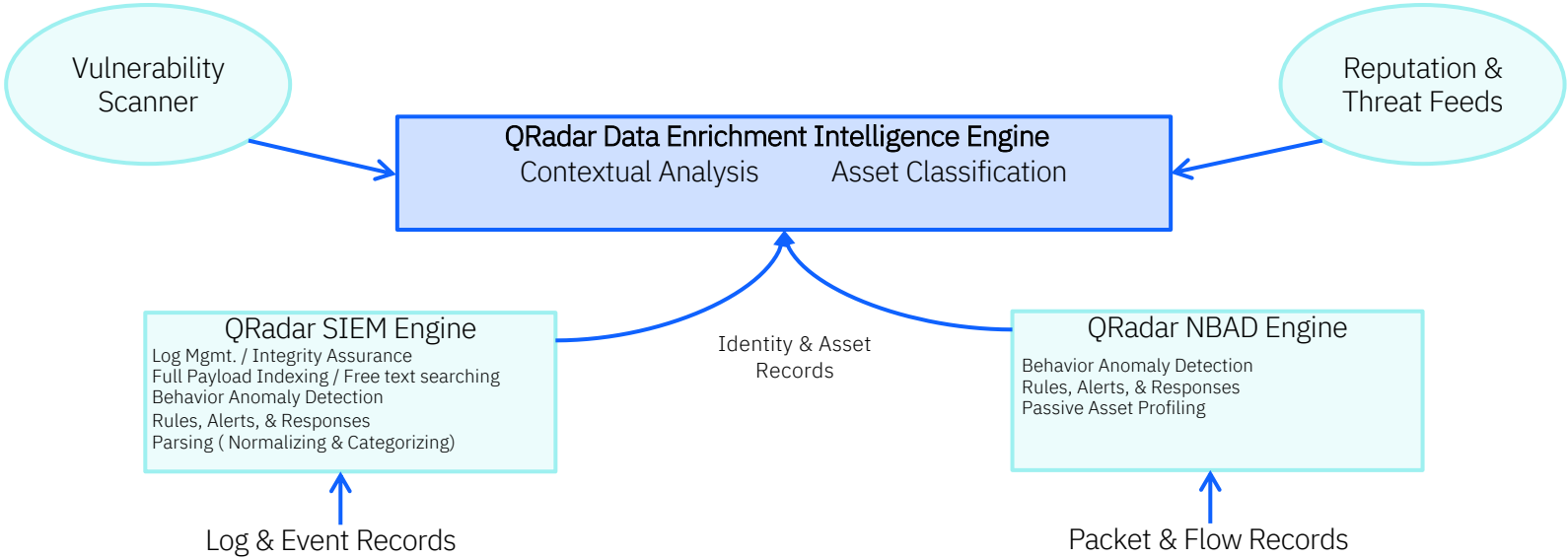
QRadar SIEM Core *Workflow*

Enrichment Engine



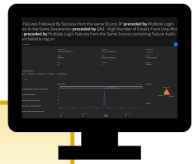
QRadar SIEM Core *Workflow*

Additional Data Sources



QRadar SIEM Core *Workflow*

Offenses



QRadar Offense SIEM Engine

- Global Correlation (chaining)
- Incident Workflow
- Data Reduction

Vulnerability Scanner

Reputation & Threat Feeds

QRadar Data Enrichment Intelligence Engine

Contextual Analysis Asset Classification

QRadar SIEM Engine

Log Mgmt. / Integrity Assurance
Full Payload Indexing / Free text searching
Behavior Anomaly Detection
Rules, Alerts, & Responses
Parsing (Normalizing & Categorizing)

Log & Event Records

Identity & Asset Records

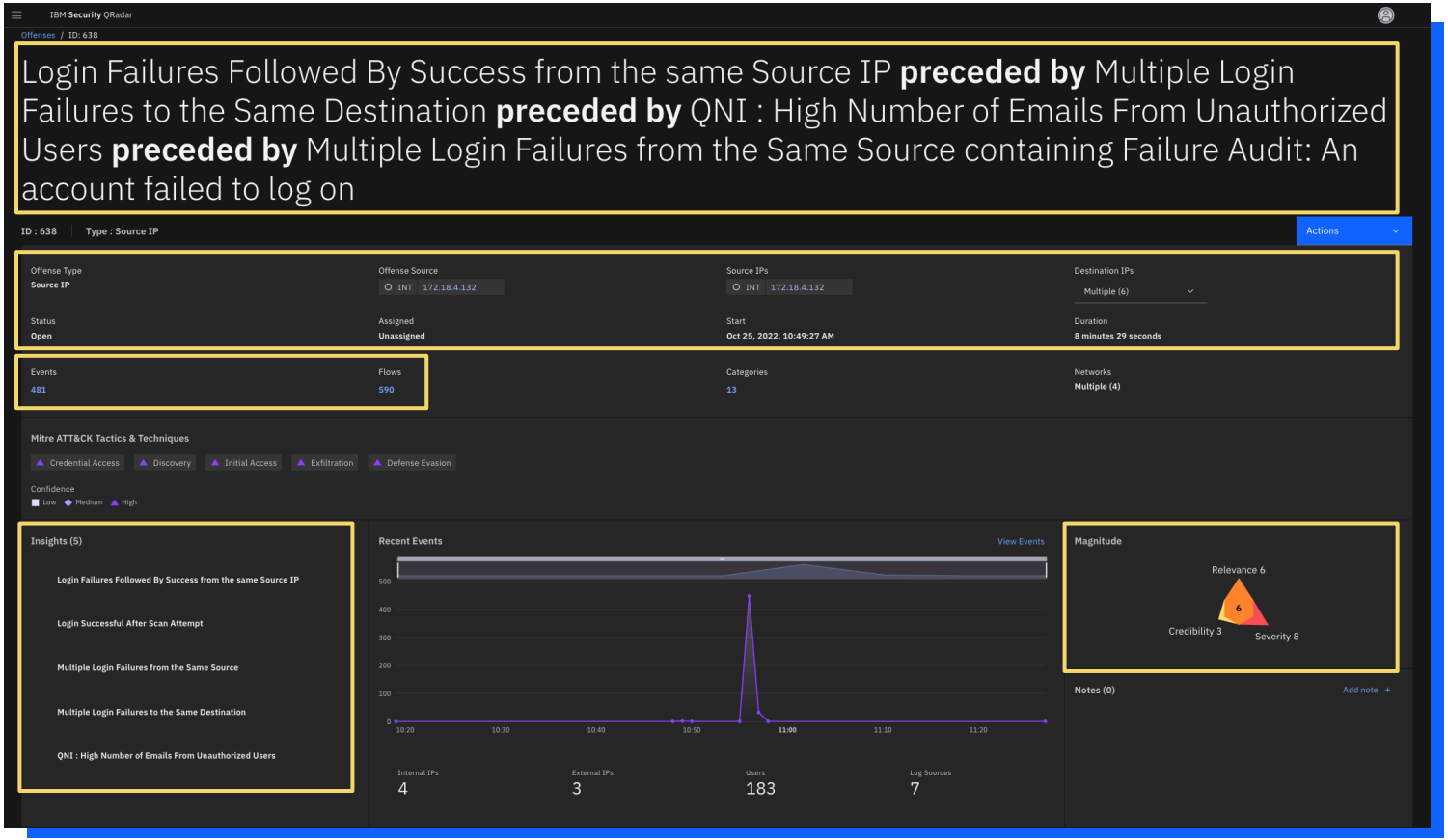
QRadar NBAD Engine

Behavior Anomaly Detection
Rules, Alerts, & Responses
Passive Asset Profiling

Packet & Flow Records

QRadar SIEM Core *Workflow*

Offenses



QRadar SIEM Core
Summary

Scalable

- Scalability for the largest deployments, using an embedded database and unified data architecture.
- High Availability and Data Redundancy functionality built-in
- On Prem, Cloud, VM or Hybrid

Automated

- Automation of data collection, asset discovery, asset profiling, Software updates, etc.

Intelligent

- Real-time correlation and anomaly detection based on broadest set of contextual data
- Integrated flow analytics with Layer 7 content visibility
- Data sources (any text data, full payload indexing, Full NBAD data capture)
- User Behavior Anomaly detection built-in
- Vulnerability integration
- Reputation and Threat Feeds built-in
- Data Enrichment Engine and Offense SIEM

Flexible

- Flexibility and ease of use enables “mere mortals” the ability to create and edit correlations rules, reports, dashboards, etc..
- Right ‘Out of the Box’ : over 450 Device Support Modules (DSMs), 620 correlation rules, and 1700 reports

IBM QRadar SIEM Core

What’s new?

QRadar SIEM Core

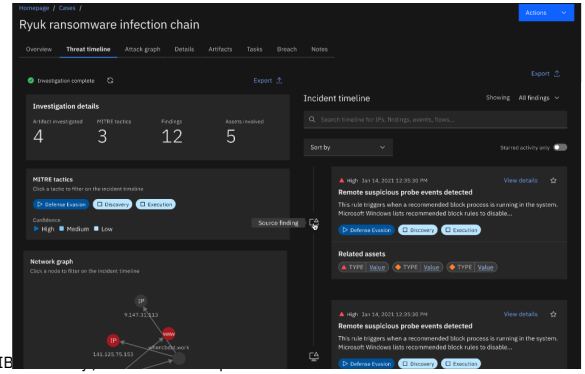
Key Functionalities

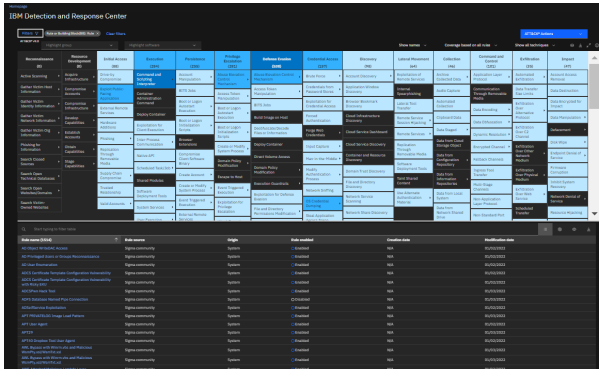
Centralized visibility and intelligent security analytics to detect, investigate and respond to your critical cybersecurity threats

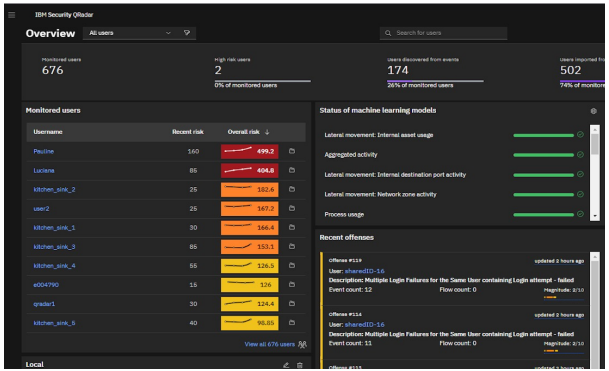
- Get complete visibility quickly and easily leveraging 700+ OOTB integrations
- Use included NDR and UBA to catch the hidden threats

- Don’t miss unknown threats with 1500+ out of the box detection rules and analytics mapped to MITRE ATT&CK
- Discover, classify network assets, devices automatically

- Detect unknown threats faster with real time offense-chaining
- Find unknown threats using Machine Learning for NTA and UBA for hidden network & insider threats



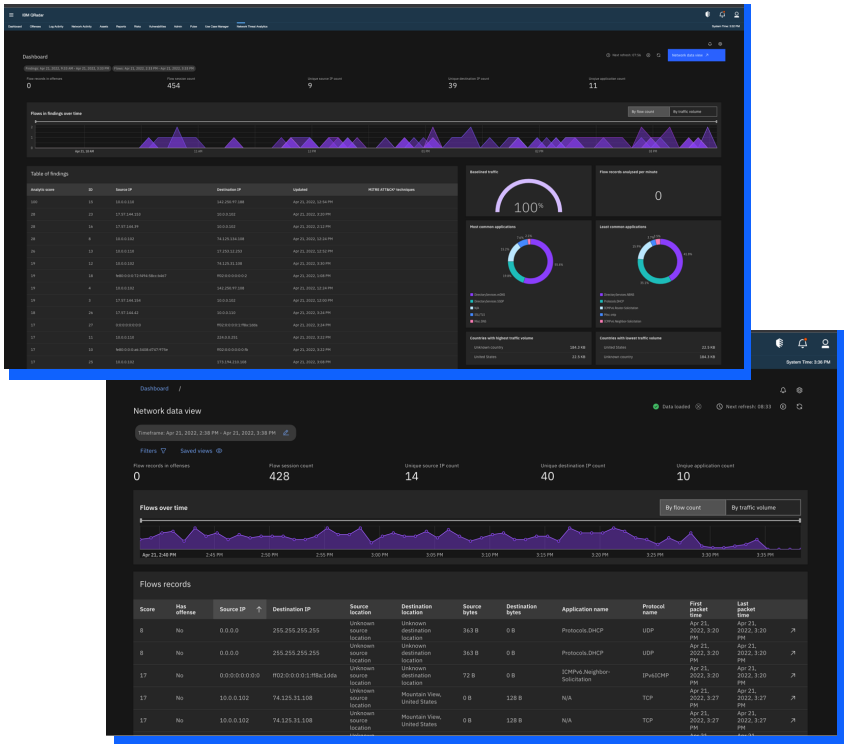




QRadar SIEM Core Key Functionalities

Network Threat Analytics (NTA)

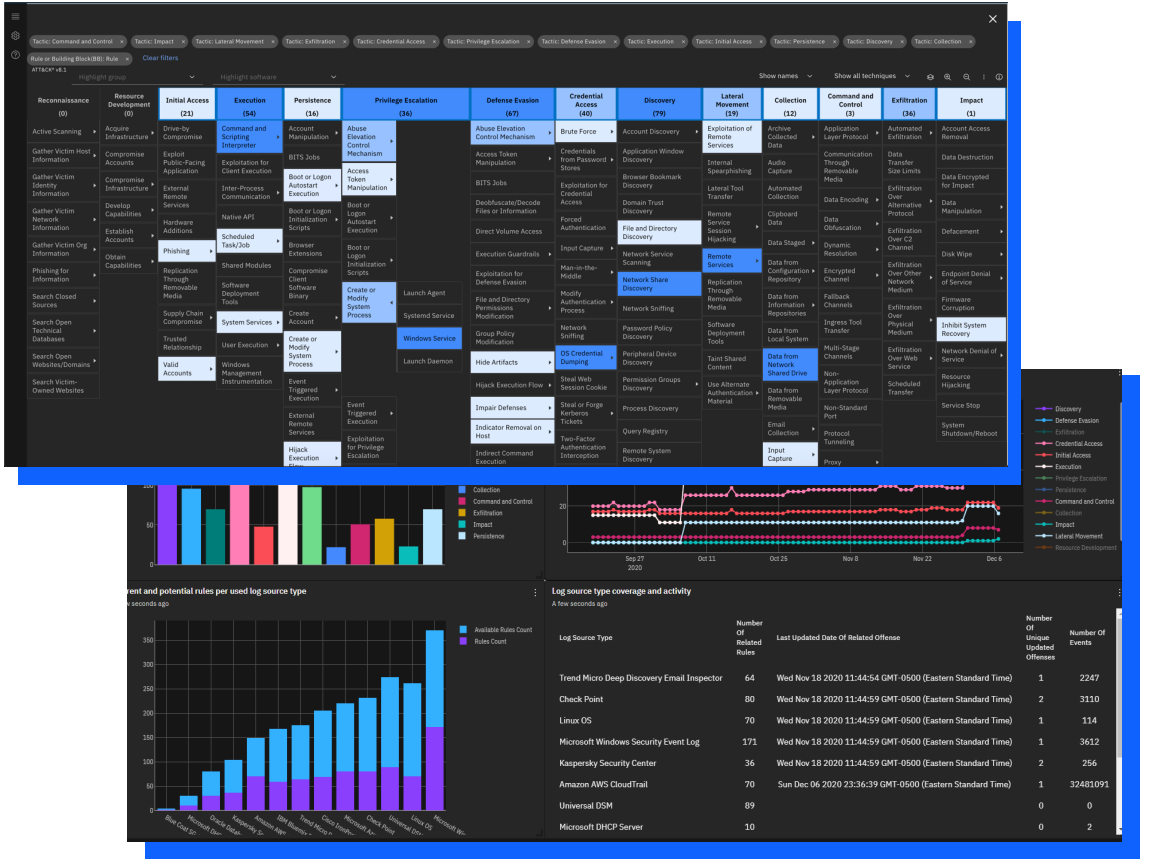
- NTA adds second tier of analytics
  - Continual analysis of related network activity
  - False positive reduction
  - MITRE ATT&CK sub-technique mapping
- Event generation
  - Events generated as new network behaviors observed or anomalies detected
  - NTA events can be used in rules, searches and other QRadar analytics
- New UI
  - Visualize all of your network communications and their analytics scores
  - Drill down into NTA tiered analytics
  - Filter and pivot across your network data and analytics during investigations or threat hunting



QRadar SIEM Core Key Functionalities

Use Case Manager

- Integration with UBA to centrally manage all use cases, and apply any rule to UBA
- New ability to report on deployed but inactive rules
- Support for all MITRE platforms, with the ability to select preferred platforms
- Updated support to MITRE ATT&CK v8.2



QRadar SIEM Core Key Functionalities

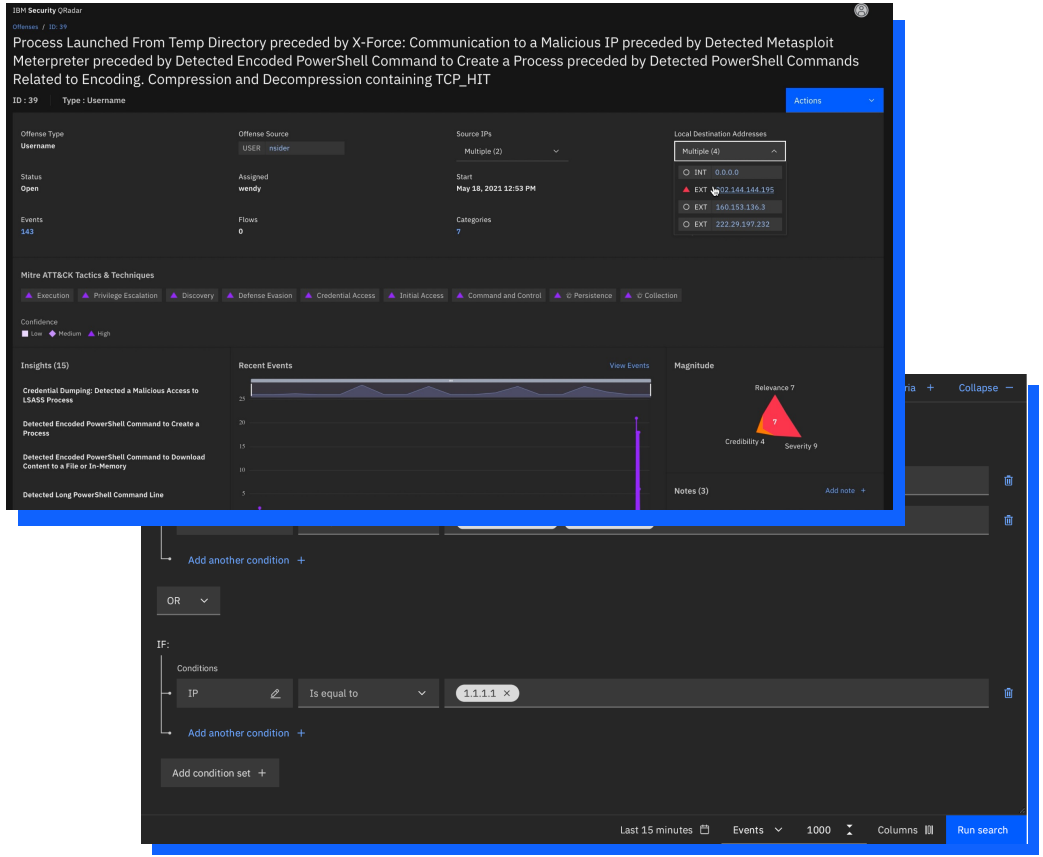
Analyst Workflow

Accelerate offense investigations

- New ability to see MITRE ATT&CK Tactics and Techniques that are part of an Offense
- Slide out panel integration with Reference Sets for greater business context
- Major performance improvements to users can navigate more quickly

Improved search experience

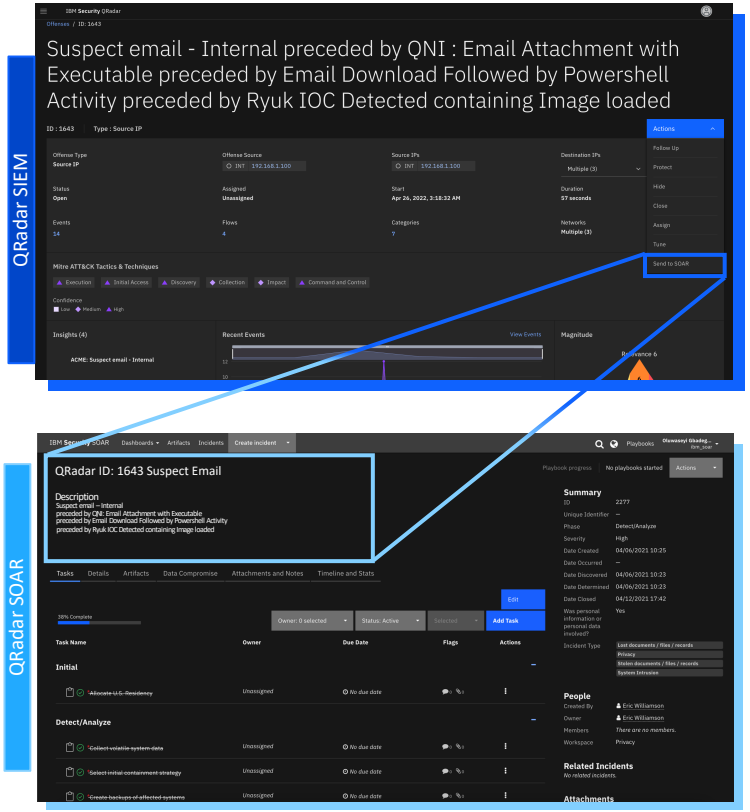
- AQL-less search experience
- Customize column views to see exactly what you're most interested in
- Shared, saved and recent searches for quicker searching
- Delivered as a standard QRadar Application starting with 7.4.3 patch



QRadar SIEM x SOAR Integration

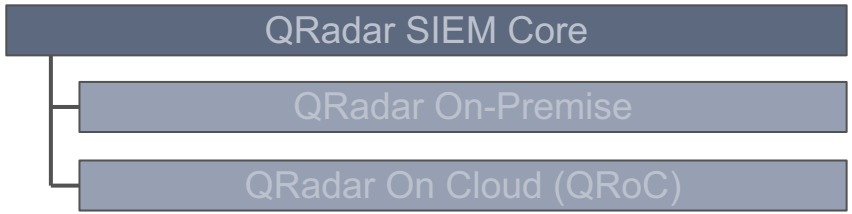
Application to empower, simplify, and streamline the process of escalating and managing cases between QRadar SIEM and QRadar SOAR.

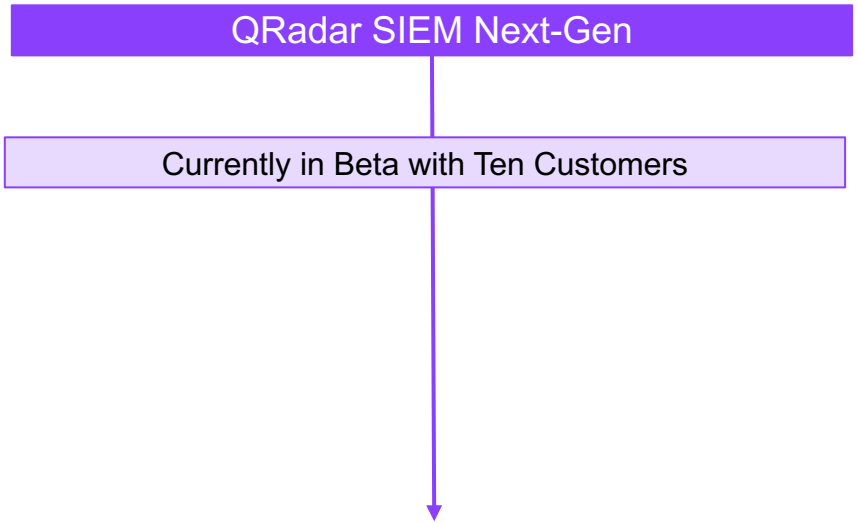
- Now with support for Analyst Workflow integration
- Automatically or manually escalate a QRadar offense to a SOAR case
- Map SOAR case fields to QRadar offense fields using JINJA2 templating syntax and filters
- Query/add SOAR artifacts to QRadar reference sets
- Synchronize notes between SOAR cases and QRadar offenses
- Close QRadar offenses and SOAR cases simultaneously



QRadar SIEM *Next-Gen*

Introducing QRadar SIEM *Next-Gen*





What Customers Have Asked Us

A solution that can...

1. Ingest telemetry, events at cloud scale with cloud elasticity to extract insights – tightly integrated w/ Cloud Security Services
2. Produce sub-second search results to large queries and enable real-time investigations
3. Offer insightful, interactive, intuitive Visualizations for quick, at-a-glance visibility to most critical threats
4. Provide flexible retention options in hot, warm and cold storage
5. Provide turn-key OOTB cloud services onboarding and automation
6. Provide correlation rules and open analytics for real-time threat detection

What IBM Security Will Deliver

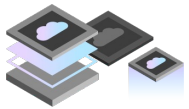
QRadar SIEM *Next-Gen*

A cloud-native SIEM solution with cloud-scale elastic ingestion, sub-second search performance, insightful visualization and open/real-time analytics

Phase 2 – QRadar SIEM

Phase 1 – QRadar NGLM

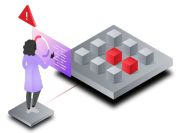
Cloud-scale Ingestion



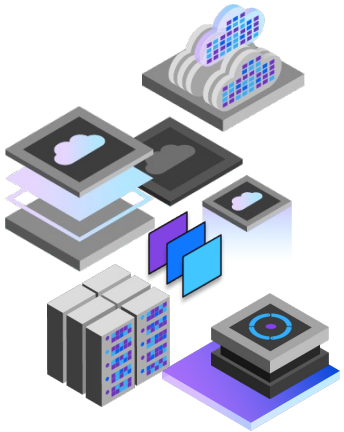
Sub-second Search

Insightful Visualization

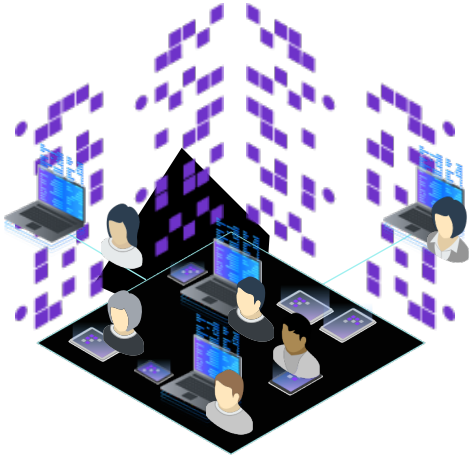
Real-Time Analytics



QRadar SIEM *Next-Gen*
Phase 2

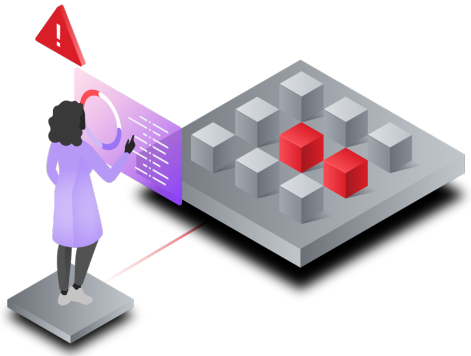


Ingestion
Cloud-scale log ingestion to improve visibility



Search
Sub-second search speed to reduce threat detection and dwell time

Visualization
Insightful data visualization for efficient threat investigation



Detection
Community driven Sigma and Yara Analytics for real-time threat detection

IBM QRadar SIEM *Next-Gen*

Architecture

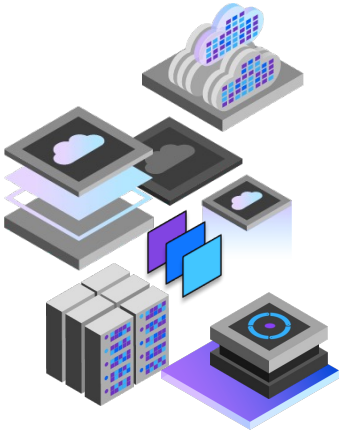
QRadar SIEM *Next-Gen* Architecture

A Targeted Transformation

- Elastically Scalable
- Cloud Native Architecture
- Multi-Tenancy and HA by Design
- Granular Access Control
- Modern High-Performant Data Warehouse
- Sub-second Search Results
- Hyper Ingestion Capable Parsers

IBM QRadar SIEM *Next-Gen*

Planned Innovations & Roadmap



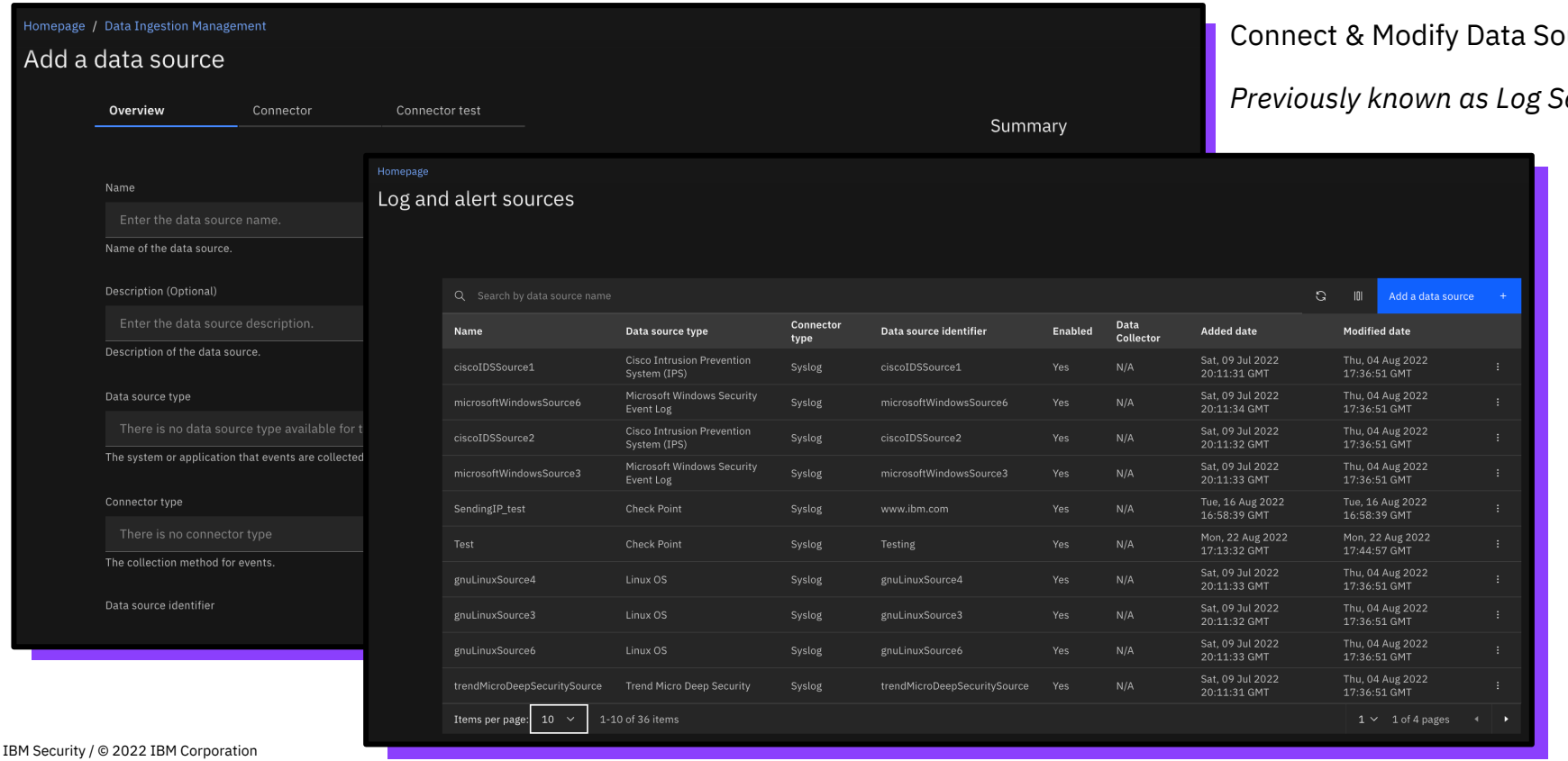
Ingestion

Cloud-scale log ingestion to improve visibility

- Connect 100+ data sources with a single, easy to follow workflow
- Ingest 500K EPS to collect essential data on all your threat vectors
- Normalize raw payloads to interpret previously unrecognizable events

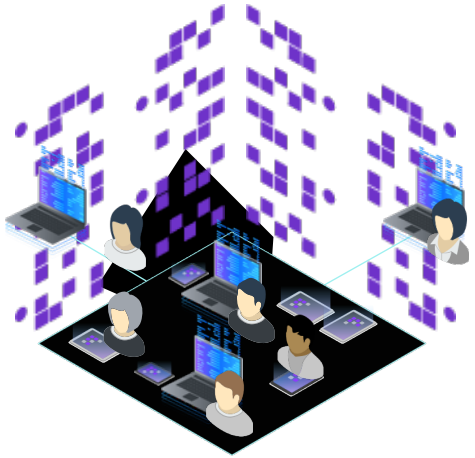
Ingestion

Data Source Management



Connect & Modify Data Sources

Previously known as Log Sources



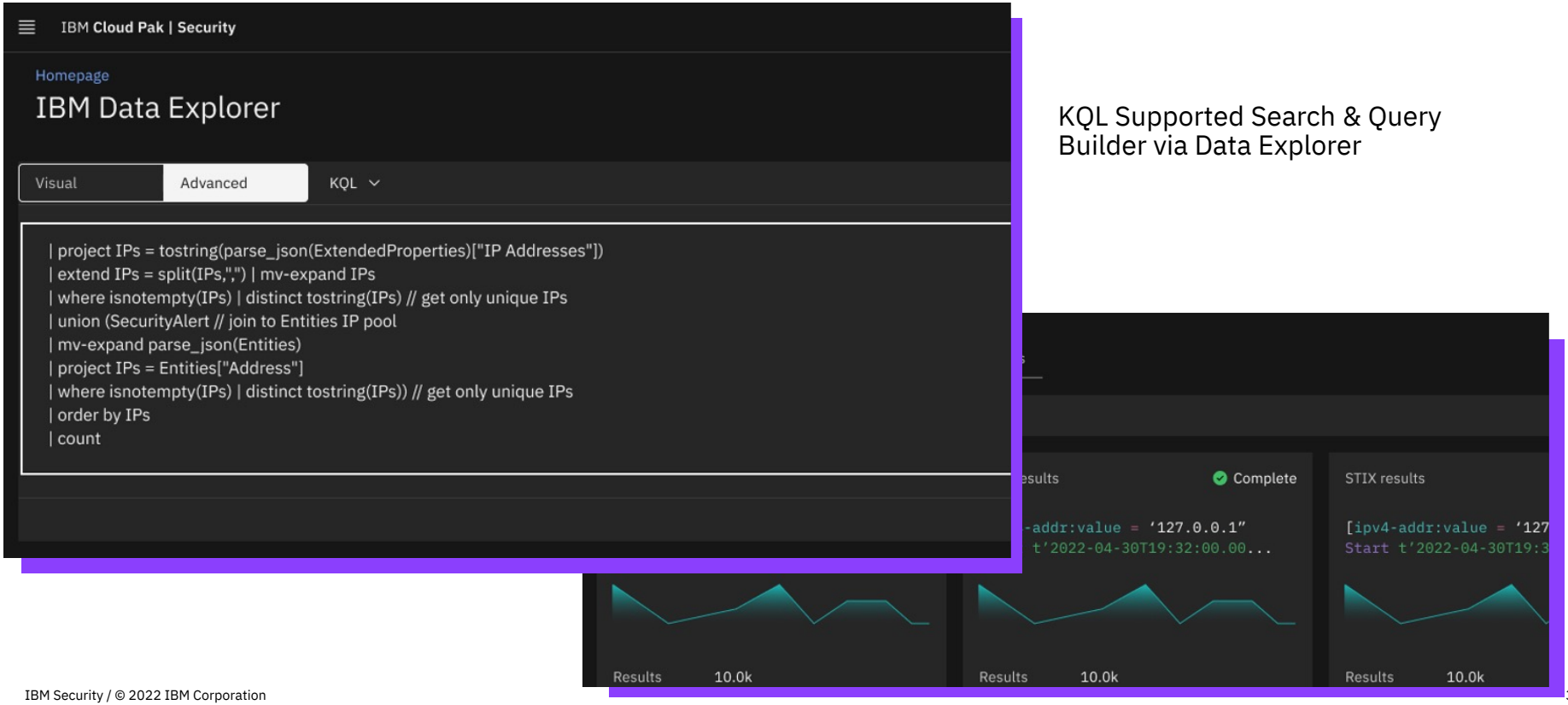
Search

Sub-second search speed to reduce threat detection and dwell time

- Identify threats in seconds by harnessing the power of high performant data warehouse
- Minimize detection time by employing KQL, an advanced intuitive query language
- Build visual queries effortlessly that require no advanced query language knowledge

Search

KQL Supported Search & Query Builder via Data Explorer



KQL Supported Search & Query Builder via Data Explorer

Visualization

Insightful data visualization for efficient threat investigation

- Insightful dashboards to obtain a centralized view of IOC
- Interactive analyst dashboards to visualize critical threats by severity and impact
- Customizable dashboards that streamline SOC Analyst workflow

QRadar SIEM *Next-Gen*

Summary

Ingestion

- Connect 100+ data sources with a single, easy to follow workflow
- Ingest 500K EPS to collect essential data on all your threat vectors
- Normalize raw payloads to interpret previously unrecognizable events

Search

- Identify threats in seconds by harnessing the power of high performant data warehouse
- Minimize detection time by employing KQL, an advanced threat hunting language
- Build visual queries effortlessly that require no advanced query language knowledge

Visualization

- Intuitive, powerful dashboards to obtain a centralized view
- Interactive analyst dashboards to visualize critical threats by severity and impact
- Customizable dashboards that streamline SOC Analyst workflow

Detection

- Community driven Sigma and Yara Analytics for real-time threat detection (Phase II)

Thank you