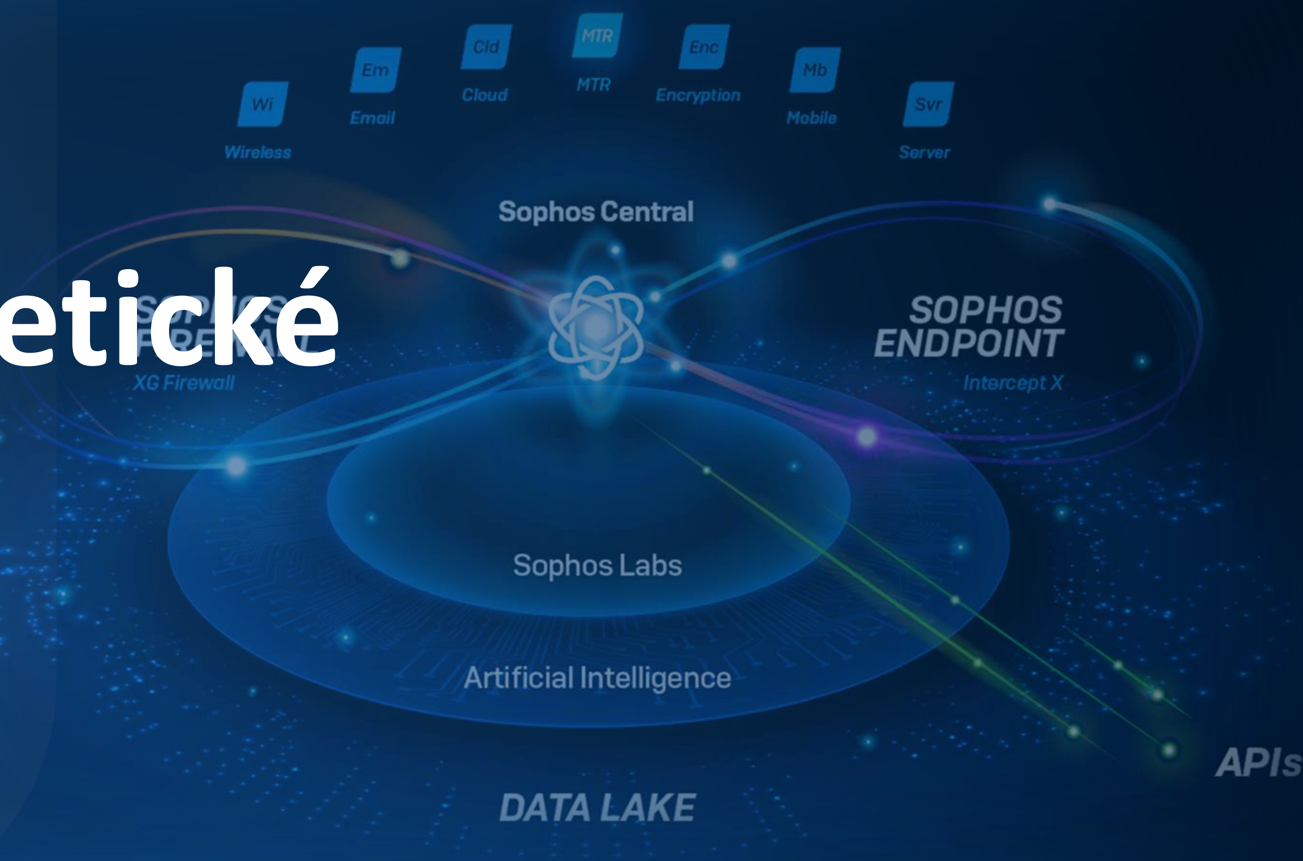
Vize a směr kybernetické bezpečnosti

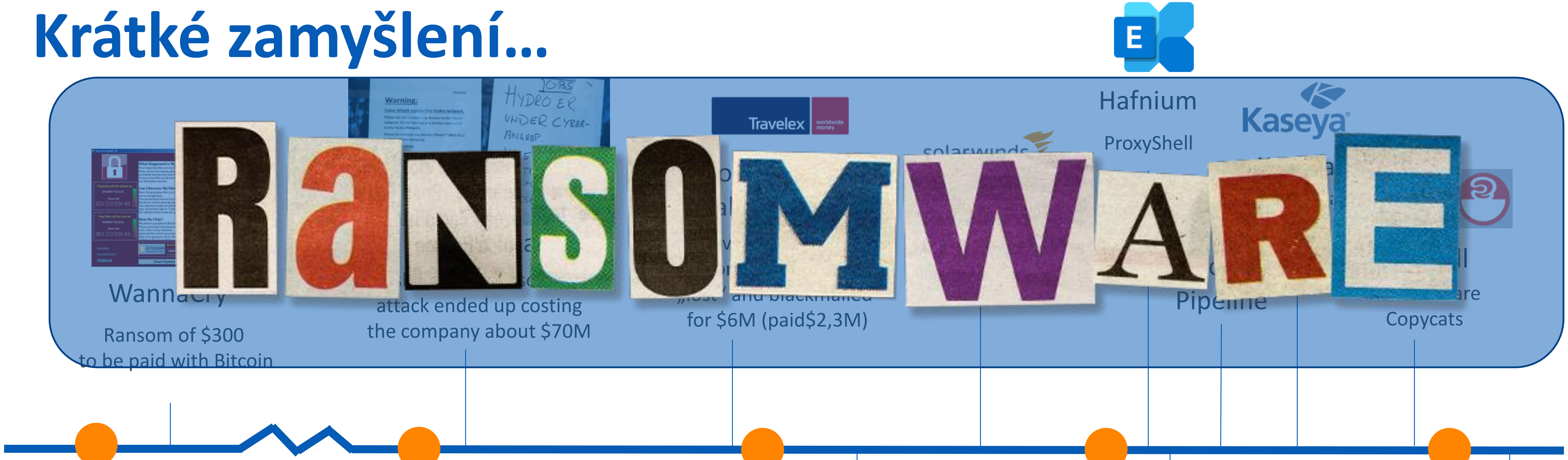


Ondrej Hubalek

Senior Sales Engineer, Team EE

SOPHOS

Krátké zamyšlení...



WannaCry

Ransom of $300 to be paid with Bitcoin

attack ended up costing the company about $70M

„lost“ and blackmailed for $6M (paid$2,3M)

Hafnium

ProxyShell

Pipeline

are

Copycats

2017

2019

2020

2021

2022

Corona forces
millions to work from home:
* VPN Booster
* RDP Madness

Hundreds of thousands companies are switching from Exchange to M365

EU and several governments warn against using Kaspersky

Vliv Malware na provoz organizací

61%

Cyberattacks increase over last year

37%

Organizations hit by ransomware

54%

Attacks too advanced for IT team alone

Adversary sophistication

Malware writers

Individual gangs

Active adversaries

Specialist attack services

Source: The State of the IT Security Team 2021, Sophos; The State of Ransomware 2021, Sophos

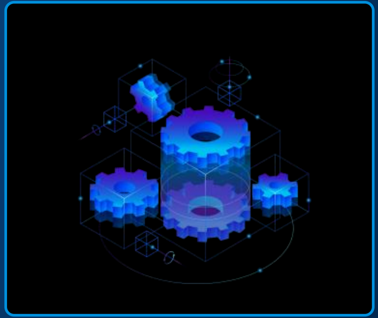
Distribuovaný, přesto propojený svět

Remote workin
environmen
Cloud m ation of
Azure
aws
ORACLE
CLOUD
kubernetes
NUTANIX
docker
Google Cloud
salesforce
box
Gmail
Dropbox
Office 365

Interconnected supply chain, infrastructure, technology

AI

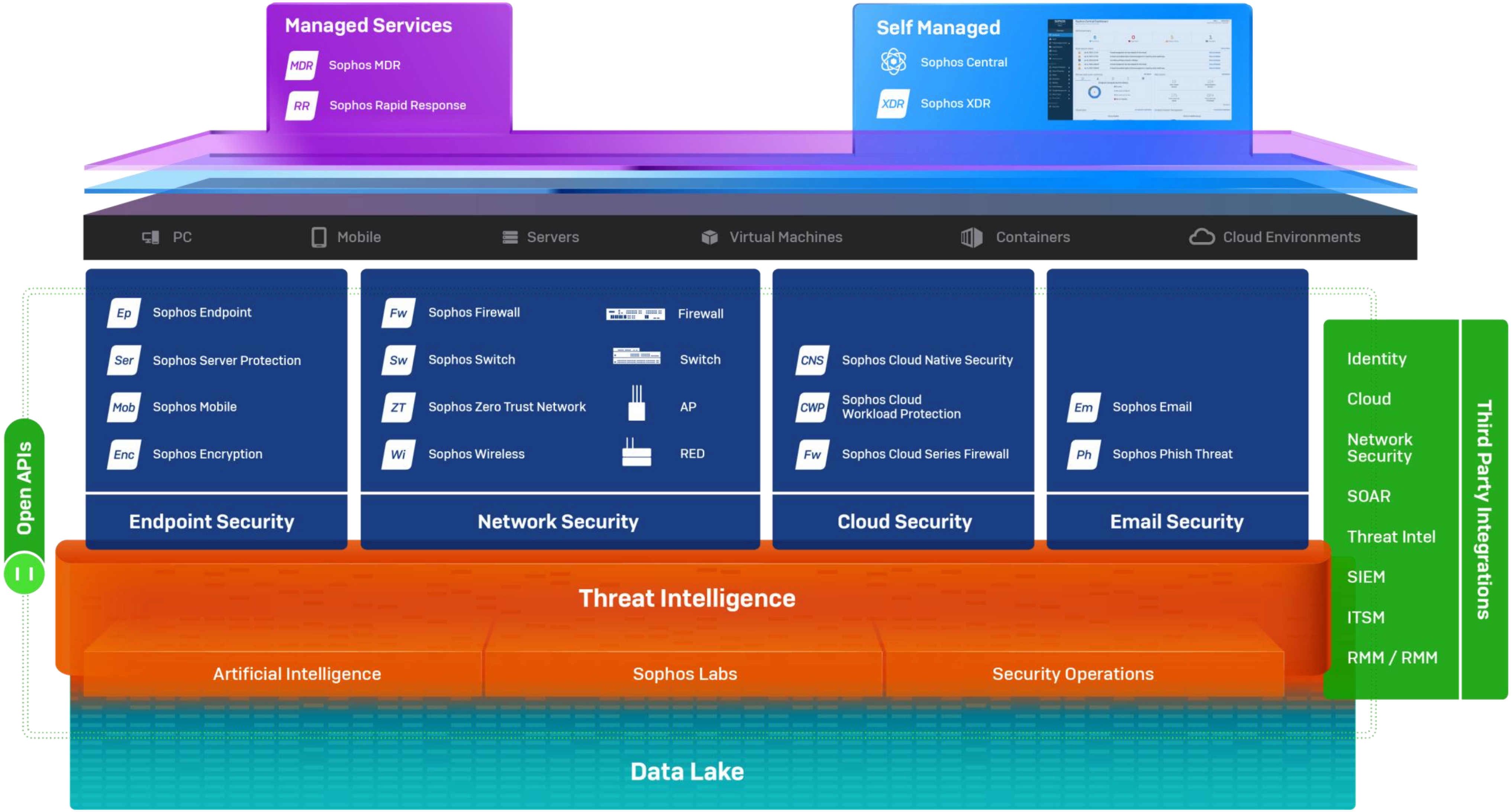
Automation



Integration

Jak se proti tomu bránit?

Adaptive Cybersecurity Ecosystem



Managed Services

- MDR Sophos MDR
- RR Sophos Rapid Response

Self Managed

- Sophos Central
- XDR Sophos XDR

PC | Mobile | Servers | Virtual Machines | Containers | Cloud Environments

Endpoint Security

- Ep Sophos Endpoint
- Ser Sophos Server Protection
- Mob Sophos Mobile
- Enc Sophos Encryption

Network Security

- Fw Sophos Firewall — Firewall
- Sw Sophos Switch — Switch
- ZT Sophos Zero Trust Network — AP
- Wi Sophos Wireless — RED

Cloud Security

- CNS Sophos Cloud Native Security
- CWP Sophos Cloud Workload Protection
- Fw Sophos Cloud Series Firewall

Email Security

- Em Sophos Email
- Ph Sophos Phish Threat

Open APIs

Threat Intelligence

Artificial Intelligence | Sophos Labs | Security Operations

Data Lake

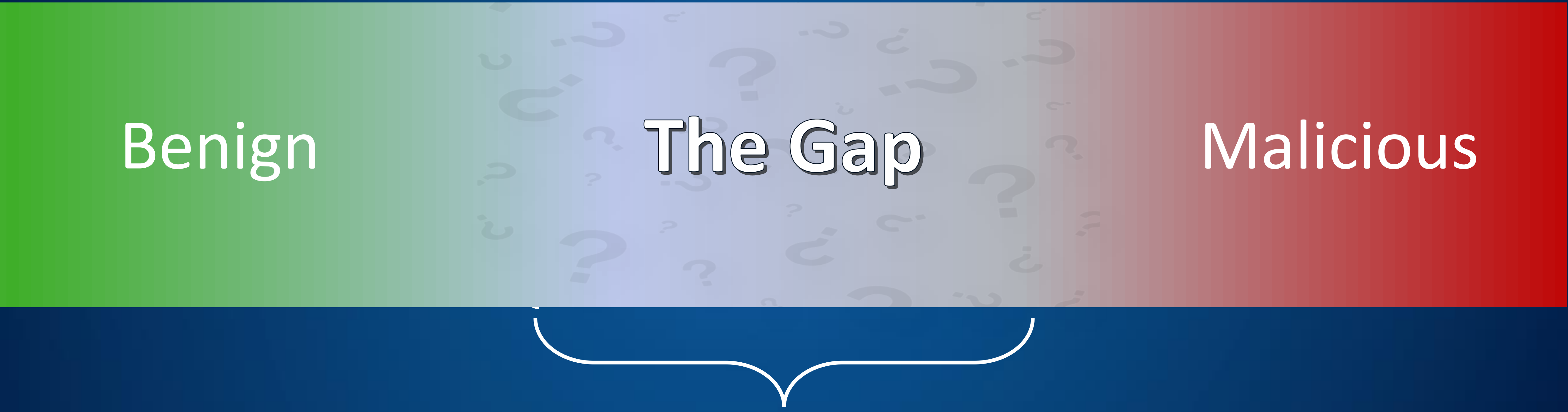
Third Party Integrations

- Identity
- Cloud
- Network Security
- SOAR
- Threat Intel
- SIEM
- ITSM
- RMM / RMM

Kde začít?

SOPHOS

Endpoint Detection and Response (EDR)



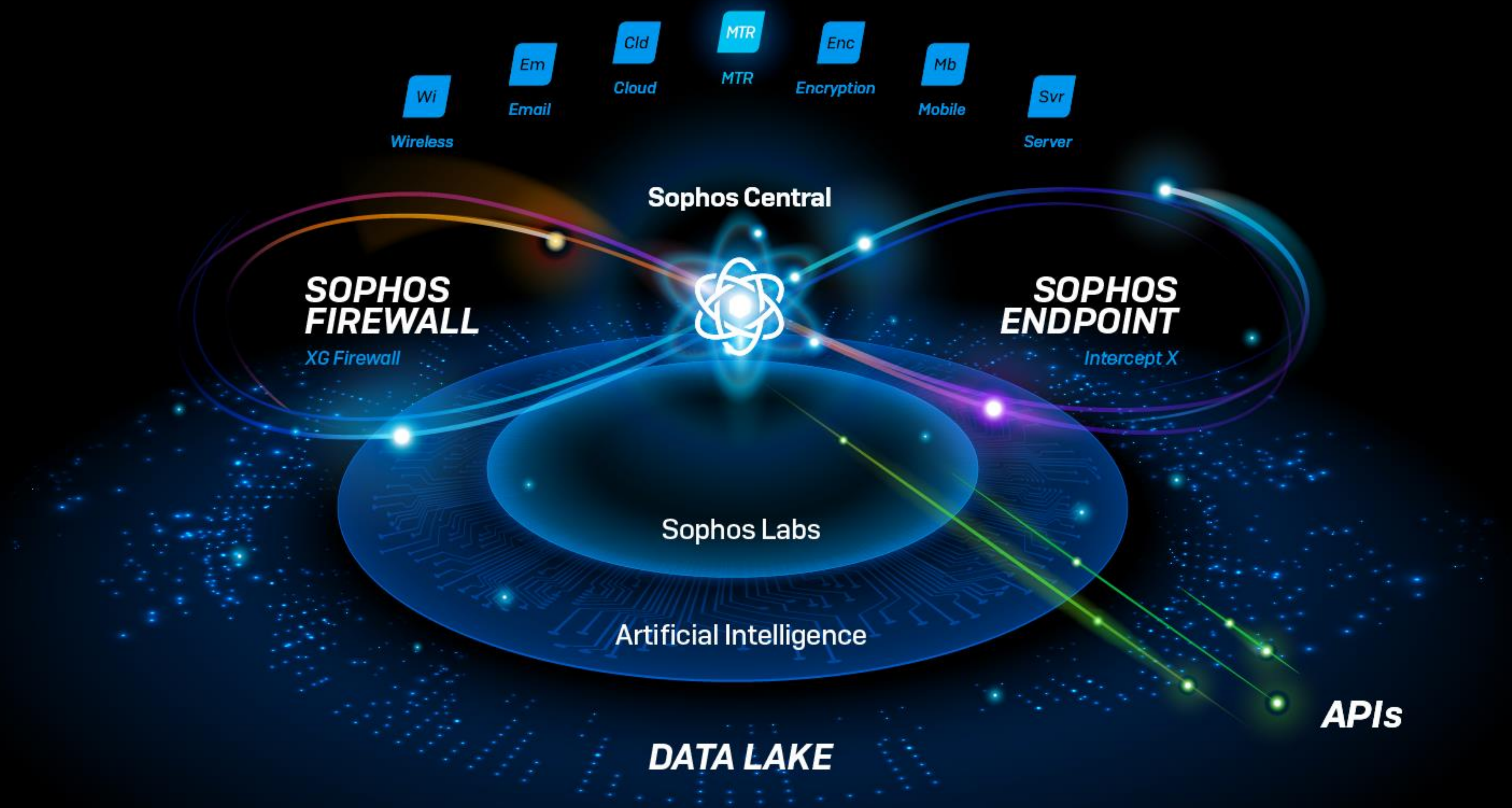
Benign

The Gap

Malicious

EDR

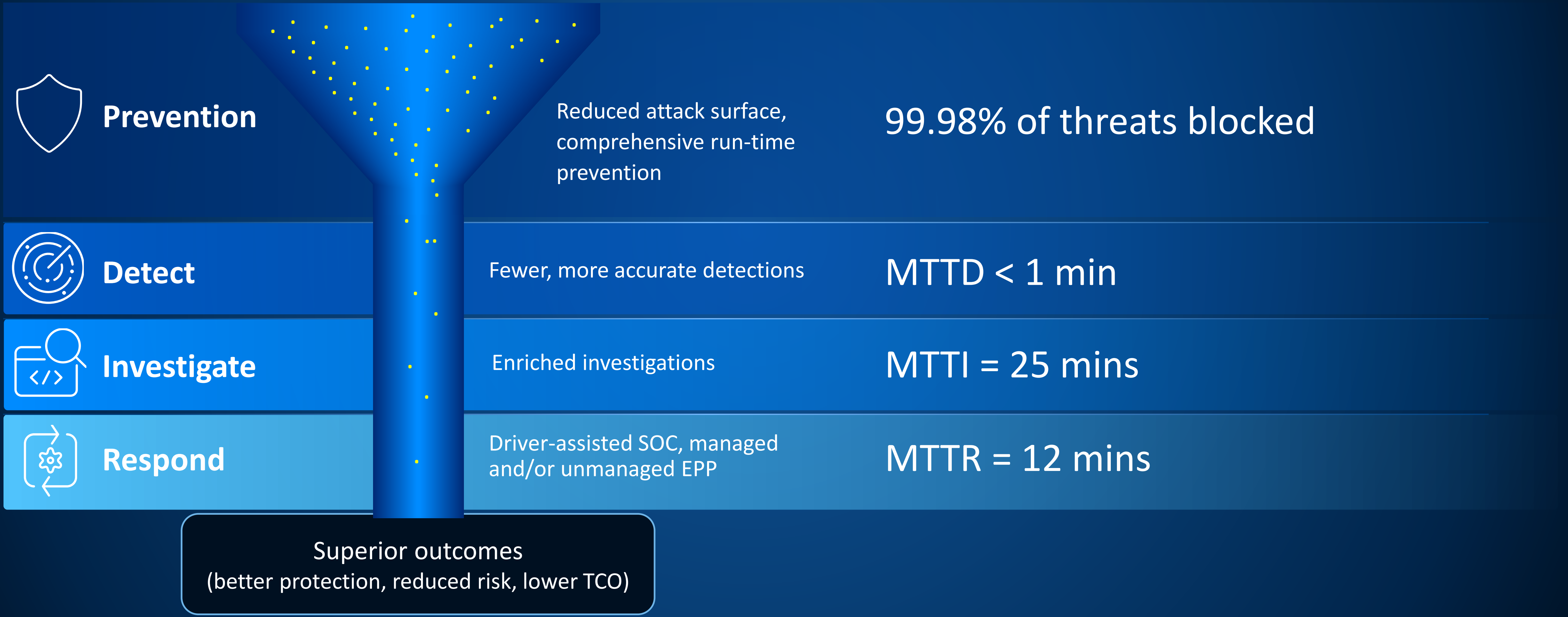
Sophos XDR: A True Cybersecurity Ecosystem



> Nejlepší investigace je ta, kterou nemusíte vůbec provádět.
>
> Pokročilé možnosti prevence umožňují bezpečnostním analytikům se soustředit pouze na několik, více relevantních investigací—což pomáhá organizacím šetří čas, úsilí a peníze.

SOPHOS

Optimize Prevention. Minimize Time to Detect and Respond



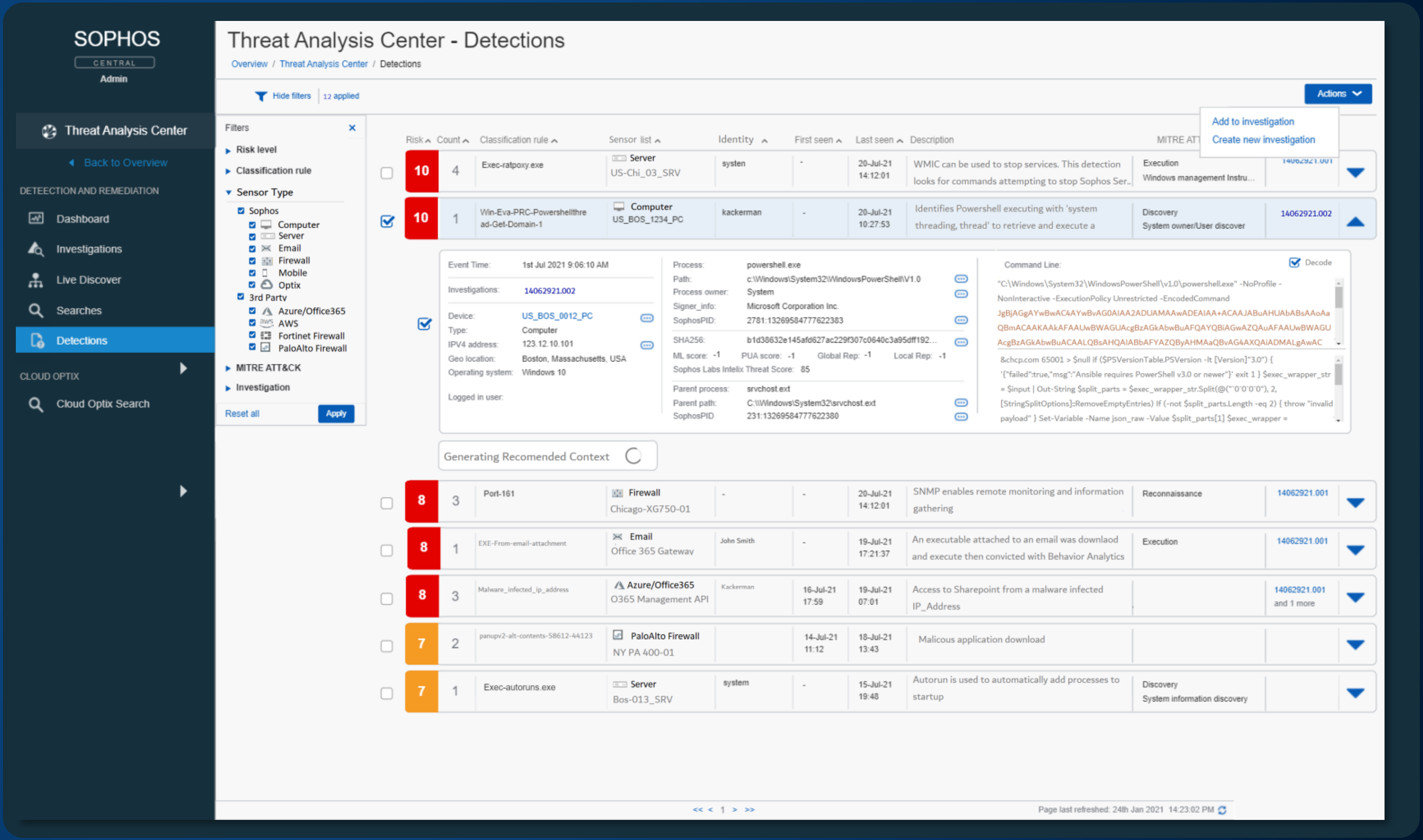
Prevention	Reduced attack surface, comprehensive run-time prevention	99.98% of threats blocked
Detect	Fewer, more accurate detections	MTTD < 1 min
Investigate	Enriched investigations	MTTI = 25 mins
Respond	Driver-assisted SOC, managed and/or unmanaged EPP	MTTR = 12 mins

Superior outcomes
(better protection, reduced risk, lower TCO)

Source: AV-Test 2021 average score; Sophos Managed Threat Response current performance metrics

Detection: Více přesné, více cílené

- AI-prioritized risk score pro lepší přehled analytiků
- Ucelené informace pro rychlou orientaci a pochopení
- Možnost začít s detekcemi na úrovní Endpointů a propojení se zbytkem Ecosystemu:
- Endpoints, server, firewall, email, cloud, mobile, Office 365, as you start an investigation



Threat Analysis Center - Detections

Overview / Threat Analysis Center / Detections

	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:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -
NonInteractive -ExecutionPolicy Unrestricted -EncodedCommand
JgBjAGgAYwBwAC4AYwBvAG0AIAA2ADUAMAAwADEAIAA+ACAAJABuAHUAbABsAAoAa
QBmACAAKAAkAFAAUwBWAGUAcgBzAGkAbwBuAFQAYQBiAGwAZQAuAFAAUwBWAGU
AcgBzAGkAbwBuACAALQBsAHQAIABbAFYAZQByAHMAaQBvAG4AXQAiADMALgAwAC
```

```
&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 =
```

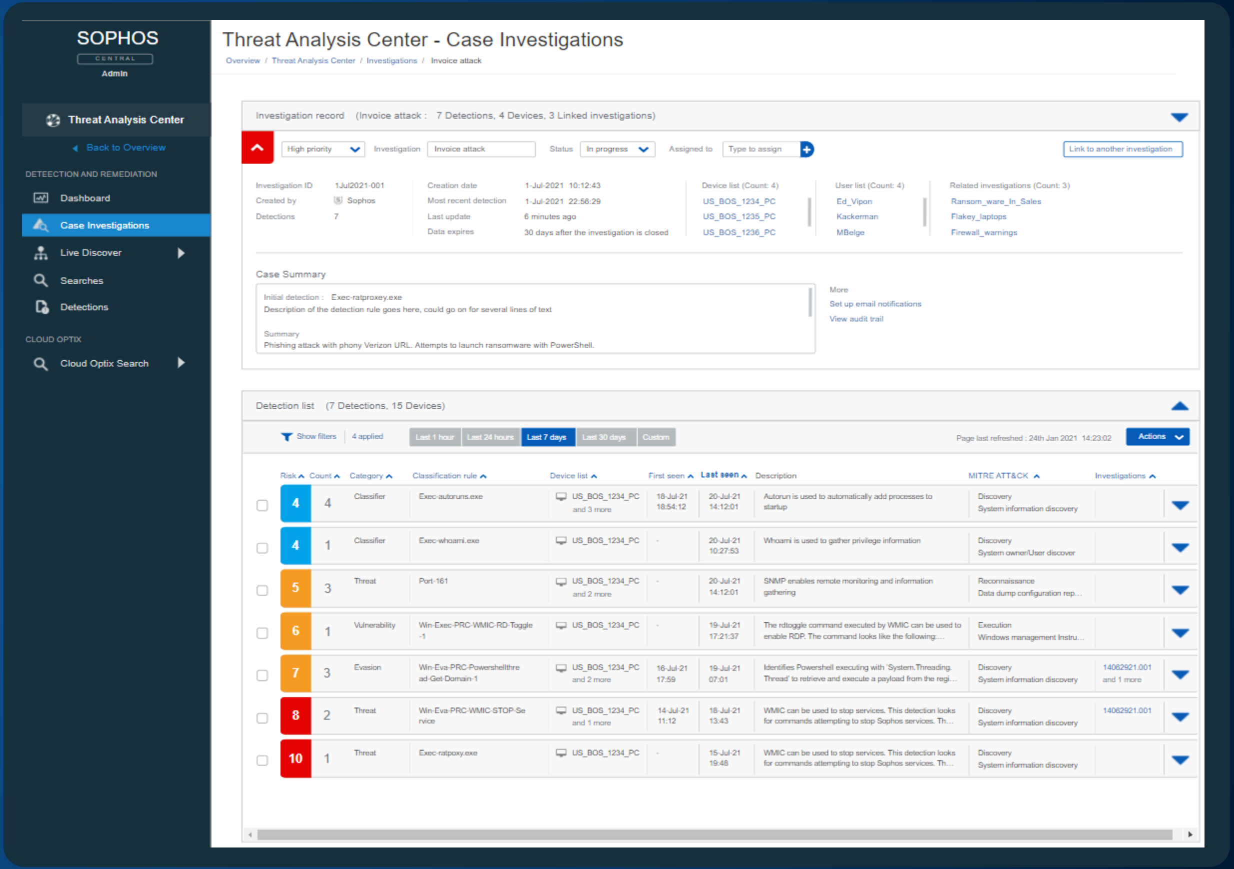
Generating Recomended Context

	Risk	Count	Classification rule	Sensor list	Identity	First seen	Last seen	Description	MITRE ATT		
☐	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		▼

Page last refreshed: 24th Jan 2021 14:23:02 PM

Investigation: Komplexní a přehledné

- Umožňuje investigování probíhajících útoků
- Kombinuje různé Detekce do konkrétní Investigace
- Investigace můžou bít přiděleny konkrétnímu analytikovi
- Je doporučeno řídit se OODA-Loop během investigace
- Základní platforma pro Sophos MDR



Threat Analysis Center - Case Investigations

Overview / Threat Analysis Center / Investigations / Invoice attack

Investigation record (Invoice attack : 7 Detections, 4 Devices, 3 Linked investigations)

High priority | Investigation: Invoice attack | Status: In progress | Assigned to: Type to assign | Link to another investigation

Investigation ID: 1Jul2021-001
Created by: Sophos
Detections: 7

Creation date: 1-Jul-2021 10:12:43
Most recent detection: 1-Jul-2021 22:56:29
Last update: 6 minutes ago
Data expires: 30 days after the investigation is closed

Device list (Count: 4): US_BOS_1234_PC, US_BOS_1235_PC, US_BOS_1236_PC

User list (Count: 4): Ed_Vipon, Kackerman, MBelge

Related investigations (Count: 3): Ransom_ware_In_Sales, Flakey_laptops, Firewall_warnings

Case Summary

Initial detection : Exec-ratproxey.exe
Description of the detection rule goes here, could go on for several lines of text

Summary
Phishing attack with phony Verizon URL. Attempts to launch ransomware with PowerShell.

More
Set up email notifications
View audit trail

Detection list (7 Detections, 15 Devices)

Show filters | 4 applied | Last 1 hour | Last 24 hours | Last 7 days | Last 30 days | Custom

Page last refreshed : 24th Jan 2021 14:23:02 | Actions

Risk	Count	Category	Classification rule	Device list	First seen	Last seen	Description	MITRE ATT&CK	Investigations
4	4	Classifier	Exec-autoruns.exe	US_BOS_1234_PC and 3 more	18-Jul-21 18:54:12	20-Jul-21 14:12:01	Autorun is used to automatically add processes to startup	Discovery System information discovery	
4	1	Classifier	Exec-whoami.exe	US_BOS_1234_PC	-	20-Jul-21 10:27:53	Whoami is used to gather privilege information	Discovery System owner/User discover	
5	3	Threat	Port-161	US_BOS_1234_PC and 2 more	-	20-Jul-21 14:12:01	SNMP enables remote monitoring and information gathering	Reconnaissance Data dump configuration rep…	
6	1	Vulnerability	Win-Exec-PRC-WMIC-RD-Toggle-1	US_BOS_1234_PC	-	19-Jul-21 17:21:37	The rdtoggle command executed by WMIC can be used to enable RDP. The command looks like the following:…	Execution Windows management Instru…	
7	3	Evasion	Win-Eva-PRC-Powershellthread-Get-Domain-1	US_BOS_1234_PC and 2 more	16-Jul-21 17:59	19-Jul-21 07:01	Identifies Powershell executing with 'System.Threading. Thread' to retrieve and execute a payload from the regi…	Discovery System information discovery	14062921.001 and 1 more
8	2	Threat	Win-Eva-PRC-WMIC-STOP-Service	US_BOS_1234_PC and 1 more	14-Jul-21 11:12	18-Jul-21 13:43	WMIC can be used to stop services. This detection looks for commands attempting to stop Sophos services. Th…	Discovery System information discovery	14062921.001
10	1	Threat	Exec-ratpoxy.exe	US_BOS_1234_PC	-	15-Jul-21 19:48	WMIC can be used to stop services. This detection looks for commands attempting to stop Sophos services. Th…	Discovery System information discovery	

SIEM vs. XDR

- Hledat jehlu v kupce sena vs. Hledat jehlu v jehelníčku

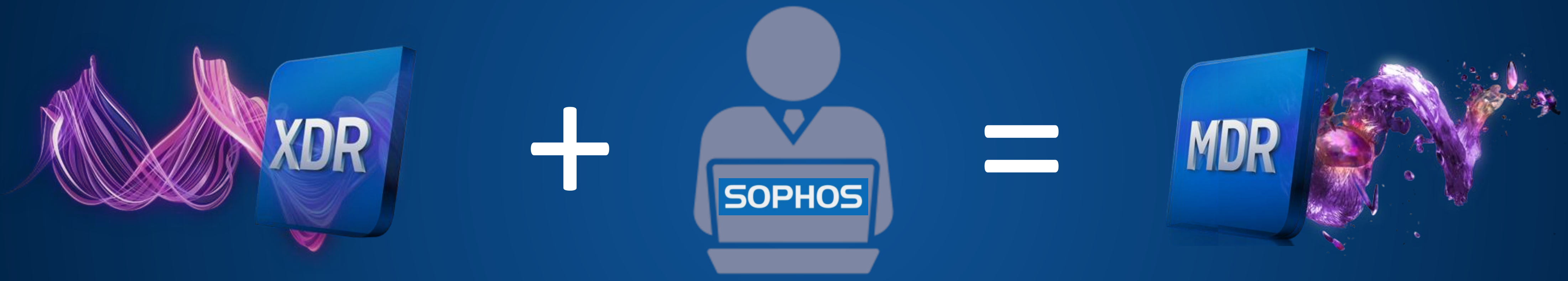
- Shoda / Důkaz

- Pojištění proti CyberSec incidentu

- Napojení produktů 3th stran?

- Potřeba pro shodu - nařízení

SOPHOS



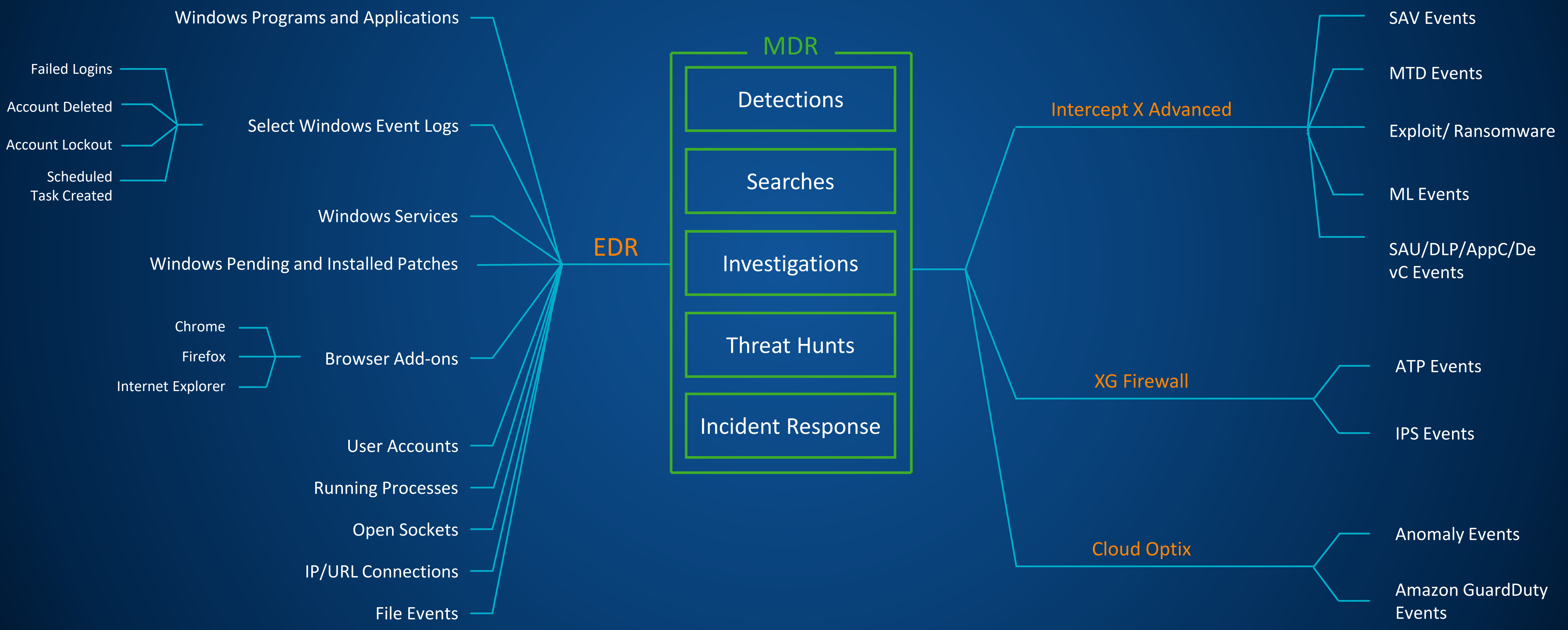
24/7 Security Operations

- Threat Hunting
- Incident Response
- Proactive Security Improvement

Sophos Managed Detection and Response

10.000+ zákazníků

Sophos MDR Data Collection and Architecture



Windows Programs and Applications

Failed Logins

Account Deleted

Account Lockout

Scheduled Task Created

Select Windows Event Logs

Windows Services

Windows Pending and Installed Patches

Chrome

Firefox

Internet Explorer

Browser Add-ons

User Accounts

Running Processes

Open Sockets

IP/URL Connections

File Events

EDR

MDR

Detections

Searches

Investigations

Threat Hunts

Incident Response

Intercept X Advanced

SAV Events

MTD Events

Exploit/ Ransomware

ML Events

SAU/DLP/AppC/DevC Events

XG Firewall

ATP Events

IPS Events

Cloud Optix

Anomaly Events

Amazon GuardDuty Events

Response Modes

Možnost vybrat nejlepší model spolupráce s MDR teamem

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

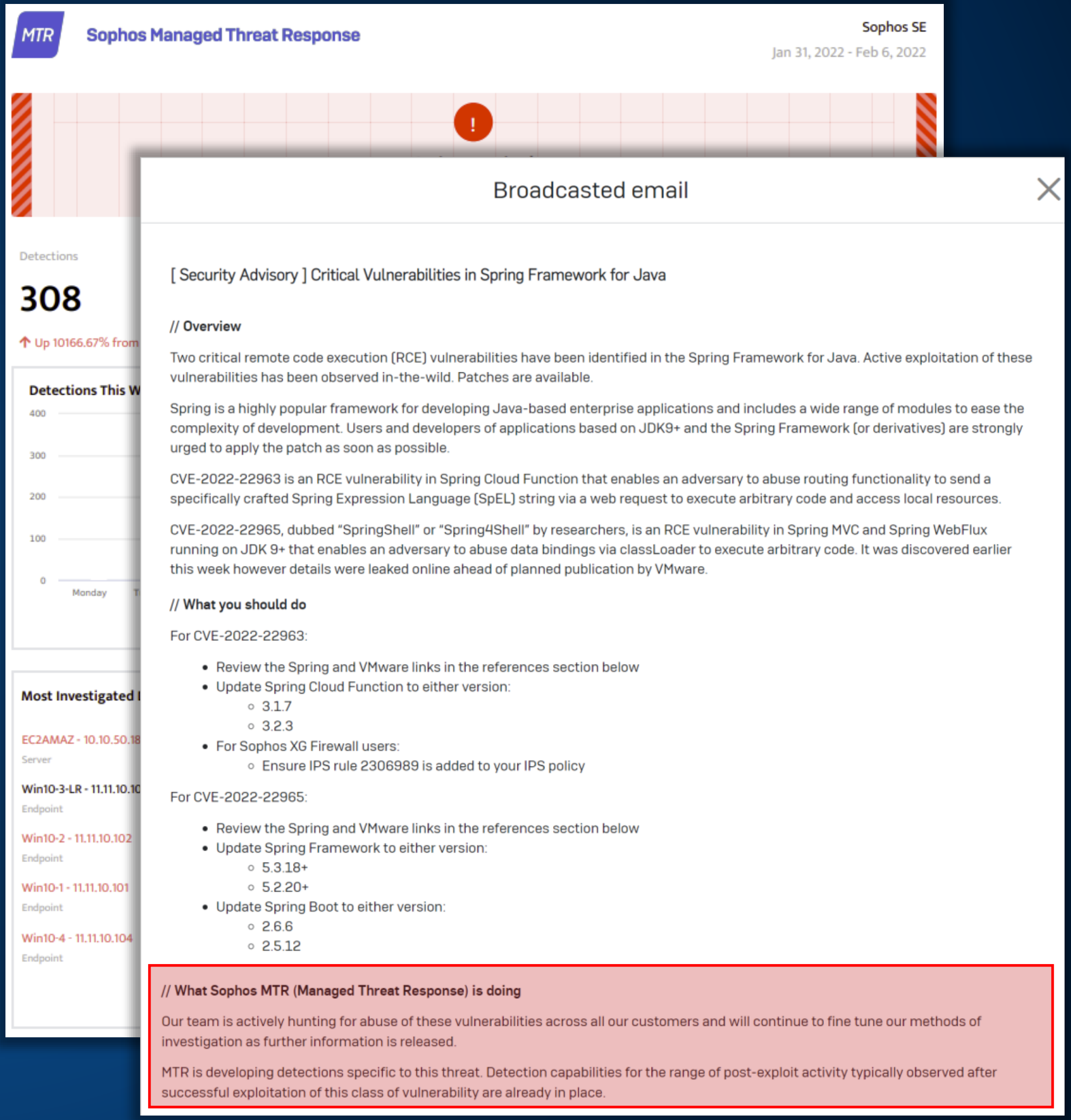
Authorize

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

MDR Reportování & Informace

- Automatické reporty
  - Měsíčně
  - Týdně

- MDR Team zasílá speciální upozornění a informace v případě special události
  - Log4Shell
  - ProxyLogon
  - ProxyShell
  - …



Sophos SE
Jan 31, 2022 - Feb 6, 2022

Detections
308
↑ Up 10166.67% from

Detections This W

Most Investigated

EC2AMAZ - 10.10.50.18
Server
Win10-3-LR - 11.11.10.10
Endpoint
Win10-2 - 11.11.10.102
Endpoint
Win10-1 - 11.11.10.101
Endpoint
Win10-4 - 11.11.10.104
Endpoint

Broadcasted email

[Security Advisory] Critical Vulnerabilities in Spring Framework for Java

// Overview

Two critical remote code execution (RCE) vulnerabilities have been identified in the Spring Framework for Java. Active exploitation of these vulnerabilities has been observed in-the-wild. Patches are available.

Spring is a highly popular framework for developing Java-based enterprise applications and includes a wide range of modules to ease the complexity of development. Users and developers of applications based on JDK9+ and the Spring Framework (or derivatives) are strongly urged to apply the patch as soon as possible.

CVE-2022-22963 is an RCE vulnerability in Spring Cloud Function that enables an adversary to abuse routing functionality to send a specifically crafted Spring Expression Language (SpEL) string via a web request to execute arbitrary code and access local resources.

CVE-2022-22965, dubbed “SpringShell” or “Spring4Shell” by researchers, is an RCE vulnerability in Spring MVC and Spring WebFlux running on JDK 9+ that enables an adversary to abuse data bindings via classLoader to execute arbitrary code. It was discovered earlier this week however details were leaked online ahead of planned publication by VMware.

// What you should do

For CVE-2022-22963:

- Review the Spring and VMware links in the references section below
- Update Spring Cloud Function to either version:
  - 3.1.7
  - 3.2.3
- For Sophos XG Firewall users:
  - Ensure IPS rule 2306989 is added to your IPS policy

For CVE-2022-22965:

- Review the Spring and VMware links in the references section below
- Update Spring Framework to either version:
  - 5.3.18+
  - 5.2.20+
- Update Spring Boot to either version:
  - 2.6.6
  - 2.5.12

// What Sophos MTR (Managed Threat Response) is doing

Our team is actively hunting for abuse of these vulnerabilities across all our customers and will continue to fine tune our methods of investigation as further information is released.

MTR is developing detections specific to this threat. Detection capabilities for the range of post-exploit activity typically observed after successful exploitation of this class of vulnerability are already in place.

SOPHOS

SOPHOS