

Prevención. - Riesgo

RISK INDEX

How can I lower the risk index?

[View Assessment Profiles](#)



32 Medium



Now
Regional avg: 39

Re

Activity and behaviors High-risk events: 0 Medium risk	Cloud app activity High-risk events: 0 Low risk	System configuration High-risk events: 0 Medium risk	XDR detection At-risk alerts: 3 Medium risk	Threat detection High-risk events: 0 Medium risk	Security configuration High-risk events: 0 Medium risk
---	--	---	--	---	---



Risk factor	Risk event	Most impacted assets	Real-time score impact	Remediation steps
Vulnerabilities	OS Vulnerability Identified	5	3	<ul style="list-style-type: none"> Apply the latest patch or upgrade the operating system version.
Account compromise	Spear Phishing Email Target High Profile User via Attachment	1	2	<ul style="list-style-type: none"> Quarantine or delete the message using the product console. Investigate the event using the Workbench.
XDR detection	Possible Web Service Abuse	1	Less than 1	<ul style="list-style-type: none"> Investigate the event using the Workbench.

Prevención - Identidades

Seguridad de punto a punto: Prevenir, Proteger, resPonder

Identity Security Posture Management (ISPM)



Discover all identities



Assess posture and prioritize risk



Provide in-depth identity profiles



Report on anomalous behavior



Analyze and visualize user activity



Evaluate asset criticality with AI



Identity Threat Detection and Response (ITDR)



Continuously monitor identity-related activities



Investigate threats in on-premises, hybrid, and multi-cloud environments



Correlate events across security layers



Augment staff with Companion AI



Gain instant access to IAM logs



Automate security response

Data Lake | Identity and Access Activity Data

Endpoint



Email



SaaS Apps



Web Traffic



IAM



Network



P

revención - Discovery

Devices

Internet-Facing Assets

Accounts

Applications

Cloud Assets

APIs

All discovered devices


180 +5

Devices can be assessed for risk

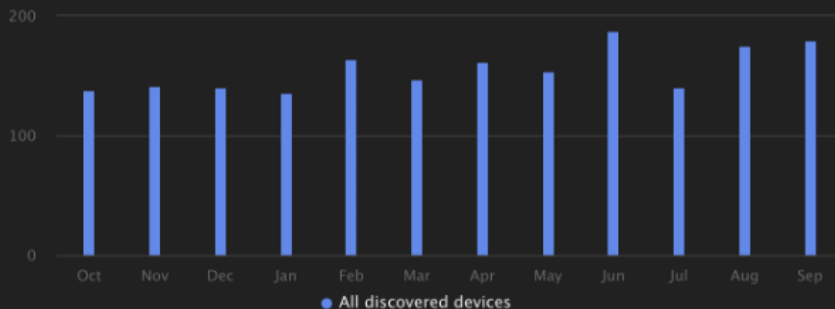
154 +3

Devices with managed agents

132 +3

Use the filter  to modify the device detected period. For unmanaged devices, only devices detected in the last 30 days can be shown.

DEVICE OVERVIEW



CONTRIBUTING DATA SOURCES

Data source	Data upload
Endpoint Sensor	<input checked="" type="checkbox"/>
Network Sensor	<input checked="" type="checkbox"/>
Trend Micro Deep Discovery Inspector	<input type="checkbox"/>
Standard Endpoint Protection	<input checked="" type="checkbox"/>
Trend Micro Apex One as a Service	<input checked="" type="checkbox"/>
Trend Micro Apex One On-premises	<input type="checkbox"/>

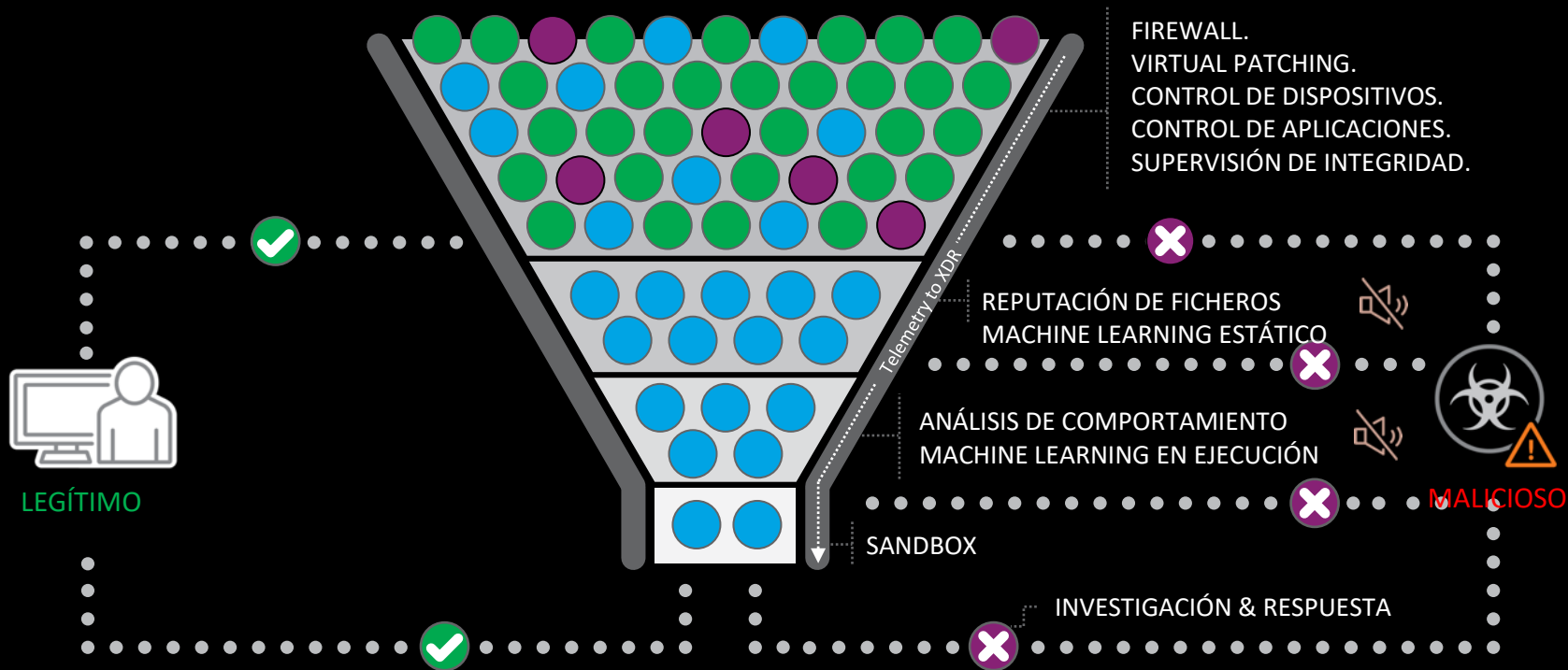
Protección - XDR

LEYENDA

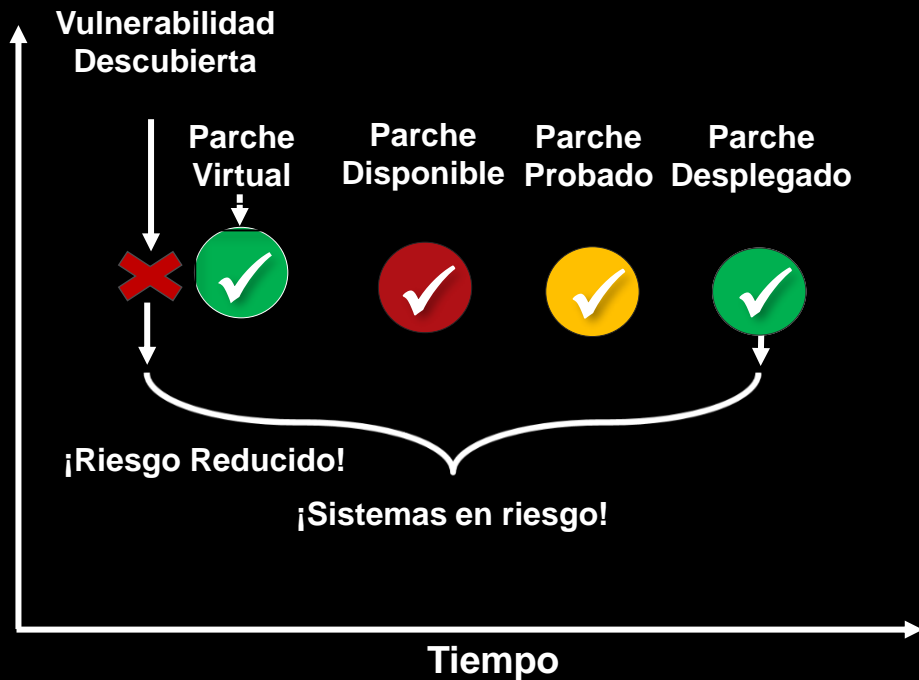
Bueno Conocido

Malo Conocido

Desconocido



Protección.



Parcheado Virtual

Más de 300 aplicaciones protegidas

Sistemas Operativos

BBDD

Servidores Web

Servidores de Correo

Servidores Aplicaciones

Servidores de Backup

Servidores de gestión

Servidores DHCP,FTP, etc

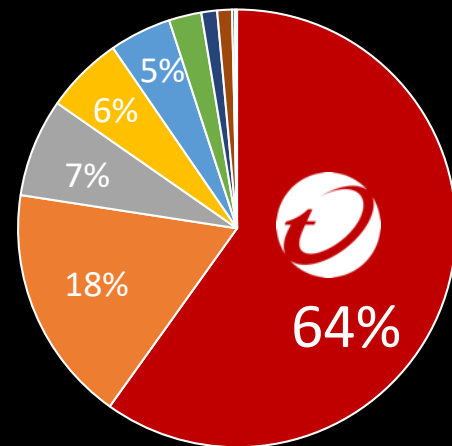
Aplicaciones de escritorio

Clientes de correo

Navegadores Web

Antivirus

Etc...



Protección

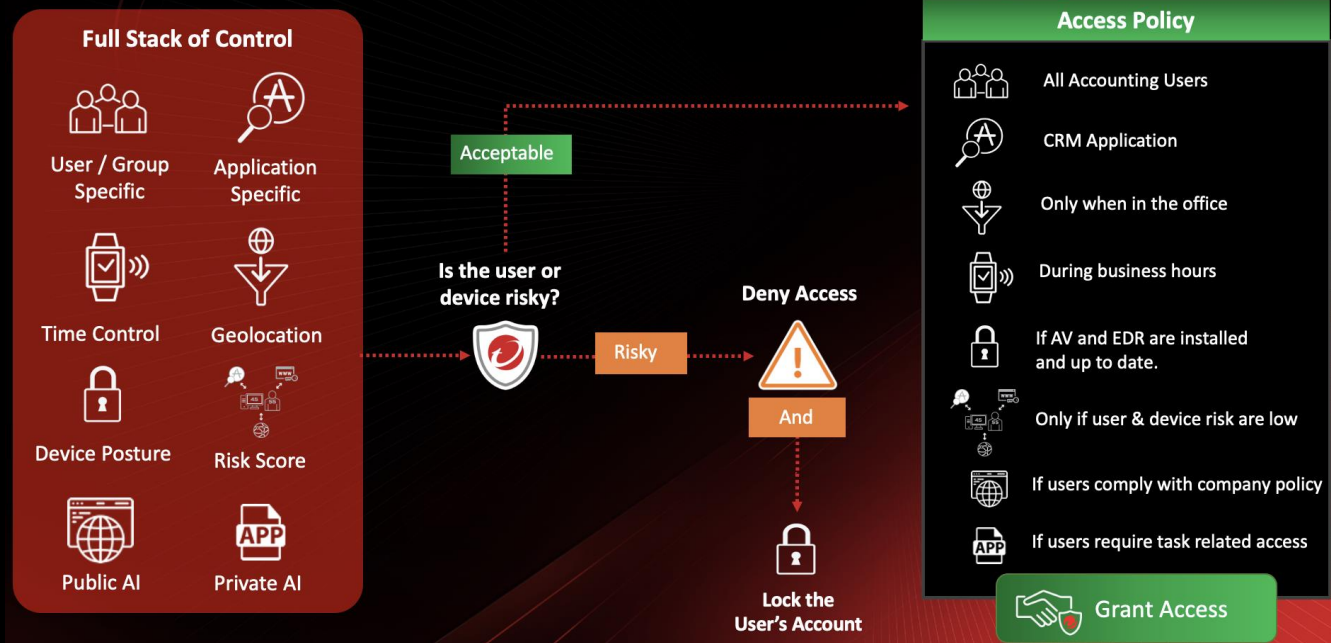
Email & Collaboration Security

- Ransomware.
- Phishing.
- Quishing.
- BEC.
- DLP.
- Inline (API)/Online (MTA).



Prevención.

- Navegación segura.
- Sustituye VPN.
- Acceso condicional.
- DLP.



Prevención.

NDR

Visibilidad de red.

Sondas físicas y virtuales.

Bloqueo de ataques de red.

The screenshot displays the Trend Micro Vision One Workbench interface. On the left, a 'Summary' panel provides details for a 'Possible APT Attack' (Score: 88, Impact scope: 0, Created: 2021-02-04T02:33:39Z) and a 'Possible Spearphishing Link' (Technique: T1192 - Spearphishing Link, Created: 2021-02-03T08:14:13Z). Below these, it lists 'Rarely Accessed and Noteworthy Domain' (Technique: T1071 - Application Layer Protocol, Created: 2021-02-04T02:27:15Z) with associated object and process details.

The main area features a network diagram with nodes representing various entities and their interactions. Nodes include email addresses like 'kaizertech.rogerm', 'remani@kaizertech.com', 'jeff@kaizertech.com', and 'kyrac@kaizertech.com', as well as domains like 'http://ca93-0.winspway.com/' and 'http://ca93-0.winspway.com/'. Other nodes represent processes like 'chrome.exe' and 'cmd /c cd /d 7002.pdf-link', and IP addresses like '44.230.33.128'. The diagram shows a complex web of connections between these entities.

At the bottom, the 'Alert View' section shows a table of alerts:

Score	Workbench ID	Model	Model severity	Impact scope
92	WB-10387-20210810-00000	Apache Struts Vulnerability Exploitation and Command Execution	Critical	3 1
81	WB-10387-20210805-00004	Ransomware Detection (Real-time Scan)	Critical	1
71	WB-10387-20210805-00009	Credential Dumping via Registry	High	2 2 1
70	WB-10387-20210804-00015	Credential Dumping via Registry	High	1 1
70	WB-10387-20210805-00006	Credential Dumping via Registry	High	1 1
70	WB-10387-20210804-00014	Credential Dumping via Registry	High	2 1 1
70	WB-10387-20210804-00013	Credential Dumping via Registry	High	2 1 1
70	WB-10387-20210804-00012	Credential Dumping via Registry	High	2 1 1
70	WB-10387-20210804-00011	Credential Dumping via Registry	High	2 1 1

Protección

Cloud

Attack Surface Risk Management

XDR (Extended Detection and Response)

Data Center On-premise



Bare-Metal Servers & Virtual Machines

- Endpoint & Workload Security
- Container Security
- File Security

Cloud Environment



Instances & Autoscaling

- Endpoint & Workload Security

Cloud-Native Application Development



Containers

- ASRM for Cloud
- Container Security
- File Security



Storage



Third-Party Libraries

- API Visibility
- ASRM for Cloud and File Security



Serverless

Multi-Cloud



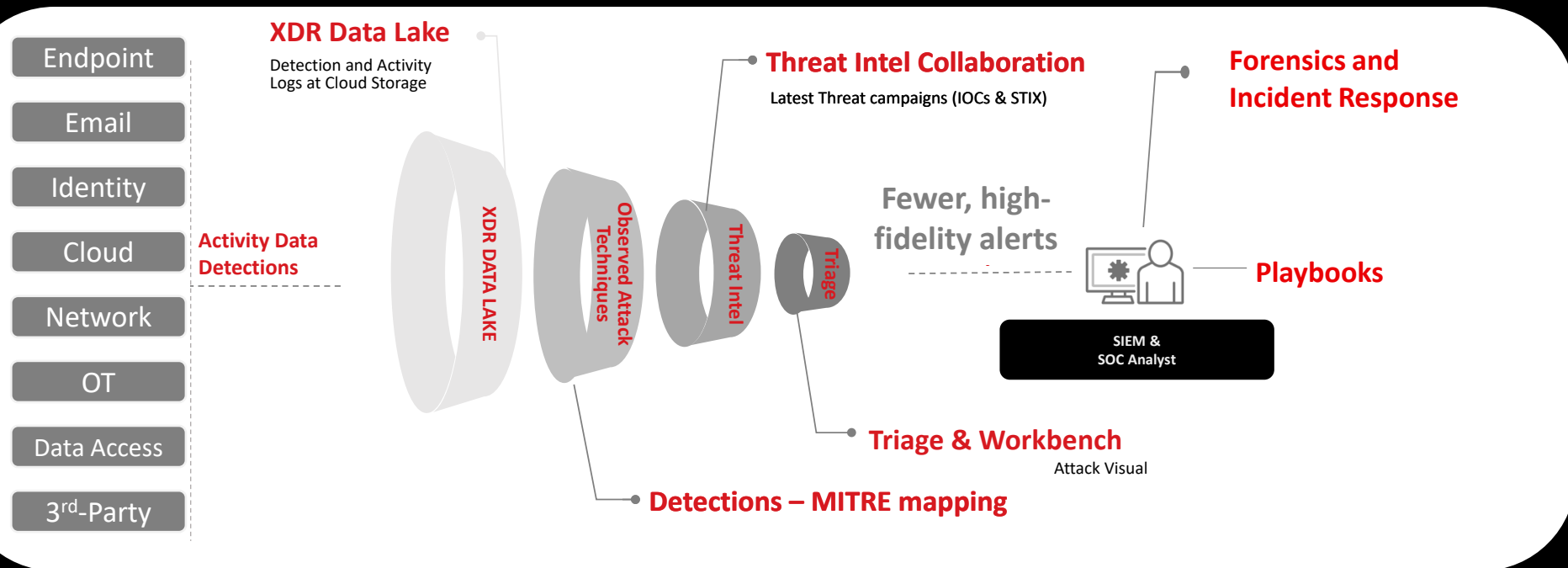
Private Cloud



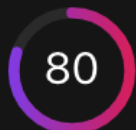
Public Cloud

- AWS
- Azure
- GCP
- Otros...

ResPuesta. XDR



ResPuesta. XDR



Score ⓘ

Adversary is trying to do Exploit Public-Facing Application which leads the Data Encrypted for Impact

They may do this, for example, by retrieving account usernames or by using OS Credential Dumping . The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material . Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell . Adversaries may abuse PowerShell commands and scripts for execution. Key attack techniques: [T1071.001](#), [T1071](#), [T1071.004](#), [T1190](#), [T1059](#), [T1059.001](#), [T1486](#), [T1003.001](#), [T1059.003](#), [T1212](#), [T1003.002](#), [T1003](#), [T1033](#), [T1016](#), [T1566.002](#), [T1192](#), [T1021.002](#), [T1021](#), [T1077](#), [T1086](#), [T1006](#), [T1102](#), [T1550.002](#), [T1550.003](#), [T1482](#)

Status: All

Created: All

Model: All

Workbench ID, Endpoint, User, Email

Apply

<input type="checkbox"/>	Score ↓ ⓘ	Workbench ID	Model	Model severity	Rela
<input type="checkbox"/>	66	WB-10253-20220325-00019	Targeted Attack Detection: Cobalt Strike - C&C Callback Traffic (Domain)	High	Simi
<input type="checkbox"/>	64	WB-10253-20220324-00034	Credential Dumping via Mimikatz	High	Simi
<input type="checkbox"/>	47	WB-10253-20220324-00038	Potential Information Gathering	Medium	Coll
<input type="checkbox"/>	47	WB-10253-20220323-00013	Suspicious Web Access After Suspicious Email	Medium	End

Res Puesta. XDR

Trend Vision One™ Workbench > WB-30353-20231211-00001

2023-12-12 10:19

Summary

Case: Open new case

Owners: None Assign owner

Possible Spear Phishing Attack via Link

A suspicious URL associated with phishing attacks was detected in an email message. [Delayed alert: Batch process detection]

Score: 23

Impact scope: 2

Created: 2023-12-11 15:39:18

Automated responses: None Execute playbook

Highlights

Spearphishing Link Addressed by RetroScan

Technique: T1566.002 - Spearphishing Link

Data source / Email Sensor processor:

2023-12-11 14:35:22 | View event

(msgUuid) AAKALgAAAAAHYQDEapmEc2b...

(msgId) <CANmeUmc=4ALXTW6MnmWYnQ...

(mailMsgSubject) Fwd: Customer Reports 202...

(highlightedRequest) https://drive.google.co...

(suser) juand7716@gmail.com

diego_sicilliani@visionarymomentum.com

juand7716@gmail.com

Fwd: Customer Reports 202...

diego_sicilliani@visionary...

https://drive.google.com/...

Detectar origen

Trend Vision One™ Workbench > WB-30429-20240110-00000

2024-01-10 19:22

Summary

Case: Open new case

Owners: None Assign owner

Demo - Possible Spear Phishing Attack via Link

A suspicious URL associated with phishing attacks was detected in an email message. [Delayed alert: Batch process detection]

Score: 23

Impact scope: 2

Created: 2024-01-10 08:52:04

Automated responses: None Execute playbook

Highlights

(Demo) Spearphishing Link Addressed by RetroScan

Technique: T1566.002 - Spearphishing Link

Data source / Email Sensor processor:

2024-01-10 08:45:34 | View event

(msgUuid) AAKALgAAAAAHYQDEapmEc2b...

(msgId) <500d1fab.69ae.18cf28c39d5.Core...

(mailMsgSubject) try-wb

(highlightedRequest) https://ca21-3.winshipw...

(suser) zqx3040010wgx@126.com

admin@casteam.onmicrosoft.com

Melissa MacBeth View asset graph

Diego Sicilliani View asset graph

David Longmuir View asset graph

Grady Archie View asset graph

Ben Anderson View asset graph

Simon Chen View asset graph

Pradeep Gupta View asset graph

日本のユーザー View asset graph

中文的用户 View asset graph

Trend Micro Cloud App Sec View asset graph

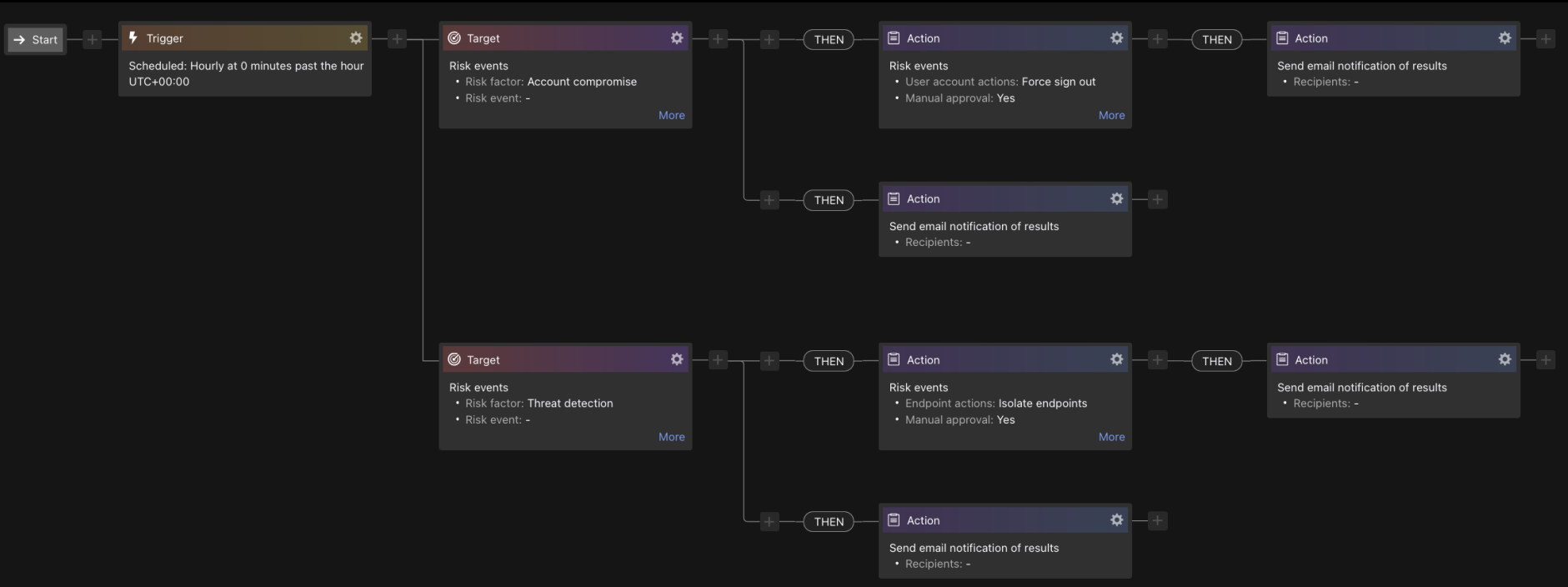
zqx3040010wgx@126.com

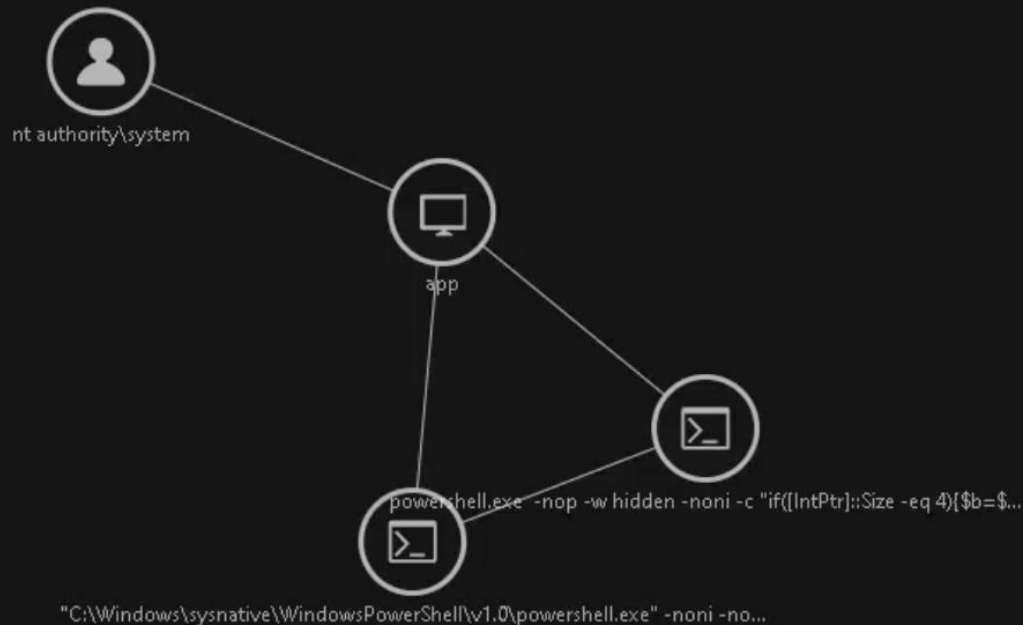
try-wb

https://ca21-3.winshipw...

Analizar Alcance y responder

ResPuesta. SOAR





Generative AI Assistant

Generative AI powered assistant — Companion — amplifies performance and is designed to enhance accessibility, accelerate workflows and threat hunting outcomes, and improve mean-time-to-detect and respond.

Companion

source of the command and the purpose of the actions it performs. It may be necessary to block the command from executing or to remove any files or shortcuts that were created by the command.

d. I have a confidence score of 80 for this explanation. The confidence score is based on the fact that the decoded Base64 string contains a sequence of commands that perform actions that are not typical of a normal PowerShell command. However, without further investigation, it is difficult to determine the exact purpose of the command and the source of the Base64 string.



Explain this alert

What is objectCmd

What is Mimikatz

Type your question here

Expansive Integration Ecosystem

Trend Micro Vision One™ Third-Party Integration

Trend Micro Vision One enables connections to key third-party applications, allowing you to analyze data from multiple sources

CATEGORY	Integration ↑	Vendor
<input type="checkbox"/> BAS (1)	Active Directory (on-premises) <i>Preview</i>	Microsoft
<input type="checkbox"/> Cloud Services (1)	Azure AD	Microsoft
<input type="checkbox"/> Firewall and Network Protection (6)	Check Point Open Platform for Security (OPSEC)	Check Point
<input type="checkbox"/> IT Service Management (1)	Cyborg Security - HUNTER Platform	Cyborg Security
<input type="checkbox"/> Identity and Access Management (4)	Cymulate	Cymulate
<input type="checkbox"/> SIEM (9)	Elastic	Elastic
<input type="checkbox"/> SOAR (3)	FortiGate Next-Generation Firewall	Fortinet
<input type="checkbox"/> Threat Intelligence (3)	Google Workspace <i>Preview</i>	Google
<input type="checkbox"/> Unified Endpoint Management (3)	MISP	MISP Project
<input type="checkbox"/> Vulnerability Management (3)	Microsoft Endpoint Manager (Intune)	Microsoft
	Nessus Pro <i>Preview</i>	Tenable
	NetSkope Cloud Threat Exchange Platform	NetSkope
	Office 365	Microsoft
	Okta	Okta
	OpenLDAP <i>Preview</i>	OpenLDAP
	Palo Alto Panorama	Palo Alto Networks

CATEGORY

- BAS (1)
- Cloud Services (1)
- Firewall and Network Protection (6)
- IT Service Management (1)
- Identity and Access Management (4)
- SIEM (9)
- SOAR (3)
- Threat Intelligence (3)
- Unified Endpoint Management (3)
- Vulnerability Management (3)

VENDOR

- Broadcom (Symantec) (1)
- Check Point (1)
- Cyborg Security (1)
- Cymulate (1)
- Elastic (1)
- Fortinet (1)
- Google (1)
- IBM (3)
- MISP Project (1)
- Microsoft (5)
- N/A (4)
- NetSkope (1)



Alineados con el CCN

Deep Security (Manager y Agente/Relay Linux/Windows)

Versión	11.0
Fabricante	Trend Micro
Familia	EDR (Endpoint Detection and Response)
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2021
Revisión de Validez	31/05/2024



Deep Discovery Inspector

Versión	6.5.1129
Fabricante	Trend Micro
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	N/A
Revisión de Validez	16/05/2026



TippingPoint Threat Protection System

Versión	5.4.1
Fabricante	Trend Micro
Familia	IDS, IPS y AntiDDoS
Tipo	Producto
Categoría ENS	MEDIA
Fecha Inclusión	01/02/2023
Revisión de Validez	31/07/2025



Certificado:

- Endpoint/Servidores.
- NDR.
- IPS.

En Curso:

- IPS OT.
- Correo.
- 5G.

