

# The open complete threat detection IBM QRadar XDR

Erasmus Volpe

[evol@ch.ibm.com](mailto:evol@ch.ibm.com)

Domenico Lojacono

[dloj@ch.ibm.com](mailto:dloj@ch.ibm.com)

February 4, 2022

# AGENDA

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

# Legal notes and disclaimer

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

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

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

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

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

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

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

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

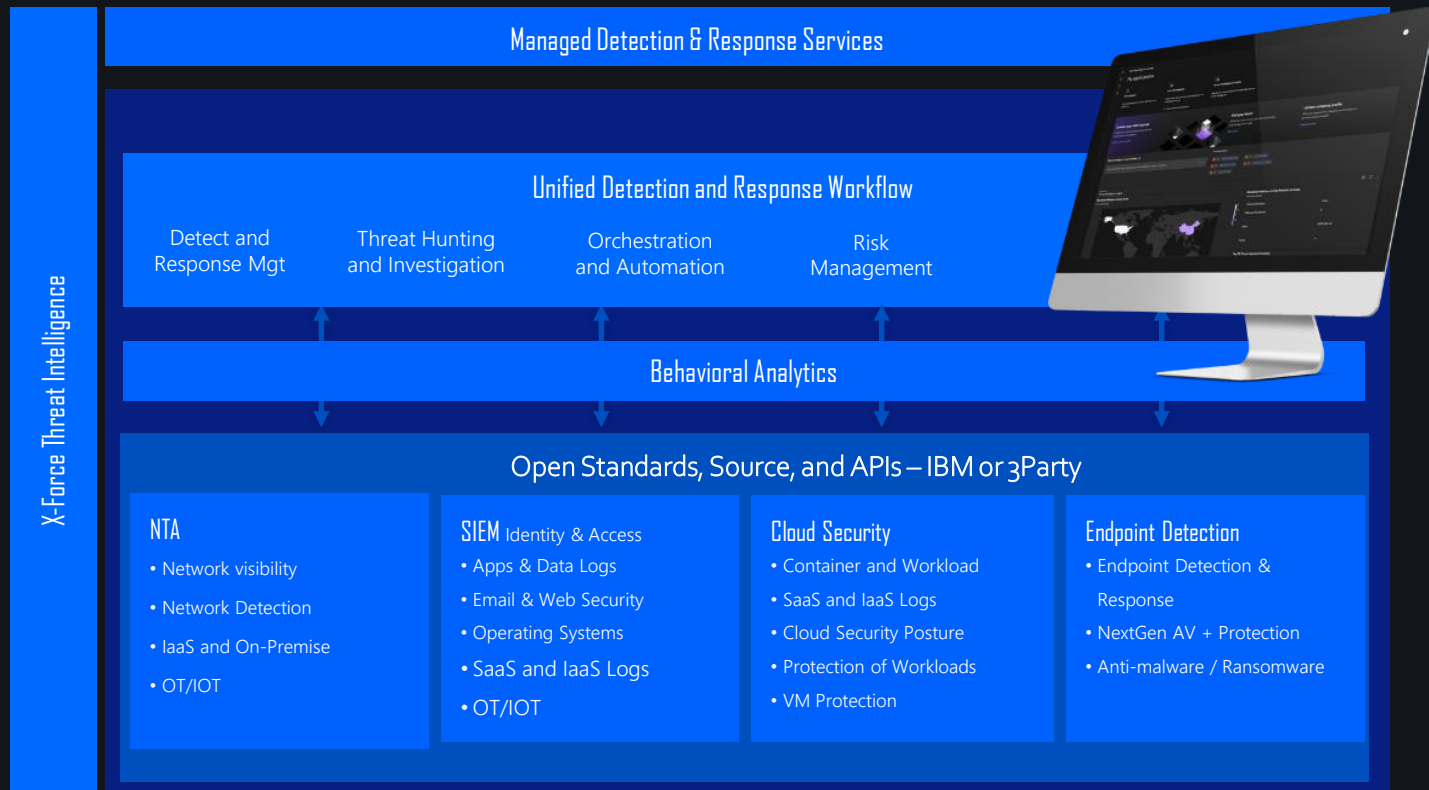
The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

Other company, product, or service names may be trademarks or service marks of others. A current list of IBM trademarks is available at "Copyright and trademark information" [www.ibm.com/legal/copytrade.shtml](http://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 3<sup>rd</sup> 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

Unified Insights and  
Investigation

Existing QRadar  
Investments

## Incident Response

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

## 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*

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

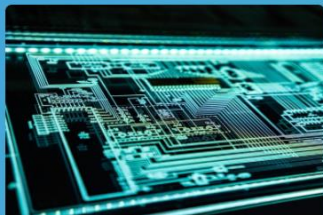
Open  
Commonly developed code & tooling  
Mutually agreed upon technologies, standards  
& procedures

### 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](#)
- [GammaTech](#)
- [Hewlett Packard Enterprise \(HPE\)](#)
- [Hitachi](#)
- [Huawei Technologies](#)
- [IXIASOFT](#)
- [Logius](#)
- [McAfee, LLC](#)
- [Microsoft](#)
- [nCipher](#)
- [NFC Corporation](#)
- [Oracle](#)
- [P&R, 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](#)

# 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



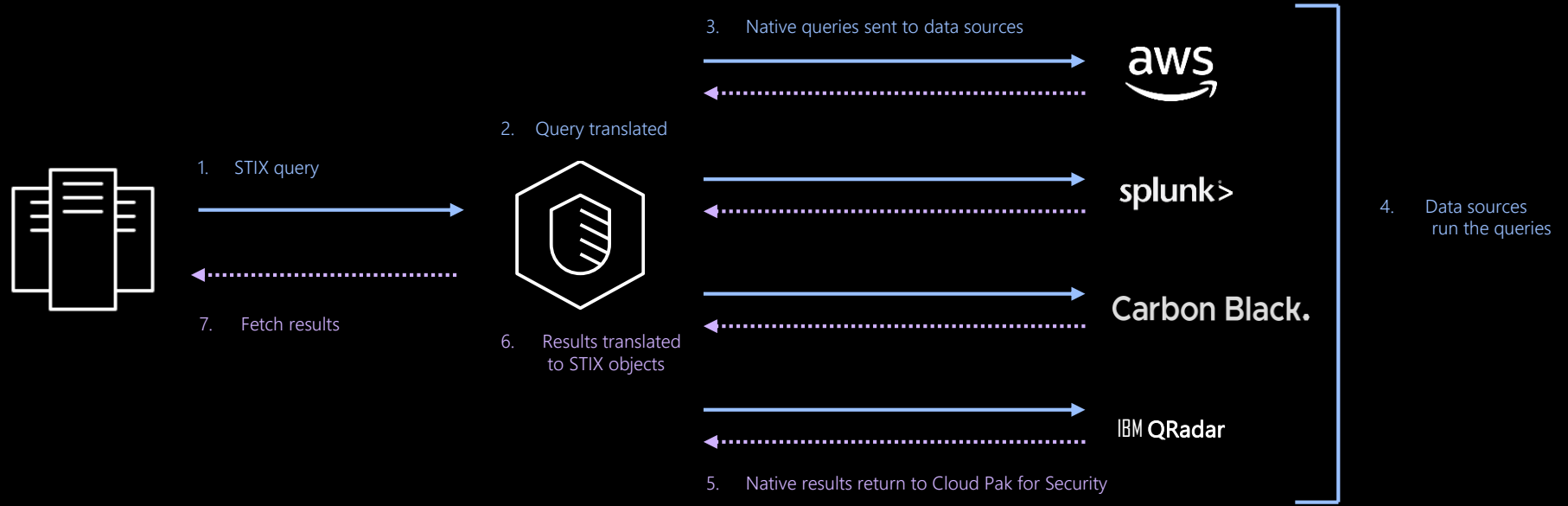
## NIST SCAP v2

### Data Collection Architecture

Supports continuous monitoring for tracking assets' policy compliance



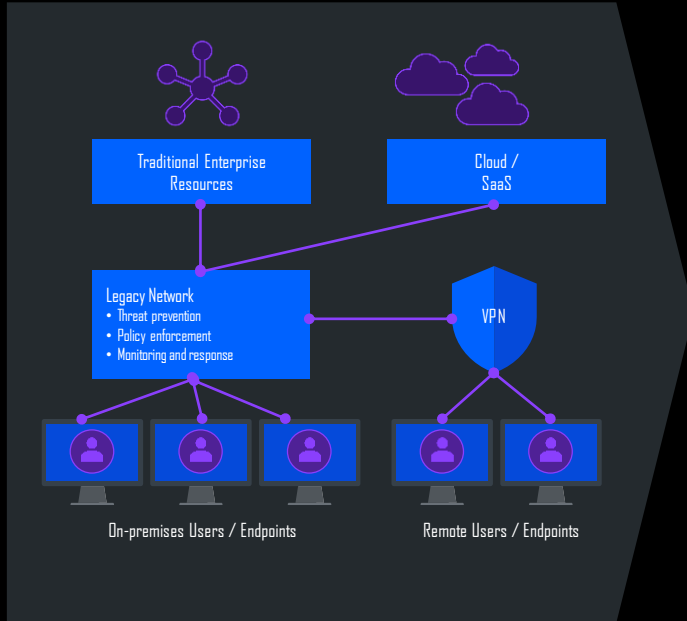
# STIX Shifter – How it works



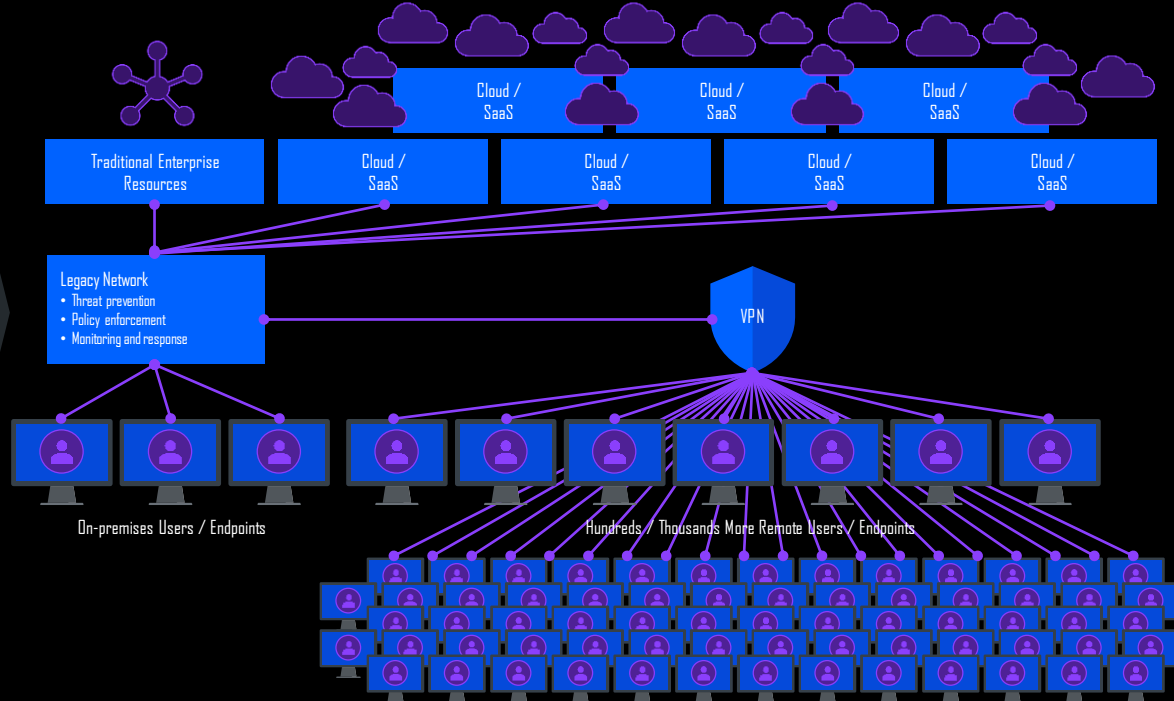
1. Federated query using a STIX pattern
2. Query is translated to the native query language of each of the data sources
3. The converted query is then sent (transmitted) to all data sources
4. Each data source runs its own native query
5. The native query results are then returned from the data source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



# Legacy defenses and security teams face challenges against advanced threats

## Costs and complexity

Many siloed tools and disjointed workflows can increase costs

## Poor visibility

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



## Missed threats

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

## 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

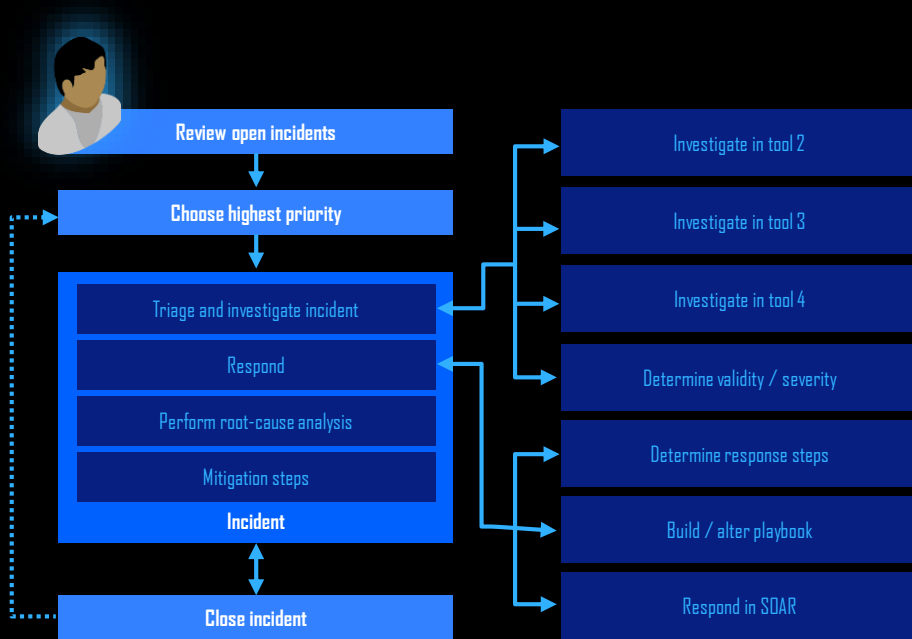


## Automate work

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

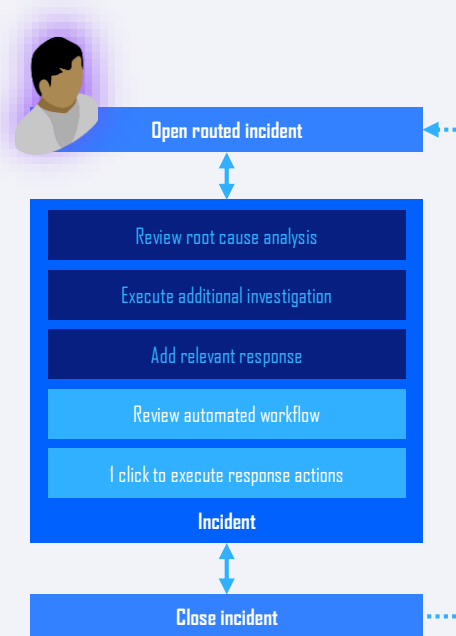
## BEFORE

# 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

# 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

### Connected XDR workflows

Hunt + Investigate + Triage + Response + Automate

Open source and standards

EDR

NDR

SIEM

SOAR

Threat intel

IBM Cloud Pak® for Security platform  
and open integrations

# IBM Security QRadar XDR, an Open, Connected Approach

## IBM Security QRadar XDR



Connect your tools and automate your SOC using IBM and open third-party integrations

## Open Source and Standards

### EDR



cybereason



vmware  
Carbon Black



More EDR  
Integrations

### SIEM

IBM Security  
QRadar SIEM



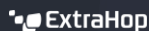
Azure Sentinel



Elastic  
Search

### NDR

IBM Security  
QRadar NDR



Vectra

Requires QRadar SIEM to integrate  
with QRadar XDR Connect

### SOAR

IBM Security  
QRadar SOAR



servicenow



### Threat Intel

IBM Security  
X-Force

Alien Vault



More Threat Intelligence Integrations

### Open Integrations



Microsoft Azure

MySQL

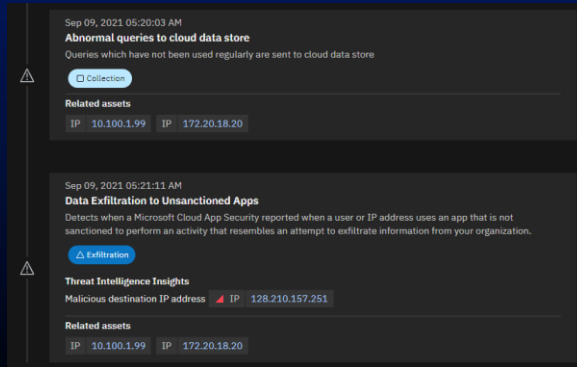


Many More  
Open Integrations

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

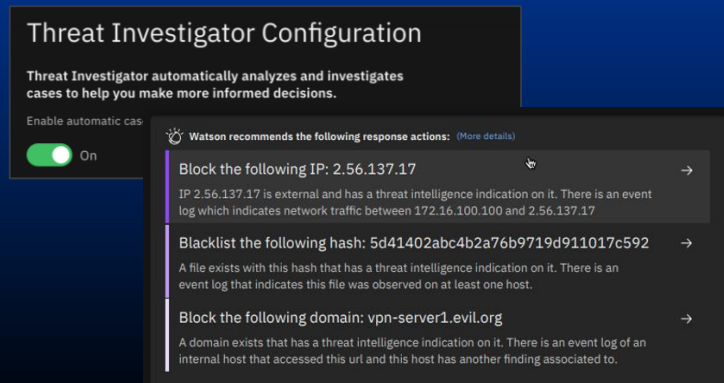
## Gain enhanced insights while improving threat detection

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.



## 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.



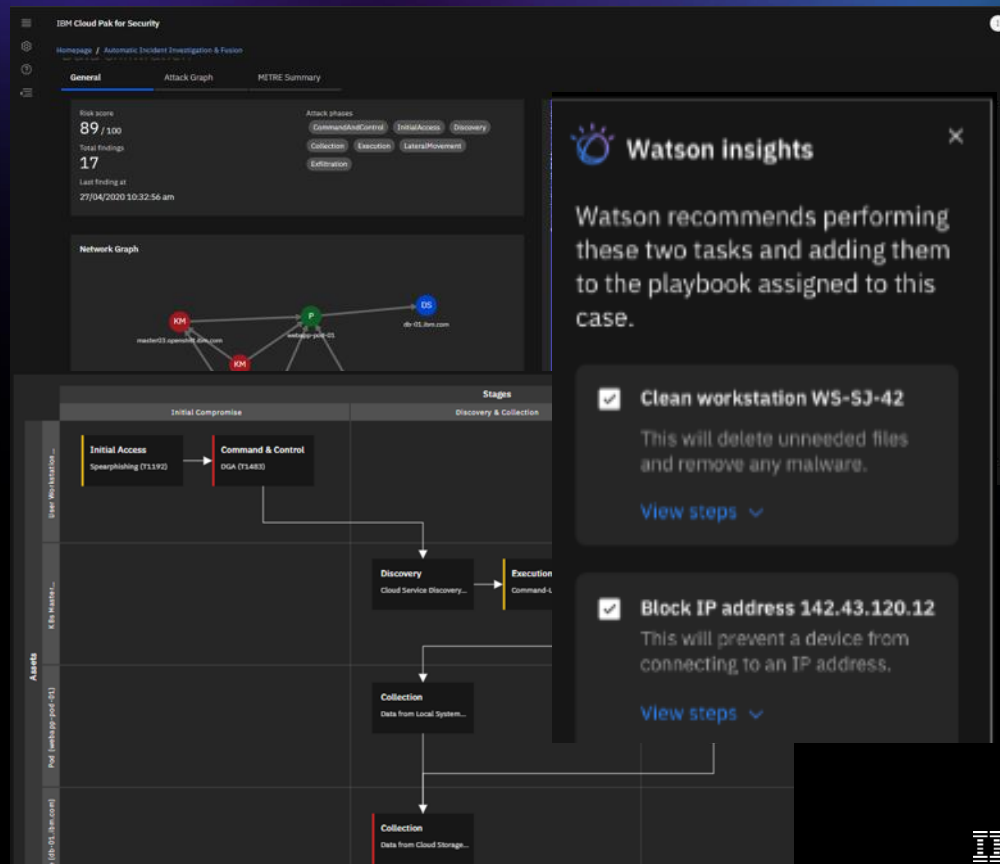


- [illegible]

# Automatic, accurate, consistent threat investigations

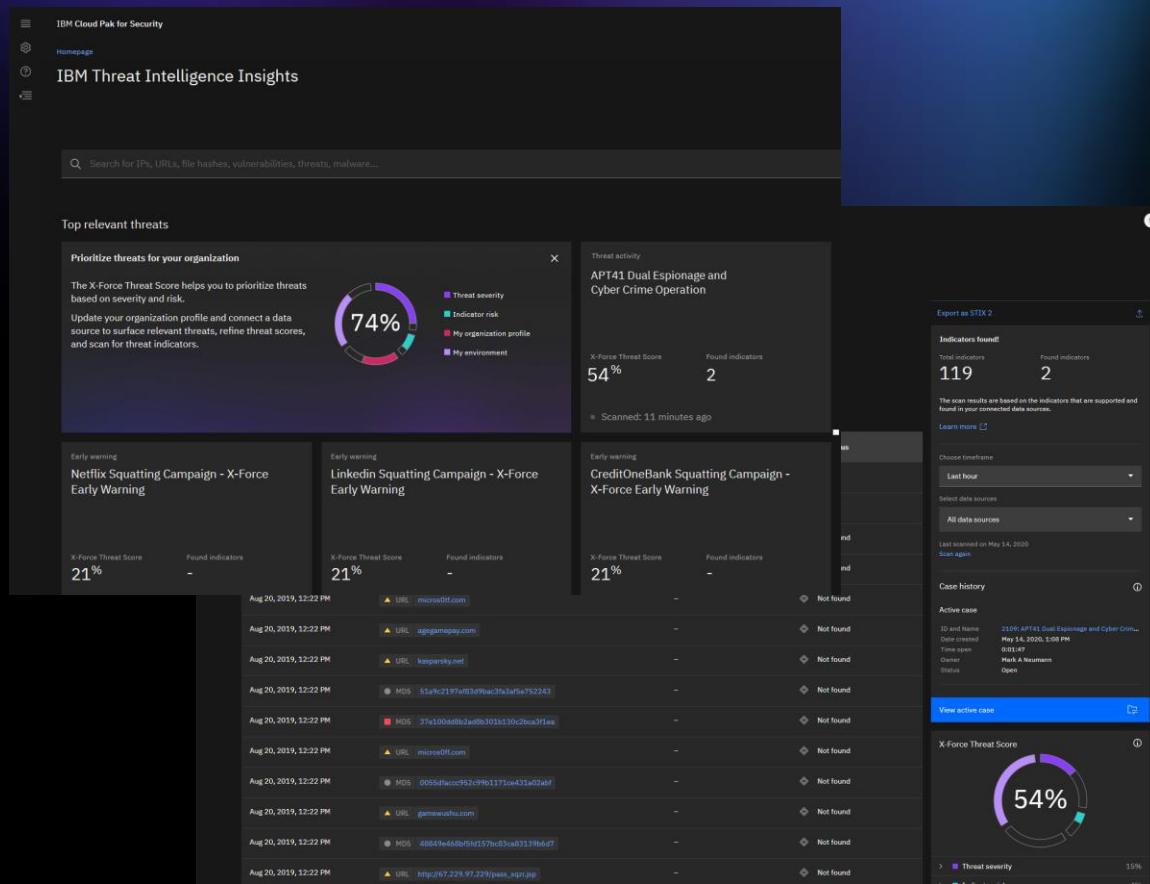
Automated case investigations increase SOC effectiveness by reducing manual effort during analysis, evidence acquisition and threat intelligence correlation.

- **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



# 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**



# 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

The screenshot displays the IBM Cloud Pak for Security interface. The top navigation bar includes 'Homepage / Cases /'. The main header shows the case title 'APT41 Dual Espionage and Cyber Crime Operation'. Below the title, a description reads: 'Suspicious activity from APT41, a prolific cyber threat group that carries out Chinese state-sponsored espionage.' The interface features a tabbed menu with 'Details', 'Tasks', 'Notes', 'Members', 'News Feed', 'Attachments', 'Stats', 'Timeline', 'Artifacts', and 'AWS IAM'. The 'Tasks' tab is active, showing a progress bar at '0% Complete' and a list of tasks: 'Initial Triage', 'Interview key individuals', 'Notify internal management chain (preliminary)', and 'Determine if inappropriate internal involvement'. The 'Engage' section is also visible. The 'Detect/Analyze' section shows a task for 'Collection of data from Xforce for specific Malware'. On the right, the 'Artifacts' tab is active, displaying a network diagram with nodes for 'IP Address 67.228.97.209', 'AWS IAM User Name DoreenJones', 'User Malware Case', 'Malware MD5 Hash 846c0b921841e6d', 'APT41 Dual Espionage and Cyber Crime Operation', 'IP Address 192.168.0.8', and 'targeted phishing attack - AWS admin'. The bottom of the interface shows 'Unassigned' and 'No due date' filters.

# ReaQta

# About ReaQta



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



- #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/>



## 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



"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

## ARCHITECTURE

Learn • Detect • Track • Respond • Protect

## Endpoint AI &amp; Nano OS

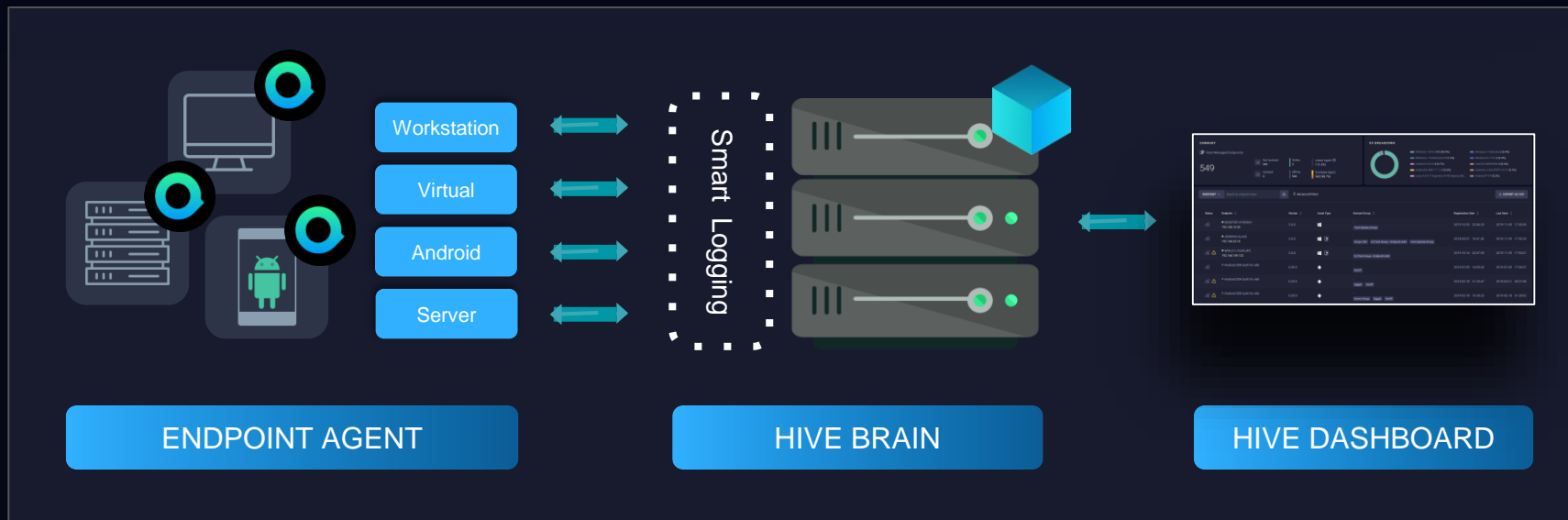
Real-Time Coverage

## Infrastructural AI

Data Collection & Behavioral  
Analysis

## Single Console

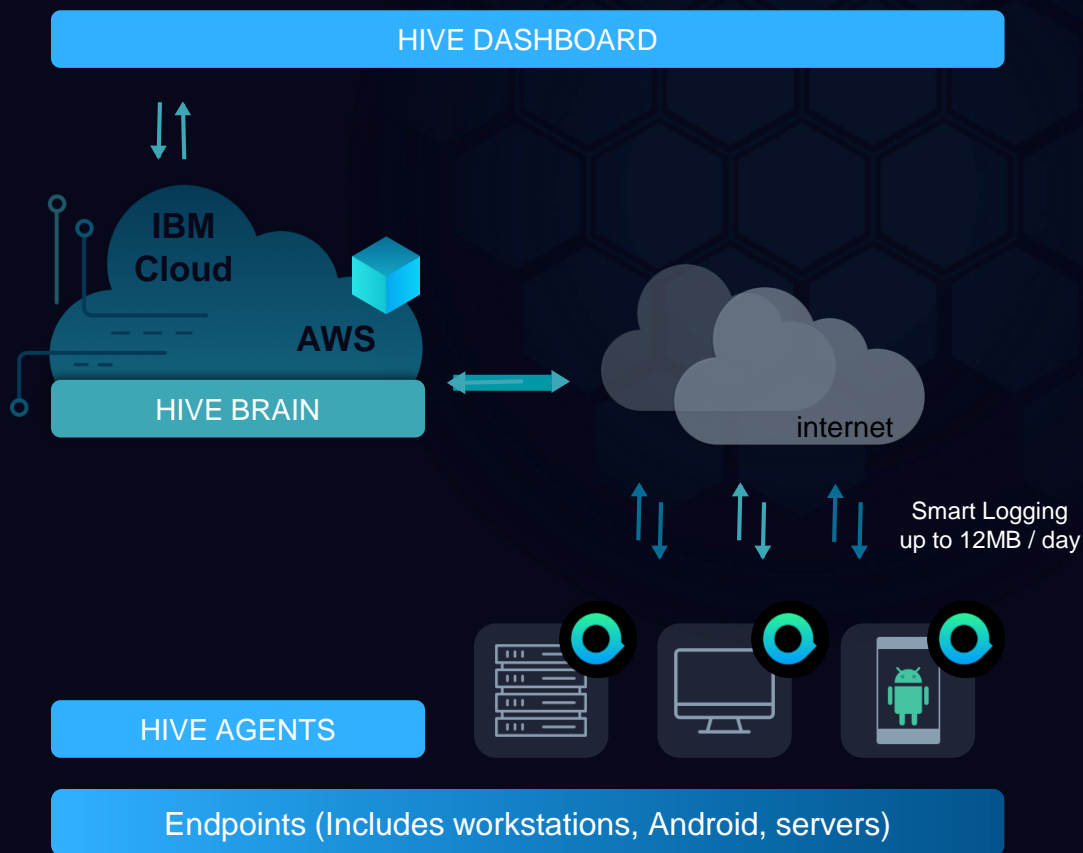
Optimised Remediation Workflow





# DEPLOYMENT

## CLOUD

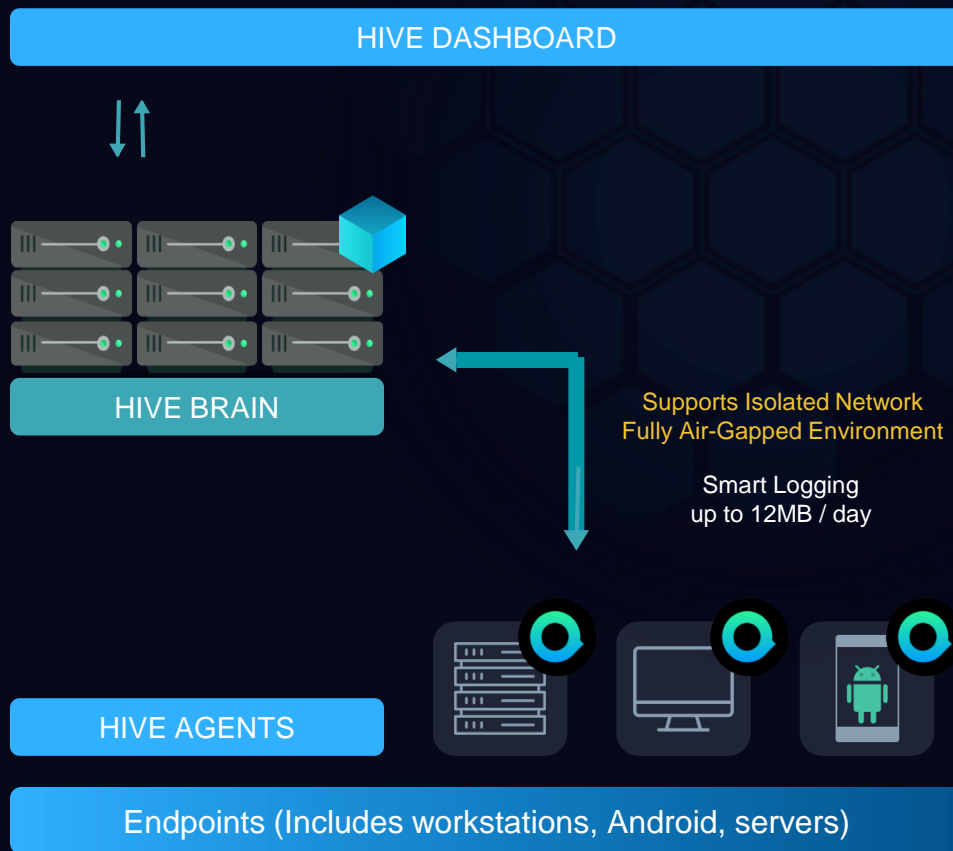


All Network Traffic

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

## DEPLOYMENT

## ON-PREM



All Network Traffic

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

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



PROCESS CREATED - NORTONSECURITY.EXE

Summary

Prevalence

SYMANTEC

**PROCESS EXPLORER**

nortonsecurity.exe (PID 6028)

**nortonsecurity.exe**

Description: nortonsecurity.exe created

Original File Name: ccsvchst.exe

Arch: x64 Certificate: **Eg (Trusted But Expired Certificate)**

Size: 321 kB Signer: Symantec Corporation

PID: 24448 Issuer: VeriSign Class 3 Code Signing 2010 CA

PPID: **"C:\Program Files\Symantec.cloud\EndpointProtectionAgent\Engine\22.15.2.26\NortonSecurity.exe" /SpnCommand 5000 0 /a /m "C:\Program Files\Symantec.cloud\EndpointProtectionAgent\Engine\22.15.2.26\SpnAvp"**

Privilege: SYSTEM Cloud Score: **Safe**

CMD Line: "C:\Program Files\Symantec.cloud\EndpointProtectionAgent\Engine\22.15.2.26\NortonSecurity.exe" /SpnCommand 5000 0 /a /m "C:\Program Files\Symantec.cloud\EndpointProtectionAgent\Engine\22.15.2.26\SpnAvp"

PATH: c:\program files\symantec.cloud\endpointprotectionagent\engine\22.15.2.26\...

SHA256: 9fc955624f9500323450f2631a1492b330580fc92277037922ef03c48a161c

SHA1: 7c63b70ebbc3e953b58b636(a97bf1cbec90a805

MD5: a25624b2a2ca4b8aaee9a7f0650155e

PROCESS TERMINATED - APEXONELOGCOUNTER.EXE

Summary

Prevalence

TRENDMICRO

**PROCESS EXPLORER**

apexonelogcounter.exe (PID 6284)

**apexonelogcounter.exe**

Description: apexonelogcounter.exe terminated

Original File Name: apexonelogcounter.exe

Arch: x32 User: NT AUTHORITY\SYSTEM

Size: 1.3 MB Certificate: **Eg (Trusted But Expired Certificate)**

PID: 8220 Signer: Trend Micro, Inc.

PID: 6284 Issuer: DigiCert High Assurance Code Signing CA-1

Privilege: SYSTEM Cloud Score: **Safe**

CMD Line: "C:\Windows\TEMP\... ApexOneLogCounter.exe"

PATH: c:\windows\temp\... apexonelogcounter.exe

SHA256: 203ec331d8f9e383b8bd088ac8b7d5167a4c0b6e062a60cfa84515a8379

SHA1: e95b38b4f93c217ad2282ad1ffe73334fcec2b8

MD5: 9837da68cce973f3f1389480ab513363

EXECUTABLE DROPPED - WSCCLIENT.EXE

Summary

Executable Info

Prevalence

BITDEFENDER

**PROCESS EXPLORER**

epsecutivityservice.exe (PID 888)

**epsecutivityservice.exe**

Description: epsecutivityservice.exe dropped a new executable to tmp00013bf6

Original File Name: epsecutivityservice.exe

Arch: x64 User: NT AUTHORITY\SYSTEM

Size: 395.2 kB Certificate: **Eg (Valid Certificate)**

PID: 3968 Signer: Bitdefender SRL

PID: 888 Issuer: DigiCert Assured ID Code Signing CA-1

Privilege: SYSTEM Cloud Score: **Safe**

CMD Line: "C:\Program Files\Bitdefender\Endpoint Security\EPService\service.exe" /service

PATH: c:\program files\bitdefender\endpoint security\epsecutivityservice.exe

SHA256: ab43779175907cdf23ef36f0e42977af7f730c42d869e06dca741ff2fb1208

SHA1: 10dedb51c7c4e0609c5880f4667c57381ab7421

MD5: 13fbb17497f15b6e7bc026c7b3c848f9

PROCESS CREATED - MCCSPSERVICEHOST.EXE

Summary

Prevalence

MCAfee

**PROCESS EXPLORER**

mccspservicehost.exe (PID 984)

**mccspservicehost.exe**

Description: mccspservicehost.exe created

Original File Name: mccspservicehost.exe

Arch: x64 User: NT AUTHORITY\SYSTEM

Size: 2.6 MB Certificate: **Eg (Valid Certificate)**

PID: 15492 Signer: McAfee, LLC.

PID: 984 Issuer: McAfee Code Signing CA 2

Privilege: SYSTEM Cloud Score: **Safe**

CMD Line: "C:\Program Files\Common Files\McAfee\CSP\3.4.105.0\McCSPServiceHost.exe"

PATH: c:\program files\common files\mcafee\csp\3.4.105.0\mccspservicehost.exe

SHA256: 55fa5d5ec28631f4e95cc276ca0b4815a942e648e988cf516fe4f4edaca322

SHA1: a39f0b3e1b2dcfa23137709263f22fb54c15d21

MD5: e55d0c1642a3b22a580b1bbd9928cbb

PROCESS DROPPED - WSCCLIENT.EXE

Summary

Prevalence

SOPHOS

**PROCESS EXPLORER**

wscclnt.exe (PID 2156)

**wscclnt.exe**

Description: wscclnt.exe created

Original File Name: wscclnt.exe

Arch: x64 Certificate: **Eg (Trusted But Expired Certificate)**

Size: 626.3 kB Signer: Sophos Ltd

PID: 4152 Issuer: DigiCert Assured ID Code Signing CA-1

PID: 2156 Issuer: Yes

Privilege: SYSTEM User: NT AUTHORITY\SYSTEM

CMD Line: "C:\Program Files (x86)\Sophos\Sophos Anti-Virus\WSCClient.exe" /status enab...

PATH: c:\program files (x86)\sophos\sophos anti-virus\wscclnt.exe

SHA256: be5ffc6899826fbb58af610f384ca8d0df7d262996bdee8961774bf4cbca

SHA1: 56014acfef16de4258f084f00d47aa92a558a962a

MD5: 2a23265dcac14e36e373f6a7eeaa5b4

+ CREATE ALERT

PROCESS EXPLORER

Summary

Prevalence

WINDOWS DEFENDER

**PROCESS EXPLORER**

services.exe (PID 600)

**msmtpeng.exe**

Description: msmtpeng.exe created

Original File Name: msmtpeng.exe

Arch: x64 Certificate: **Eg (Valid Certificate)**

Size: 100.8 kB Signer: Microsoft Windows Publisher

PID: 2480 Issuer: Microsoft Windows Production PCA 2011

PID: 600 Expired: No

Privilege: **"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2001.10-0\MsMpEng.exe"**

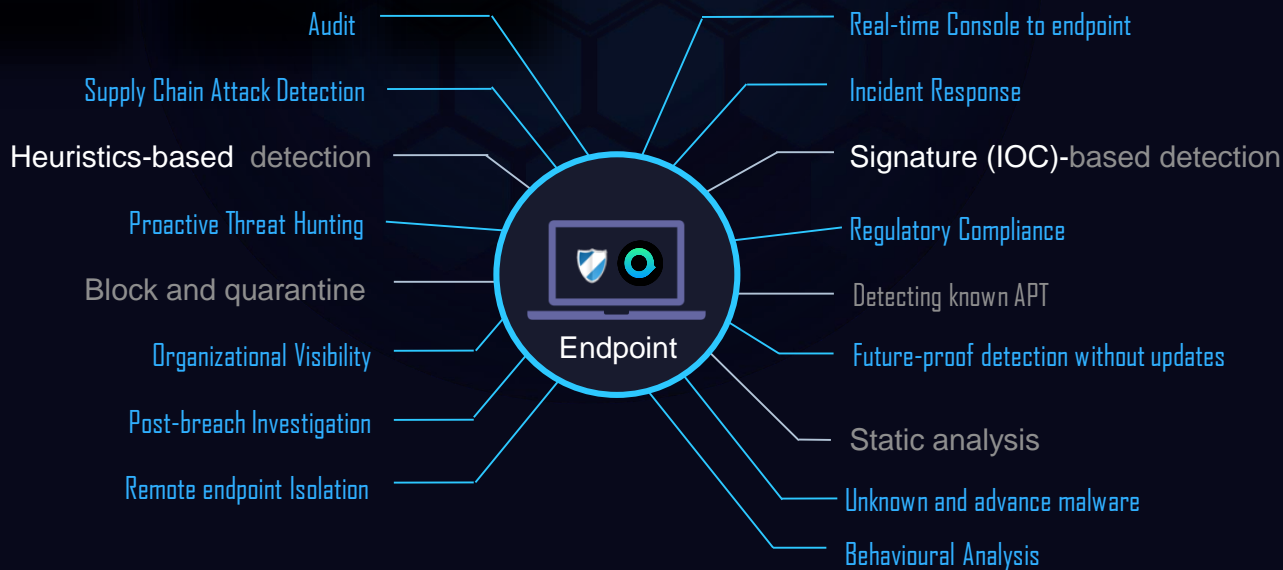
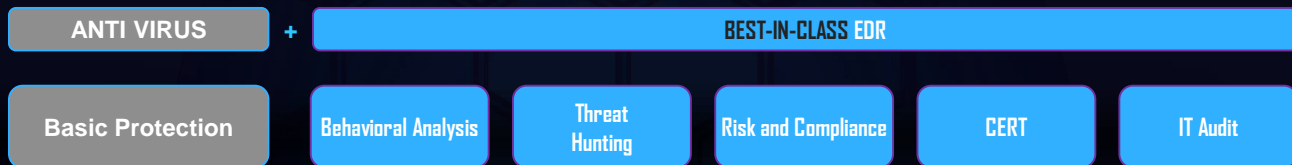
CMD Line: "C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2001.10-0\MsMpEng.exe"

PATH: c:\programdata\microsoft\windows defender\platform\4.18.2001.10-0\msmpe...

SHA256: 55cb6465f403830e4705440cc5623d79805b5bd1d33db0cf8b016eb2ac20d3f

SHA1: 4f40e568e2c63c6aaf4d28157bafa50c01694ab9

MD5: f6b04d08ecc4b9ff446cab52ec622618

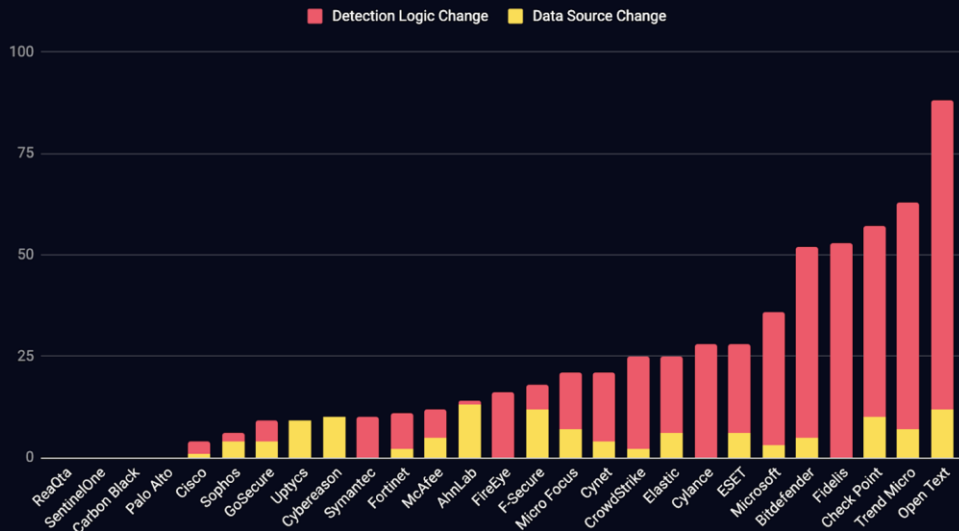


# Results in MITRE ATT&CK evaluation



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

MITRE Round 3 - Configuration Changes



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?





# THANK YOU

FOLLOW US ON:



[ibm.com/security](https://ibm.com/security)



[securityintelligence.com](https://securityintelligence.com)



[ibm.com/security/community](https://ibm.com/security/community)



[xforce.ibmcloud.com](https://xforce.ibmcloud.com)



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



[youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2021. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

