IBM Security

The open complete threat detection IBM QRadar XDR

Erasmo Volpe
evol@ch.ibm.com

Domenico Lojacono
dloj@ch.ibm.com

February 4. 2022

IBM

AGENDA

1. QRadar XDR
2. ReaQta EDR
3. Q&A

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

QRadar XDR

QRadar Vision

- Provides intelligence, automation, openness and seamless workflow across threat detection and response
- Utilizes existing investments in 3rd party tools
- Based on open technologies and standards to avoid lock in and future choice

Evolution and modernization of QRadar

Single Pane of Glass

Unified Threat Insights

Incident Management

Reporting / Compliance

Automated and Orchestrated Response

Incident Response

- Case and Incident Management
- Automation and Orchestration
- Ecosystem Partners
- Threat Playbooks
- Compliance and Privacy
- Ansible IT Automation

Unified Insights and Investigation

Intelligence Driven Detection & Investigation

- Reduce security alerts
- Correlate siloed insights
- Provide contextual data
- Prioritize findings
- AI and MITRE ATT&CK
- No data duplication/movement

Elastically scalable common platform infrastructure

Existing QRadar Investments

QRadar Classic

Open Ecosystem

EDR
CASB
CWP
Email Security
Data Security
Identity ...

QRadar Data Lake

QRadar SIEM

QRadar NDR

QRadar User Insights

Modular components delivered on common infrastructure

Open Cybersecurity Alliance (OCA): Co-founded by IBM to promote and and support open security

https://opencybersecurityalliance.org/
https://oasis-open-projects.org/

Who

Global like-minded cybersecurity vendors, end users, thought leaders & individuals

Vision

Open Cyber Security Ecosystem:
Products freely exchange information, insights, analytics & orchestrated response

How

Open
Commonly developed code & tooling
Mutually agreed upon technologies, standards & procedures

Technical Committee Sponsors

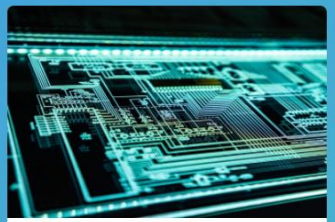
- Accenture, LLP
- Adobe Systems
- Anomali Incorporated
- Cisco Systems
- Copado
- Cryptsoft
- Cyware Labs
- Dell
- EclecticIQ
- EMQ Technologies
- European Union Publications Office
- File and ServeXpress
- Fujitsu
- GrammaTech
- Hewlett Packard Enterprise (HPE)
- Hitachi
- Huawei Technologies
- IXIASOFT
- Logius
- McAfee, LLC
- Microsoft
- nCipher
- NEC Corporation
- Oracle
- P6R, Inc.
- Red Hat
- SAP
- Security Compass
- SEKOIA
- Sophos Ltd
- Sopra Steria Group
- TELUS
- ThreatQuotient, Inc.
- Trend Micro, Inc.
- Tyler Technologies
- US Department of Defense (DoD)
- US Federal Bureau of Investigation
- US NIST

OPEN CYBERSECURITY ALLIANCE

Home Benefits Projects About Contact News

PROJECTS

OCA advances a growing body of open source projects.



Kestrel

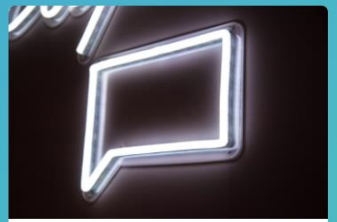
Threat Hunting Language

Provides an abstraction for threat hunters to focus on what to hunt instead of how to hunt.

STIX Shifter

Patterning Library

Allows data to be normalized across domains for comprehensive security analysis



OpenDXL Ontology

Messaging Format

Enables real-time data exchange and cross-vendor orchestration

NIST SCAP v2

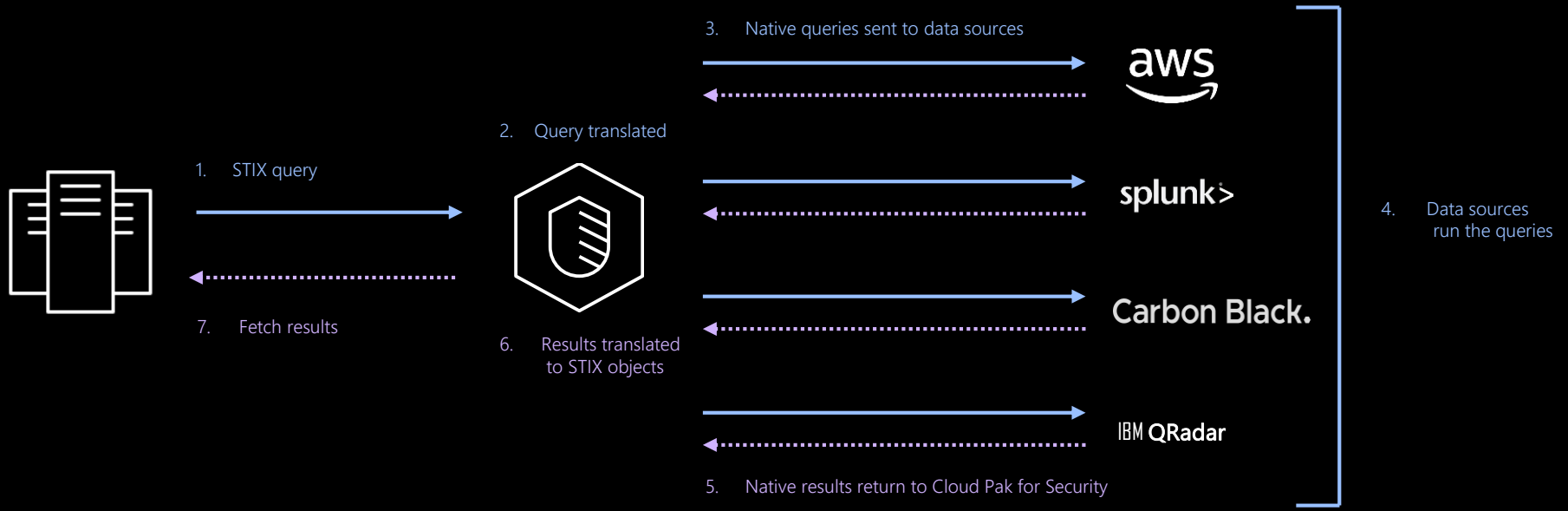
Data Collection Architecture

Supports continuous monitoring for tracking assets' policy compliance

IBM Security

IBM

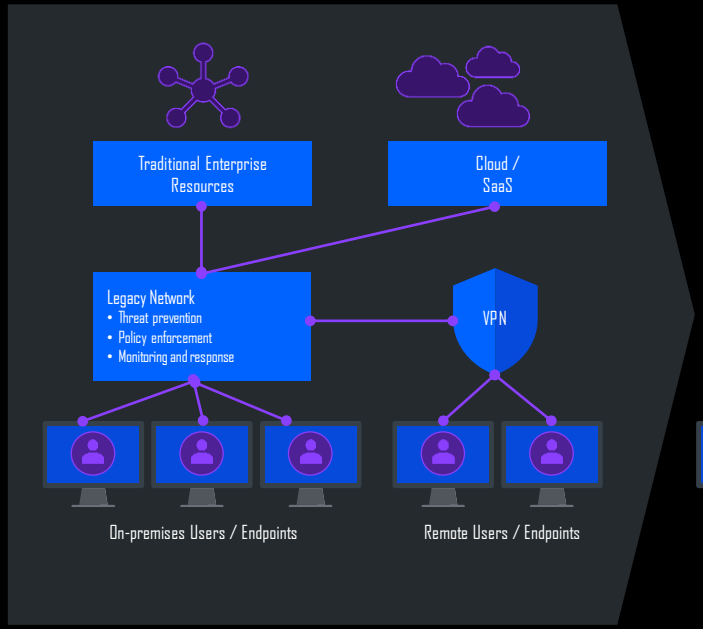
STIX Shifter – How it works



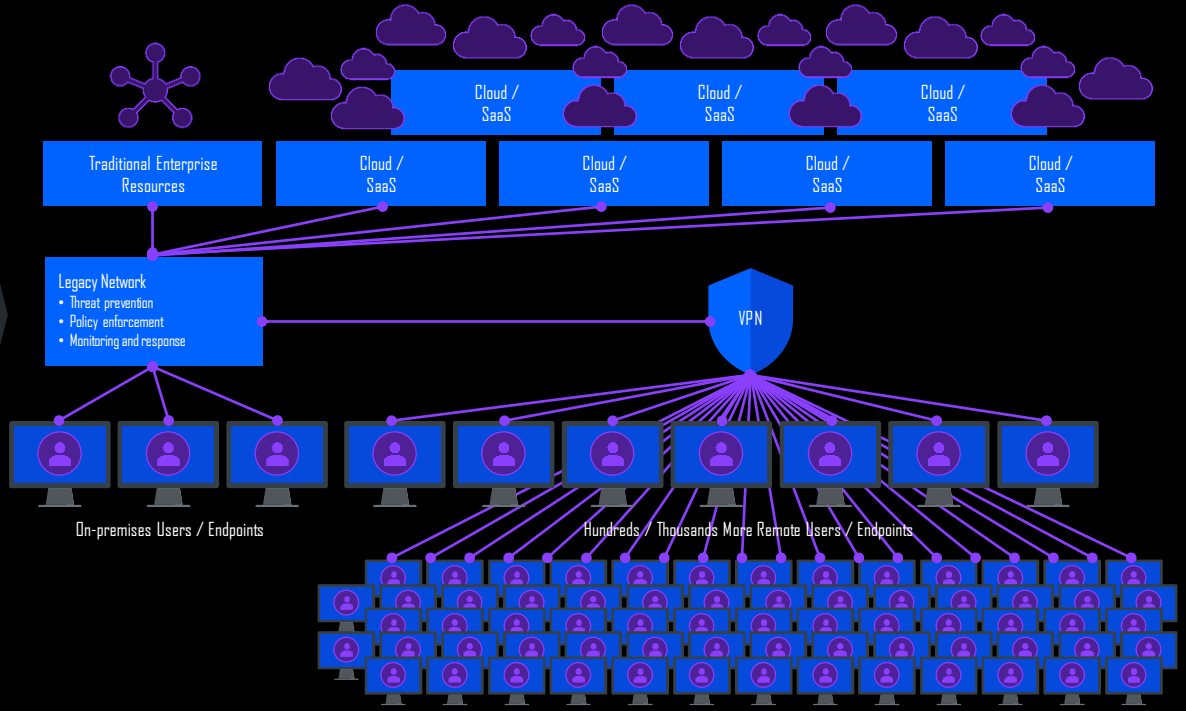
1. Federated query using a STIX pattern
2. Query is translated to the native query language of each of the data sources
3. The converted query is then sent (transmitted) to all data sources
4. Each data source runs its own native query
5. The native query results are then returned from the data source
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

Evolving enterprise architectures is forcing enterprises to rethink their security approach

Previous Enterprise Architectures



Current Enterprise Architecture Complexity



Source: Scott Crawford, 451 Research, part of S&P Global Market Intelligence

Legacy defenses and security teams face challenges against advanced threats

Costs and complexity

Many siloed tools and disjointed workflows can increase costs

Missed threats

Traditional approaches rely on finding what's known and can miss new attacks

Poor visibility

Digital transformation and cloud adoption have expanded monitoring needs, but there can be blind spots

Struggle to keep up

Today's threats are extremely complex and automated, humans can have difficulty evaluating many fast-moving parts at once

How organizations can modernize threat detection and response

Eliminate silos

Gain visibility across data sources — from the cloud to the core

Unify workflows

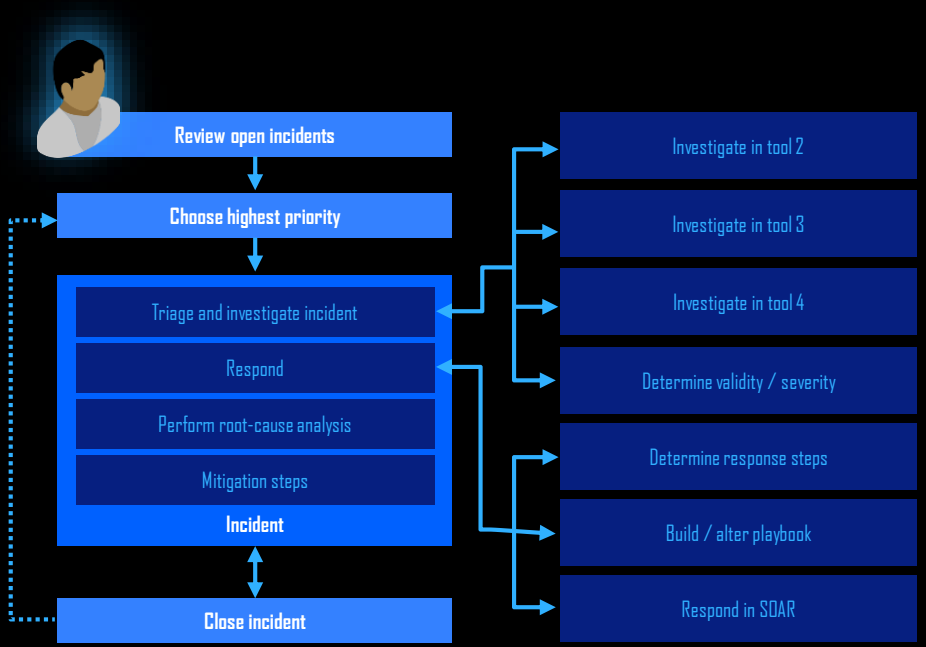
Work without pivoting between tools

Automate work

Let machines do the heavy lifting — whether mundane tasks or complex analysis

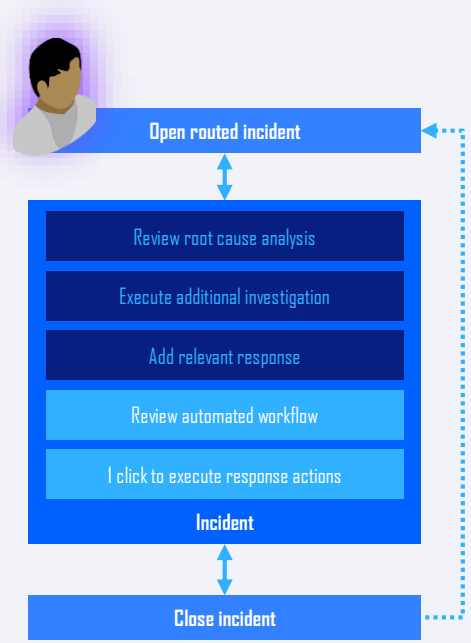
BEFORE

Security analysts typical workflow complexity



AFTER

Simplified workflow using QRadar XDR



- Fewer, more accurate alerts with an open scalable approach
- Leverage existing tools and avoid vendor lock in
- Streamlined workflow, reduced manual effort thanks to automation
- Pre-built detection and response so teams can protect your organization, even without deep security expertise

Source: Forrester Report, Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR, April 2021

IBM Security QRadar XDR, an Open, Connected Approach

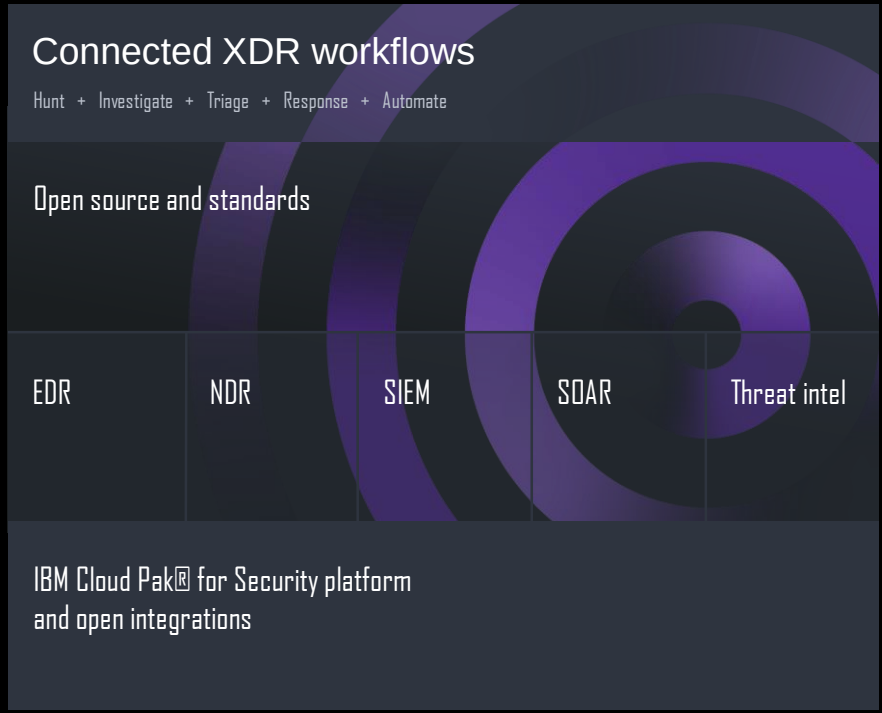
Connected - Integration with Existing Tools or IBM's
The industry's largest Open XDR ecosystem can integrate your EDR, SIEM, NDR, SOAR and Threat Intelligence, while leaving data where it is for a complete XDR approach

Unified - Single User Experience across Tools & Teams
Simple XDR workflows, co-designed with experts, help speed up alert triage, threat hunting, investigation and response

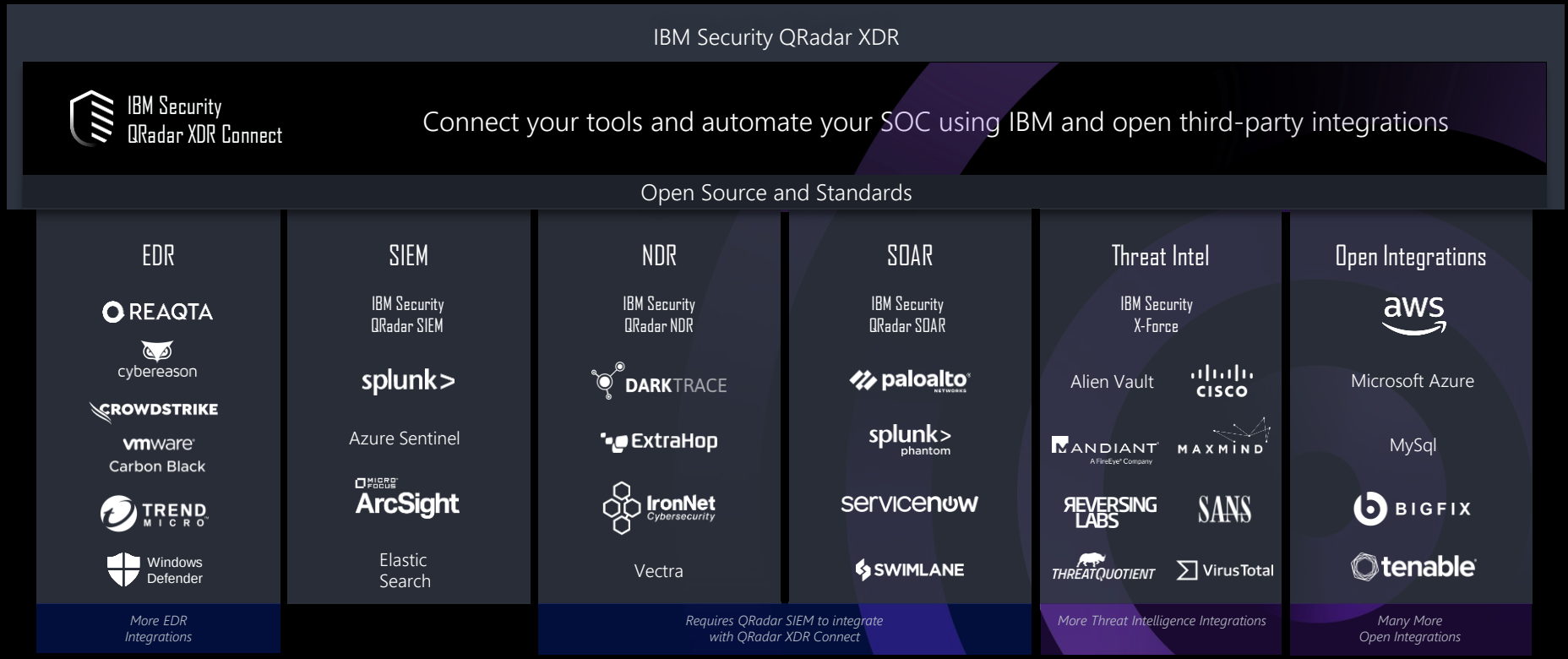
Intelligent - AI Built for Analyst Productivity
Automate the work of enriching, correlating, and investigating threats with purpose-built AI and pre-built playbooks, including automated root cause analysis and MITRE ATT&CK mapping

Open – Adaptable Architecture to Help Avoid Lock-In
Built on IBM Cloud Pak for Security for deployment on premises or on cloud, and ready for use by security service providers

IBM Security QRadar XDR



IBM Security QRadar XDR, an Open, Connected Approach

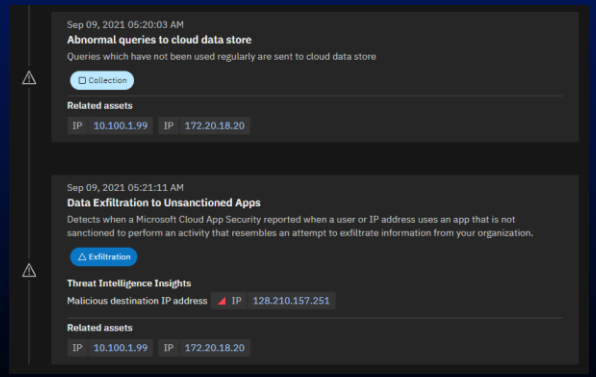


IBM Security QRadar XDR Connect

Connect your tools, automate your SOC, and free up time for what matters most

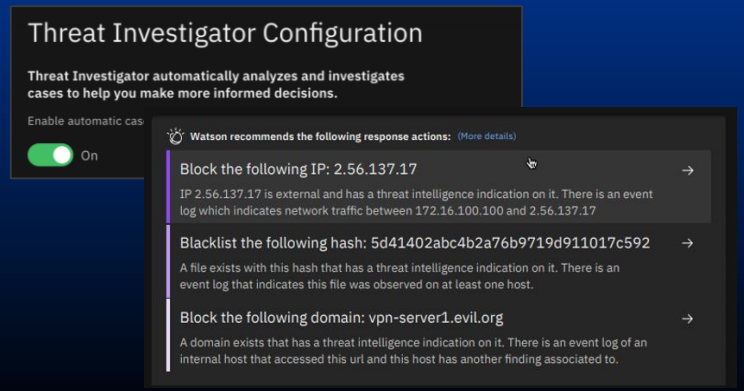
Gain enhanced insights while improving threat detection

Correlate related alerts by connecting additional telemetry and prioritize threats to eliminate alert fatigue.



Act quickly with automated threat investigations and accelerated threat hunting

Use AI to automate case investigation and correlate data, allowing more time for strategic imperatives. Improve prioritization, root-cause analysis and response with MITRE ATT&CK mapping and contextual intelligence.



Response recommendation planned for Q1 2022

Leverage your existing security tools with an open approach

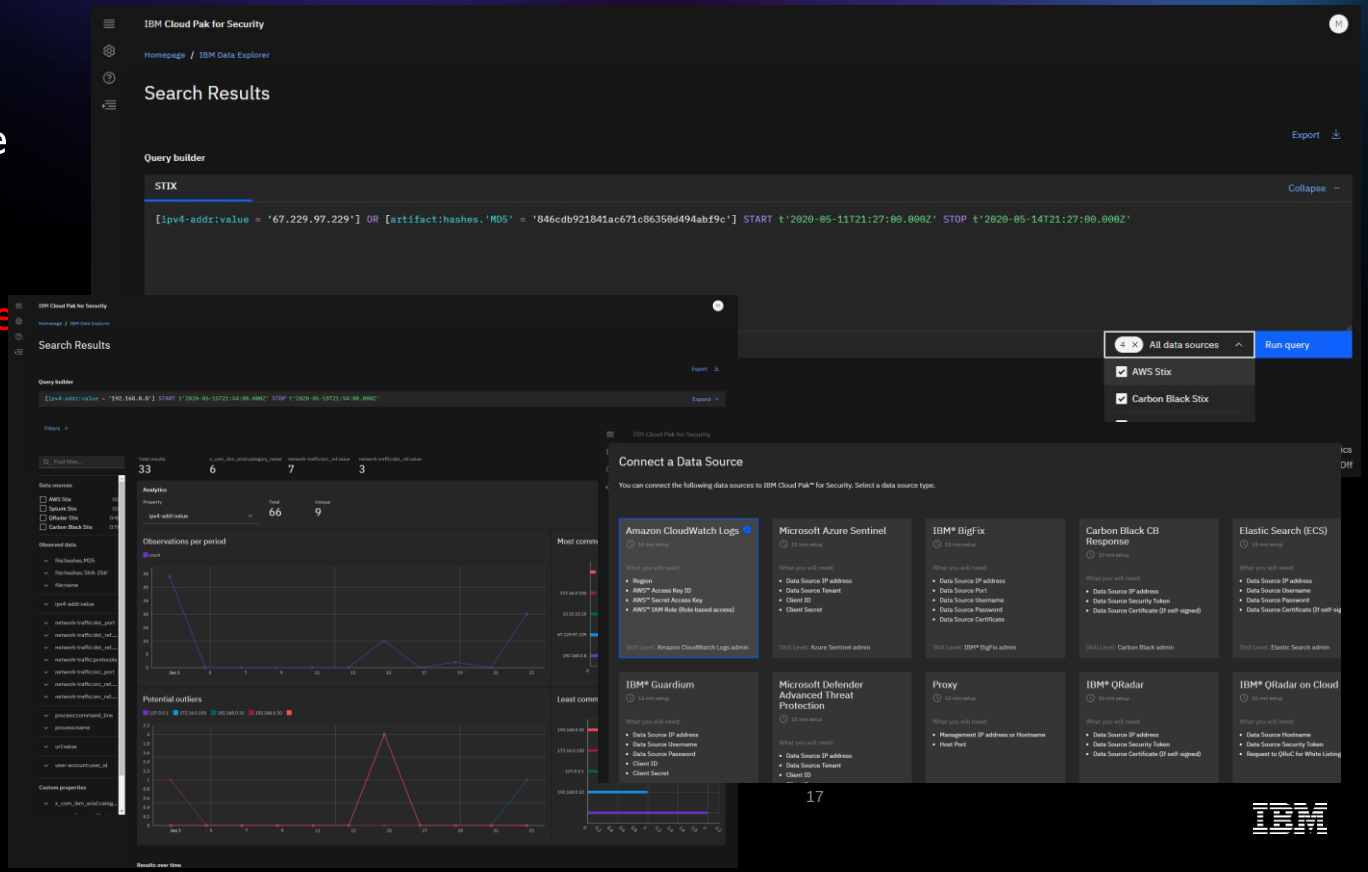
Enable your teams to connect a full range of tools, data and intel feeds to modernize your SOC.

OPEN CYBERSECURITY ALLIANCE

Data Explorer

Federated search & investigation

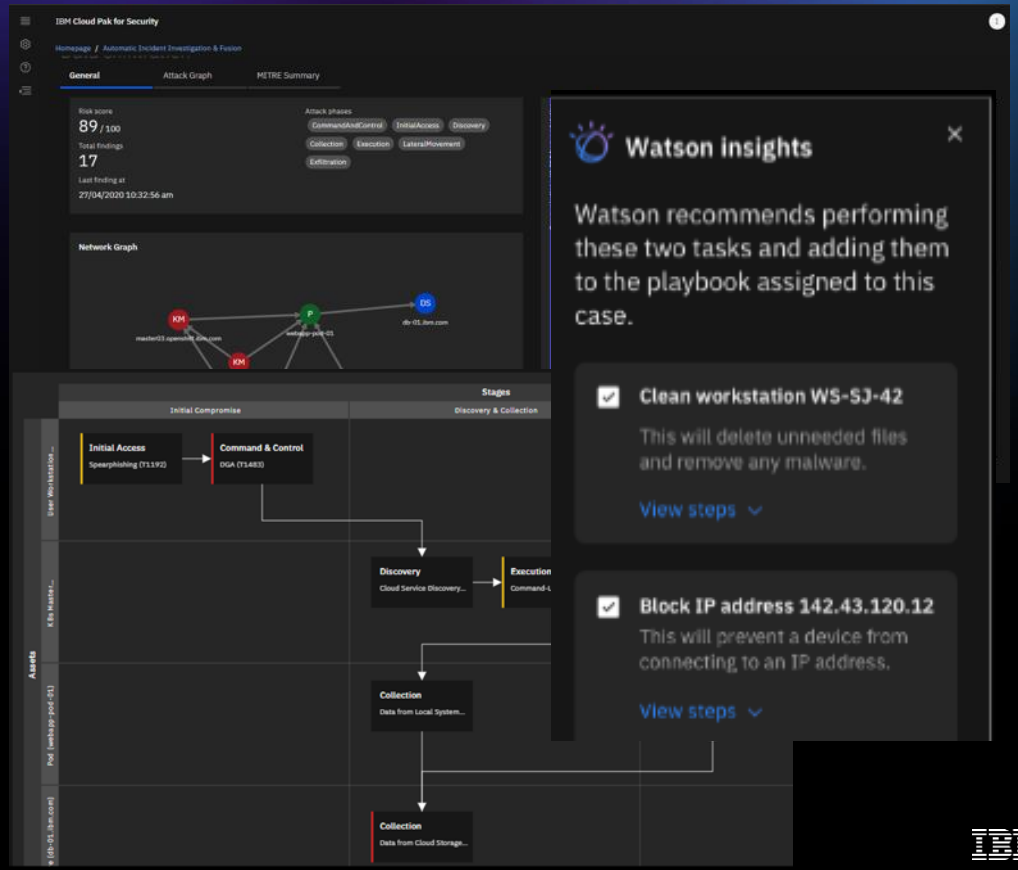
- Run queries and find insights against multiple data sources without moving your data
- Investigate from a single unified interface to search threats and IOCs
- Immediately see the attributes in a log and pivot to discover statistically relevant attributes



Threat Investigator

Automatic, accurate, consistent threat investigations

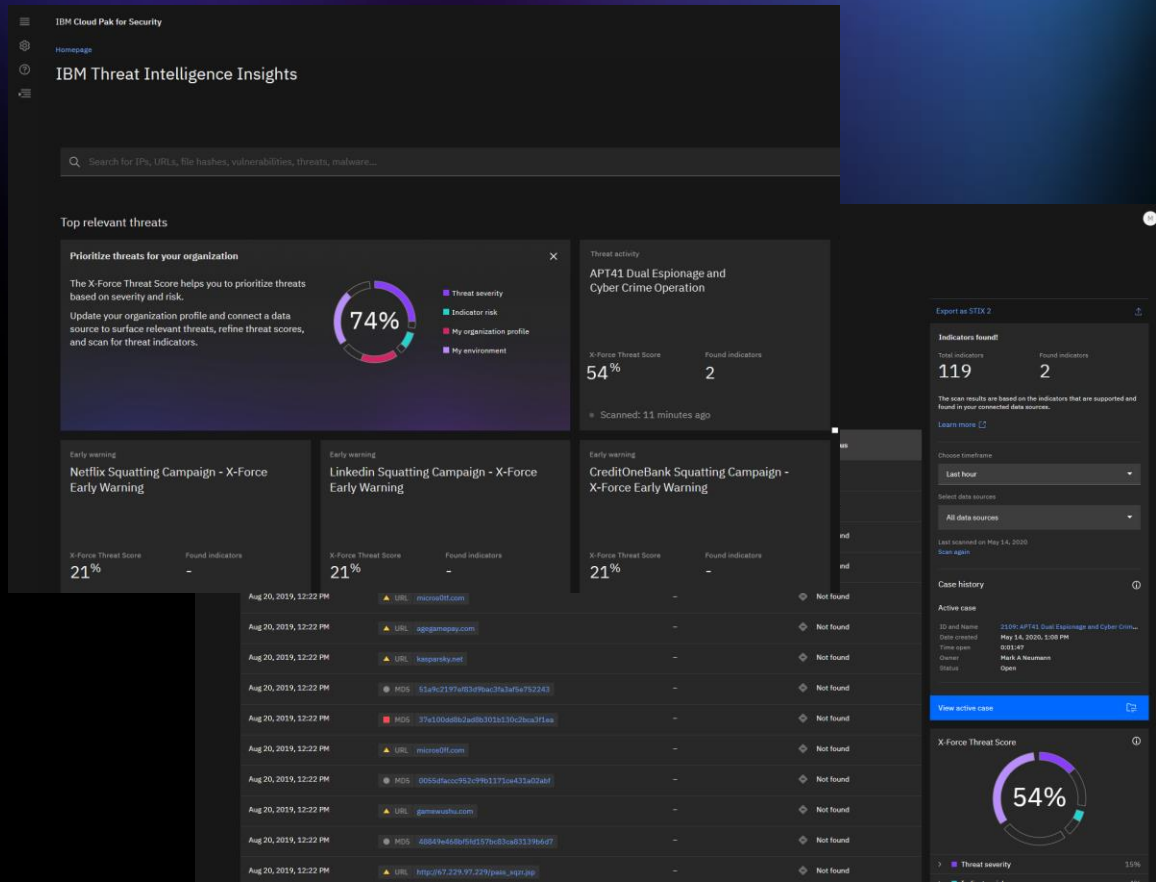
- Automatic Case Investigations increase SOC effectiveness by reducing manual effort during analysis, evidence acquisition and threat intelligence correlation.
- Simplified Timeline View of the Attack sequences the threat allowing the analyst to better comprehend the issue.
- Mitre ATT&CK Chain Classification provides a clear and concise asset centric view of the threat .
- Recommended remediation steps enables a fast response



Threat Intelligence Insights

Prioritized, actionable threat intelligence

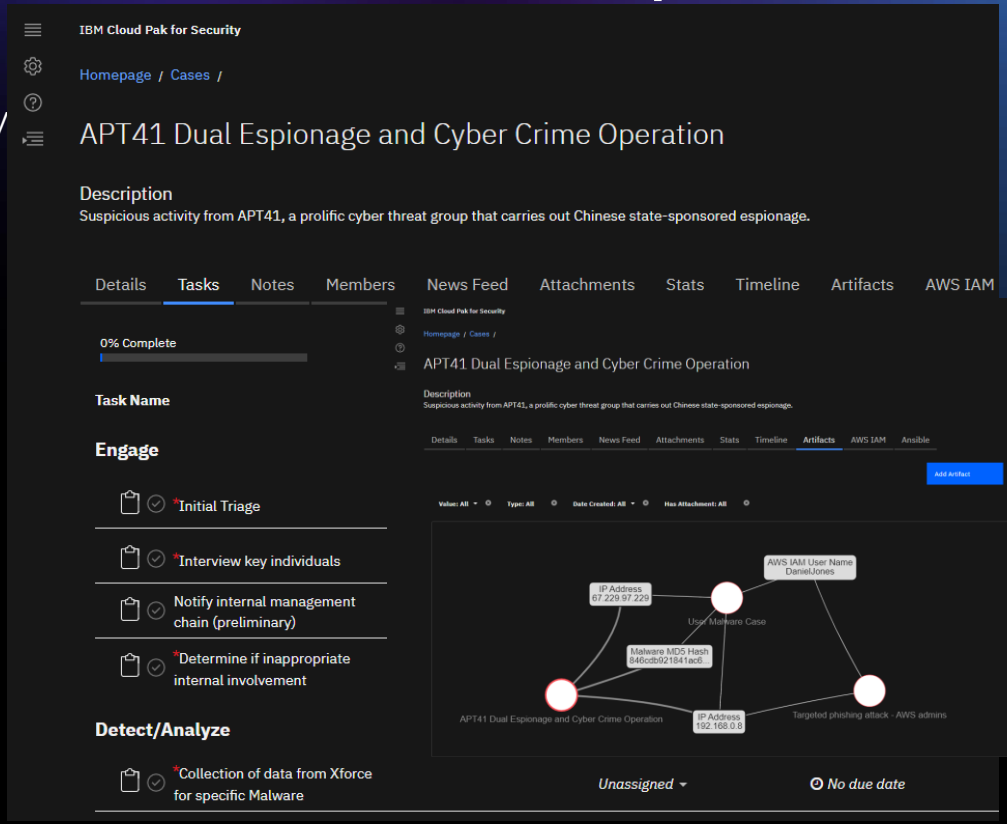
- Prioritize threats with X-Force Threat Score, an adaptive score, calculated based on your relevance, severity, penetration, impact and actual environmental sightings
- Identify threats active in your environment with Am I Affected, which runs continuous and automated searches across connected data sources



Cloud Pak for Security - Case Management

Orchestration, automation, and response

- Reduce time to respond to and remediate complex cyber threats by automating Incident Response processes with robust case management and tasks
- Streamline and automate manual and repetitive tasks such as IOC enrichment
- Prioritize analyst workload on high-value investigation and response activities by guiding analyst response



ReaQta

About ReaQta

REAQTA

- Founded in 2014 by cybersecurity professionals with deep AI / ML expertise
- Headquarters in Amsterdam and Singapore
- 30+ employees

MITRE ENGENUITY | ATT&CK Evaluations

- #1 in Attack Coverage per Alert Generated
- #2 in Alerts Actionability
- #2 in Alerts Quality
- #3 in Captured Telemetry
- 90% of Attack Contained

Source: https://reaqta.com/2020/04/mitre-attack-evaluation-confirms-reaqta-hive-advanced-detection-capabilities/

Gartner COOL VENDOR 2020

FROST & SULLIVAN 2020 BEST PRACTICES AWARD

ENTERPRISE SECURITY TOP 10 ENDPOINT SECURITY SOLUTION PROVIDERS 2020

Industry Recognition

- Gartner Cool Vendor in Network and Endpoint Security, 2020
- Frost & Sullivan's European Technology Innovation Award for Behavioral Cyber Threat Detection, Europe - 2020
- Enterprise Security Magazine's Top 10 Endpoint Security Solution Providers in Europe, 2019 - 2020
- EDR of choice from the 2020 Cyber Security Agency of Singapore Cybersecurity Industry Call for Innovation

Gartner peerinsights customers' choice 2021 ™

"Endpoint Security without the extra headache or headcount!"
- Energy and Utilities Company

"Great to have a silent assassin in your corner!" - Financial Company

What makes ReaQta a different endpoint protection solution?

WORLD'S FIRST
AND ONLY

NANO OS

Live-Hypervisor
based monitoring

- Monitors the Operating System (OS) from the outside
- Offers broad visibility and insight over application's life
- Designed to be invisible to malware
- Proprietary detection of high-level malicious behaviors:
  - Keylogging, Dynamic Impersonation, Credential Harvesting, Kernel Exploits, Screen captures

217+ READY PARAMETERS 80+ BEHAVIORS

ADVANCED THREAT DETECTION

Automated AI-driven threat detection

- 80+ threat behavioral models deployed at the endpoint
- 217+ specific parameters for all detection and hunting needs
- Remediation with single click to help remote kill in real-time
- Allows user to build own detection strategies and playbooks

CAN HELP REDUCE FALSE POSITIVES BY
80%+

CYBER ASSISTANT

One-shot learning system

- Learns from analyst decisions and applies actions
- Can help free up time for analysts to focus on higher level tasks
- Available for single customers or for multi-tenant MSSPs

IBM

ARCHITECTURE

Learn • Detect • Track • Respond • Protect

Endpoint AI & Nano OS

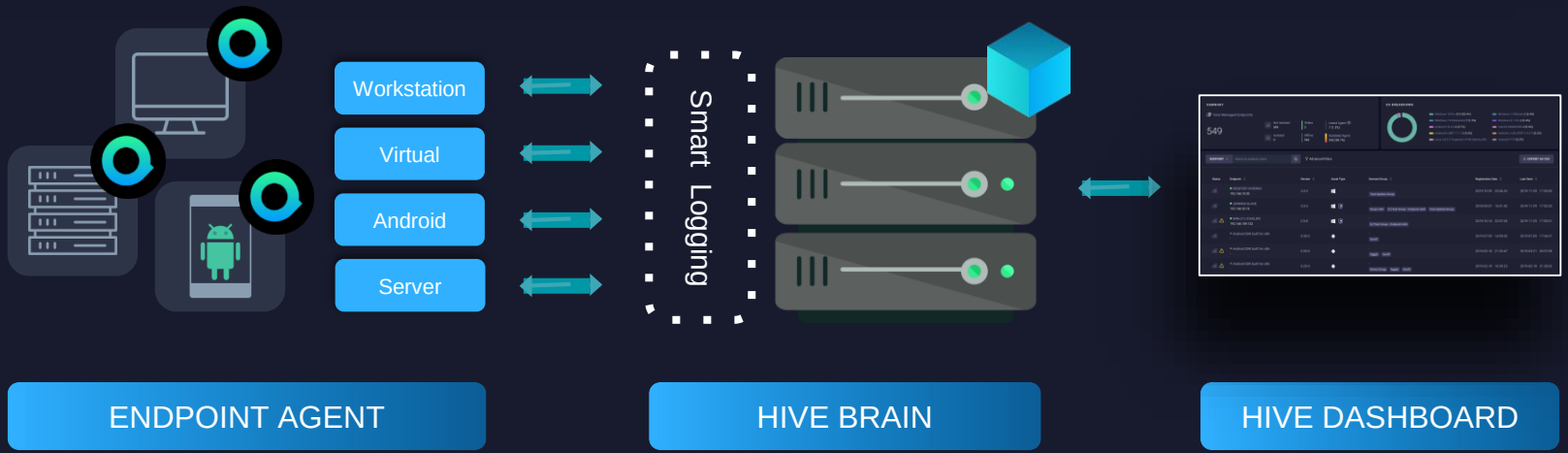
Real-Time Coverage

Infrastructural AI

Data Collection & Behavioral Analysis

Single Console

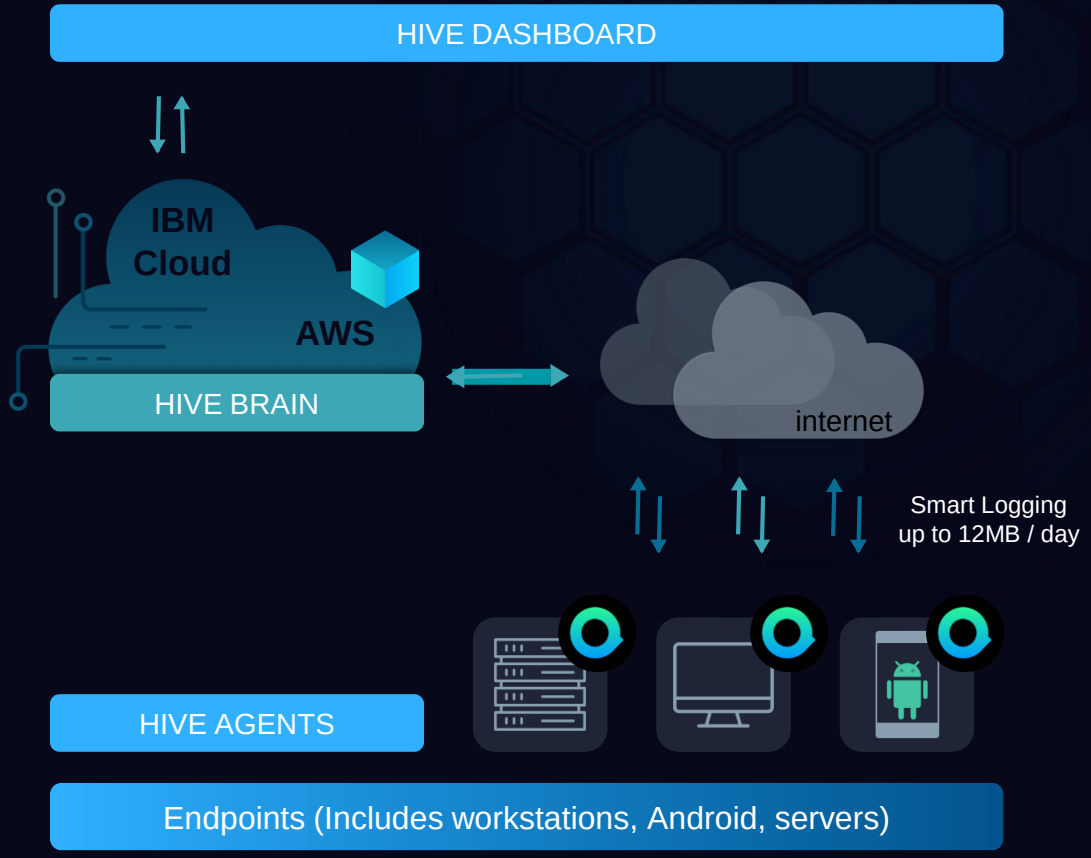
Optimised Remediation Workflow



REAQTA

DEPLOYMENT

CLOUD



All Network Traffic

* MSI Package Deployment via GPO (15Mb) with no Internet required

REAQTA

DEPLOYMENT

ON-PREM

HIVE DASHBOARD

HIVE BRAIN

Supports Isolated Network
Fully Air-Gapped Environment

Smart Logging
up to 12MB / day

HIVE AGENTS

Endpoints (Includes workstations, Android, servers)

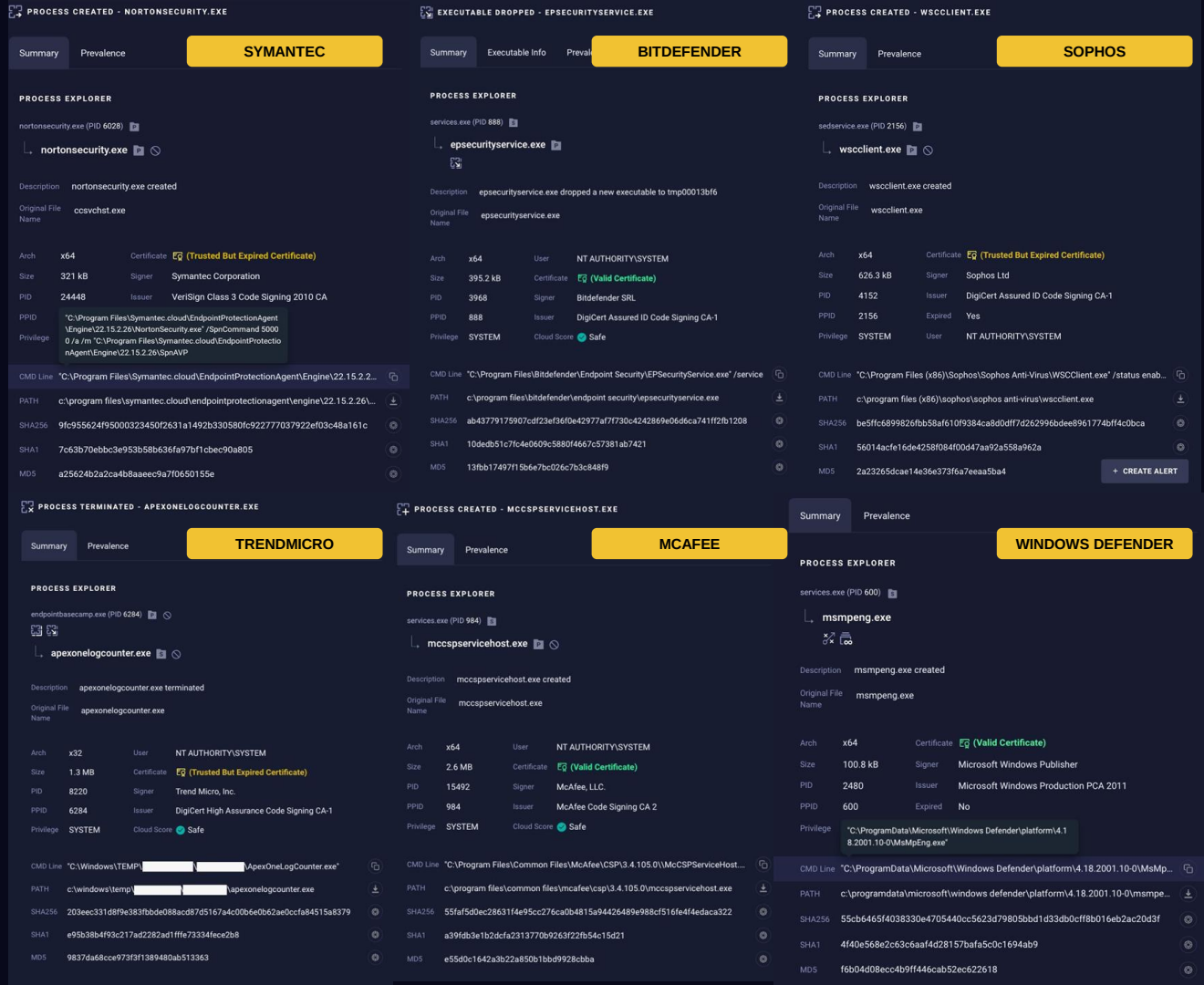
All Network Traffic

* MSI Package Deployment via GPO (15Mb) with no Internet required

REAQTA

ReaQta-Hive coexists with any Antivirus solutions to provide an enhanced layer of security, visibility and control.

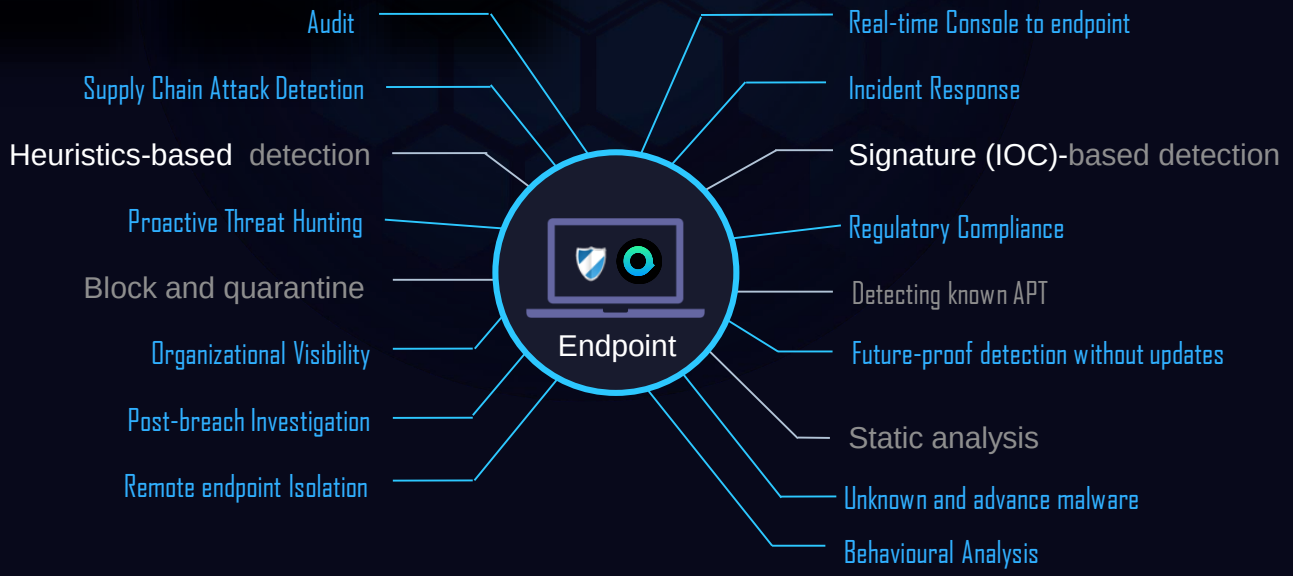
REAQTA



IBM

ANTI VIRUS + BEST-IN-CLASS EDR

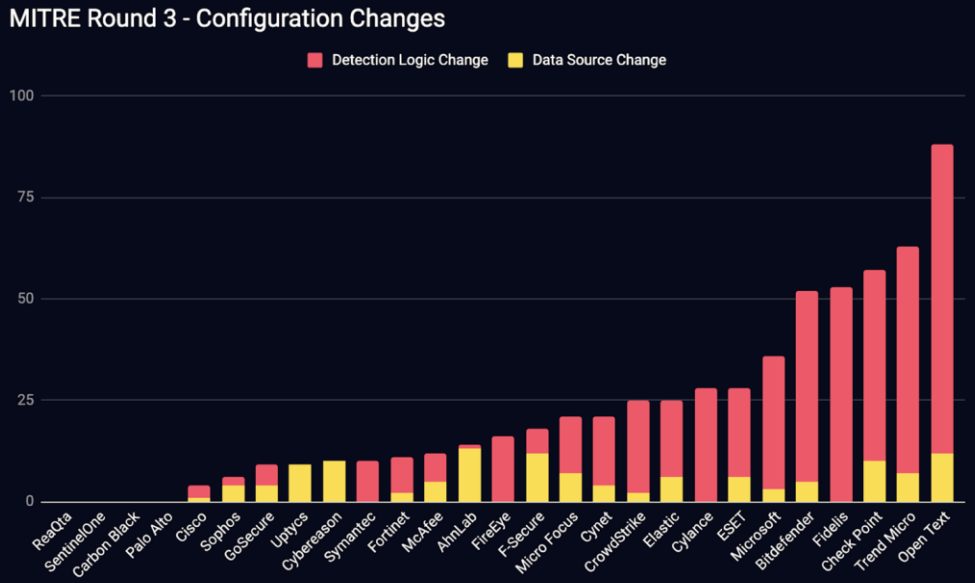
Basic Protection | Behavioral Analysis | Threat Hunting | Risk and Compliance | CERT | IT Audit



REAQTA

Results in **MITRE ATT&CK** evaluation

100% detection coverage across the cyber kill chain
No configuration changes during the entire evaluation



MITRE | REAQTA

ReaQta-Hive did **100% of detections without configuration changes**. Configuration changes help vendors adjust their detections as the attack progresses. **Most vendors had to tweak their product 'antennas' multiple times before being able to detect alerts**.

Why is this Important?

In real-life scenarios, configuration changes are usually unrealistic. **Attackers do not give defenders a second chance to tweak their detections** before moving to the next step. If a platform requires several configuration changes to operate at peak efficiency – or to detect an active threat – its autonomous detection capabilities are inevitably impaired, as with its ability to respond in real-time.

Questions?

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM