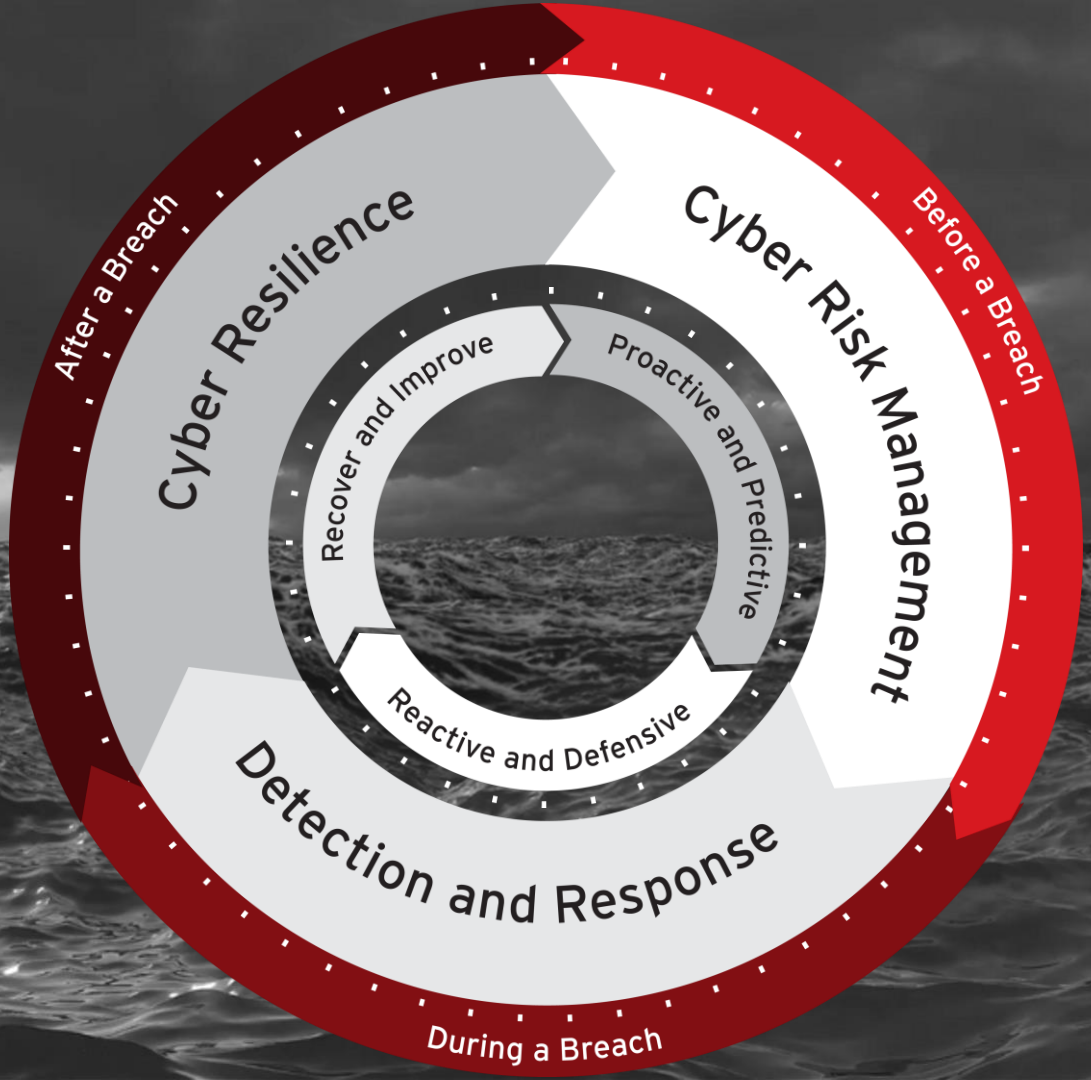
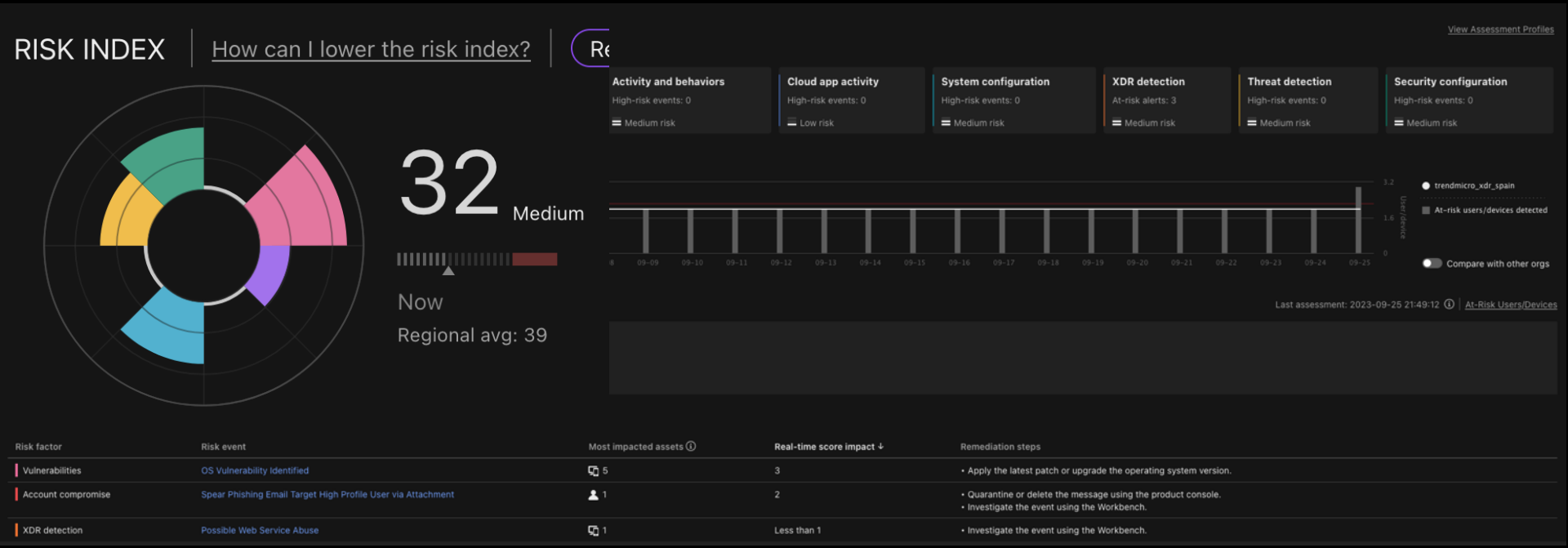


Prevención. - Riesgo



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

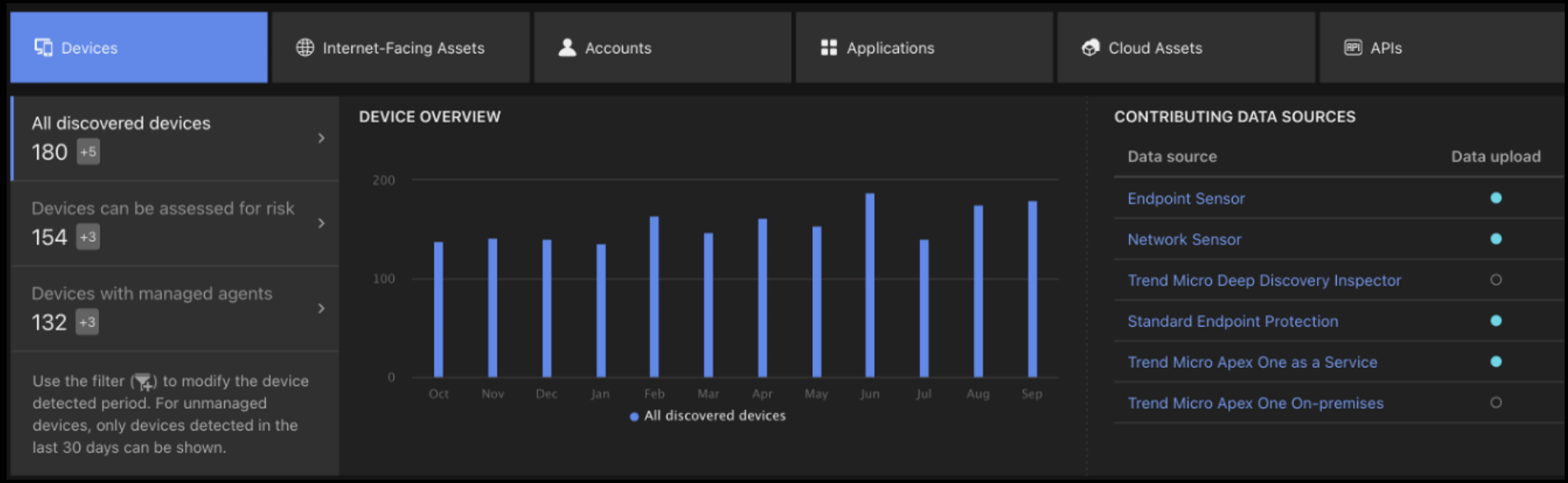
Identity Threat Detection and Response (ITDR)

- 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

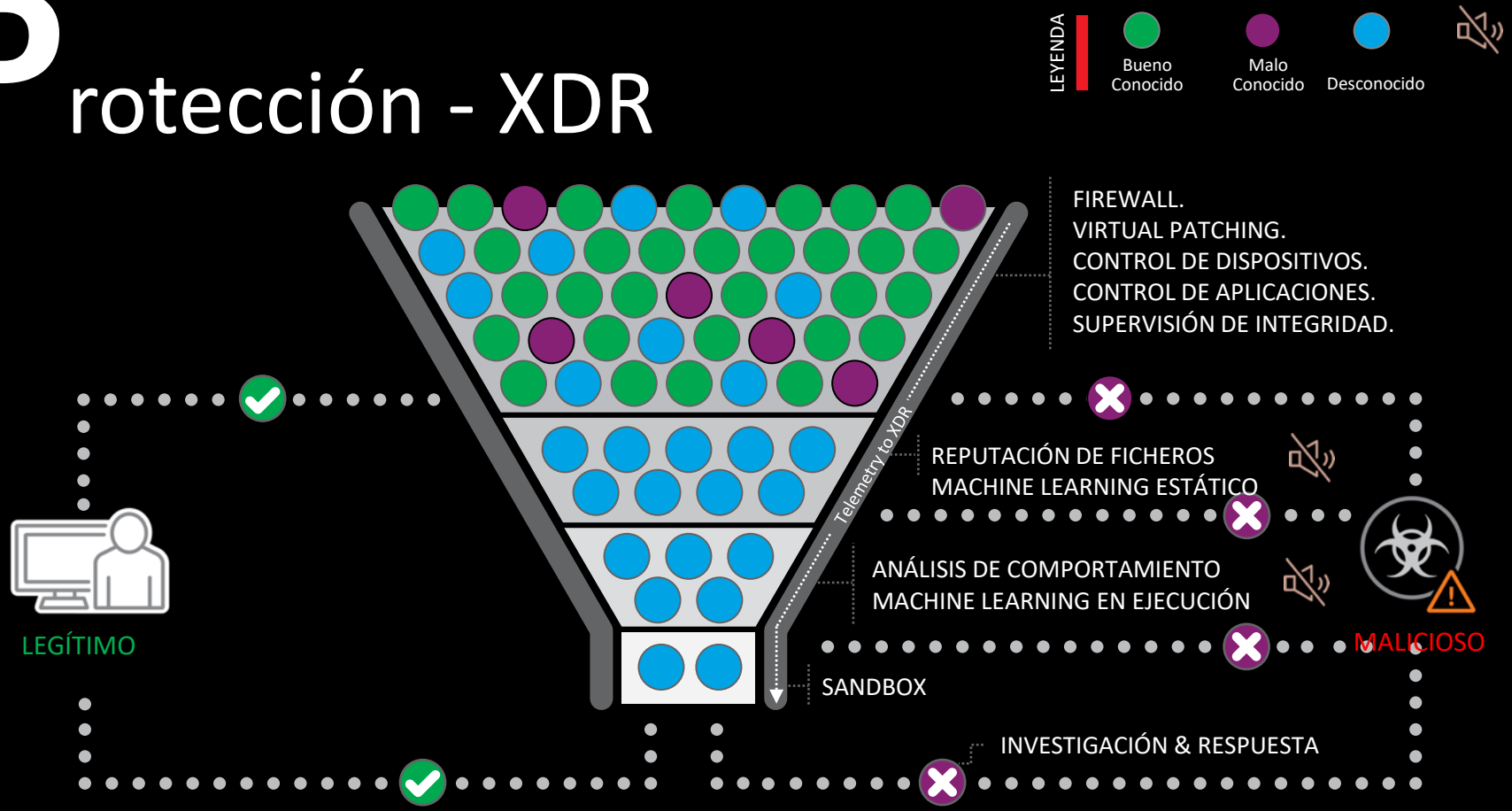
Data Lake | Identity and Access Activity Data

- **Endpoint**
- **Email**
- **SaaS Apps**
- **Web Traffic**
- IAM
- Network

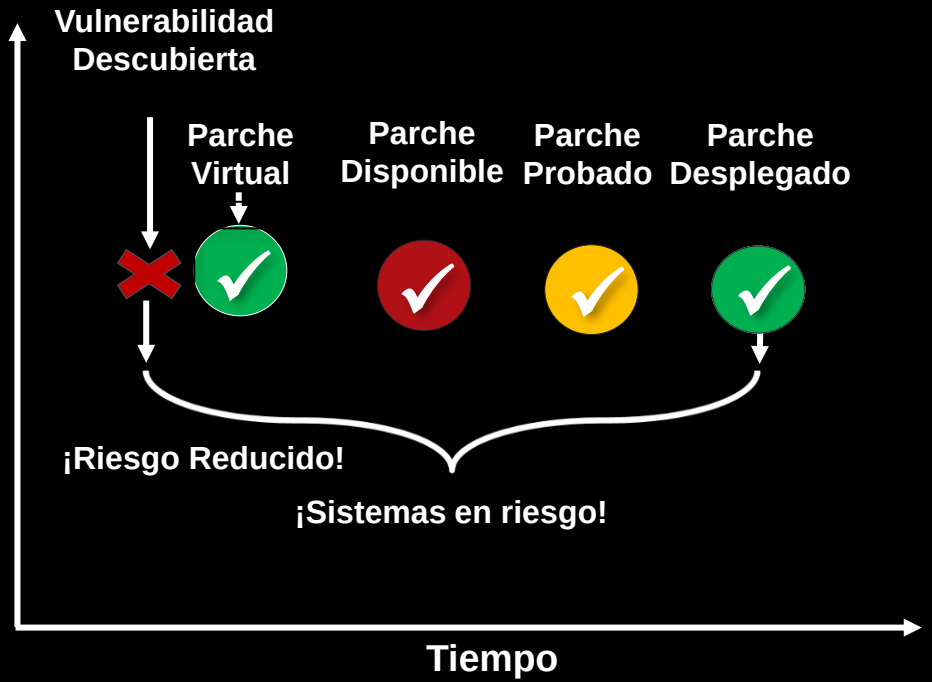
Prevención - Discovery



Protección - XDR

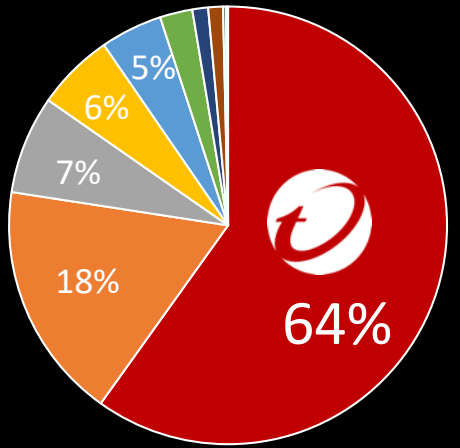


Protección.



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…



Incluido soporte para SO descontinuados por fabricante (Win 2000,2003,2008, XP,7, Ubuntu 10.04, RHEL etc)

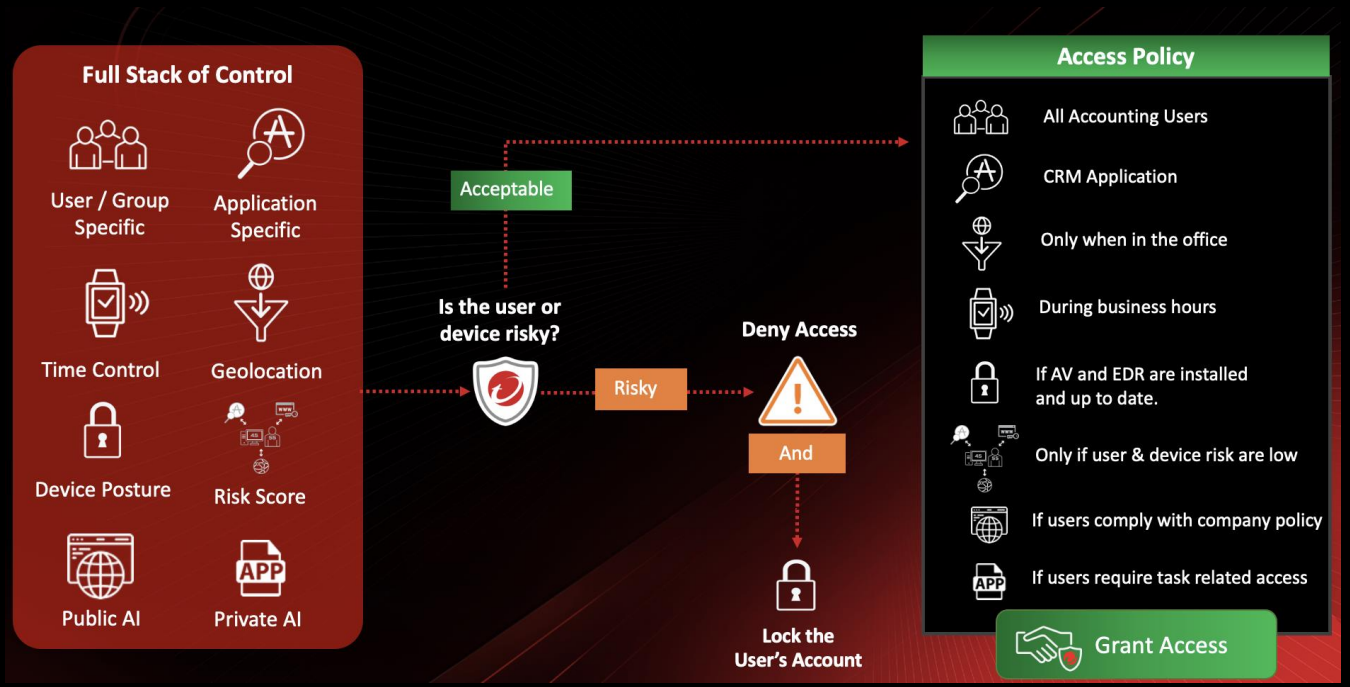
Protección

Email & Collaboration Security

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

Prevención.

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



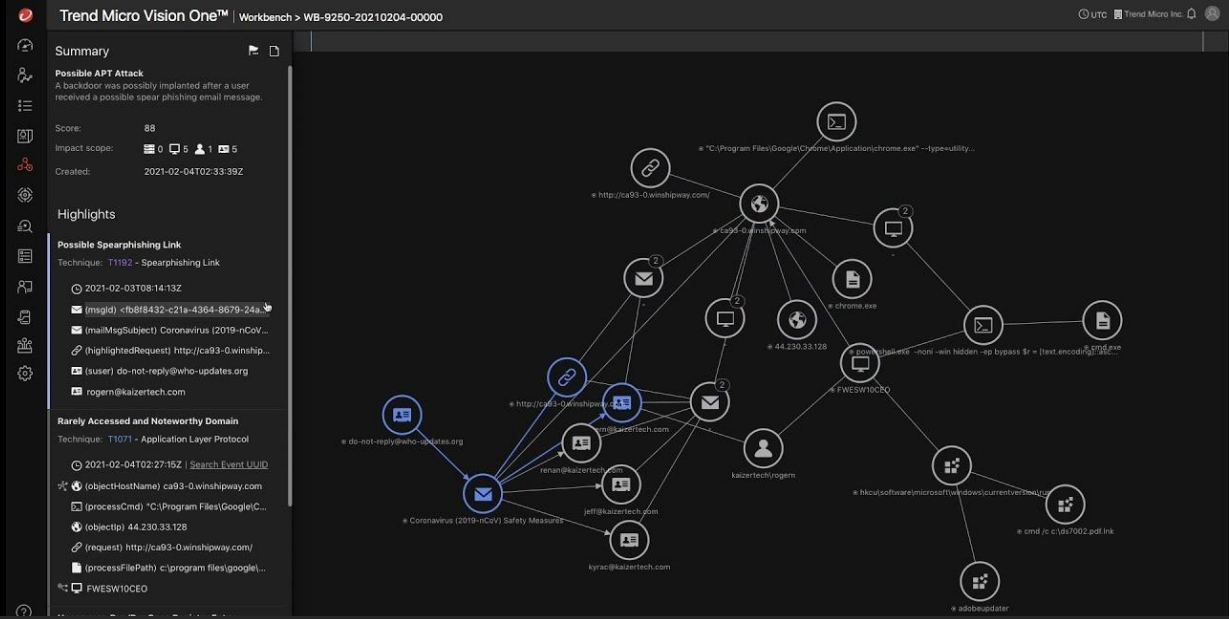
Prevención.

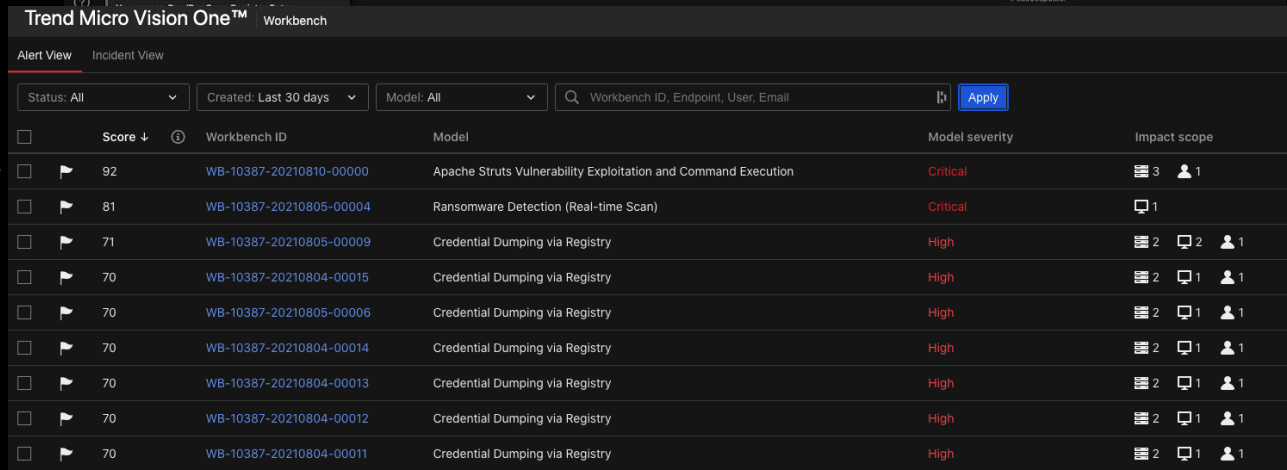
NDR

Visibilidad de red.

Sondas físicas y virtuales.

Bloqueo de ataques de red.





Protección Cloud

Attack Surface Risk Management

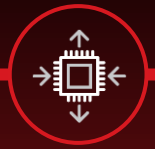
XDR (Extended Detection and Response)

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

Storage

Third-Party Libraries

Serverless

- ASRM for Cloud
- Container Security
- File Security
- API Visibility
- ASRM for Cloud and File Security

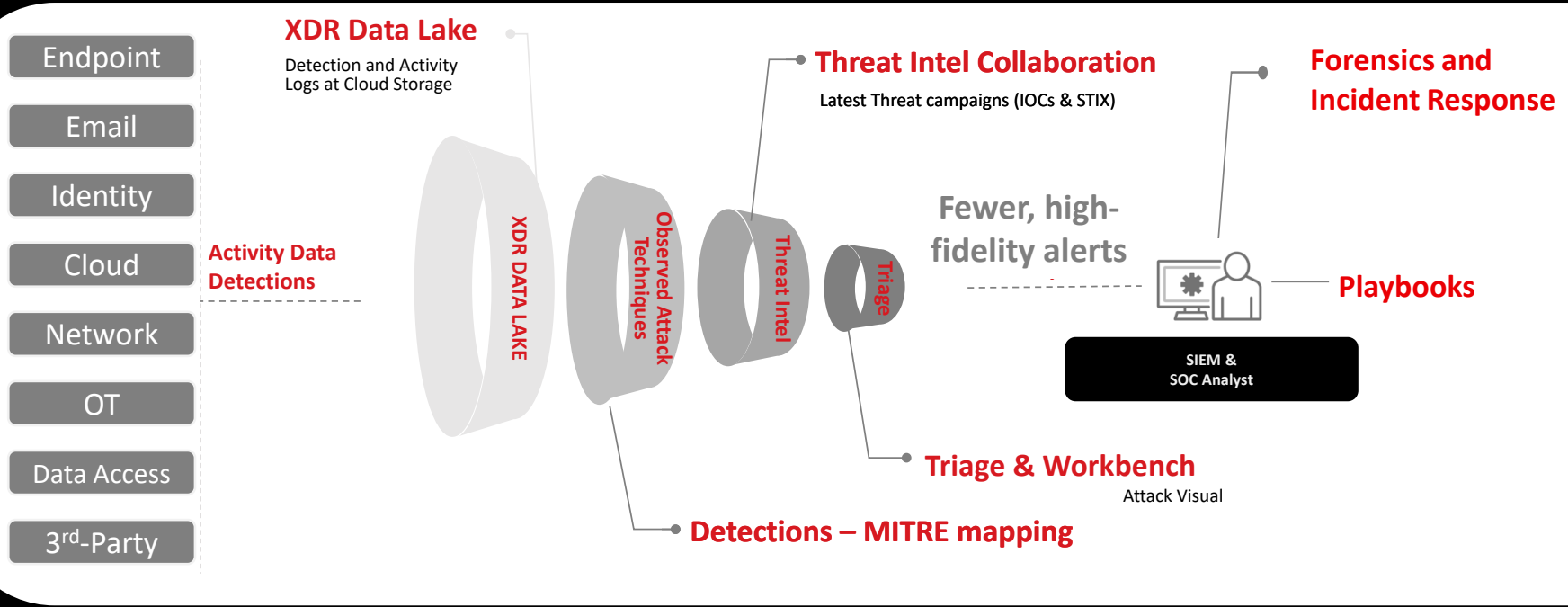
Multi-Cloud

Private Cloud

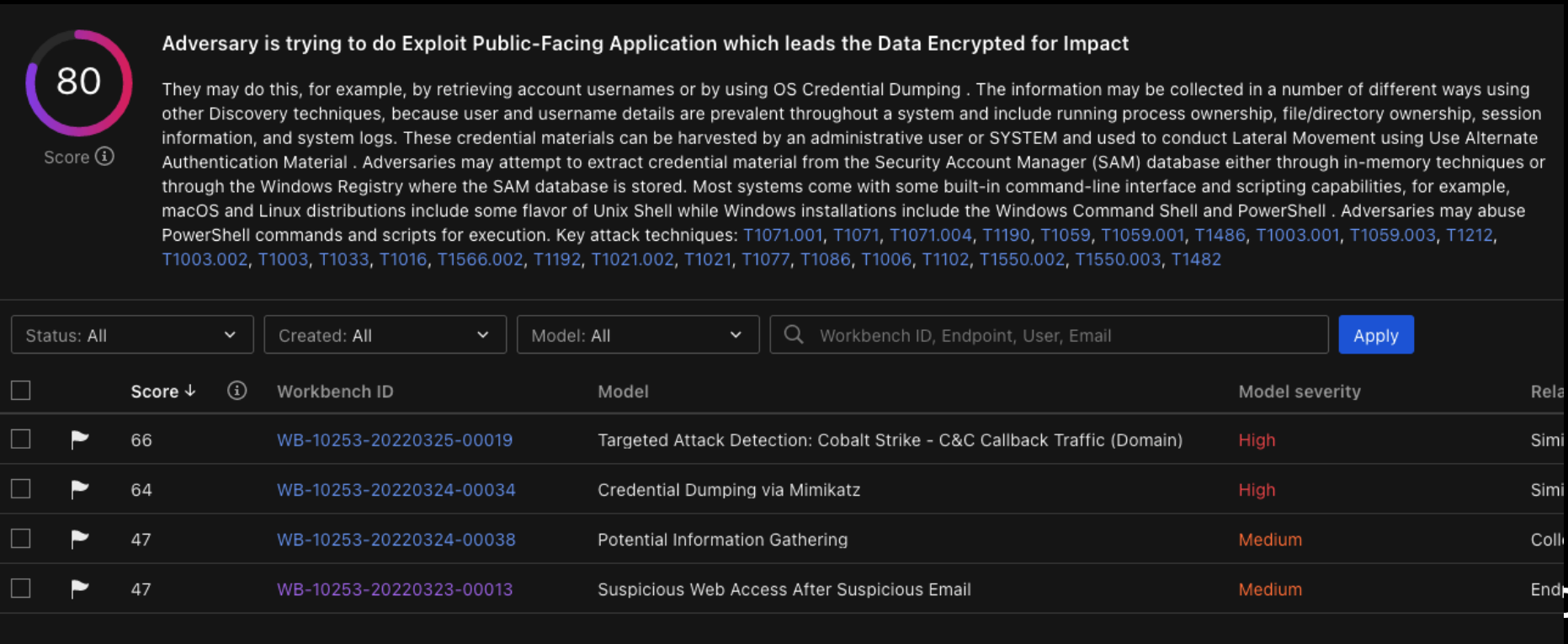
Public Cloud

- AWS
- Azure
- GCP
- Otros...

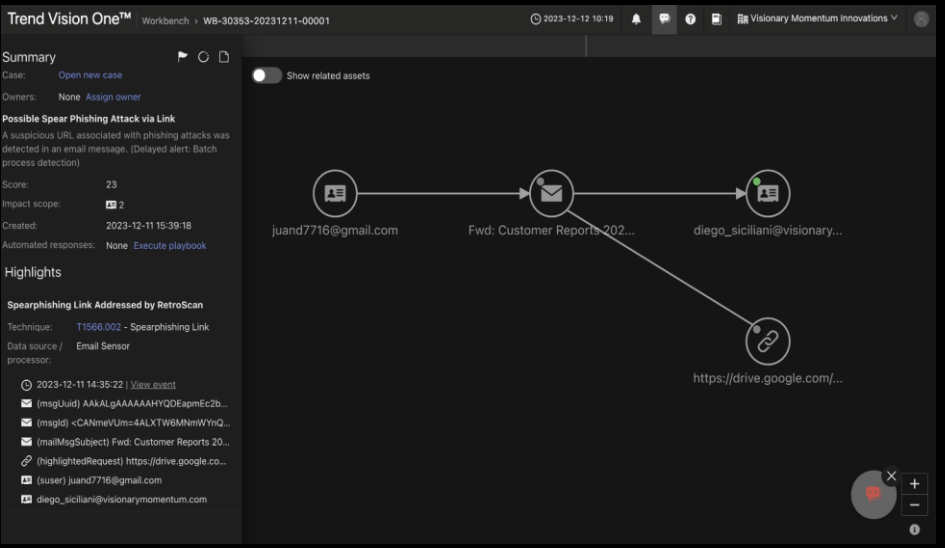
resPuesta. XDR

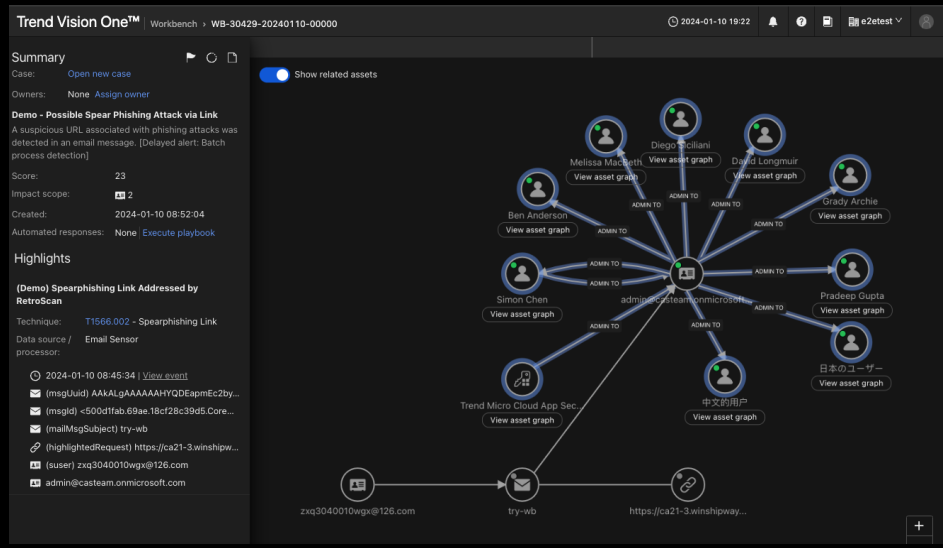


resPuesta. XDR



respuesta. XDR

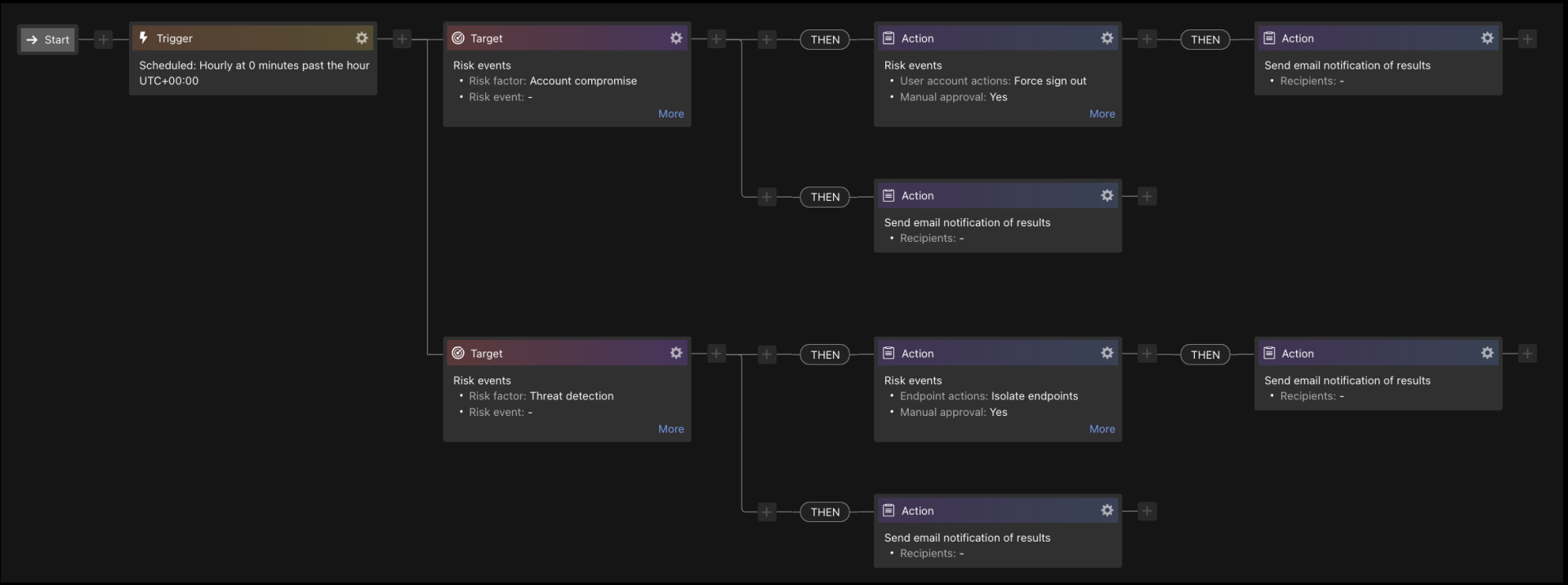


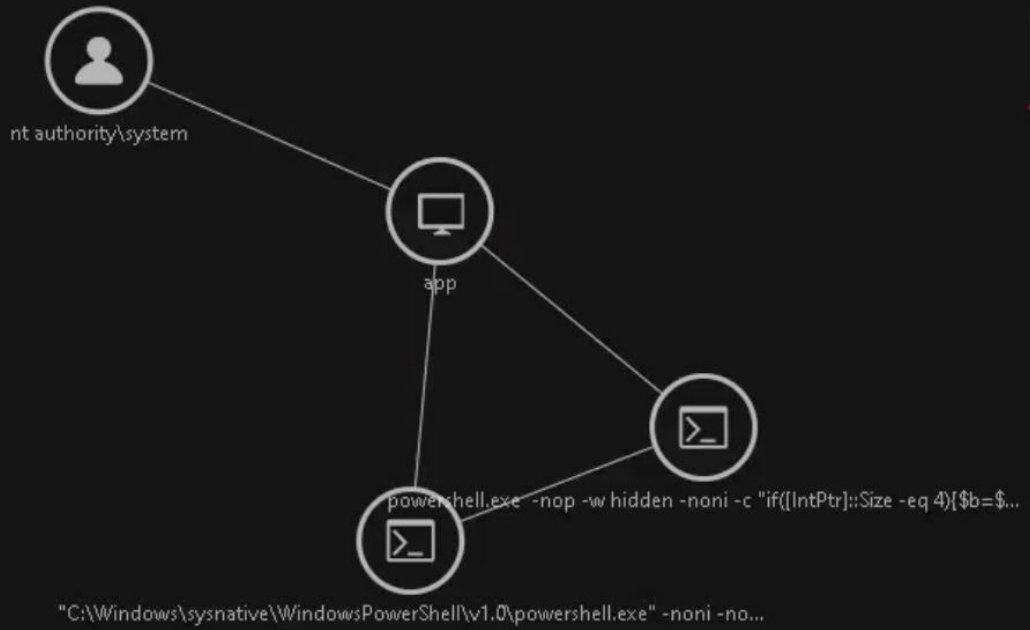


Detectar origen

Analizar Alcance y responder

resPuesta. SOAR





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

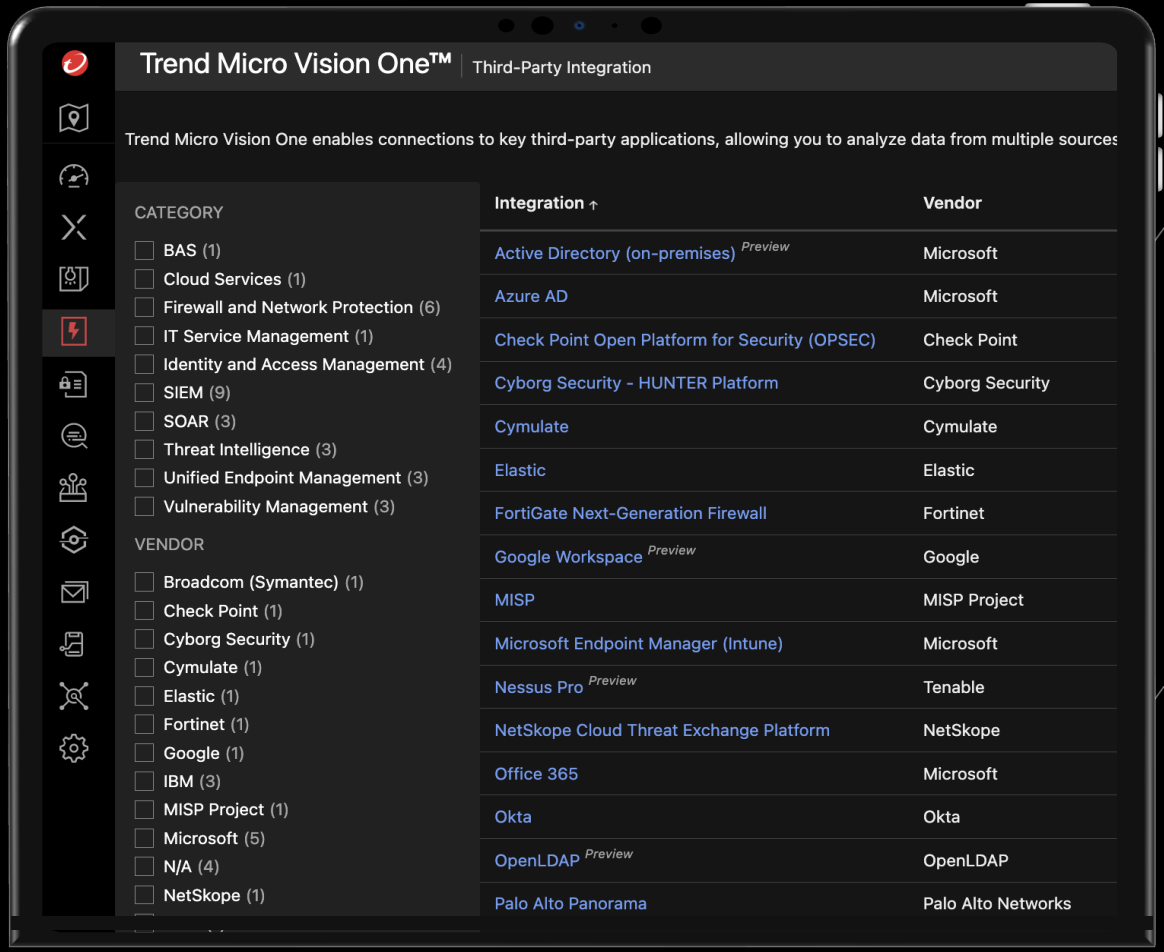
What is Mimikatz

Type your question here

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.

Expansive Integration Ecosystem



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.