
SOPHOS
INTERCEPT X
SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

The most comprehensive endpoint protection

Unknown Threats

Protect Against the Unknown

- Deep Learning Behavior Model
- Signatureless Exploit Prevention
- Malicious and Benign identification
- Tiny Footprint & Low False Positives

UNKNOWN THREATS

No User / Performance Impact
No File Scanning
No Signatures

Crypto-Ransomware

Stop Ransomware

- Behavioral Based Conviction
- Blocks Encryption and Boot Attacks
- Automatically Reverts Affected Files
- Identifies Source of Attack

CRYPTO RANSOMWARE

Prevent Ransomware Attacks
Roll-Back Changes
Attack Chain Analysis

Real-Time Attacks

Deny the Hacker

- Protects against Real-Time Breaches
- Stops Credential Harvesting Attacks
- Prevents Persistence Techniques
- Blocks APC and Process Attacks

EVASIVE ATTACKER

Prevent 'Land and Expand'
Protect Login Credentials
Expose Hackers in plain sight

Threat Lifecycle

Intercept X Feature Map

SYNCHRONIZED SECURITY
Heartbeat

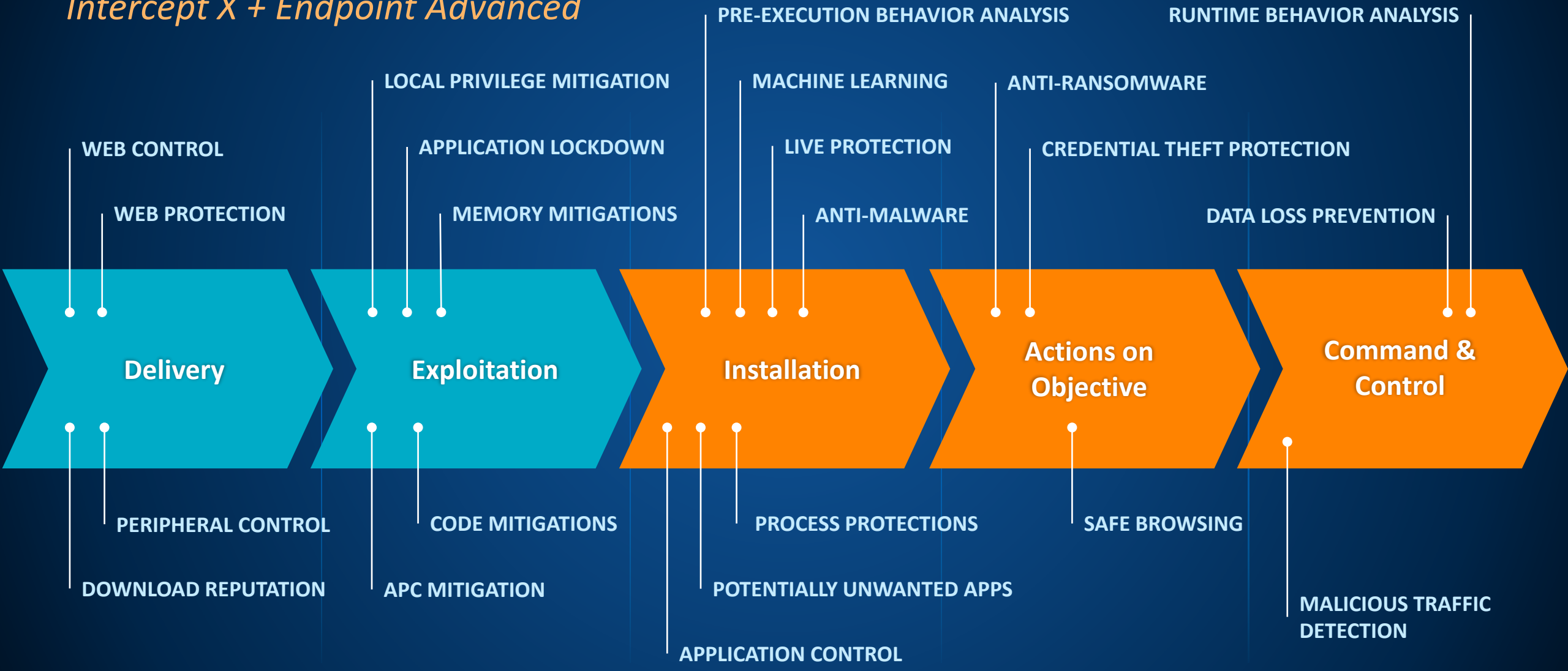
INVESTIGATE & REMOVE
Root Cause Analysis (RCA)
Sophos Clean M with SafeStore

Threat Lifecycle

Intercept X + Endpoint Advanced

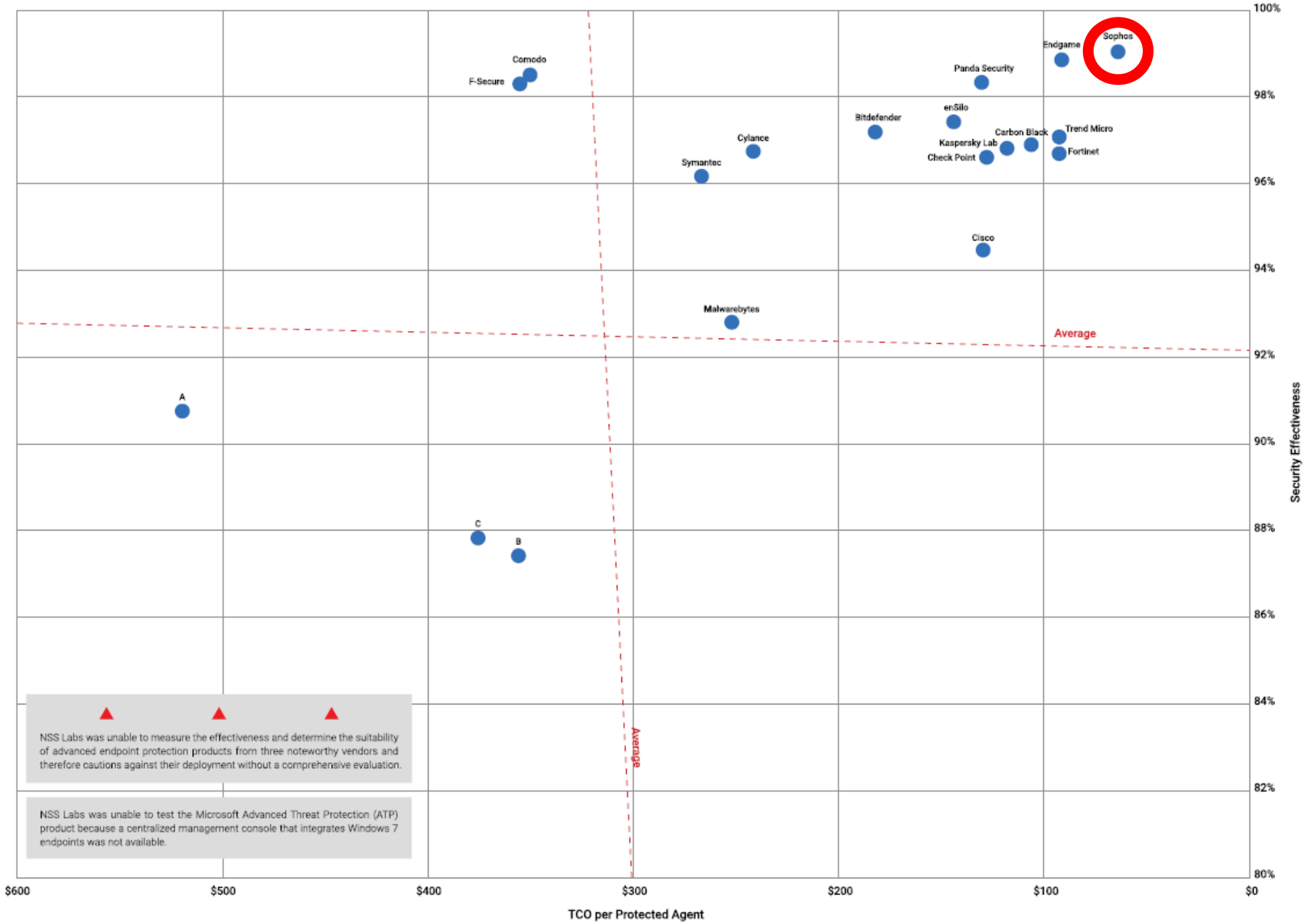
SYNCHRONIZED SECURITY
Heartbeat

INVESTIGATE & REMOVE
Root Cause Analysis (RCA)
Sophos Clean M with SafeStore



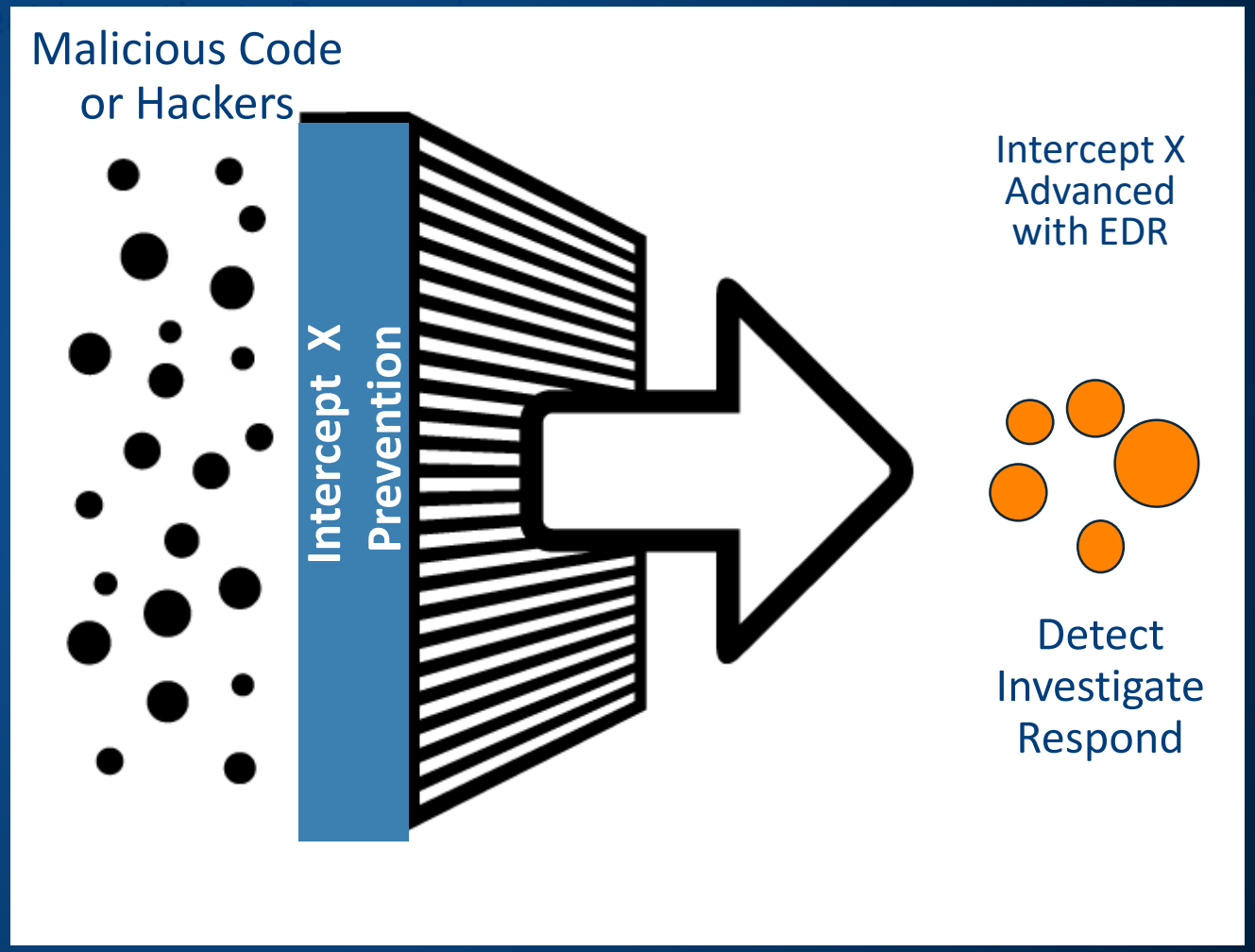
NSS LABS

MARCH 5, 2019

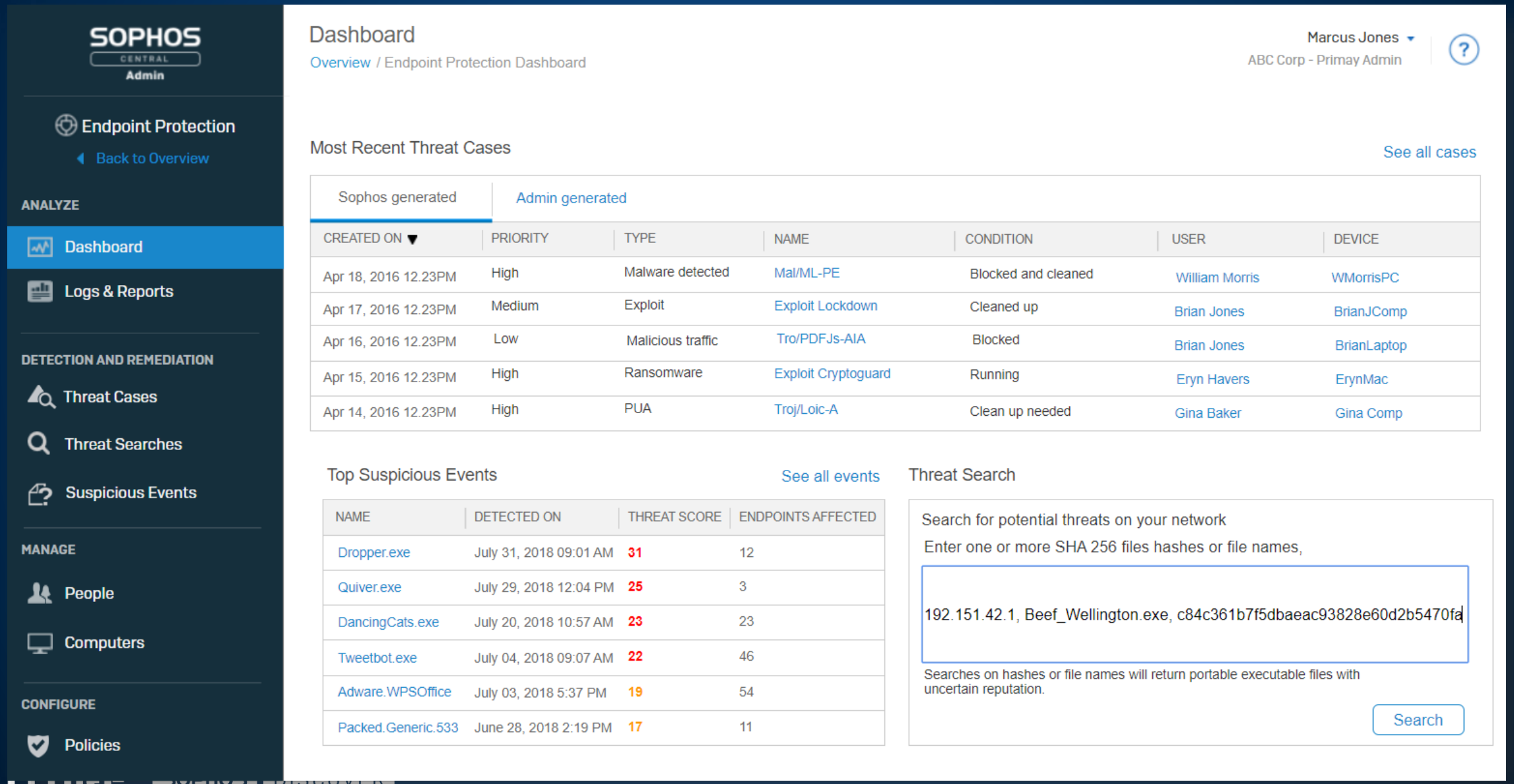


Stop breaches before they start

- Top-rated endpoint protection stops more threats
- Reduces the Overall Attack Surface
- Significantly lightens the EDR workload
- Optimizes resources by reducing noise



Intercept and EDR



About Rook Security

MDR Provider Acquired by Sophos in May 2019

ROOK SECURITY

Company Overview

Founded
2008

Headquarters
Indianapolis, IN

Core Service
MDR

- Significant expertise in deep security forensics, MDR and security operations management
- Dedicated to monitoring, analyzing and protecting customer environments in real-time via remote SOC
  - Experience across endpoint, firewall, IDS/IPS
- 24/7 team of cyberthreat hunters and incident response experts who monitor, hunt for, analyze, and respond to security incidents
- Served companies of any size, from SMB to Large Enterprise

SOPHOS

ROOK SECURITY

Advanced monitoring, detection and response capabilities delivered as a fully-managed service

24/7 team of highly-trained experts means a faster response to known threats and the ability to discover new threats from sophisticated attackers

Able to offer MDR services across the entire market spectrum from small business to large enterprise

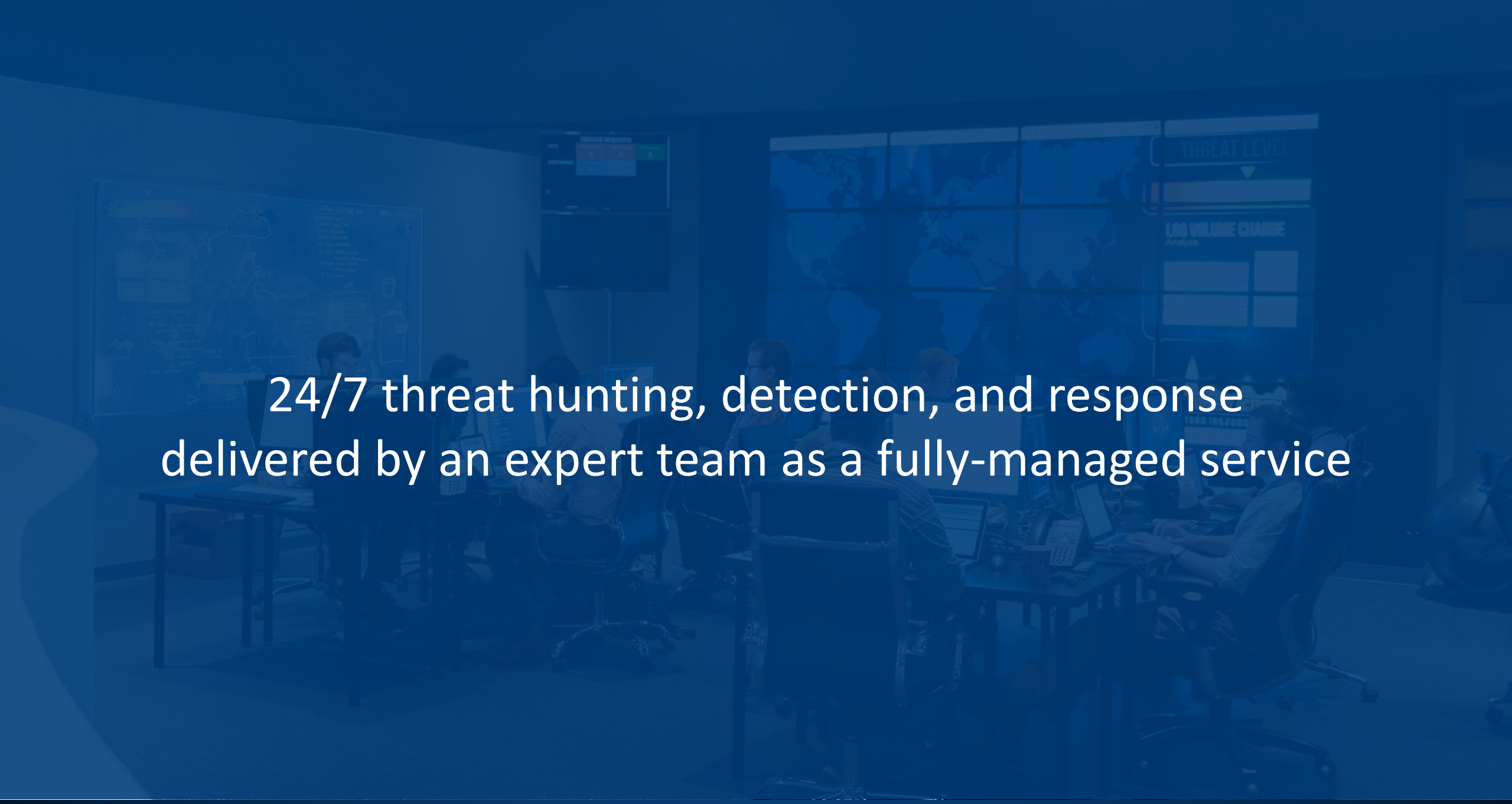
DarkBytes

Able to detect abnormal and anomalous activities missed by other security tools

Reduces incident remediation times by automating security workflows created by expert analysts

Continuously identifies and prioritizes the most important security metrics including threats, vulnerabilities, and compliance issues

About Managed Threat Response (MTR)



24/7 threat hunting, detection, and response
delivered by an expert team as a fully-managed service

What is Managed Threat Response?

Machine-Accelerated Human Response

MTR fuses machine learning technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate more sophisticated and complex threats.

Why You Need Humans + Machines

Machine Intelligence

Rapidly processes massive pools of data to detect activity that could potentially be malicious

Draws correlations based on patterns or behaviors commonly associated with malicious activity

Takes automatic actions in near real-time to block or terminate confirmed malicious activities (strong signals)

Derives conclusions based on the data previously fed into the system (“only as good at its teacher”)

Human Intelligence

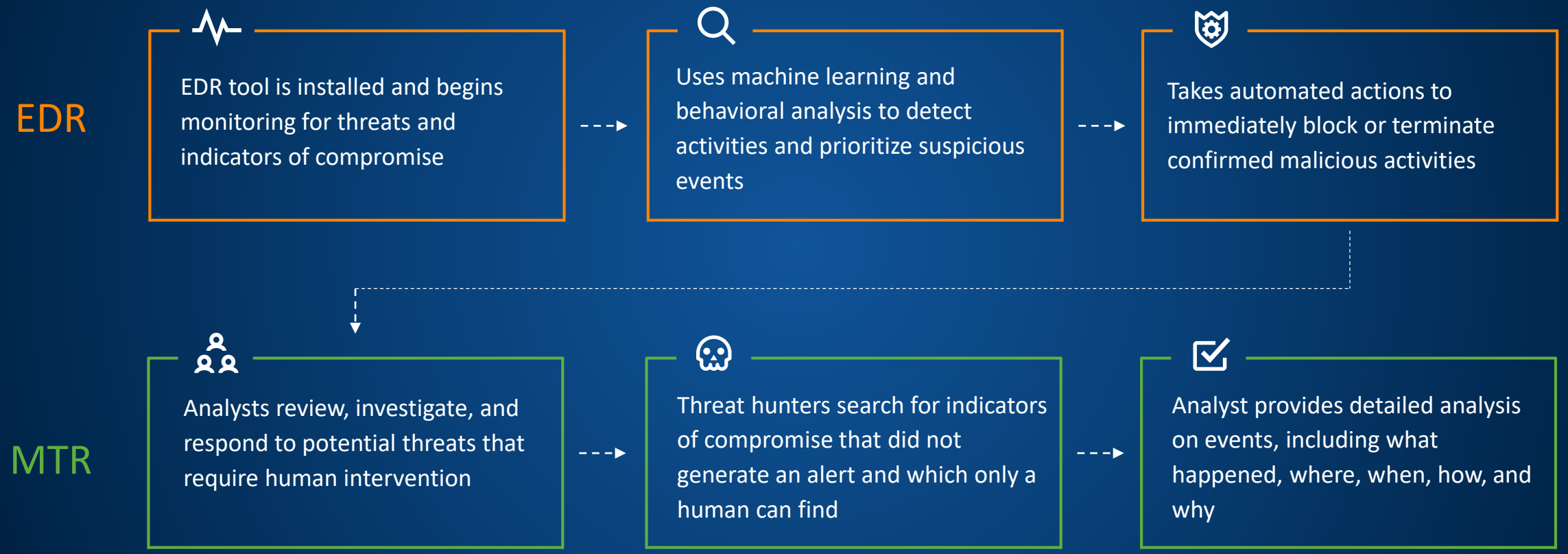
Uses investigative techniques to conclude whether a suspicious activity is malicious or benign

Applies the business context of why an attacker might be after a piece of data and what their motivations are

Investigates causal and adjacent events (weak signals) to discover new threats that previously could not be detected

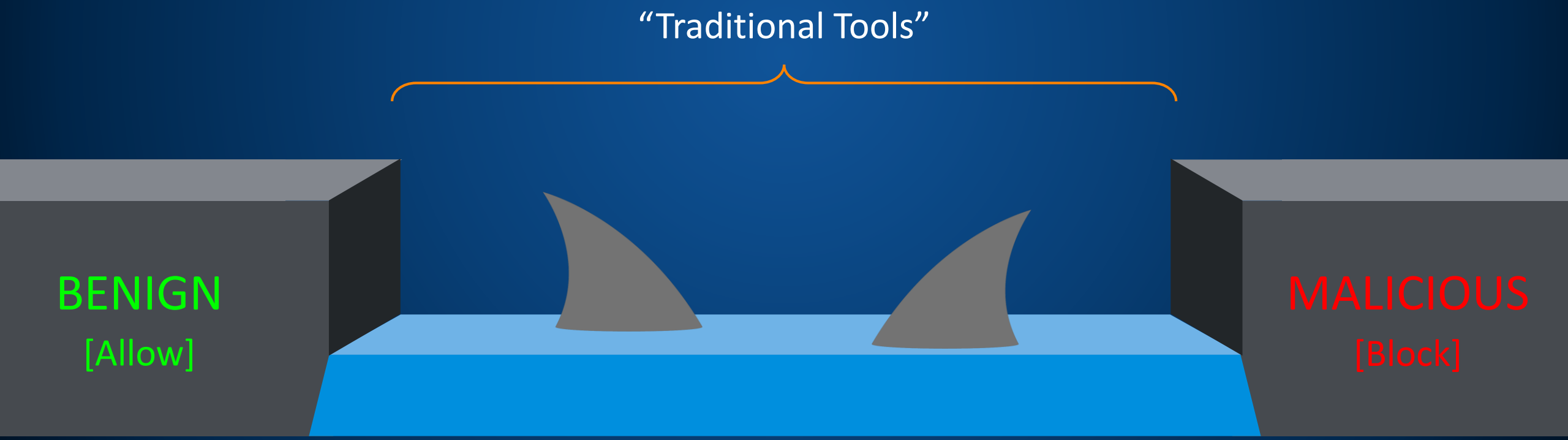
Evaluates output from multiple sources and employs creative thinking and problem solving to make decisions

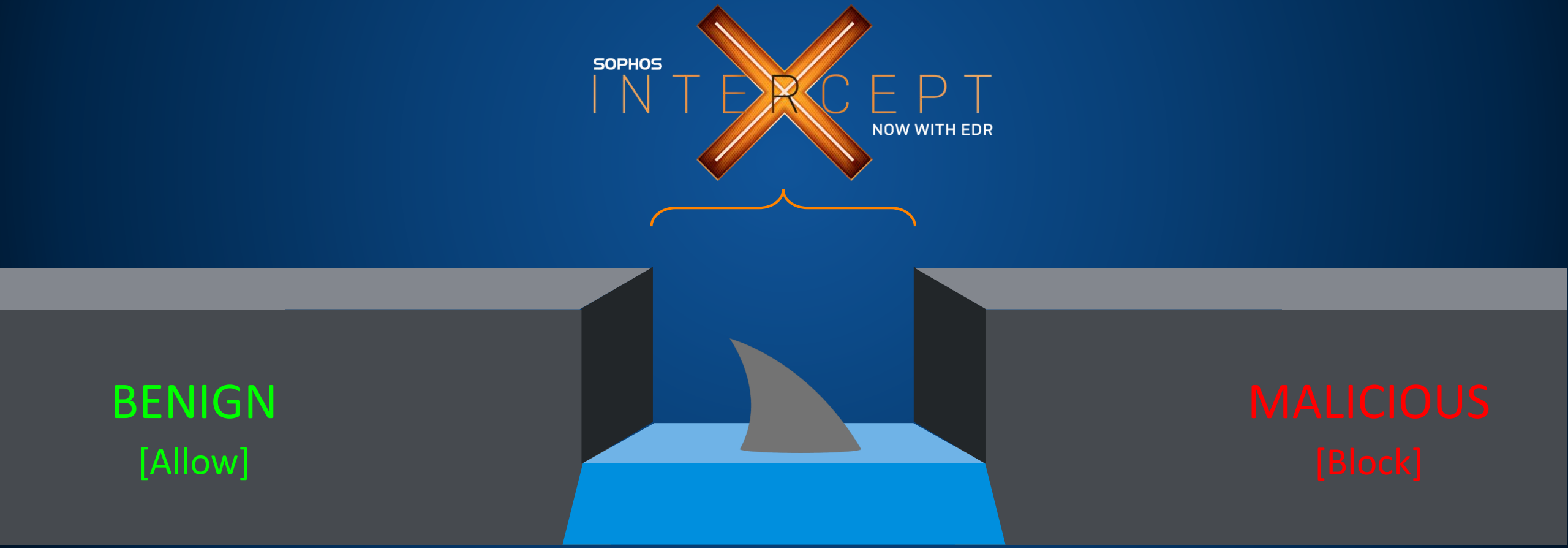
EDR + MTR


EDR
EDR tool is installed and begins monitoring for threats and indicators of compromise
Uses machine learning and behavioral analysis to detect activities and prioritize suspicious events
Takes automated actions to immediately block or terminate confirmed malicious activities
MTR
Analysts review, investigate, and respond to potential threats that require human intervention
Threat hunters search for indicators of compromise that did not generate an alert and which only a human can find
Analyst provides detailed analysis on events, including what happened, where, when, how, and why

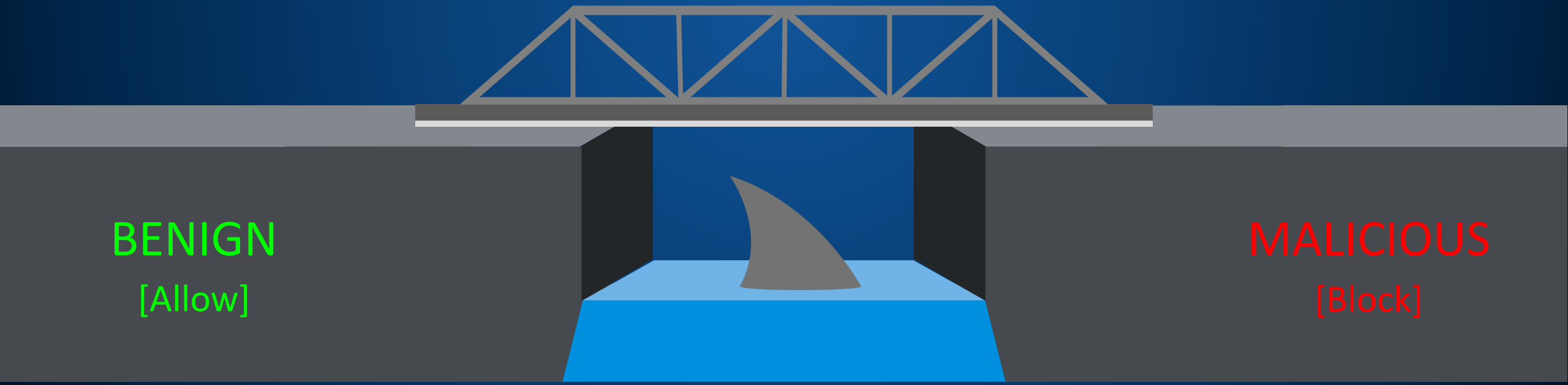
The Gap

The Gap


“Traditional Tools”
BENIGN
[Allow]
MALICIOUS
[Block]


SOPHOS
INTERCEPT X
NOW WITH EDR
BENIGN
[Allow]
MALICIOUS
[Block]

Managed Threat Response



Core Security Capabilities

Protect

Prevent attacks and proactively secure known vulnerabilities

Detect

Detect active attacks and identify potentially malicious behaviors

Respond

Rapidly investigate and remediate incidents to minimize impact

Core Security Capabilities

Service Offerings

SOPHOS

Detect

Tools detect an attack or suspicious behavior

Respond

Tools know enough about the attack/behavior to automate the correct response

Detect

Tools detect an attack or suspicious behavior

Respond

Tools DO NOT know enough about the attack/behavior to automate a response

Analyst conducts investigation to confirm if attack/behavior is malicious or benign

Analyst determines what response action(s) to take and executes on that plan

Analyst-led remediation actions are turned into playbooks for future automation

Detect

Tools DO NOT detect an attack or suspicious behavior

Respond

Nothing was detected so no response actions can be taken

Analyst conducting a threat hunt discovers a brand new indicator of compromise (IoC)

Analyst conducts investigation to confirm if the new IoC is malicious or benign

Analyst determines what response action(s) to take and executes on that plan

Analyst-led remediation actions are turned into playbooks for future automation

Key Service Benefits

High-Fidelity Detections

Going beyond traditional detections, we combine deterministic and machine learning models to spot suspicious behaviors and the tactics, techniques and procedures used by the most advanced adversaries.

Elite Expertise

Our highly-trained team of threat hunters, engineers, ethical hackers and SOC specialists has your back 24/7, investigating anomalous behavior and responding to threats with speed and precision.

Proactive Defense

Combining threat intelligence with newly-discovered Indicators of Compromise (IoC) and Indicators of Attack (IoA) that are identified through analyst-led threat hunts, Intercept X proactively protects customer environments.

Transparency and Control

You own the decisions and control how and when potential incidents are escalated, what response actions (if any) you want us to take, and who should be included in communications.

Response Modes

You choose the best way for our MTR team to work alongside you

Notify

We notify you about the detection and provide detail to help you in prioritization and response

Collaborate

We work with your internal team or external point(s) of contact to respond to the detection

Entrust

We handle containment and neutralization actions and will inform you of the action(s) taken

Standard MTR Offering

24/7 Threat Hunting

Confirmed malicious artifacts or activity (strong signals) are automatically blocked or terminated, freeing up threat hunters to conduct Lead-Driven threat hunts. This type of threat hunt involves the aggregation and investigation of causal and adjacent events (weak signals) to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.

Adversarial Detections

Most successful attacks rely on the execution of a process that can appear legitimate to monitoring tools. Using proprietary investigation techniques, our team determines the difference between legitimate behavior and the tactics, techniques, and procedures (TTPs) used by attackers.

Security Health Check

Keep Intercept X operating at peak performance with proactive examinations of your operating conditions and recommended configuration improvements.

Data Retention

Data from all sensors are ingested and stored based on event hierarchy and data lifecycle. Incidents and associated critical events will be stored for periods up to 2 years.

Activity Reporting

Summaries of case activities enable prioritization and communication so your team knows what threats were detected and what response actions were taken within each reporting period.

Advanced MTR Offering

Includes all Standard features, plus the following:

Advanced Threat Hunting

Applying data science, threat intelligence, and the intuition of veteran threat hunters, we combine your company profile, high value assets, and high risk users to anticipate attacker behavior and identify new Indicators of Attack (IoA).

Enhanced Telemetry

Investigations are supplemented with telemetry from other Sophos Central Products extending beyond the endpoint to provide a full picture of adversary activities.

Proactive Posture Improvement

Proactively improve your posture and harden your defenses with prescriptive guidance for addressing configuration and architecture weaknesses that diminish your overall security capabilities.

Dedicated Incident Response Lead

When an incident is confirmed, a dedicated incident response lead is provided to directly collaborate with your on-premise resources (internal team or external partner) until the active threat is neutralized.

Direct Call-in Support

Our security operations team is switched on around-the-clock and backed by support teams spanning 26 locations worldwide.

Asset Discovery

From asset information covering OS versions, applications, and vulnerabilities to identifying managed vs. unmanaged assets, valuable insights are available during impact assessments, threat hunts, and for providing resilience recommendations.

MTR Onboarding

SOPHOS

MTR Onboarding Process

Sales Operations

ORDER PROCESSING

Customer receives License Schedule

- Includes MTR Activation Code
- *Includes Getting started guide***
  - *Completing activation*
  - *How to identify escalation contacts*
  - *Response Modes and how they work*
  - *How to contact us*

CUSTOMER DEPLOYMENT

Customer completes activation

- Apply license code in Sophos Central (new customer is created in MTR platform)
- Define 1-3 escalation contacts
- Selects MTR Response Mode
- Starts assigning MTR licenses to endpoints

MTR Operations

MTR ONBOARDING

MTR Provisioning

- MTR team receives license codes, escalation contacts, and Response Mode preference
- A Health Check case is automatically generated

Customer receives MTR Welcome Kit

- *Welcome Kit is delivered via email***
  - *How we work*
  - *How to reach us*
  - *Scope of service*
  - *How we collect data*
  - *How we conduct investigations*
  - *How we conduct threat hunts*

Customer receives Health Check results

- Health Checks are delivered via Threat Analysis Center

Customer Success and MTR Operations

ADVANCED CUSTOMERS

Customer Orientation

- CSM send welcome email with a request to schedule an orientation call (30 mins)
- Customer orientation call (CSM, TAM, MTR rep)
  - Reiterate Welcome Kit information
  - Walk through Health Check results
  - Answer any outstanding questions

Ongoing MTR Operations (Advanced Offering)

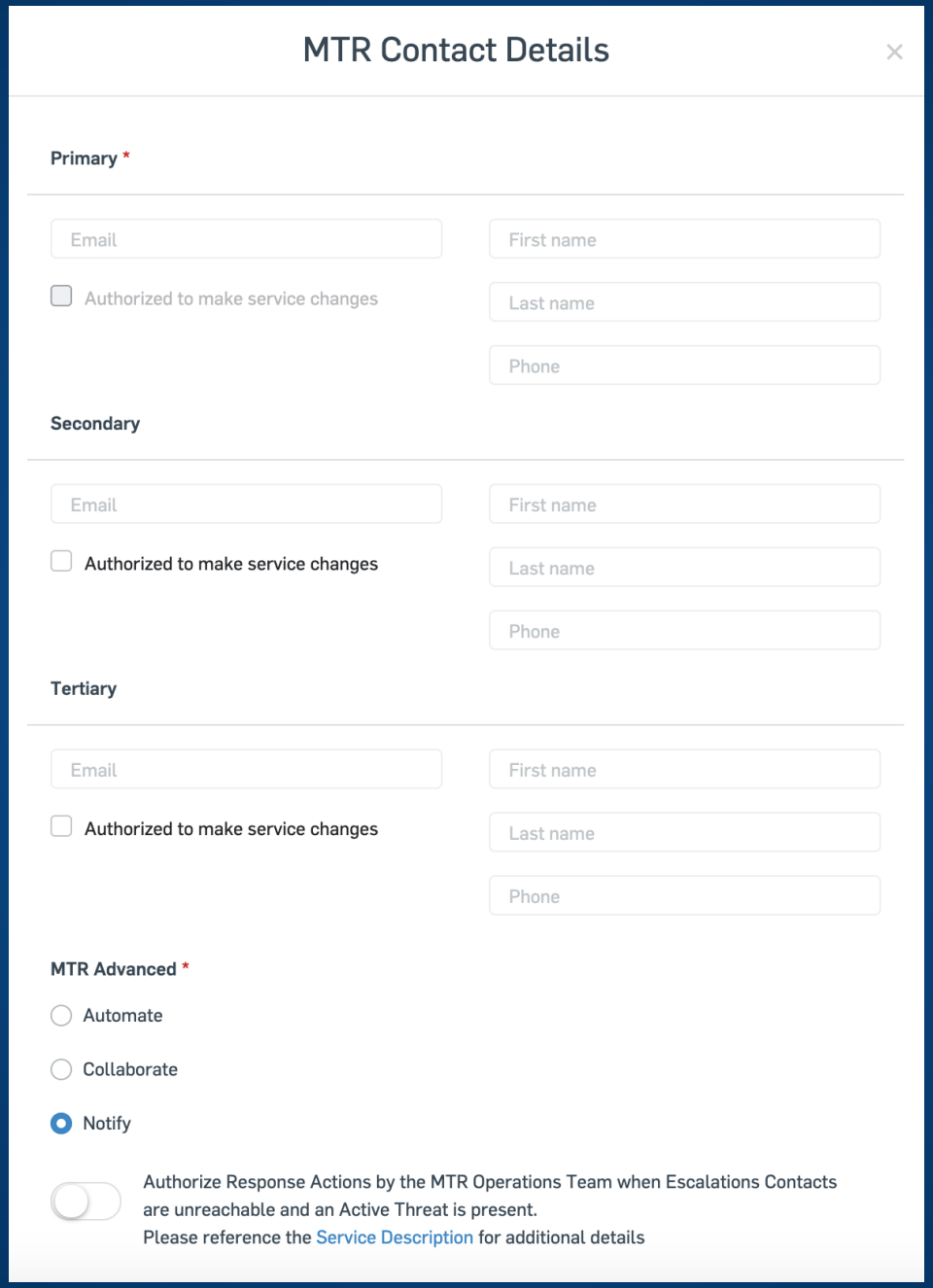
- 24/7 threat hunting, detection, and response
- MTR Operations Reviews

STANDARD CUSTOMERS

Ongoing MTR Operations (Standard Offering)

- 24/7 threat hunting, detection, and response

***denotes items that are in progress or not fully implemented*


MTR Contact Details
Primary *
Email
First name
Authorized to make service changes
Last name
Phone
Secondary
Email
First name
Authorized to make service changes
Last name
Phone
Tertiary
Email
First name
Authorized to make service changes
Last name
Phone
MTR Advanced *
Automate
Collaborate
Notify
Authorize Response Actions by the MTR Operations Team when Escalations Contacts are unreachable and an Active Threat is present.
Please reference the Service Description for additional details

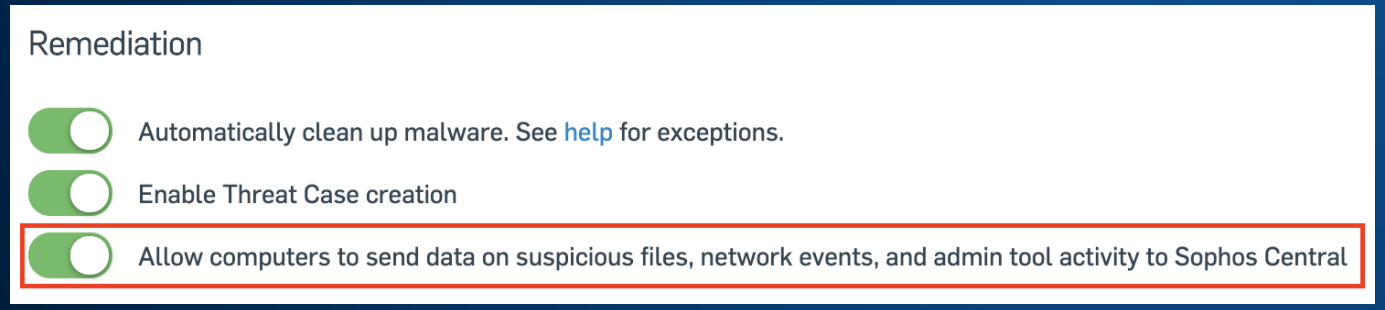
Health Check Overview

Health Check

When we receive notification that a customer has activated, our team will immediately begin assessing the customer's Central policy set (endpoint and server).

What is Reviewed?

Threat Protection Policies | Exclusions | Update Policies | General Configuration



<--- Necessary for MTR

Health Check Observations

- 123 Health Checks performed to date
  - This includes customer sub-estates

- Common Findings
  - Deep Learning and Active Adversary Mitigations are disabled
  - Dangerous Exclusions:
    - *.<filename>
    - Admin Tools / PUA's
    - Suspicious Tools (nmap, coin miners, keygens, metasploit)

Our objective is to ensure the customer is using the best protection settings possible given constraints in their environment.

The Sophos Managed Threat Response (MTR) team has conducted a Security Health Check on your Intercept X with EDR policies. The goal of this exercise is to review your operating conditions and identify quick configuration changes to improve your endpoint security posture. Below are our findings and recommendations.

Please respond to this email when you have reviewed our recommendations, have additional questions, or have made the suggested changes. Any best practice recommendations not followed may result in diminished service quality.

// HEALTH CHECK RECOMMENDATIONS

[Endpoint Protection > Policies > Threat Protection > Base Policy]
Deep Learning: [Disabled] - Recommendation is to enable this policy option
Active Adversary Mitigations: [Disabled] - Recommendation is to enable this policy option
Policy Exclusions: - We recommend removing the following exclusion:

- Psexecsvc

[Endpoint Protection > Policies > Threat Protection > NeuroWorks Policy (Not Assigned)]
Deep Learning: [Disabled] - Recommendation is to enable this policy option
Active Adversary Mitigations: [Disabled] - Recommendation is to enable this policy option
Policy Exclusions: - If exclusions are not required for business use, we recommend disabling them. Otherwise, we advise against whitelisting entire directories or utilizing wildcards, and recommend being as specific as possible with exclusions:

- *.avi
- *.doc
- *.edf
- *.ecg
- *.emg
- *.emgs
- *.emgworkstest
- *.ent
- *.ent.old
- *.ent.txt
- *.epo
- *.epr
- *.epworkstest
- *.erd
- *.etc
- *.iom
- *.jpeg
- *.jpg
- *.lay
- *.mg2
- *.mg2.backfill
- *.mg2.indx
- *.mg2.xml
- *.mpg
- *.mtg
- *.pdf
- *.psx

Managed Threat Response Report

Aug. 17, 2019 - Sept. 17, 2019

SOPHOS

Overall protection rating

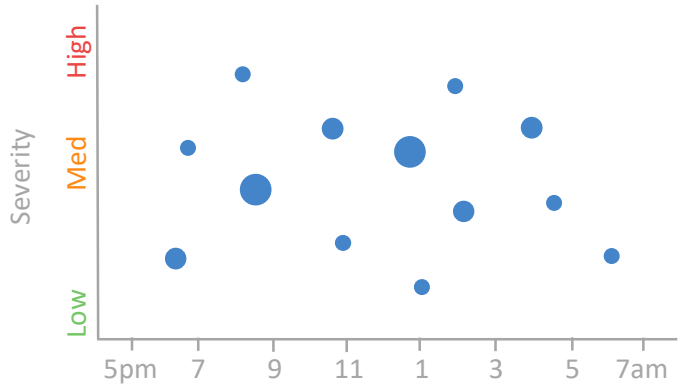
Green

See Health Check results for steps to enhance your security

1416 Nodes protected

869 unprotected

After hours detections



Average daily detections

547,843 Detections

Technology-generated threat indicators.

9 Cases

Detections requiring an analyst investigation.

1 Escalations

Cases requiring customer input or action.

0 Incidents

Escalated cases that could severely impact customer operations.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
0	1	6	0	0	0

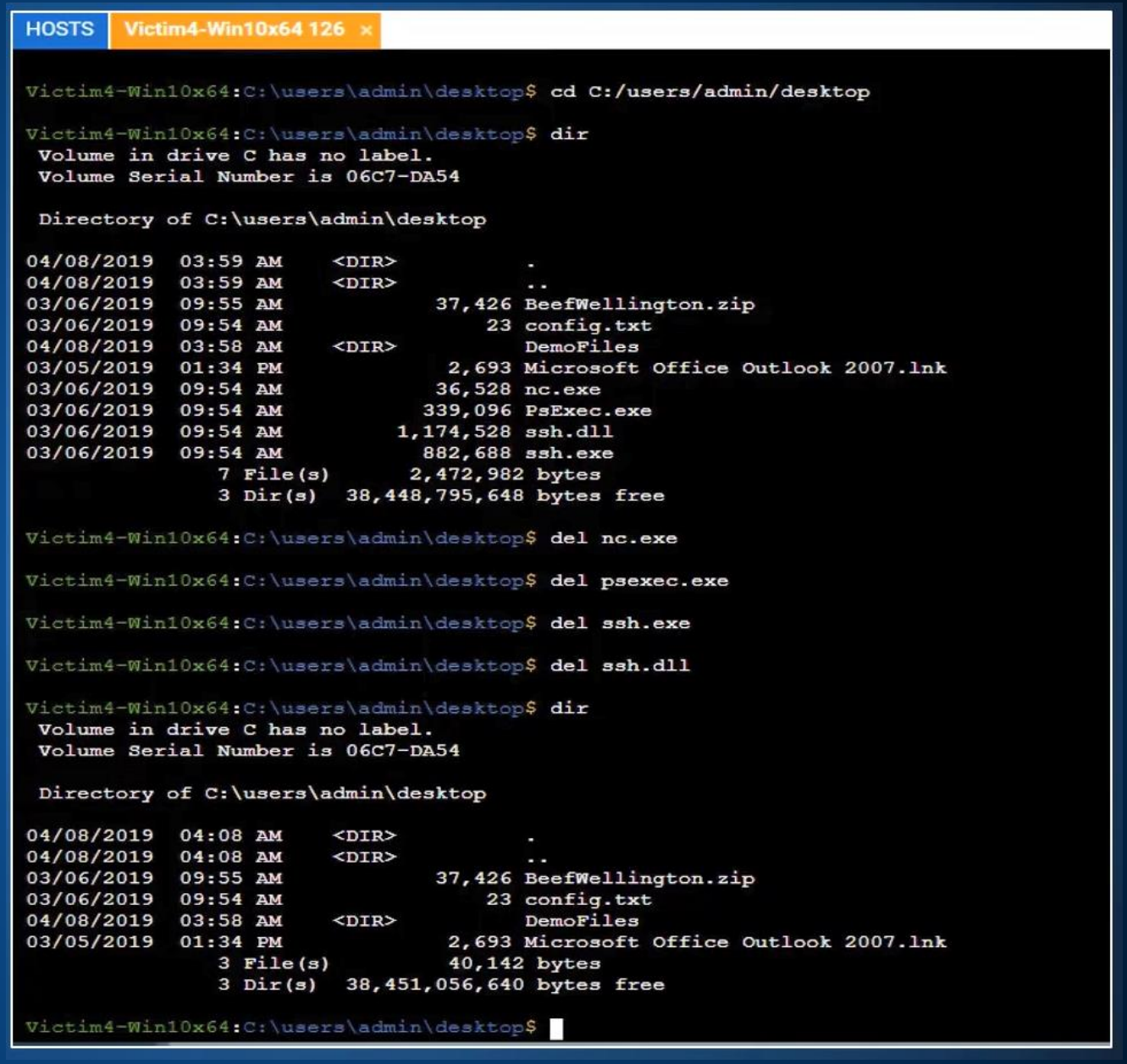
Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
0	0	0	0	2	0

Next EDR Release

SOPHOS

Remote Terminal

- Direct system access
- Full shell capabilities
- All actions are logged
- Enable/Disable by policy



SOPHOS

SOPHOS CENTRAL Admin

Threat Analysis Center

Back to Overview

DETECTION AND REMEDIATION

- Dashboard
- Threat Cases
- Live Query
- Threat Searches
- Threat Indicators

☐	10398e7e-76bd-4bf9-b87c-6a056374aa40	Victim-2-Win7	!	Computer	Windows 7 Ultimate Service Pack 1	VICTIM-2-WIN7\test	172.16.18.102	
☑	3dd7801d-a5a7-4f60-9d71-a6bc4931d4d7	DESKTOP-RB61UC8	✓	Computer	Windows 10 Pro	DESKTOP-RB61UC8\Admin	10.85.96.56,172.16.16.1	fe80::3df8:cd44:625f:c8d9,fe80::c82
☑	4a3583e0-0480-4a82-bc7f-ed7ae7b85e1c	Victim5-Win10	✓	Computer	Windows 10 Pro	VICTIM5-WIN10\Admin	169.254.80.156,172.16.18.104	fe80::b5e1:8805:9710:483,fe80::ec9
☐	9c2f8b54-26d7-427f-904c-82deb09bcba3	31621-timrayme	✓	Computer	Windows 10 Enterprise	31621-TIMRAYME\Administrator	10.55.56.114	fe80::5c25:3209:b646:5c11
☑	b8f65a76-7dd1-47e2-8542-e257e835db75	Victim4-Win10	✓	Computer	Windows 10 Pro	VICTIM4-WIN10\Admin	172.16.18.101	fe80::7849:c1f7:536a:854d
☐	fc301785-2123-47dd-b60c-5d9d9e5c6a14	Victim1-EDR	✓	Computer	Windows 7 Ultimate Service Pack 1	VICTIM1-EDR\test	172.16.18.100	

Query : Select One - 14 Categories, 21 Queries

Create new query

Search

All Queries [21]
This is a list of ALL queries

Favorites [0]
Admins can mark a query as a favorite

Recent Queries [7]
This is a list of the last 20 saved queries that have been run recently

Anomaly [1]
Detection of variance first use, rare use, large data transfers etc

Compliance [0]
Basic security compliance queries, like is the device listening for RDP connections

Device [4]
Device details from os version, patches and video and disk information

Event [1]
Access to the system event logs

File [7]
Queries that look at files and activity done to files. These queries primarily use the file table in OSQ

Mitre Attack [0]
Queries that map to tactics and techniques

Network [0]
Network information including live and historic connections and data sent/received from the journals

Other [1]
Everything else

Process [4]
Information on both running processes and process that have run in the past.

Registry [2]
Details on registry changes and access

User [2]
Information from current users to failed authentications

Query results 0 / 0 Devices completed

Telemetry view

SOPHOS CENTRAL Admin

Threat Analysis Center

Back to Overview

DETECTION AND REMEDIATION

- Dashboard
- Threat Cases
- Live Query
- Threat Searches
- Threat Indicators

	10398e7e-76bd-4df9-887c-6a056374aa40	Victim-2-Win7	Computer	Windows 7 Ultimate Service Pack 1	VICTIM-2-WIN7\test	172.16.18.102	
☑	3dd7801d-a5a7-4f60-9d71-a6bc4931d4d7	DESKTOP-RB61UC8	Computer	Windows 10 Pro	DESKTOP-RB61UC8\Admin	10.85.96.56,172.16.16.1	fe80::3df8:cd44:625f:c8d9,fe80::c82
☑	4a3583e0-0480-4a82-bc7f-ed7ae7b85e1c	Victim5-Win10	Computer	Windows 10 Pro	VICTIM5-WIN10\Admin	169.254.80.156,172.16.18.104	fe80::b5e1:8805:9710:483,fe80::ec9
☐	9c2f8b54-26d7-427f-904c-82deb09bcba3	31621-timrayme	Computer	Windows 10 Enterprise	31621-TIMRAYME\Administrator	10.55.56.114	fe80::5c25:3209:b646:5c11
☑	b8f65a76-7dd1-47e2-8542-e257e835db75	Victim4-Win10	Computer	Windows 10 Pro	VICTIM4-WIN10\Admin	172.16.18.101	fe80::7849:c1f7:536a:854d
☐	fc301785-2123-47dd-b60c-5d9d9e5c6a14	Victim1-EDR	Computer	Windows 7 Ultimate Service Pack 1	VICTIM1-EDR\test	172.16.18.100	

Query : Select One - 14 Categories, 21 Queries

Back to categories

All Queries

All OS types | All Performance types | Search

Name	Description	Category	Supported OS	Performance	Author	Last Modified
dlls loaded by process SophosPID	List of dlls loaded by a process by SophosPID	Other	Windows, Windows Server	Not Available		-
Encoded CMD Lines	List processes with encoded command lines	Process	Windows, Windows Server	Not Available		-
File Details by MD5 Hash	Provide location, hash, size, creation time, owner, permission info, last access time, last change time, last status change	File	Windows, Windows Server	Not Available		-
File Details by name	Provide filename, directory, hash, size in KB, creation time, owner, permission info, last access time, file type (File/Directory)	File	Windows, Windows Server	Not Available		-
File Downloads	List all files in download folders	File	Windows, Windows Server	Not Available		-
File history by hash	List processes that have read or written to a file by file SHA 256 Hash	File	Windows, Windows Server	Not Available		-
File history by Path and name	List processes that have read or written to a file by file name	File	Windows, Windows Server	Not Available		-
Get Registry details by name	List the registry info for name	Registry	Windows, Windows Server	Not Available		-
Last 10 Installed programs	List last 10 Installed programs	File	Windows, Windows Server	Not Available		-
List last 10 powershell events	List last 10 powershell events	Event	Windows, Windows Server	Not Available		-
List processes by user ID	List all processes with the userId as the owner	User	Windows, Windows Server	Not Available		-
OS Version	OS Version	Device	Windows, Windows Server	Not Available		-

Query results 0 / 0 Devices completed

Telemetry view