



Trellix

21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Endpoint Security

Breakout Session





El equipo

Endpoint Security

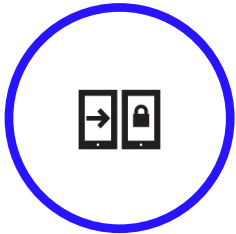
- Alejandro Garcia
- Fernando Segura
- David Nieto
- Julio Quintero

Antes de comenzar

Use the following WIFI:
SID: **to_be_defined**
Password: **to_be_defined**

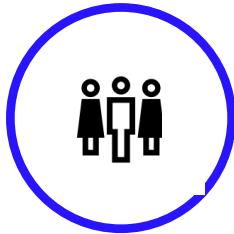
Ponga atención a las siguientes instrucciones....

Silenciar los teléfonos



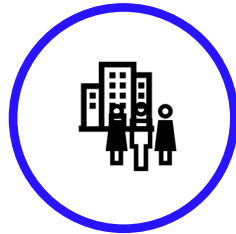
Please mute or turn off your smartphones and other electronic devices to minimize distractions during the presentation.

Baños



Restrooms are located before the reception on your right.

Salidas de emergencia



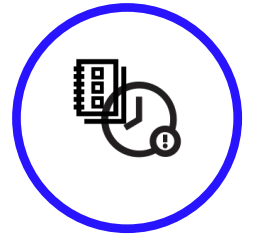
Familiarize yourself with the nearest emergency exits, located just before the reception on your left. In case of an emergency, follow the exit signs and proceed calmly to the nearest exit.

Q&A



We will have a Q&A session at the end of the presentation. Please save your questions until then.

Horarios



The session is expected to last approximately 3 hours with one 30 min. break.

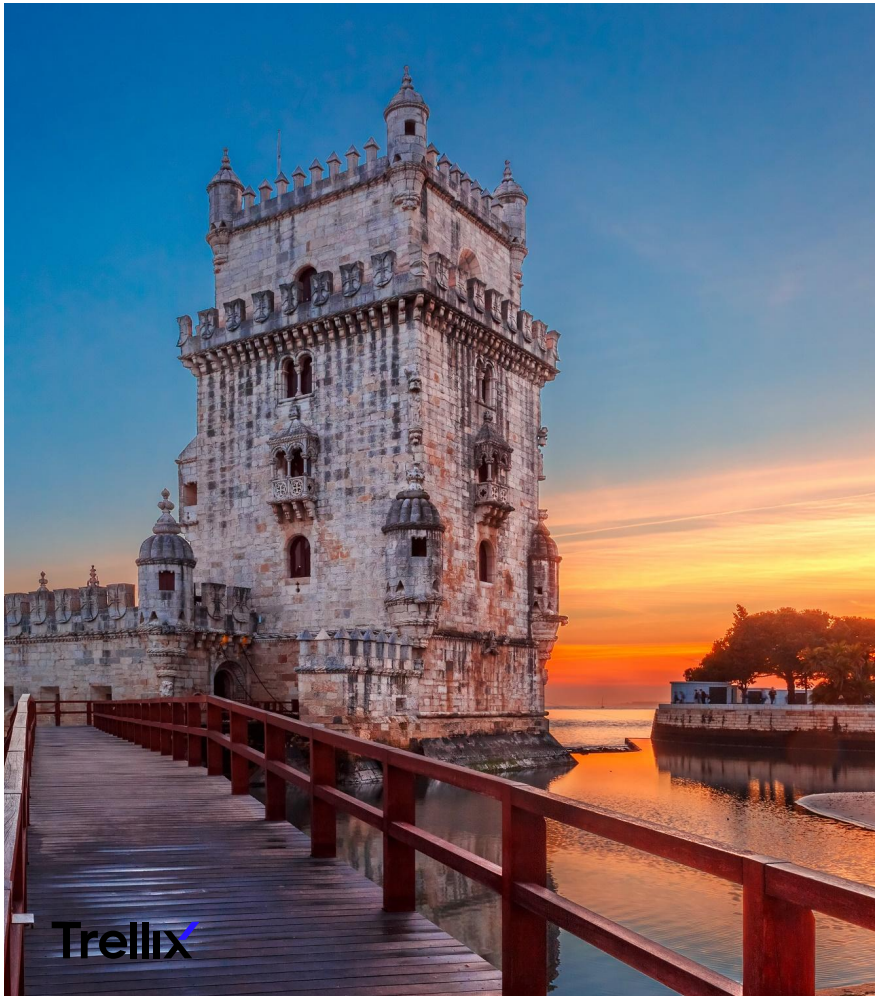
Trellix

Endpoint Security

EMEA & LTAM
Partner Tech Summit

October, 2024





Agenda

Endpoint Security

- Bienvenida
- Línea de productos
- Trellix EDR con Forensics
- Trellix Wise
- Práctica

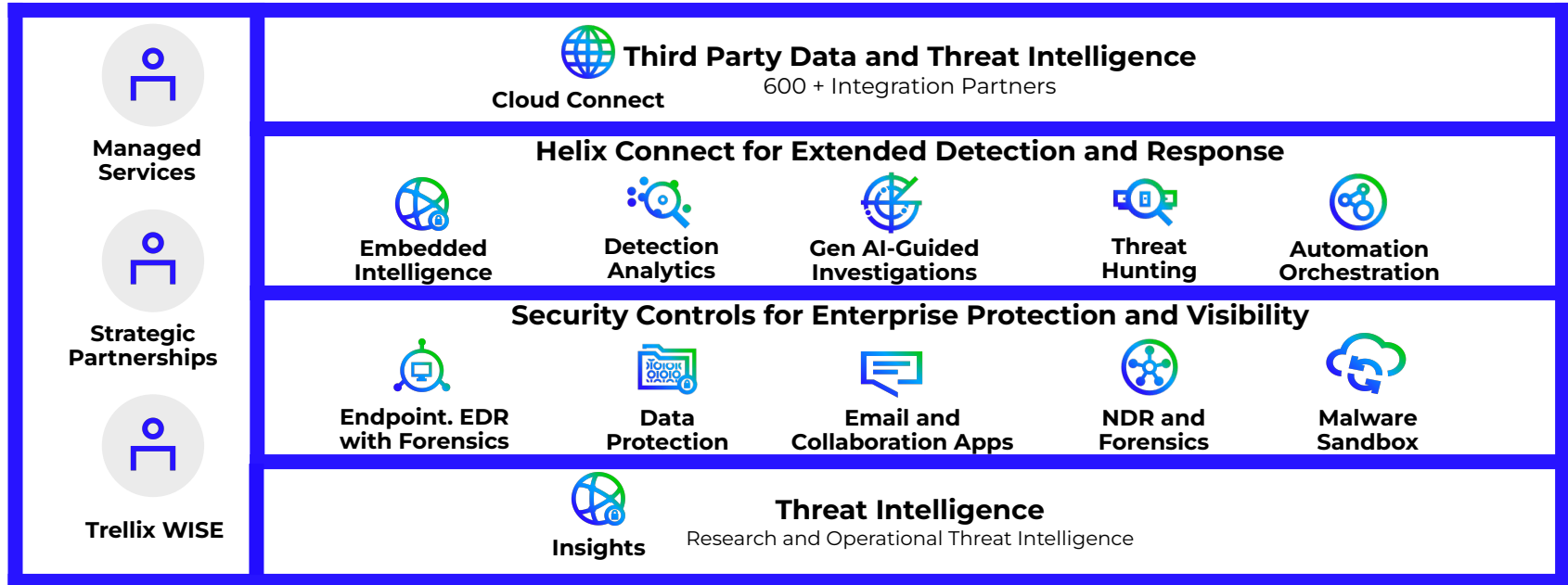
Trellix

Linea de productos

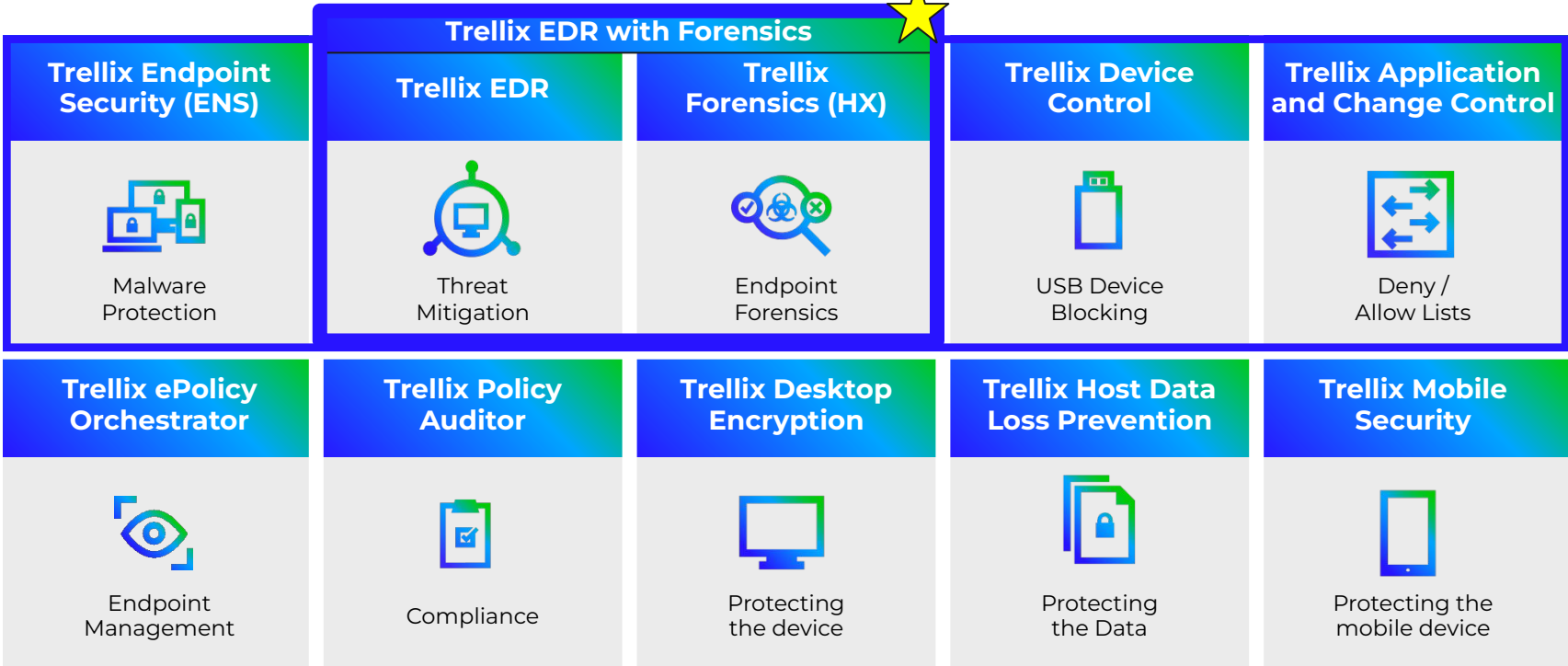
Endpoint Security



Plataforma de XDR



Trellix endpoint



Trellix Endpoint Security Products

Trellix Endpoint Security (ENS)



Malware Protection

Trellix Forensics (HX)



Endpoint Forensics

Trellix Application and Change Control (TACC)



Deny/Allow Lists

Trellix Host Data Loss Prevention (DLP)



Protecting the Data

Trellix Desktop Encryption (DE)



Protecting the device

Trellix Endpoint Detection & Response (EDR)



Threat Mitigation

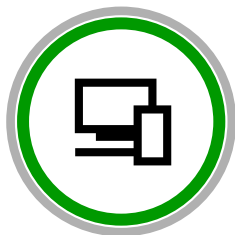
Trellix Mobile Security (TMS)



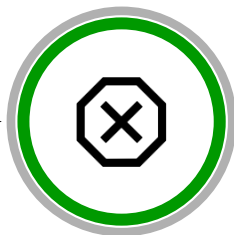
Protecting the mobile device

Fundamentos de endpoint suite

ANTES
ATTACK

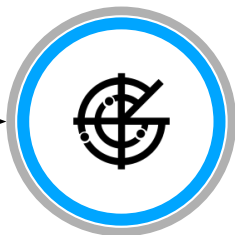


Manage

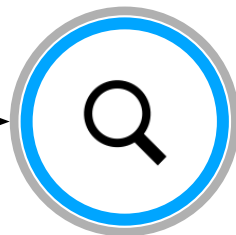


Protect

DURANTE
ATTACK

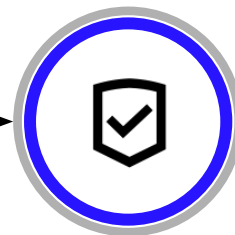


Detect



Investigate

DESPUES
ATTACK



Respond

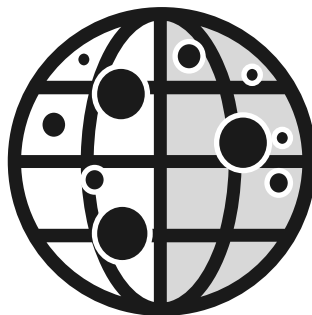
Visibility & Control over the full life cycle of all your Endpoints

ANTES The Attack

Machine Learning and Advanced Remediation

ML Protect

Block zero-day malware before it executes with static analysis machine learning and dynamic behavioral cloud based machine learning



ML Protect Static (Pre-Execution)

Detect malware based on pre-execution static binary analysis using machine learning and comparison to known malware attributes

ML Protect Dynamic (Post-Execution)

Detect dynamic behavior of Greyware on the endpoint, compare to known malware behaviors for a match via behavioral cloud-based machine learning

Pre-and Post Execution is critical to maximize your detection capabilities.

ANTES The Attack

Optimize Endpoint Security Posture – Exploit Protection

The screenshot displays the configuration interface for Exploit Protection. On the left, the 'Filter' section includes checkboxes for 'Type' (Files, Services (Windows only), Registry (Windows only), Processes) and 'Severity' (High, Medium, Low, Others). A 'Quick find' search bar is also present. The main table lists several rules, including T1562 - Evasion Attempt: Suspicious AMSI DLL Loading Detection (ID 6134) and T1055 - Fileless Threat: Reflective DLL Remote Injection (ID 6115). On the right, the 'Exclusion' configuration panel is shown, with 'File - Process - Registry' selected in the 'Exclusion Type' dropdown. A green callout box highlights the exclusion criteria: User /Group ID, File/Hash, Process /Signer, and Signatures !!.

Filter

Type:

- Files
- Services (Windows only)
- Registry (Windows only)
- Processes

Severity:

- High
- Medium
- Low
- Others

Quick find: Show selected rows

<input type="checkbox"/>	ID	Name
<input type="checkbox"/>	6134	T1562 - Evasion Attempt: Suspicious AMSI DLL Loading Detection
<input type="checkbox"/>	6133	T1562 - Evasion Attempt: Suspicious AMSI DLL Creation Detection
<input type="checkbox"/>	6115	T1055 - Fileless Threat: Reflective DLL Remote Injection

Exclusion

Exclusion Type:

Name:

Process:

File name or path (can include * or ? wildcards):

MDS hash:

Signer:

- Enable digital signature
- Allow any signature
- Signed by:

User SID:

Group SID:

Hostname:

File name or path (can include * or ? wildcards):

Signatures ID (comma-separated):

Exclude:

- User /Group ID
- File/Hash
- Process /Signer
- Signatures !!

Tuning Exploit Protection Policy:

- Includes Many Rules covering MITRE
- Enable with “Report” first
- Granular Exclusions possible

ANTES The Attack

Optimize Endpoint Security Posture – Expert Rules

The screenshot displays the GitHub repository for Trellix Expert Rules. The main view shows a directory listing for the 'TRELLIX' folder on the 'main' branch. The directory contains several subfolders: ACCESS_PROTECTION, DEFENSE_EVASION, GENERIC_RULES, MALWARE_BEHAVIOR, PAYLOAD_EXECUTION, and PRIVILEGE_ESCALATION. A pull request by pradeep-bhandary is visible. A table of rule files is shown on the right, with a green callout box highlighting the 'Extensible Detection and Protection' features.

File Name	Description
T1175 - COM - WMI using PowerShell WMIC MSHTA VB...	Renamed McAfee to Trellix
T1175 - COM - Word.Application using MSHTA ...IScript	Renamed McAfee to Trellix
T1175 - COM - Word.A...	
T1204_Payload_execut...	
T1222_Windows_File_a...	
T1486_Attempt_to_End...	
T1503 - Credentials fro...	
T1547.001_Registry_Ru...	
T1547.004_Winlogon_f...	
T1547.005_Security_Su...	
T1548.002_UAC_Bypass...	
T1552_Credential_in_Reg...	
T1561_MBR_protection_through_DISK_REGION_matchin...	Renamed McAfee to Trellix
T1561_MBR_protection_through_LBA_matching_criteria...	Renamed McAfee to Trellix
T1569_Service_execution_using_PSEXEC.md	Renamed McAfee to Trellix
T1570_Lateral_Tool_Transfer-File_Modification_From_A_R...	Renamed McAfee to Trellix
T1570_Lateral_tool_transfer-Host_to_Remote.md	New COM Hijacking using Powershell and update to Rule T1570

Extensible Detection and Protection:

- Expert Rules
- MITRE Mapping
- Sources:
 - Insights Recommendations
 - KBs
 - GitHub

ANTES The Attack

Optimize Endpoint Security Posture – Expert Rules

Protection against entry vector Threats (KB91836)

Below are the countermeasures. Click to advance to the section that you want to view:

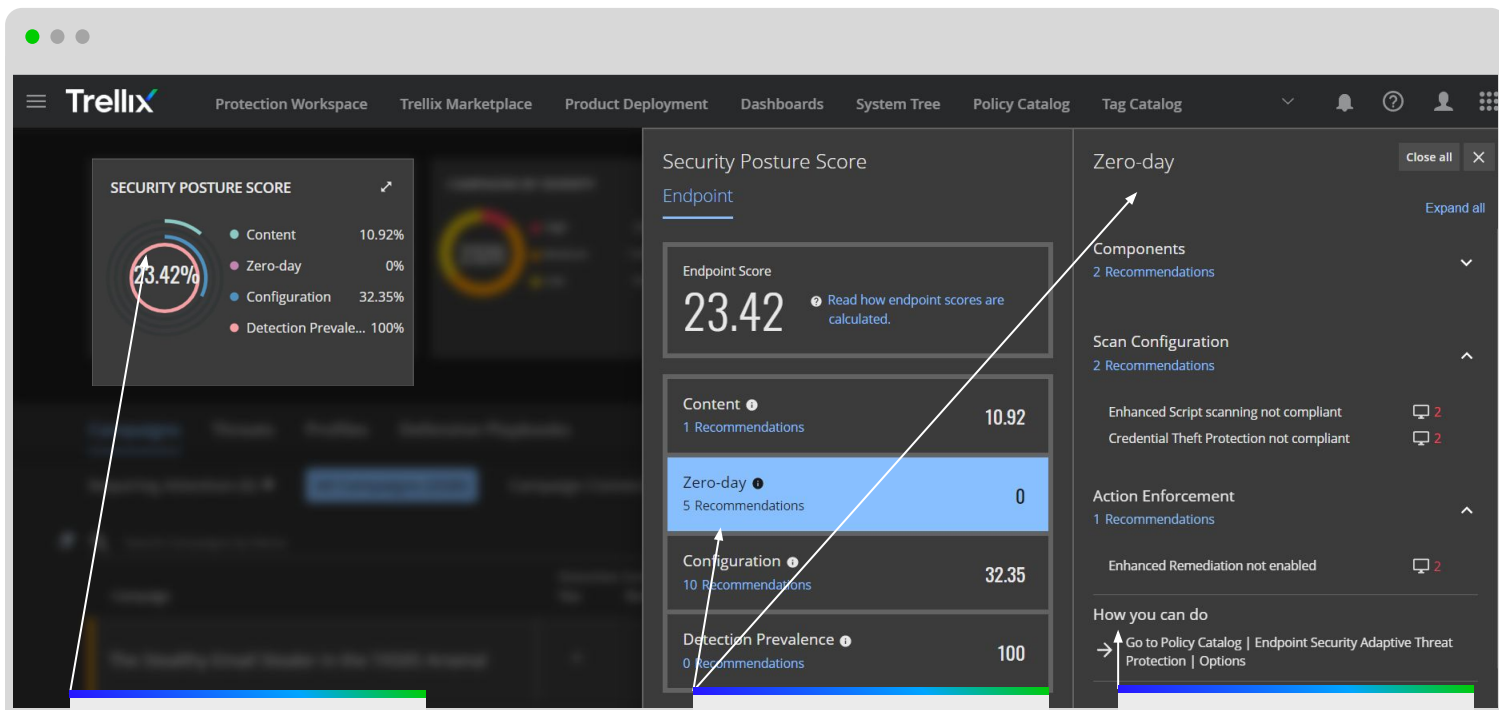
- ENS Adaptive Threat Protection (ATP)
- ENS Dynamic Application Containment (DAC)
- ENS Threat Prevention Antimalware Scan Interface (AMSI)
- ENS Exploit Prevention
- ENS Exploit Prevention Expert Rules
- ENS Access Protection default rules
- ENS Access Protection custom rules
- ENS Firewall Rules
- VSE Access Protection default rules
- VSE Access Protection custom rules
- Host IPS signatures
- MSME antispam and on-access scan policies
- More user recommendations

The screenshot displays the Trellix endpoint security console interface. The top navigation bar includes 'Campaigns', 'Threats', 'Profiles', 'CVEs', 'MITRE Explorer', and 'View more'. The main content area is titled 'Campaigns > CVE-2021-40444 - Microsoft MSHTML Remote Code Execution Vulnerability'. Below this, there are tabs for 'Overview', 'Your Environment', 'Indicators of Compromise (IOCs)', 'Hunting Rules', and 'Connections'. The 'Hunting Rules' tab is active, showing a list of rules under the 'Trellix Defense Rules' category. The selected rule is expanded, showing its configuration:

```
Rule {
  Process {
    Include OBJECT_NAME { -v "winword.exe" }
    Include DLL_LOADED -name "iframe" { -v 0x1 }
  }
  Target {
    Match SECTION {
      Include OBJECT_NAME { -v "mshtml.dll" }
    }
  }
}
```

MUCHO ANTES The Attack

Optimize Endpoint Security Posture
– Scoring based on attacks



1. Visibility:
Zero-day protection not enabled

2. Recommendations:
five actions to improve
Zero-day protection

3. Action:
jump to Policy Catalog

MUCHO ANTES The Attack

Determine Potential Impact

The screenshot displays the Trellix interface for configuring a hunting rule. The breadcrumb path is 'Campaigns > CVE-2021-40444 - Microsoft MSHTML Remote Code Execution Vulnerability'. The 'Hunting Rules' tab is active, and the 'Trellix Defense Rules' sub-tab is selected. A search filter 'mshtml' is applied. The rule being configured is 'Rule - EDR Real-Time Search', described as 'McAfee defense to detect malicious activity. (ENS, VSE, EDR, Endpoint, etc...)'. The rule's logic is defined as: 'HostInfo hostname and LoadedModules where LoadedModules process_name contains "winword" and LoadedModules module_name contains "mshtml"'. A sidebar on the left shows search filters and categories, with 'EDR Real-Time Search' selected.

- Proactive Search
- Realtime queries from Insights to EDR
- Identify devices on risk

ANTES The Attack

Optimize Endpoint Security Posture – Expert Rules

Proactive Attack Surface Reduction



Insights Threat
Intelligence &
Security Posture



Web Control



Host Firewall

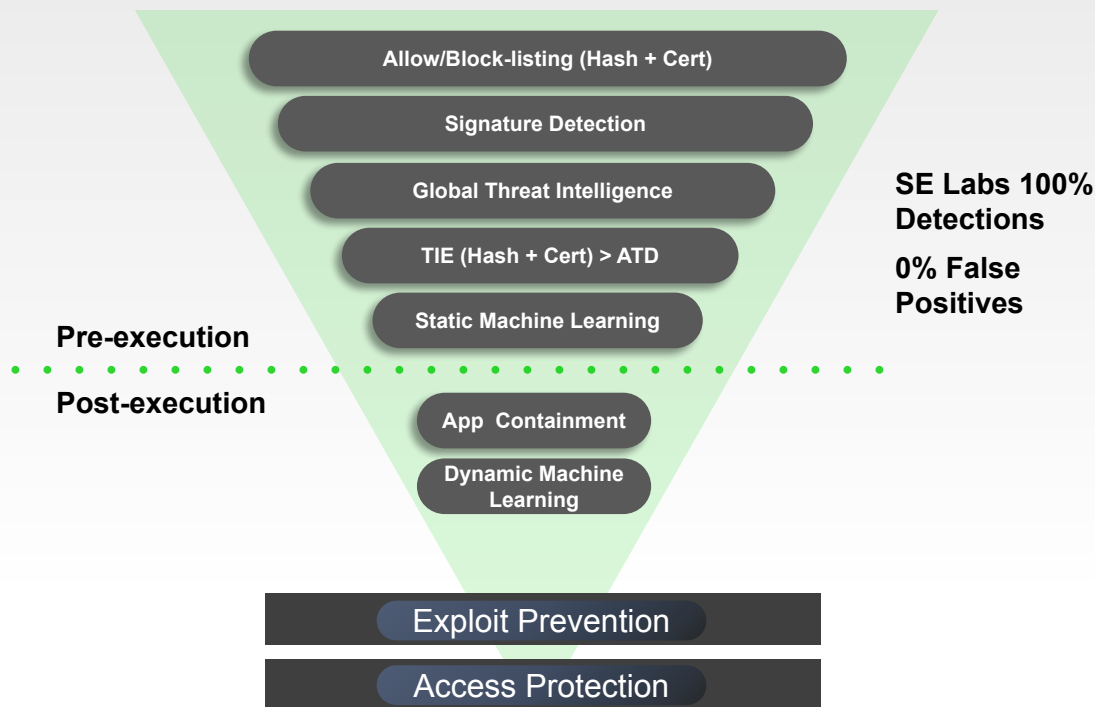


Device
Control



Application
Control

Threat Prevention



DURANTE The Attack

Endpoint Detection & Response – Detect hidden threats

Trellix | EDR

Monitoring: 2 Total Threats, 2 High, 0 Medium, 0 Low

Threats by Ranking: Filter by keyword, View: All

Threat Details: Device: MUC-SRV-CSI, Apr 26, 2023 1:56:21 PM, 1 affected devices

Threat Behavior: Proc Filesystem T1003.007 (Credential Access)

Process Activity: Sequential View, Filter events by severity, Showing 9 of 74 events

Process Activity Graph: psexecsv.exe → meatgrindr_firmw... → powershell.exe → whoami.exe

EDR

- Highly Aggregated and Prioritized Threats
- Combining EDR Detection and ENS Threats
- MITRE Mapping

Immediate Actions

- Quarantine
- Kill Process
- Delete File

DURANTE The Attack

Optimize Alert Triage - AI-guided Investigations

1.
2,000 artifacts analyzed,
narrowed down to 252 key
and 8 findings

Suspicious Winword Behavior
Last updated: 19 days ago

Investigating

Search

All Investigations

This Investigation

All Investigations

2 minutes ago

Key Findings 8

Key Artifacts 252

Artifacts 20k

Finding Details

Processes running from suspicious directories

Artifacts

- MV-Win10-2
- C:\Users\Base\AppData\Local\Microsoft\O...
- C:\Users\Base\AppData\Local\SquirrelTem...
- C:\Users\Base\AppData\Local\Temp\CEB6...
- C:\Users\Base\AppData\Local\Microsoft\Te...
- C:\Users\Base\AppData\Local\Microsoft\Te...
- C:\Users\Base\AppData\Local\Adobe\C9D...
- C:\Users\Base\AppData\Local\Temp\E6367...
- C:\Windows\SysWOW64\explorer.exe
- FileCoAuth.exe

Artifact type

- Device (external)
- Other (external)
- Device (internal)
- Other (internal)

Show Answered questions

Is there any process opening a socket that do not commonly do it?

Sockets being opened by processes which do not commonly do it

Does the endpoint contain processes running from suspicious directories?

Processes running from suspicious directories

Does the endpoint contain evidence of malicious auto-start entries?

Files referenced in auto-start entries with suspicious indicators

Does the endpoint contain evidence of

2.
Trellix automatically
provides answers to the
SOC analysts

3.
Graphical view of step 2 results to
guide the analyst to get further
details

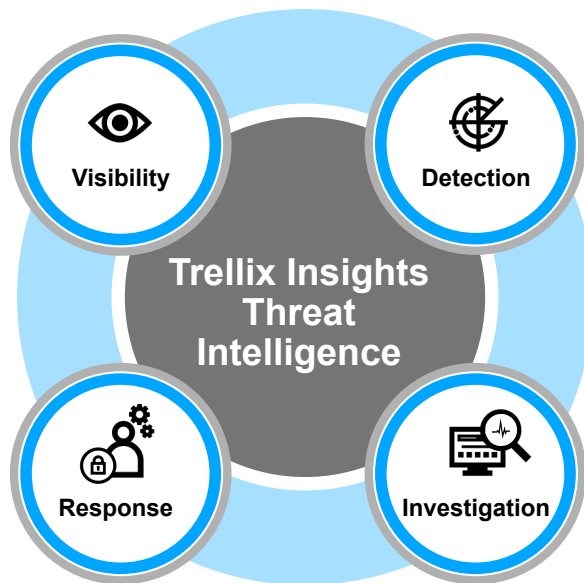
DURANTE The Attack

Effective endpoint alert
triage and prioritization

Simpler investigation
workflows

- Broad Visibility
- Flexible Retention
- Always-on data collection

- Data Visualization & Search
- Robust Response



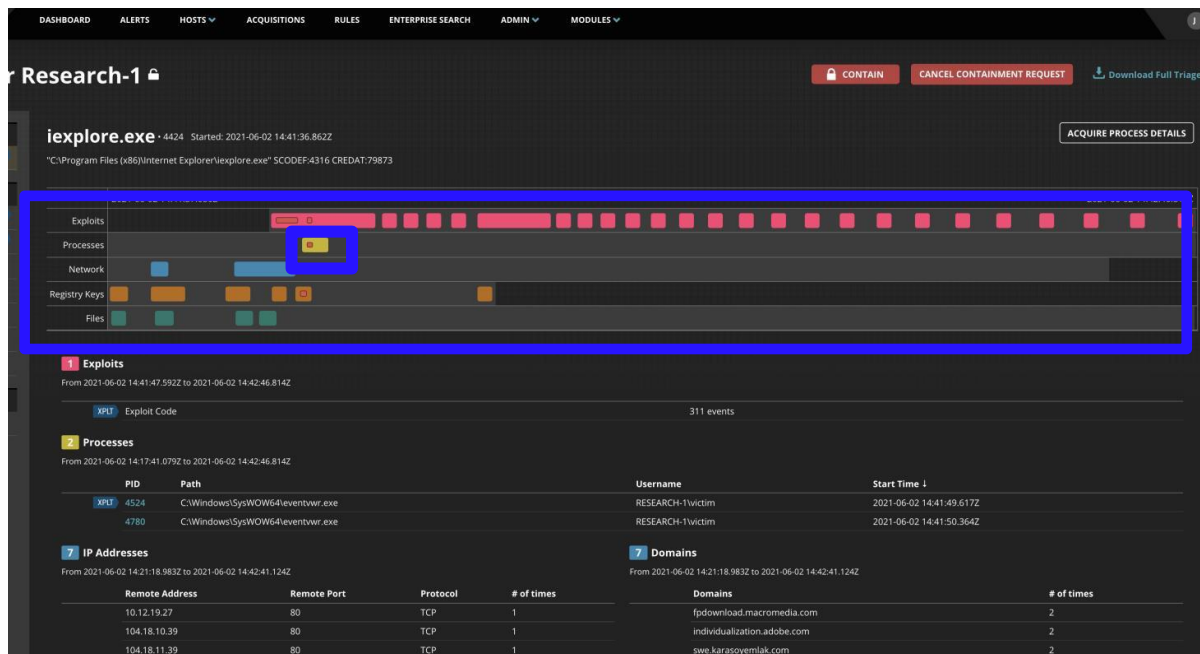
- File and Fileless threats
- MITRE framework driven detection and mapping

- Force-multiply expertise with AI
- Automatic Alert Triage

DESPUES The Attack

Alert Timeline and Triage Viewer

- Show timeline of alerts
- Simplifies investigation
- Filters results based on selection
- Red Dot shows indicator trigger
- Full triage download for deeper analysis



The screenshot displays the Trellix Alert Timeline and Triage Viewer interface. The top navigation bar includes: DASHBOARD, ALERTS, HOSTS, ACQUISITIONS, RULES, ENTERPRISE SEARCH, ADMIN, and MODULES. The main header shows 'Research-1' with buttons for 'CONTAIN', 'CANCEL CONTAINMENT REQUEST', and 'Download Full Triage'. Below this, the process details for 'iexplore.exe' are shown, including its path and SCODEF. The central part of the interface is a timeline view with a red dot indicating a trigger. Below the timeline, there are sections for 'Exploits', 'Processes', 'IP Addresses', and 'Domains'.

Exploits
From 2021-06-02 14:41:47.592Z to 2021-06-02 14:42:46.814Z

XPLT	Exploit Code	# of events
		311 events

Processes
From 2021-06-02 14:17:41.079Z to 2021-06-02 14:42:46.814Z

PID	Path	Username	Start Time ↓
XPLT 4524	C:\Windows\SysWOW64\eventvwr.exe	RESEARCH-1\victim	2021-06-02 14:41:49.617Z
4780	C:\Windows\SysWOW64\eventvwr.exe	RESEARCH-1\victim	2021-06-02 14:41:50.364Z

IP Addresses
From 2021-06-02 14:21:18.983Z to 2021-06-02 14:42:41.124Z

Remote Address	Remote Port	Protocol	# of times
10.12.19.27	80	TCP	1
104.18.10.39	80	TCP	1
104.18.11.39	80	TCP	1

Domains
From 2021-06-02 14:21:18.983Z to 2021-06-02 14:42:41.124Z

Domains	# of times
fpdownload.macromedia.com	2
individualization.adobe.com	2
swe.karasoyemlak.com	2

DESPUES The Attack

Data Acquisitions

Actions

Actions

- Run a Malware Scan
- Restart Agent
- Cancel containment request
- Contain

Acquire

- Single File
- Triage
- Multiple Files
- Standard Investigative Details
- Comprehensive Investigative Details
- Quick File Listing
- Command Shell History
- Process Memory
- Driver Memory
- Full Memory
- Raw Disk
- PowerShell History (From Event Logs)
- test101

928 Acquisitions

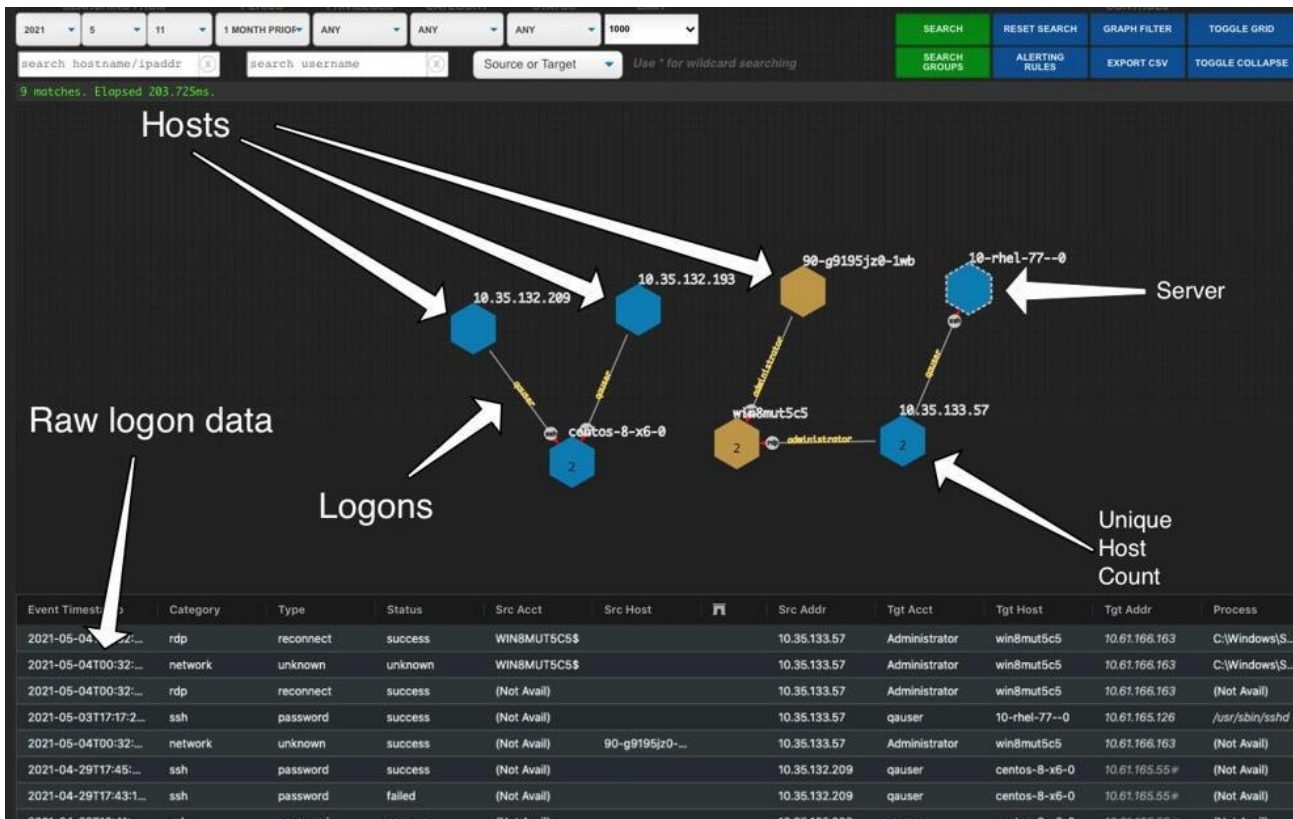
FILTER BY: Acquisition type: All Status: All Requested by: Not Enricher Platform: All

0 acquisitions selected 301 - 350 of 928

		Hostname	IP Address	Requested	Acquisition	Download Size	Status
<input type="checkbox"/>	Windows	VICTIM-7FHS0H5	10.12.10.136	14 days ago	Triage (automatic)	6.2MB	Acquired
<input type="checkbox"/>	Windows	victim-win10-AQ	10.12.10.174	14 days ago	Triage (automatic)	6.3MB	Acquired
<input type="checkbox"/>	Windows	victim-win10-AQ	10.12.10.174	14 days ago	Data: Quick File Listing	28.4MB	Acquired
<input type="checkbox"/>	Windows	victim-win10-AQ	10.12.10.174	14 days ago	Data: Command Shell History	1.4MB	Acquired
<input type="checkbox"/>	Windows	victim-win10-AQ	10.12.10.174	14 days ago	Data: PowerShell History (From Event Logs)	691.6KB	Acquired
<input type="checkbox"/>	Windows	victim-win10-AQ	10.12.10.174	14 days ago	Data: Raw Disk	26.3GB	Acquired
<input type="checkbox"/>	Windows	victim-win10-AQ	10.12.10.174	14 days ago	Data: Full Memory	2.4GB	Acquired
<input type="checkbox"/>	Windows	VICTIM-7FHS0H5	10.12.10.129	14 days ago	Triage (automatic)	15.4MB	Acquired

DESPUES The Attack

Logon Tracker - Lateral Movement Detection



- Analysis typically starts with a clue (an account or a host)
- Essential to gather **historical logon data**
- Account, host, and logon metadata speeds up analysis

DESPUES The Attack

Host Remediation – Remote Shell

Endpoint Security interface showing a Remediation Session for host WIN73a913c4cace. The terminal output shows a successful 'whoami' command returning 'nt authority\system'. The host information panel displays IP Address 10.61.153.181, Operating System Windows 10 Enterprise, and Agent Version 32.30.0. The interface includes a 'Use Custom Script' section with a file upload area and buttons for 'DOWNLOAD AUDIT TRACE' and 'END SESSION'.

- Remote Console
- Audited
- Kill processes
- Remove Files
- Scriptable

DESPUES The Attack

Windows Event Log Forwarding

Event Streamer

The Event Streamer module provides the ability to send Windows Event log data directly to Helix or a Syslog server.

Enable Event Streamer on the host

ON

Destinations

Stream to FireEye Helix

Enable this setting to forward Windows event logs to your FireEye Helix instance.

ON

No syslog destination has been added yet

Start by adding a syslog destination for forwarding Windows event logs.

ADD SYSLOG DESTINATION

Add Syslog Destination

Add the syslog destination you want to connect and send your Windows event logs to.

Name

Name

IP Address

IP Address

Port

Port

Enable TLS

Security ⓘ

ON

System ⓘ

ON

Terminal Services ⓘ

ON

Task Scheduler ⓘ

ON

Powershell ⓘ

ON

Windows Defender ⓘ

ON

Application Experience ⓘ

ON

Application ⓘ

ON

AppLocker ⓘ

ON

Printer Service ⓘ

ON

An Endpoint Security

Powerhouse

Optimize all your Endpoints Protection

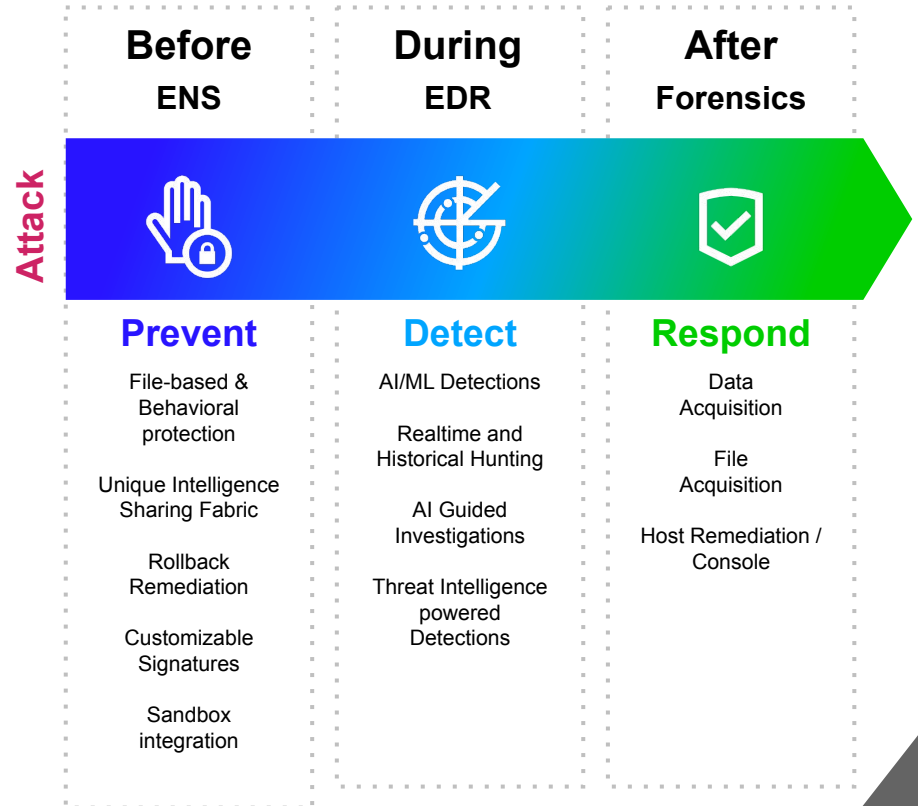
- Manage at Enterprise Scale, on-prem & cloud
- Desktop, Servers & Fixed functions devices
- Proactively Protect against sophisticated threats

Simplify & Improve Triage, Investigation & Response

- High Fidelity Endpoint Alerts and Telemetry
- AI Guided Investigations

Minimize Impact

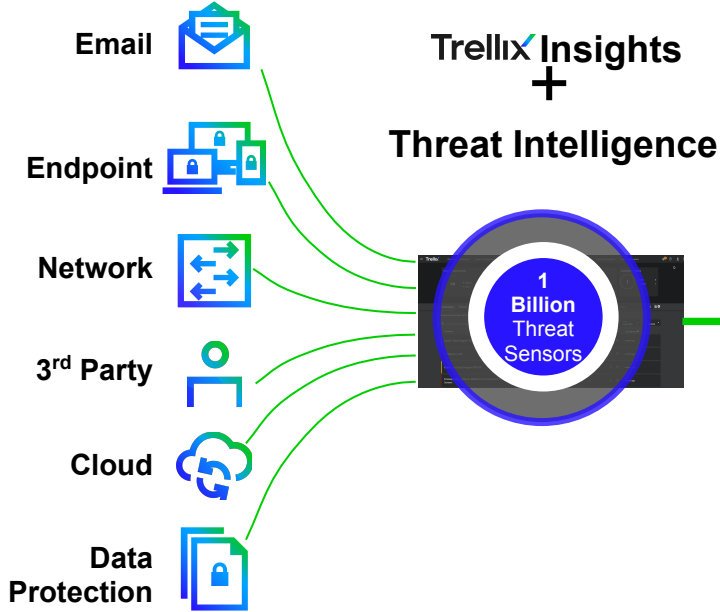
- Real-Time Blocking and Containment at Scale
- Endpoint Forensic & Root Cause Analysis



Security Tools

Trellix XDR Platform

Automated Responses and Playbooks



Trellix | Investigation | Initial Access, Execution, Exfiltration and Co... (ID: #124)

CRITICAL 98 / 124

Initial Access, Execution, Exfiltration and Command & Control

Detected by Trellix Email, Endpoint, Network, DLP and a Third-Party Identity Vendor.

RISK SCORE

MITRE ATT&K Techniques™ 4 / 188

Recommended Actions

- TRELLIX DETECTION ON DEMAND: Enrich Indicators
- TRELLIX ENDPOINT SECURITY: Contain Host
- THIRD-PARTY NETWORK SECURITY: Sinkhole FQDN DNS Re...
- THIRD-PARTY NETWORK SECURITY: Drop Network Commun...
- TRELLIX INCIDENTS: Review Defensive Playb...

Incident Assignee: ... | Status: Open

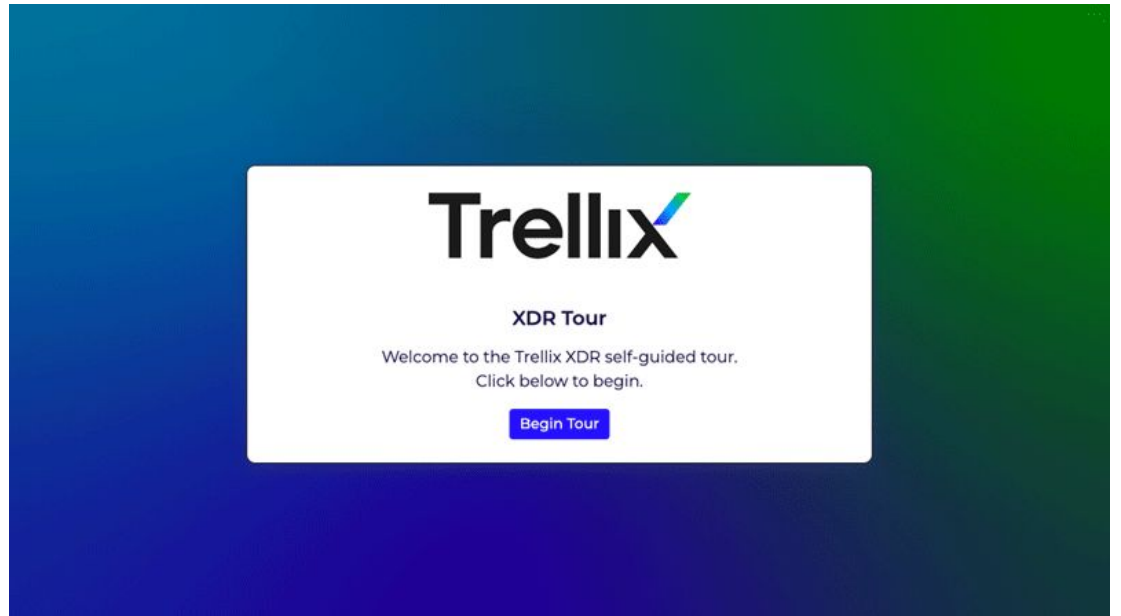
The screenshot shows a detailed investigation view in the Trellix XDR platform. It features a central network diagram with nodes for "THIRD-PARTY IDENTITY ALERT", "VALID ACCOUNTS", "REMOVED MAILBOXES", "TRELLIX EMAIL SECURITY ALERT", "AFFECTED ACCOUNT", "Multiple Gmail Accounts (3)", "Phishing Alerts (4)", "ryan@gmail.com", "http://paandorasong.com/04631ogrn", and "Initial Access".

- Sandbox Enrichment
- Disabling AD Account
- Quarantine Endpoint Host
- Quarantine Cloud Instance
- ServiceNow Ticket

Trellix XDR Tour

trellix.com/tours/xdr-tour/

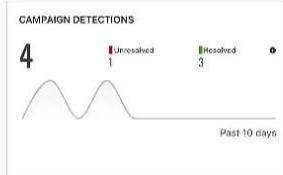
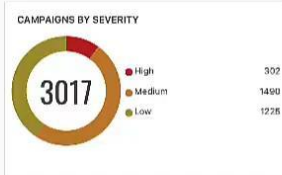
To get started with the Trellix XDR tour, **please fill out this form and click Submit.** When you're done, you can request a demo directly from the tour to learn more.





DEMO #1

Complex Attack Surface



Campaigns Threats Profiles CVEs MITRE Explorer View more

Search Insights 🔍 ⚙️

Requiring Attention (1085) All Campaigns (3017) Campaign Connections

Search Campaigns by Name

Sector: Telecom | Country: United States | Sort by: Last Detected

Campaign	Detection Comparison				Your Devices Exposed Endpoints	Insufficient Coverage	Defensive Play...	Last Detected
	You	Telecom	USA	Worldwide				
Threat Profile: DarkPower Ransomware	●	●	●	●	0	0	🔄 🛡️	6 days ago
Operation Iron Ore	●	●	●	●	1	1	🔄 🛡️	6 days ago
The Stealthy Email Stealer in the TA505 Arsenal	●	●	●	●	0	1	🔄 🛡️	Never
BlueNoroff APT Group Targets macOS With RustBucket Malware	●	●	●	●	0	0	🔄 🛡️	Never
Bitxor20 Backdoor Spreading Via Log4j Vulnerability	●	●	●	●	0	1	🔄 🛡️	Never

Showing 1-5 out of 3017 rows | 1 2 3 4 5 ... 004 | Show 5 rows



DEMO #2

Ransomware Attacks Cause Damage

Recycle Bin se_email

Acrobat Reader ImportantD...

Cyginwin64 Terminal prep

Firefox 22997_cubepu ppvjpg

Google Chrome exfil

WinSCP

Wireshark

EPO_Login

ePO_Updater

sample

ImportantDocuments

File Home Share View

ImportantDocuments

Search ImportantDocuments

Quick access

- Desktop
- Documents
- Downloads
- Pictures
- Music
- Videos
- OneDrive
- This PC
- Removable Disk (F:)
- Network

_0025_p822_famil y_1117_003_E	3a6c5b7c17ee874 10bf6eb59aba0e cc	11_202101282056 40_10739526_larg e	13insider-family- interrupted-1-wid eoSixteenByNine Jumbo1600	016c3f75588de3e 8773dd175db8f50 93	0021-C_MiniSho ot	136b8ede-e65c-4 0bf-a9ee-dabf7e 08bce1-AP_20351 380871747	514cee75991605e cf499bf6328a272 0b	
679A8823-683x10 24	1080x1080-action -block-3_1	2020-08-26_0002	60105f2eb743a6 f41869ea1_kauai- family-photogra phy	1623226539.famil y-studio-portrait	808499162018304 1	Amanda-Lennon 4	Beachum-36-683 x1024	
Belhaven-Farm- Harrisonburg-Fa mily-Photograph y-Be-Thou-My...	best-los-angeles- family-photogra phers-1080x600	best-nyc-family- photographers	boise-family-pho tographer-4790a	chapelhillfamily photography_cha pelhillfamilyphot ographer_ncbo...	Choosing-Outfits -for-Family-Pictu res	CL_OUTDOOR_FAL L_FAMILY_PHOTO SESSION_CT	Cincinnati-ohio-f amily-portrait-ph otographer-1-78 1x1024	

77 items

Activate Windows
Go to Settings to activate Windows.

Trellix

Partner and SE Tools

Endpoint Security



Types of Partners



Trellix Xtend

Partner Levels	Sales Certifications	Architect Certifications
Collaborate	4	4
Momentum	2	2
Growth	1	1
Distribution	4	4
MSSP	4	4

Partner Success Engines



**Profitability
Programs**



**Demand
Generation &
Marketing Support**



**Trellix
University**



**Dedicated
Technical & Sales
Resources**

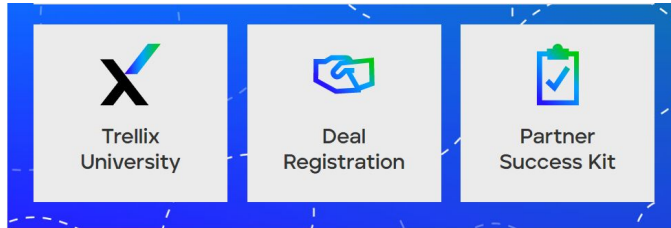


The Hive

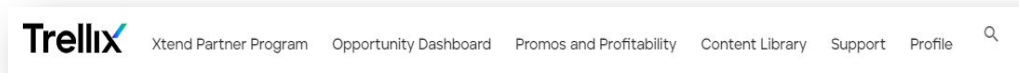


**Tools &
Resources
Partner Care**









Call to Action Buttons



Updated Navigation



Trellix Quick Links

-  Onboarding
-  Salesforce
-  Marketing
-  Events
-  Customer Assets & Entitlements
-  Customer Service Request
-  Support ServicePortal
-  Technical Resources

Trellix Partner Portal

<https://partners.trellix.com>

Xtend Partner Program

Overview

Program Guide

Newsletter

Opportunity Dashboard

Registration

Management

Promos and Profitability

Deal Registration

Renewals

Global Sales Plays

Rebates Guideline and Portal

MDF

Content Library

Trellix Platform

Sales Resources

Resource Library

Sales Tools

Competitive Battle Cards

Corporate Strategy

Product Solution Guides

Sales Plays

Trellix Market Place

3rd Party Research

Ordering

Quote and Ordering Policies

End User Purchase Policy

Price Books

NFR Ordering

Quoting Product Requirements

Technical Documentation Portals

Cloud Lab Access

Expert Center

Technical Support & Services

Customer Success Plans

Consulting Services

Trellix Partner Portal – Sales Kits

<https://partners.trellix.com/partner/en-us/solution-provider/product-sales-kits.html>

Product Sales Kits will be updated frequently

Partner Portal – Solution Provider

Trellix.com



[Xtend Partner Program](#) [Opportunity Dashboard](#) [Promos and Profitability](#) [Content Library](#) [Support](#) [Profile](#)



Partner Portal – Solution Provider

Trellix.com



[Xtend Partner Program](#) [Opportunity Dashboard](#) [Promos and Profitability](#) [Content Library](#) [Support](#) [Profile](#)



Trellix Quick Links



[Onboarding](#)



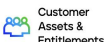
[Salesforce](#)



[Marketing](#)



[Events](#)



[Customer Assets & Entitlements](#)



[Customer Service Request](#)



[Support ServicePortal](#)



[Technical Resources](#)

Price Books

[Service Provider Partners](#)

Getting Started



Sunny days for MDF, Rebate and Levelling come October 9!

The Trellix Hive is a busy place! A new look and feel across MDF, Rebate and Levelling sections, going live Oct 9. Please look out for emails with reminders, trainings and more!

[Trellix University](#) [Deal Registration](#) [Product Sales Kits](#)

Product Sales Kits

How to Sell Email Security

How to Sell

[Sales Play Training – Email Security](#) [↗](#)
[How to Sell Email Security](#) [↓](#)
[Value Discovery Guide – Email Security](#) [↓](#)
[Sales Play Training – Collaboration Security](#) [↗](#)
[How to Sell Collaboration Security](#) [↓](#)
[Value Discovery Guide – IVX for Collaboration Security](#) [↓](#)

Competitive Intelligence

[Trellix Email Security vs Proofpoint](#) [↓](#)
[Trellix Email Security vs Microsoft Battlecard](#) [↓](#)
[Trellix Email Security vs Microsoft Competitive Positioning](#) [↓](#)
[Trellix Email Security vs Proofpoint Competitive Positioning](#) [↓](#)

Pitch Decks

[Customer Overview Deck – Email Security](#) [↓](#)
[Customer Overview Deck – Collaboration Security](#) [↓](#)
[How Email Security Prevents Ransomware \(video\)](#) [↗](#)
[How Trellix Email Security Prevents Ransomware](#) [↓](#)

3rd Party Validation & Product Testing

[SE Labs Report](#) [↓](#)
[How to Use SE Labs Report with Customers \(video\)](#) [↗](#)
[SE Labs Conversation Guide](#) [↓](#)
[SE Labs Fact Sheet](#) [↓](#)
[IDC Vendor Spotlight on Collaboration Security](#) [↓](#)

Data Sheets

[Trellix Email Security – Cloud](#) [↓](#)
[Trellix Email Security – Server](#) [↓](#)
[Trellix Collaboration Security – Executive Brief](#) [↓](#)
[Trellix Intelligent Virtual Execution \(IVX\)](#) [↓](#)

Product training and demos

[Trellix Certified Architect: Email Security](#) [↗](#)
[Trellix Service Provider: Email Security](#) [↗](#)
[SE Demo Kit](#) [→](#)

Ready



Badge



Explore



I DO #
Soulful Work



**All Badges are valid for 1 year or until a new version is released (whichever comes first)
Must meet enablement requirements within 90 days of joining program**

Access through Partner Portal or
<https://training.trellix.com>

Same login and password as the Trellix Partner Portal

Contact PartnerCare@Trellix.com with login issues

Trellix Partner SE Technical Bookmarks



Product Technical Documentation Portal

- Product Documentation:
• <https://docs.trellix.com/>
- Administration Guides
- Deployment Guides
- System Security Guides
- Release Notes
- Hardware Guides
- Reference Guides



Cloud Lab

- CrossFire (ASH):
• <https://login.trellix.com/>
- MDemo:
• <https://trellix-mdemo.skytap-portal.com/>
- Consolidation in progress...



Communication

Partner Care Team

- partnercareemea@trellix.com
- MSP Partner Care Team
• mssppartnercare@trellix.com



Expert Center

Knowledge Base

Forum

- Trellix-F Community:
• <https://community.fireeye.com/>
- Trellix-M Community:
• <https://communitym.trellix.com/>
- Consolidation in progress...

Trellix

Point of Contacts

Endpoint Security



Contact us

Email

partnercareltam@trellix.com



Thank you for your
Participation

The image features the Trellix logo in a bold, white, sans-serif font, centered on a background with a blue-to-green gradient. The background is decorated with two horizontal bands of white dashed lines that curve slightly. The bottom right corner of the image is cut off at a 45-degree angle.

Trellix