La brújula de la Ciberseguridad

Raúl Guillén

Evangelizador de Estrategias de Ciberseguridad

Profesionalización del Cibercrimen

Cibercrimen
como Servicio

+ Recursos

hacktivismo

Phishing notimiups eycaks
Digiile cliiFes votiess iennanalsteion
vidce eaiemullattion
sepition mniasltion
ai dlecting anenesionmalge orielemorrors
nolevons otiao
cpn

Colaboración

IA

Eficiencia

€€€

Nuevo paradigma regulatorio EU

NIS 2

18 Octubre 2024 (*)

Introduce medidas mínimas de seguridad obligatorias para **infraestructuras críticas y sectores importantes.**

DORA

17 Enero 2025

Medidas mínimas de seguridad obligatorias y requisitos de pruebas de resiliencia para el **sector financiero.**

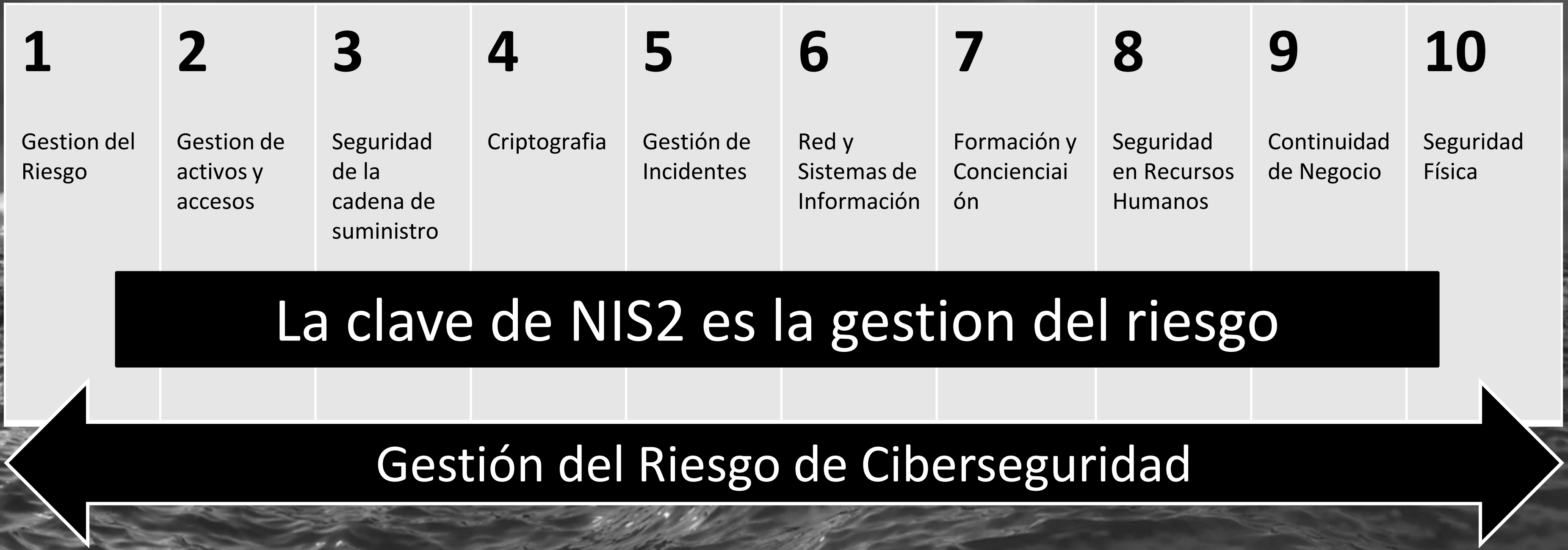
CER

17 Julio 2026

Nuevo marco general para abordar la resiliencia de las entidades críticas en un enfoque que incluya **todos** los peligros.

(*) Anteproyecto de ley aprobado, actualmente en fase de consultas, APROBACIÓN URGENTE

Directiva NIS 2

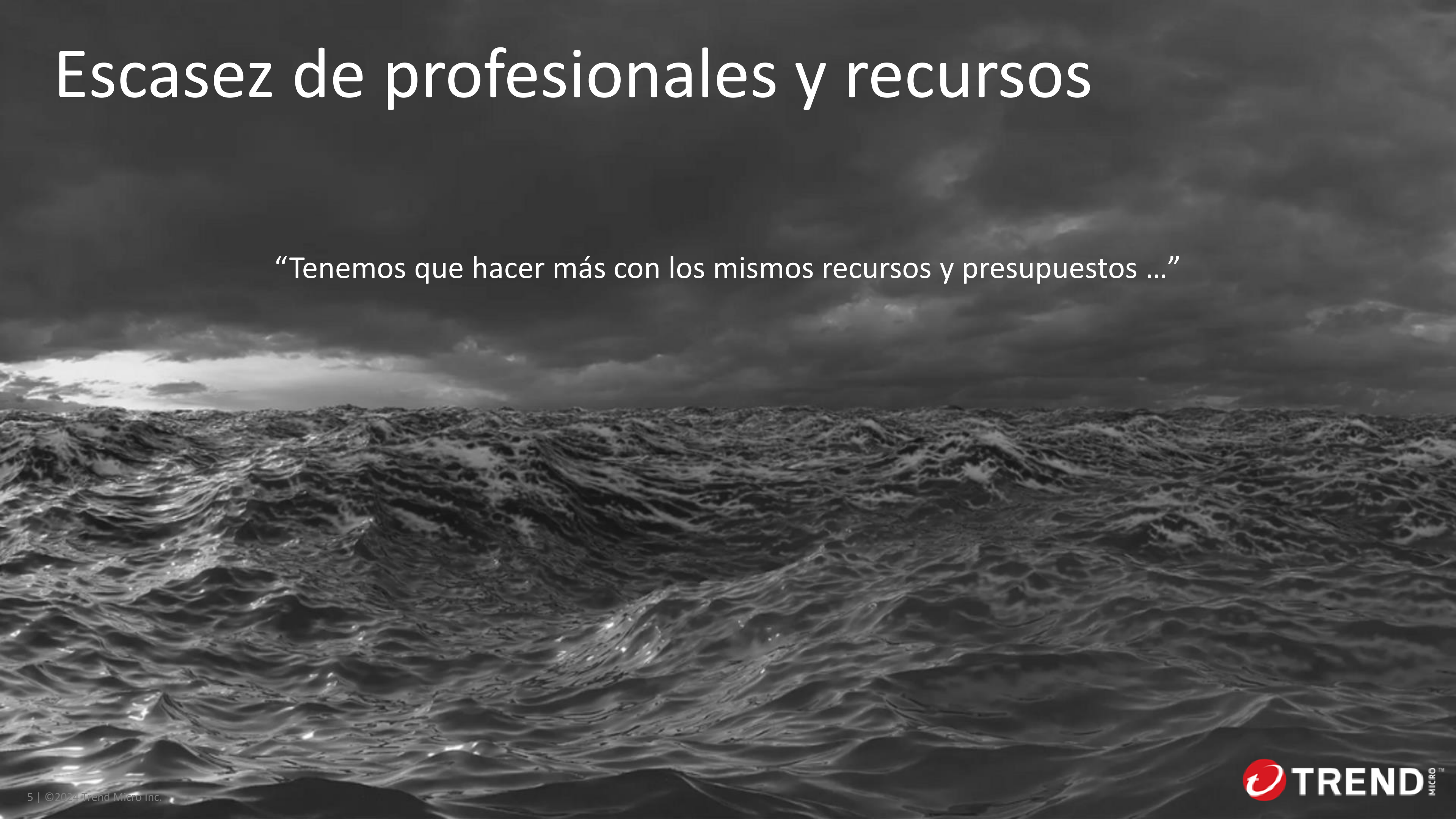


1	2	3	4	5	6	7	8	9	10
Gestion del Riesgo	Gestion de activos y accesos	Seguridad de la cadena de suministro	Criptografia	Gestión de Incidentes	Red y Sistemas de Información	Formación y Concienciaión	Seguridad en Recursos Humanos	Continuidad de Negocio	Seguridad Física

La clave de NIS2 es la gestion del riesgo

Gestión del Riesgo de Ciberseguridad

Escasez de profesionales y recursos



“Tenemos que hacer más con los mismos recursos y presupuestos …”

RISCO
INFORMATION SECURITY
RISC2
CHIEF INFORMATION SECURITY OFFICER
NIS2
URITY
CYBEF-ECURITY OFFICEF
RISCO
INF SECURITY
NIS2
CATAQUES
NIS2
NIS2
TREND MICRO

Antes del incidente

Análisis de postura

Proactivo

Análisis de Postura

RIESGO = PROBABILIDAD x IMPACTO

impacto = g (criticidad del negocio)

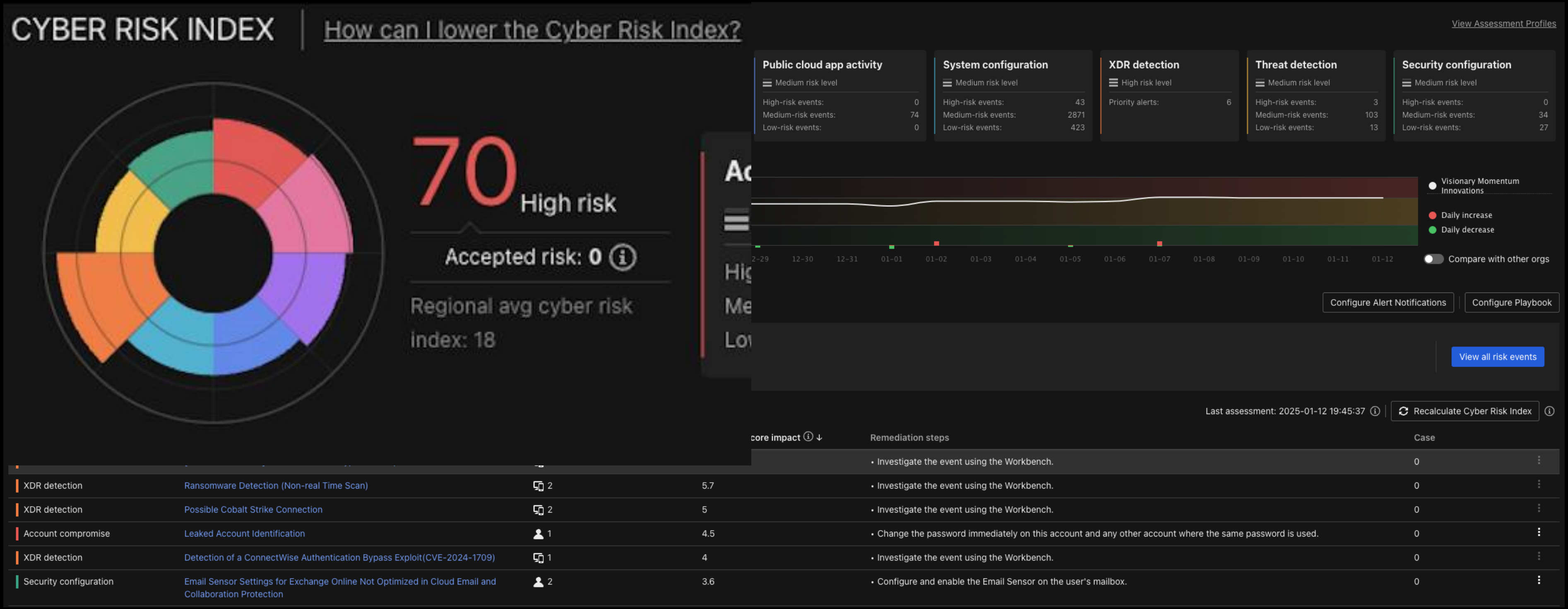
¿Por dónde accedo más facilmente?

Attack Path = Punto de Entrada + Activos x Joyas de la Corona

¿Cuál es el valor de los activos?
¿Cuántos activos puedo comprometer?

probabilidad = f (vulnerabilidades, exposición, amenazas, controles de mitigación)

Análisis de Postura



CYBER RISK INDEX | How can I lower the Cyber Risk Index?

70 High risk

Accepted risk: 0 ⓘ

Regional avg cyber risk index: 18

View Assessment Profiles

Public cloud app activity	
Medium risk level	
High-risk events:	0
Medium-risk events:	74
Low-risk events:	0

System configuration	
Medium risk level	
High-risk events:	43
Medium-risk events:	2871
Low-risk events:	423

XDR detection	
High risk level	
Priority alerts:	6

Threat detection	
Medium risk level	
High-risk events:	3
Medium-risk events:	103
Low-risk events:	13

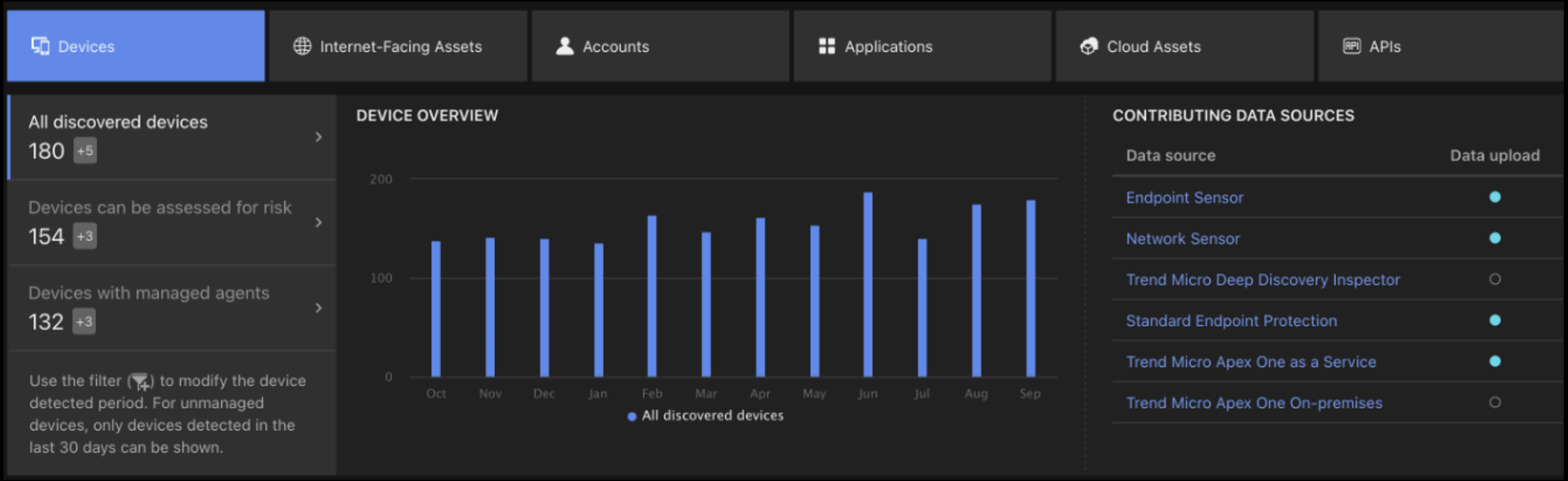
Security configuration	
Medium risk level	
High-risk events:	0
Medium-risk events:	34
Low-risk events:	27

Last assessment: 2025-01-12 19:45:37 ⓘ

			core impact ⓘ ↓	Remediation steps	Case
				• Investigate the event using the Workbench.	0
XDR detection	Ransomware Detection (Non-real Time Scan)	2	5.7	• Investigate the event using the Workbench.	0
XDR detection	Possible Cobalt Strike Connection	2	5	• Investigate the event using the Workbench.	0
Account compromise	Leaked Account Identification	👤 1	4.5	• Change the password immediately on this account and any other account where the same password is used.	0
XDR detection	Detection of a ConnectWise Authentication Bypass Exploit(CVE-2024-1709)	1	4	• Investigate the event using the Workbench.	0
Security configuration	Email Sensor Settings for Exchange Online Not Optimized in Cloud Email and Collaboration Protection	👤 2	3.6	• Configure and enable the Email Sensor on the user's mailbox.	0

Análisis de Postura

Visibilidad



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

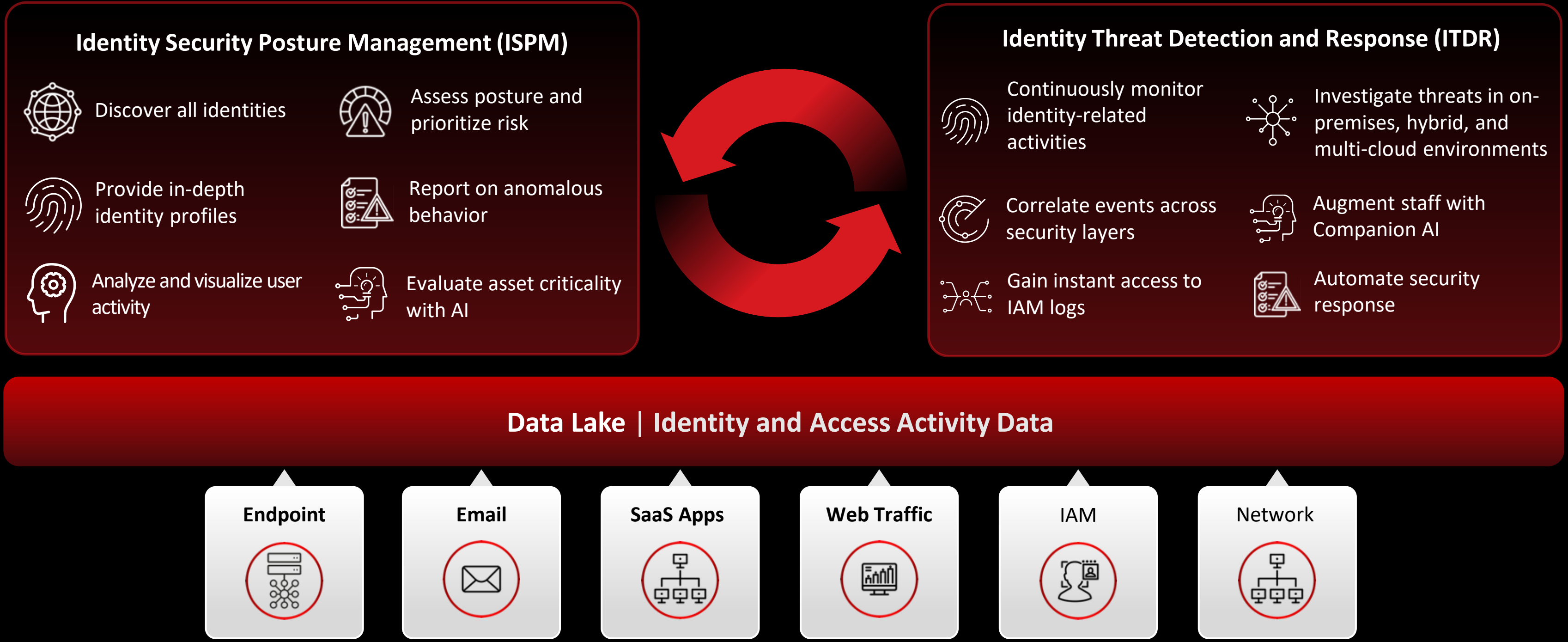
CONTRIBUTING DATA SOURCES

Data source	Data upload
Endpoint Sensor	●
Network Sensor	●
Trend Micro Deep Discovery Inspector	○
Standard Endpoint Protection	●
Trend Micro Apex One as a Service	●
Trend Micro Apex One On-premises	○

Usuarios, Infraestructuras, Aplicaciones y Datos

Análisis de Postura

Identidades



Identity Security Posture Management (ISPM)

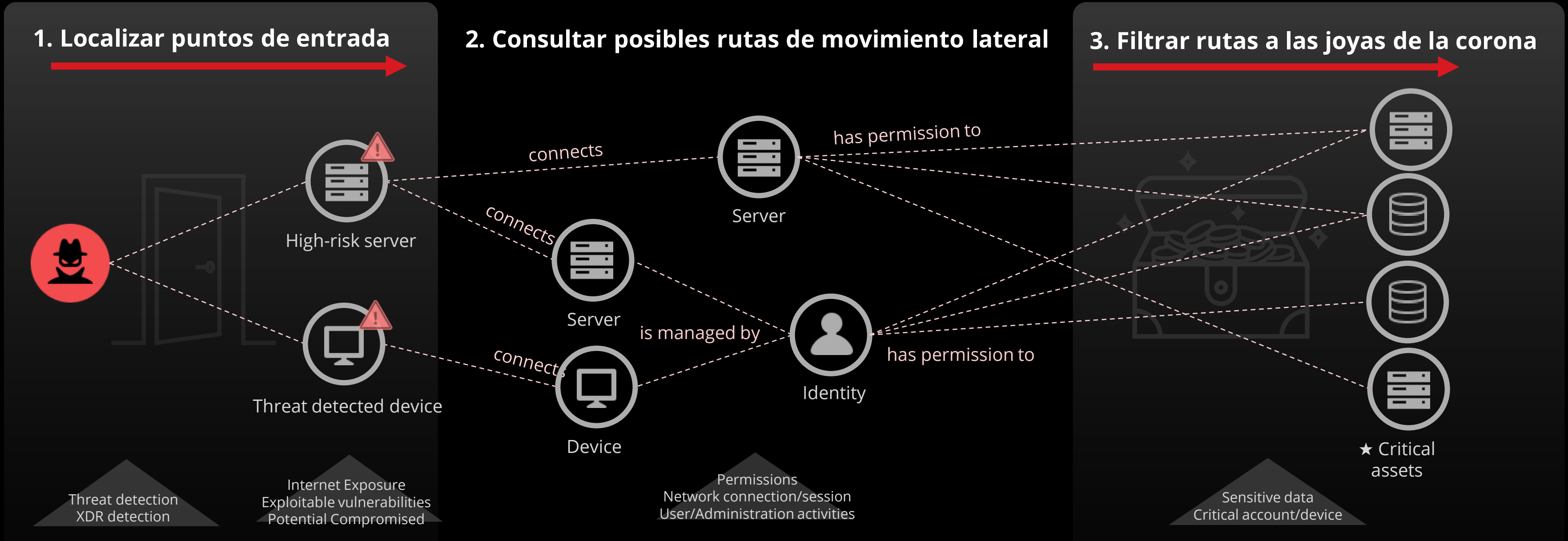
- Discover all identities
- Assess posture and prioritize risk
- Provide in-depth identity profiles
- Report on anomalous behavior
- Analyze and visualize user activity
- Evaluate asset criticality with AI

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

Análisis y PREVENCIÓN de ataques gracias al USO de la IA



Orígenes de datos

Datos de detección

XDR

Eventos de Riesgo

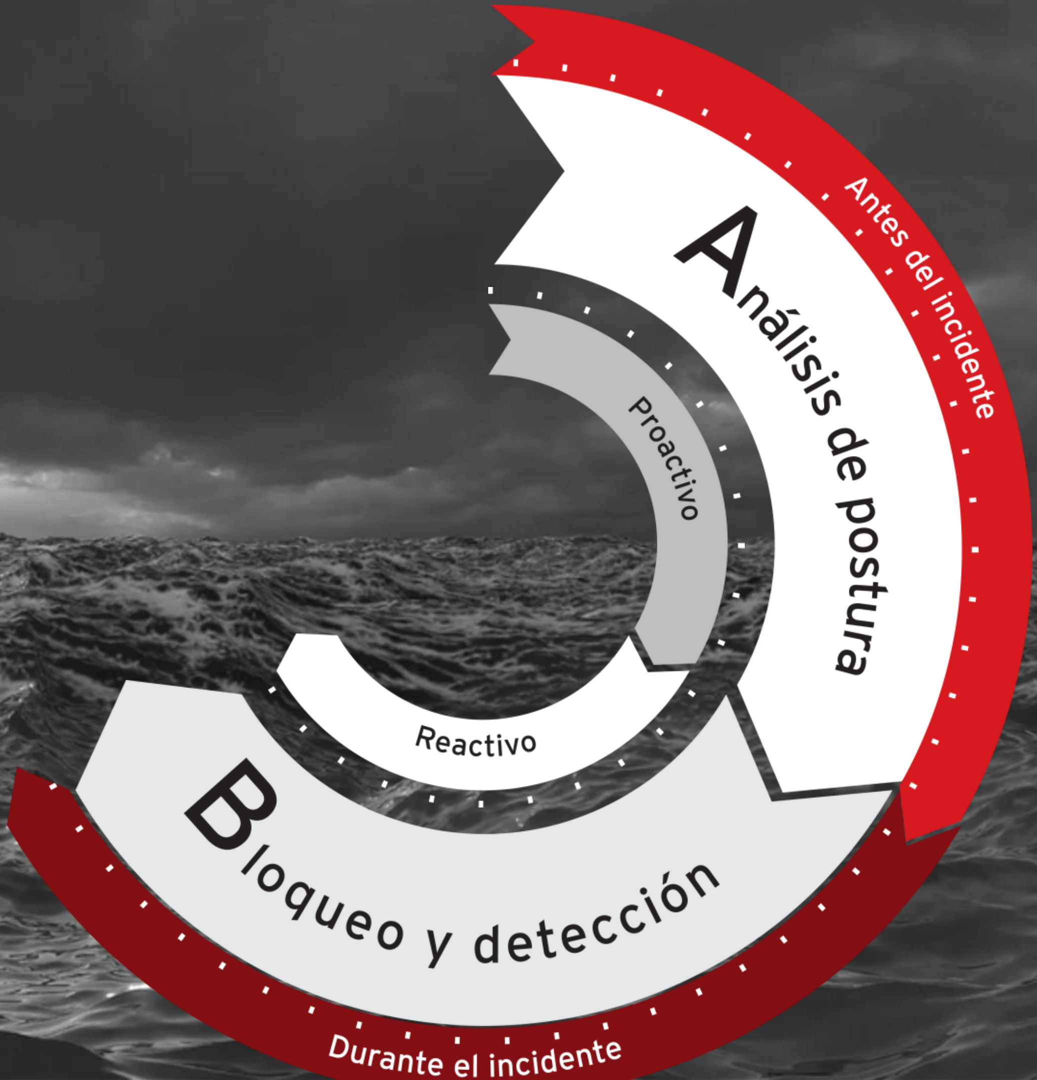
Conocimiento para el riesgo de activos

Criticidad de los Activos

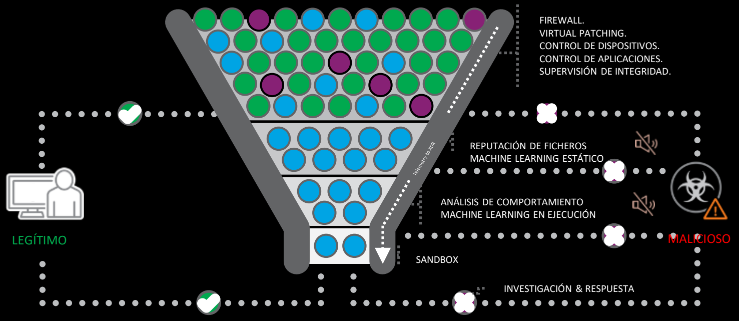
ASRM

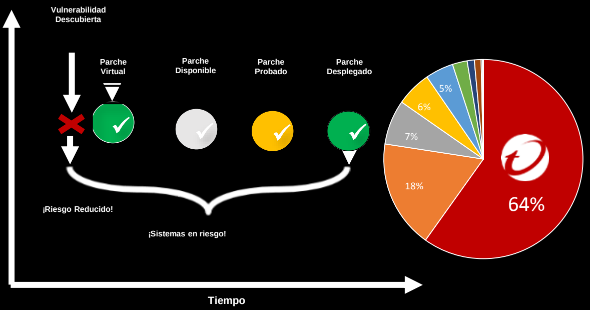
Inteligencia de Amenazas (Threat Intelligence)

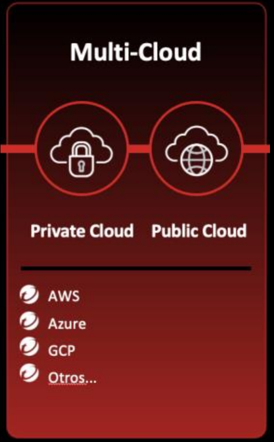
Endpoints	Cloud	Email	Redes	Datos	Identidades

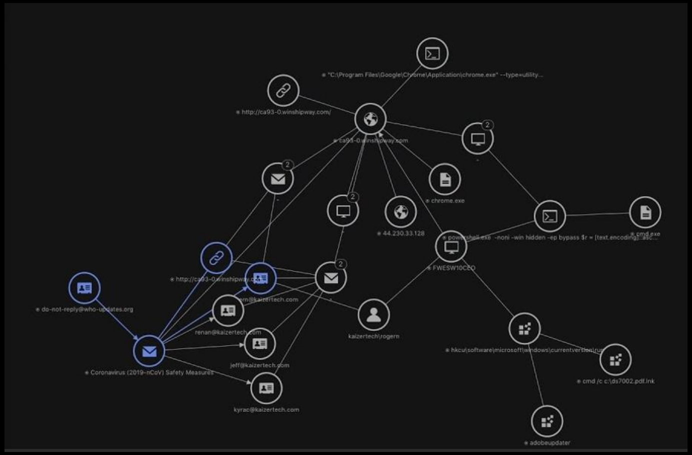

Antes del incidente
Análisis de postura
Proactivo
Reactivo
Bloqueo y detección
Durante el incidente

Bloqueo & Detección

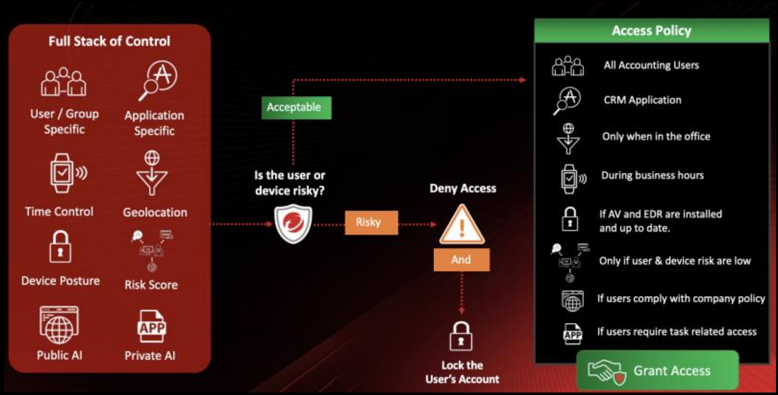


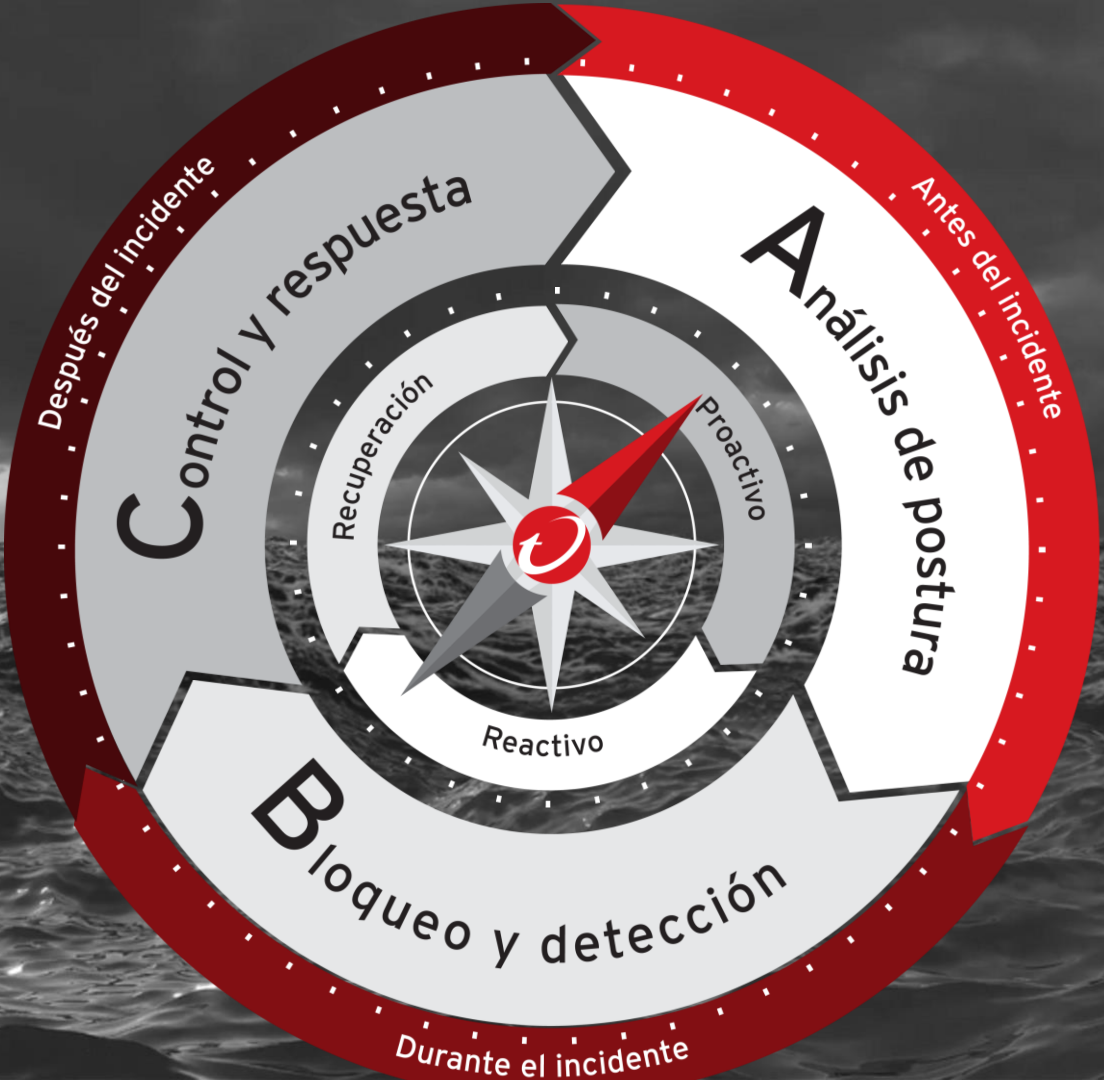




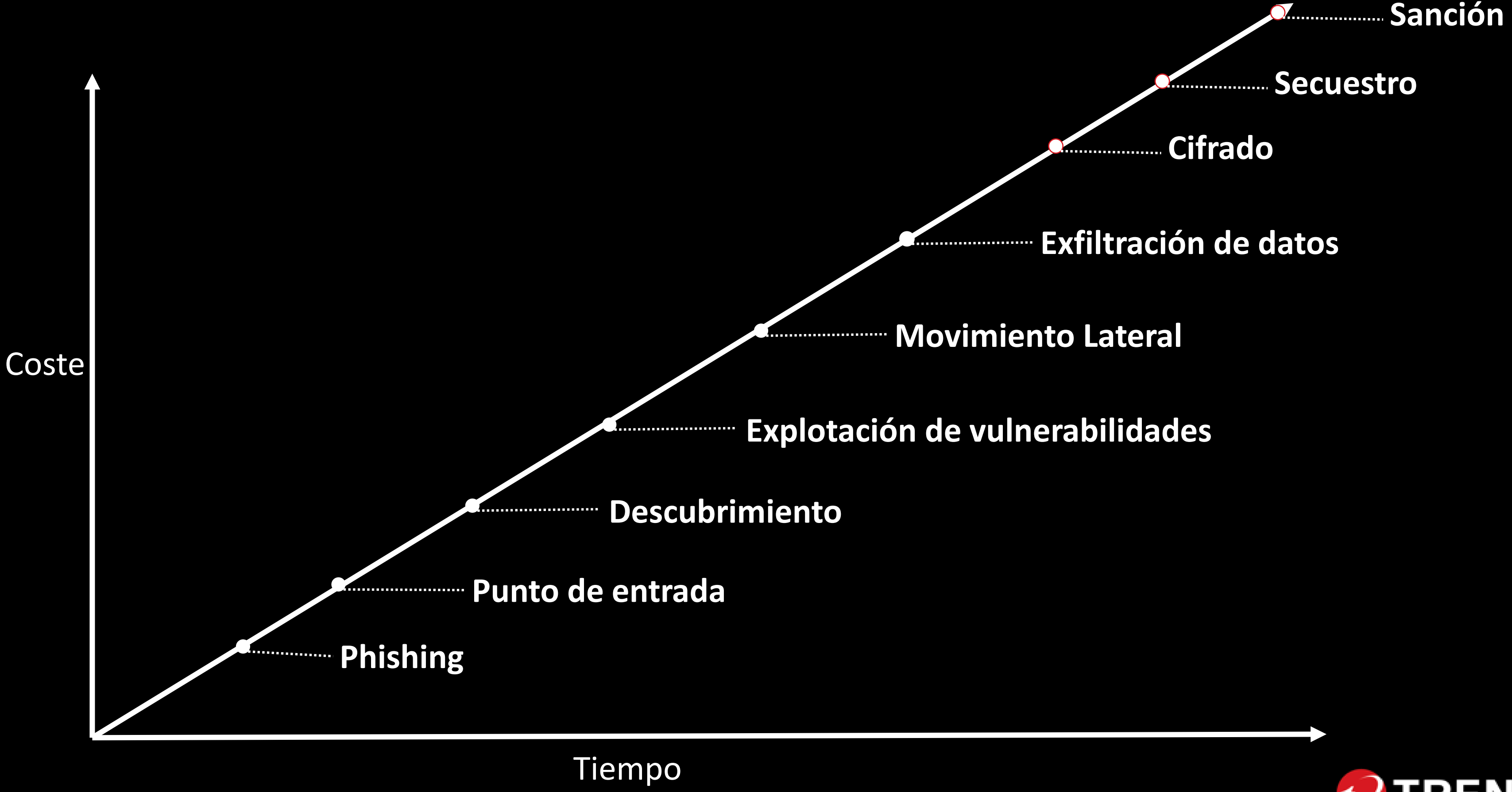


"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility...
http://ca93-0.winshipway.com/
ca93-0.winshipway.com
chrome.exe
44.230.33.128
powershell.exe -noni -win hidden -ep bypass $r = [text.encoding]::asc...
cmd.exe
FWESW10CEO
http://ca93-0.winshipway.com
do-not-reply@who-updates.org
rogern@kaizertech.com
renan@kaizertech.com
jeff@kaizertech.com
kyrac@kaizertech.com
Coronavirus (2019-nCoV) Safety Measures
kaizertech\rogern
hkcu\software\microsoft\windows\currentversion\run
cmd /c c:\ds7002.pdf.lnk
adobeupdater
2



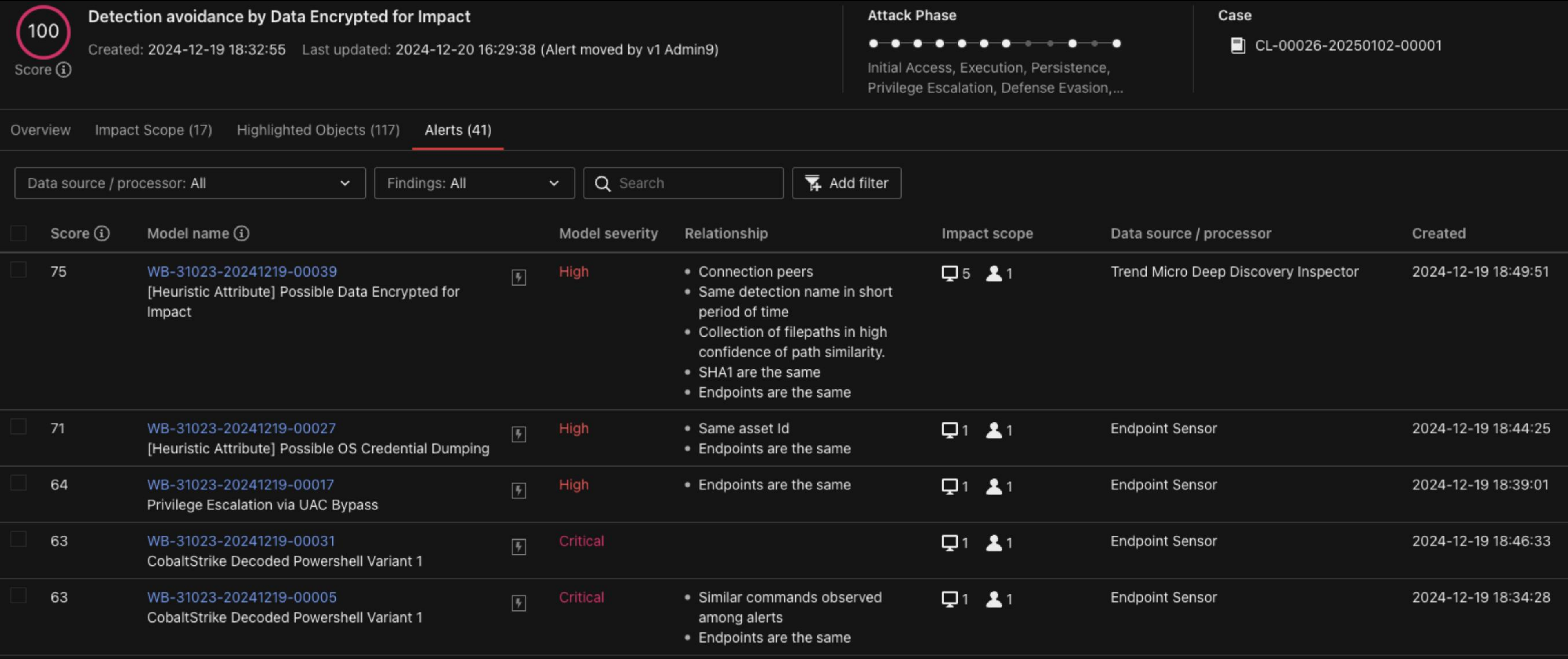

Antes del incidente
Análisis de postura
Durante el incidente
Bloqueo y detección
Después del incidente
Control y respuesta
Proactivo
Reactivo
Recuperación

Coste = Cómo x Cuándo



Control & Respuesta

XDR



100 Score ⓘ

Detection avoidance by Data Encrypted for Impact

Created: 2024-12-19 18:32:55   Last updated: 2024-12-20 16:29:38 (Alert moved by v1 Admin9)

Attack Phase

Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion,...

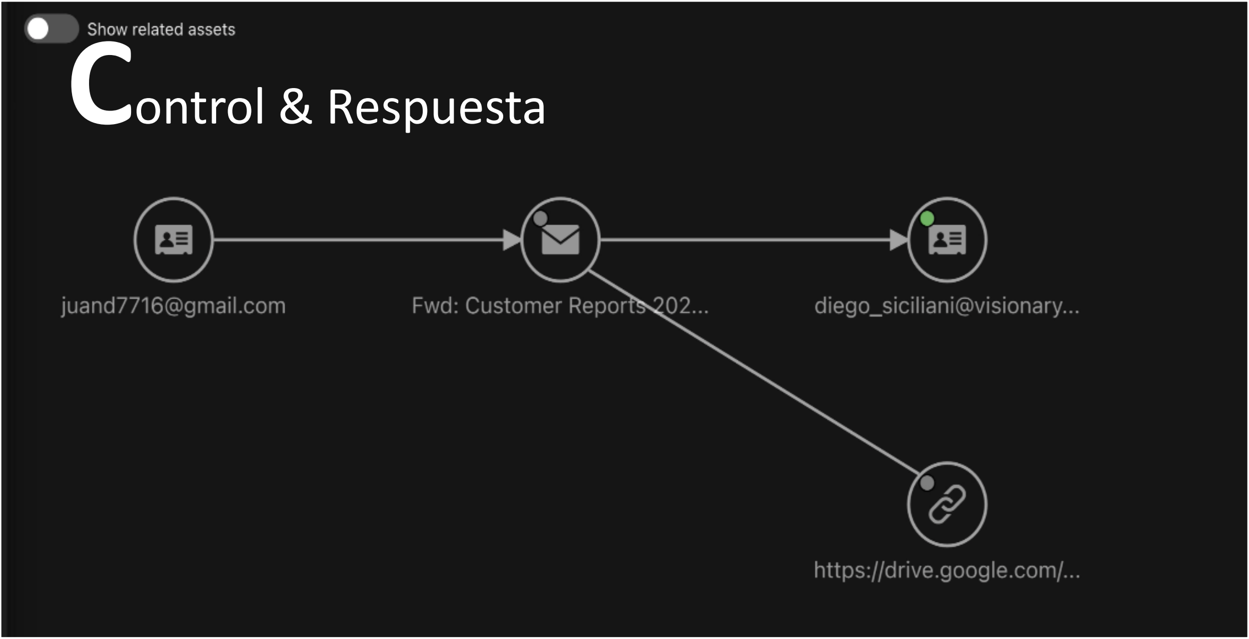
Case

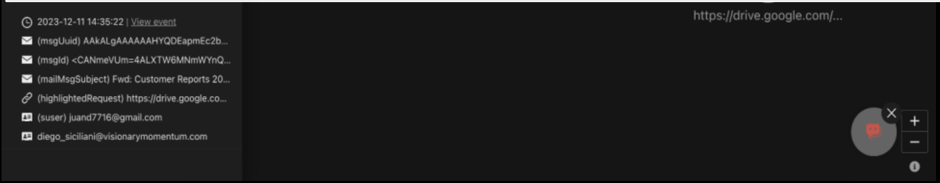
CL-00026-20250102-00001

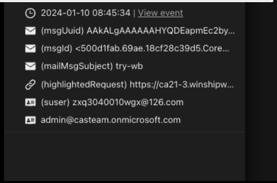
Score ⓘ	Model name ⓘ	Model severity	Relationship	Impact scope	Data source / processor	Created
75	WB-31023-20241219-00039 [Heuristic Attribute] Possible Data Encrypted for Impact	High	• Connection peers • Same detection name in short period of time • Collection of filepaths in high confidence of path similarity. • SHA1 are the same • Endpoints are the same	🖥 5 👤 1	Trend Micro Deep Discovery Inspector	2024-12-19 18:49:51
71	WB-31023-20241219-00027 [Heuristic Attribute] Possible OS Credential Dumping	High	• Same asset Id • Endpoints are the same	🖥 1 👤 1	Endpoint Sensor	2024-12-19 18:44:25
64	WB-31023-20241219-00017 Privilege Escalation via UAC Bypass	High	• Endpoints are the same	🖥 1 👤 1	Endpoint Sensor	2024-12-19 18:39:01
63	WB-31023-20241219-00031 CobaltStrike Decoded Powershell Variant 1	Critical		🖥 1 👤 1	Endpoint Sensor	2024-12-19 18:46:33
63	WB-31023-20241219-00005 CobaltStrike Decoded Powershell Variant 1	Critical	• Similar commands observed among alerts • Endpoints are the same	🖥 1 👤 1	Endpoint Sensor	2024-12-19 18:34:28

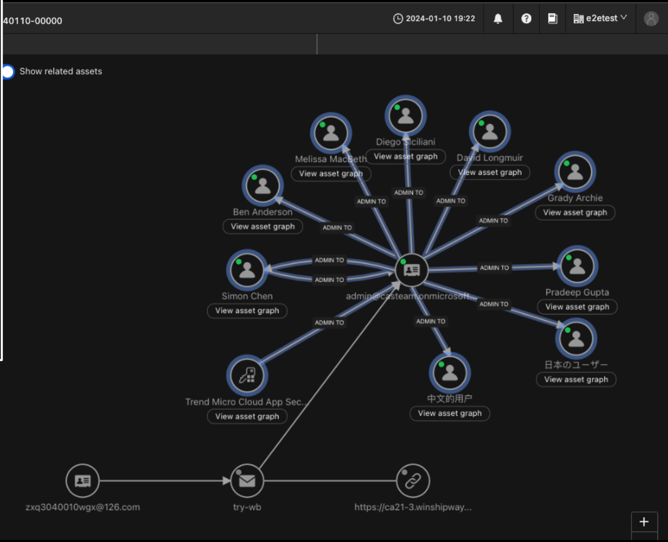
Control & Respuesta

XDR


Show related assets
juand7716@gmail.com
Fwd: Customer Reports 202...
diego_siciliani@visionary...
https://drive.google.com/...


2023-12-11 14:35:22 | View event
(msgUuid) AAkALgAAAAAAHYQDEapmEc2b...
(msgId) <CANmeVUm=4ALXTW6MNmWYnQ...
(mailMsgSubject) Fwd: Customer Reports 20...
(highlightedRequest) https://drive.google.co...
(suser) juand7716@gmail.com
diego_siciliani@visionarymomentum.com

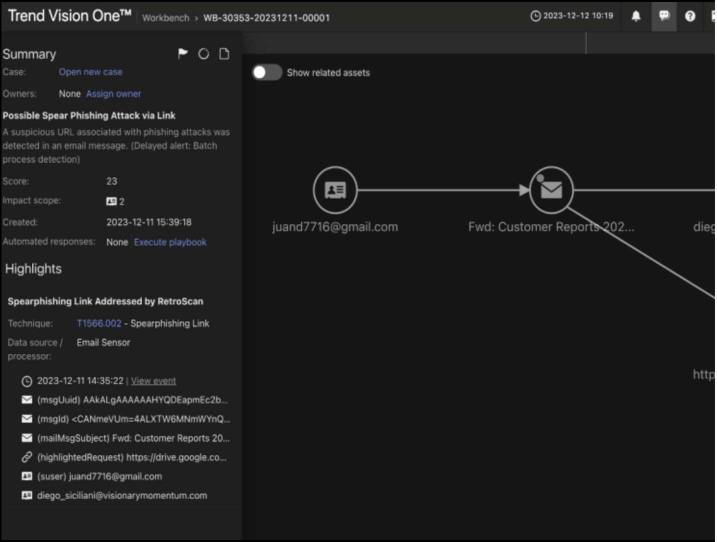

2024-01-10 08:45:34 | View event
(msgUuid) AAkALgAAAAAAHYQDEapmEc2by...
(msgId) <500d1fab.69ae.18cf28c39d5.Core...
(mailMsgSubject) try-wb
(highlightedRequest) https://ca21-3.winshipw...
(suser) zxq3040010wgx@126.com
admin@casteam.onmicrosoft.com



Detectar el origen

Analizar el alcance y Responder

Control & Respuesta



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 / processor: Email Sensor

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

(msgUuid) AAkALgAAAAAAHYQDEapmEc2b...

(msgId) <CANmeVUm=4ALXTW6MNmWYnQ...

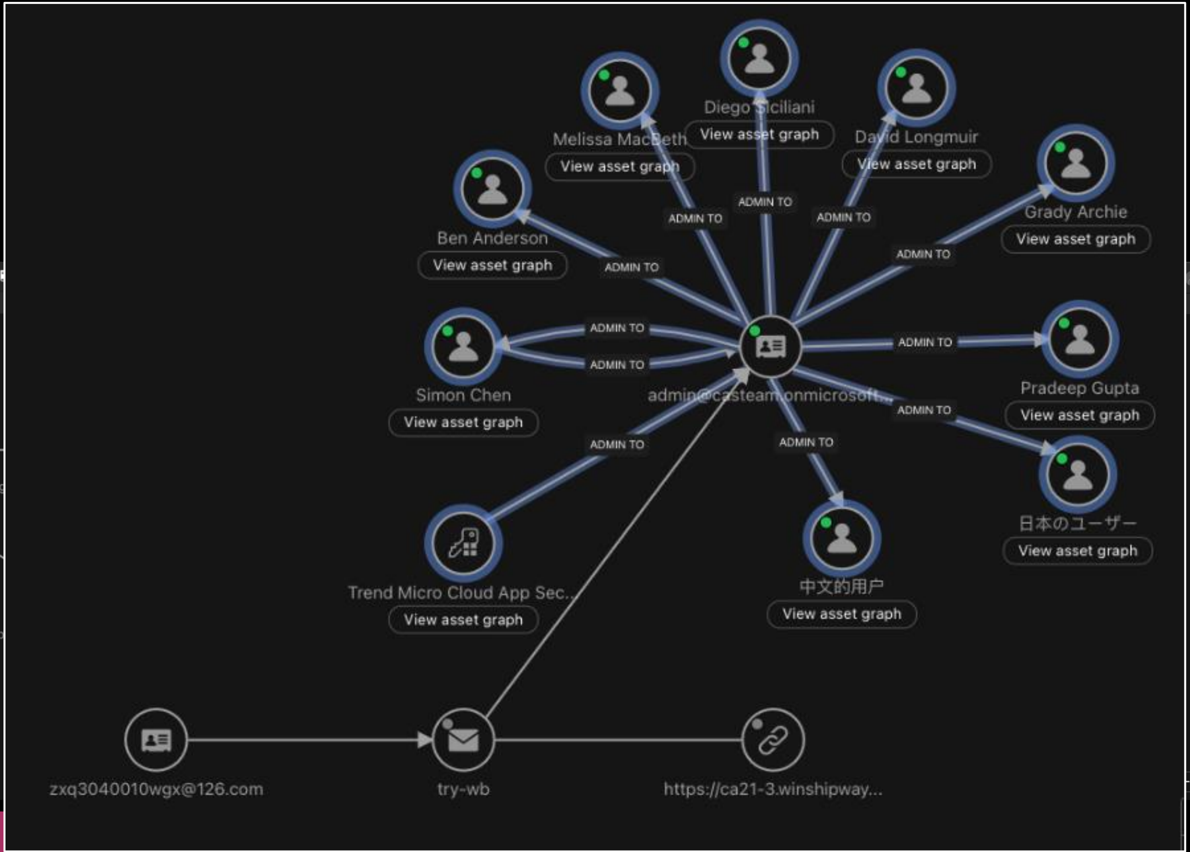
(mailMsgSubject) Fwd: Customer Reports 20...

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

(suser) juand7716@gmail.com

diego_siciliani@visionarymomentum.com

Show related assets

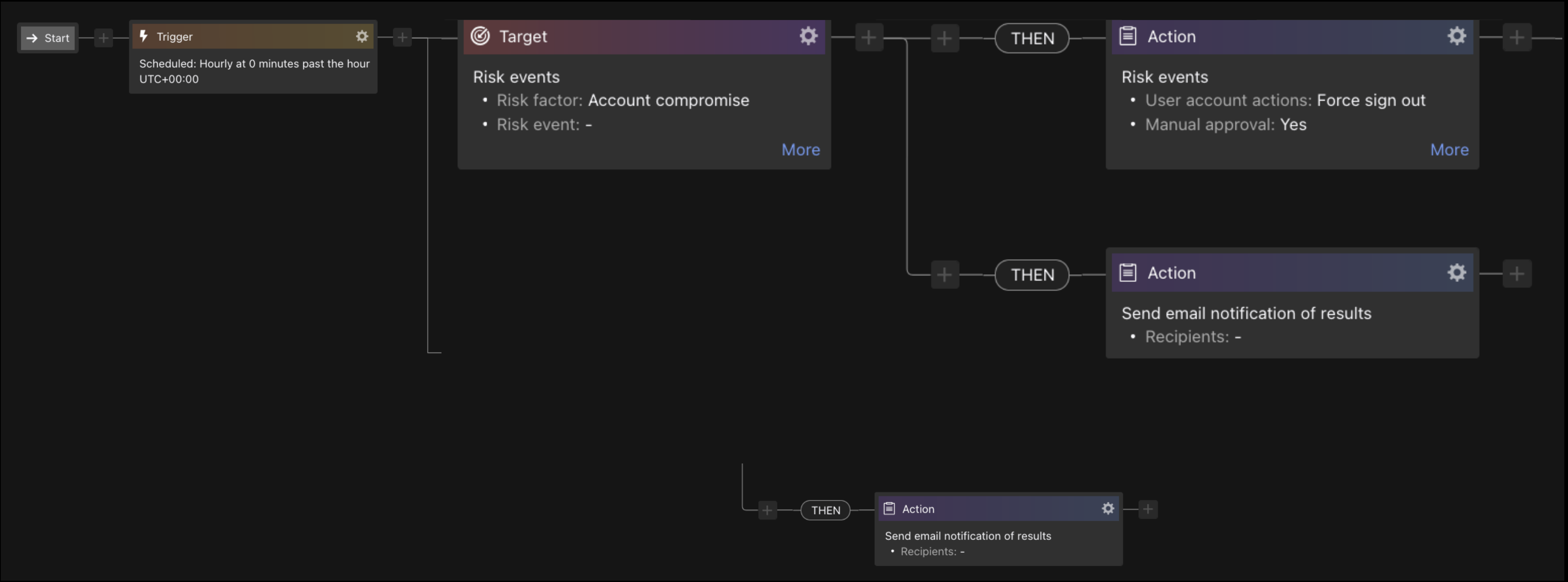


Detectar el origen

Analizar el alcance y Responder

Control & Respuesta

Automatización



Scheduled: Hourly at 0 minutes past the hour UTC+00:00

Risk events
- Risk factor: Account compromise
- Risk event: -

More

Risk events
- User account actions: Force sign out
- Manual approval: Yes

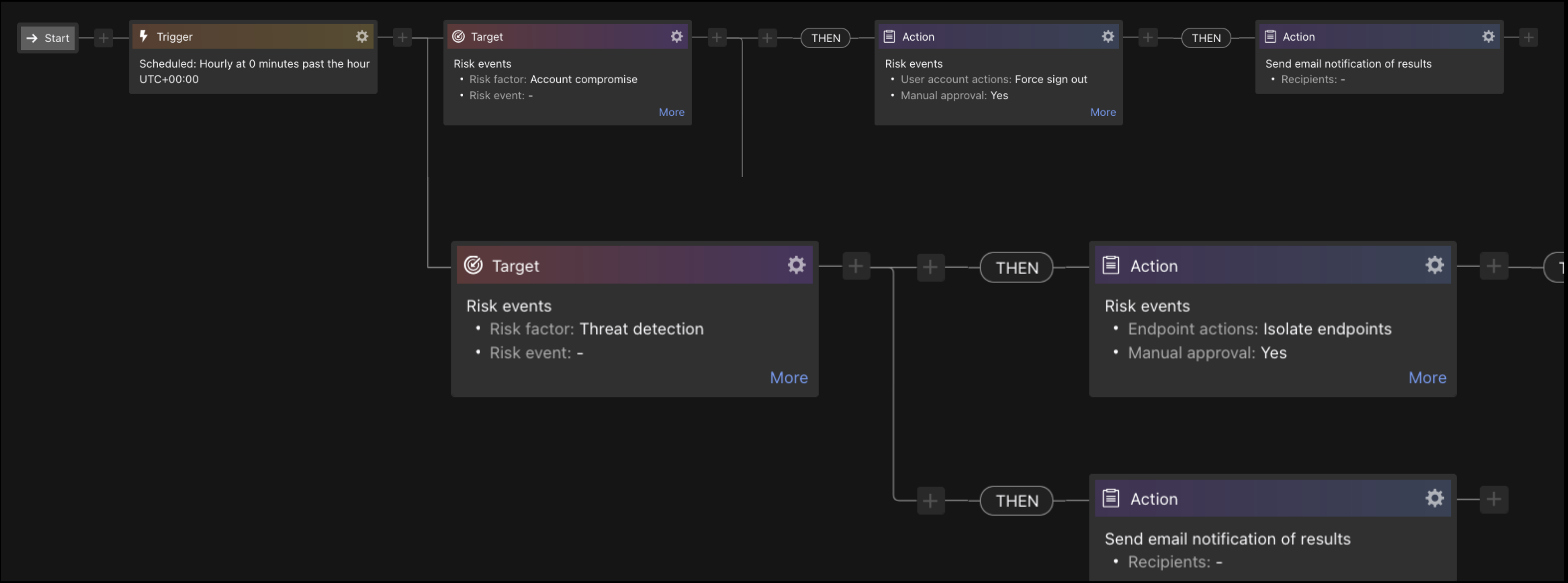
More

Send email notification of results
- Recipients: -

Send email notification of results
- Recipients: -

Control & Respuesta

Automatización



Trigger
Scheduled: Hourly at 0 minutes past the hour UTC+00:00

Target
Risk events
- Risk factor: Account compromise
- Risk event: -

More

Action
Risk events
- User account actions: Force sign out
- Manual approval: Yes

More

Action
Send email notification of results
- Recipients: -

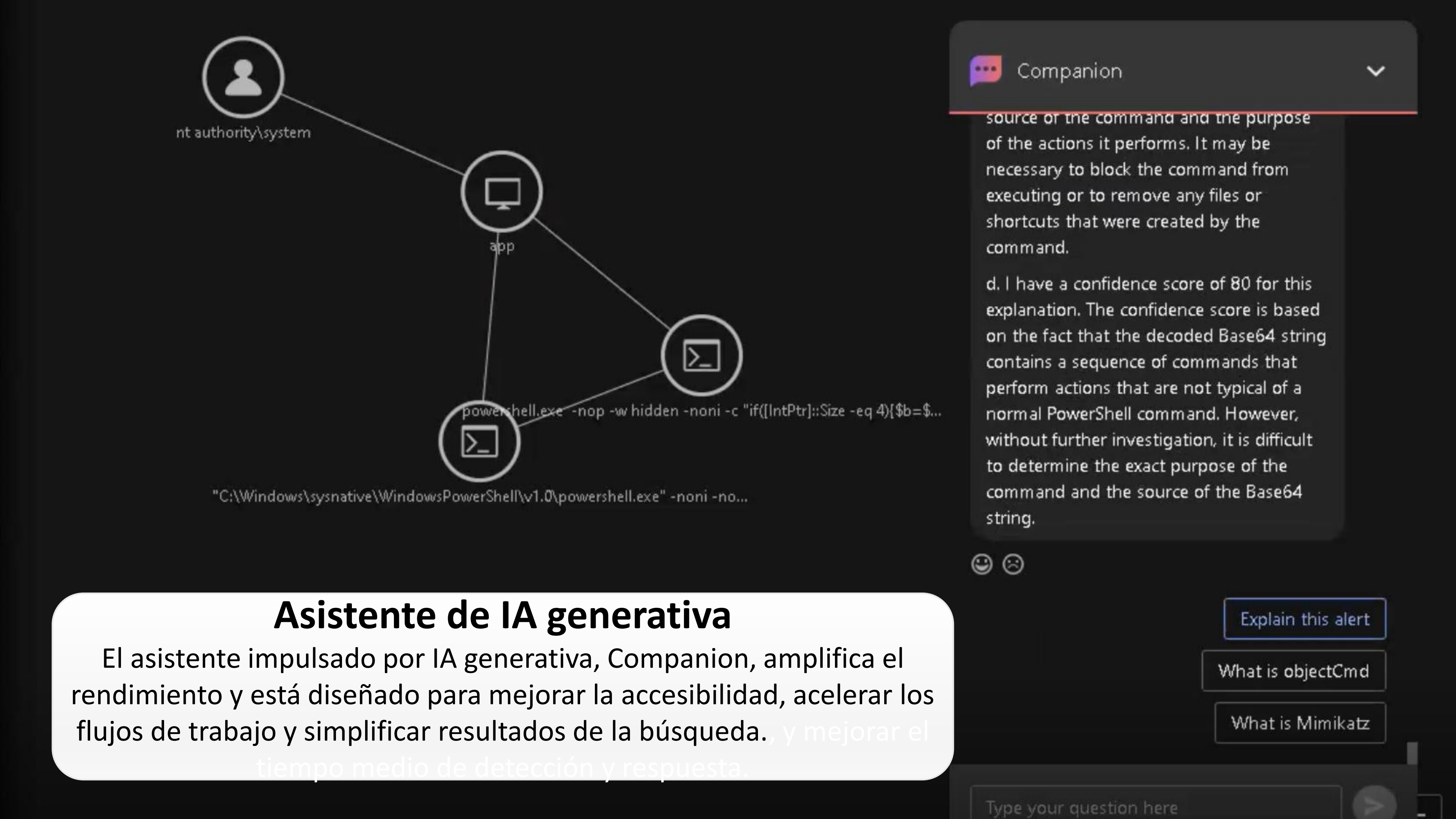
Target
Risk events
- Risk factor: Threat detection
- Risk event: -

More

Action
Risk events
- Endpoint actions: Isolate endpoints
- Manual approval: Yes

More

Action
Send email notification of results
- Recipients: -


nt authority\system
app
powershell.exe -nop -w hidden -noni -c "if([IntPtr]::Size -eq 4){$b=$...
"C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe" -noni -no...
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.

Asistente de IA generativa

El asistente impulsado por IA generativa, Companion, amplifica el rendimiento y está diseñado para mejorar la accesibilidad, acelerar los flujos de trabajo y simplificar resultados de la búsqueda., y mejorar el tiempo medio de detección y respuesta.

Integración

Expansiva

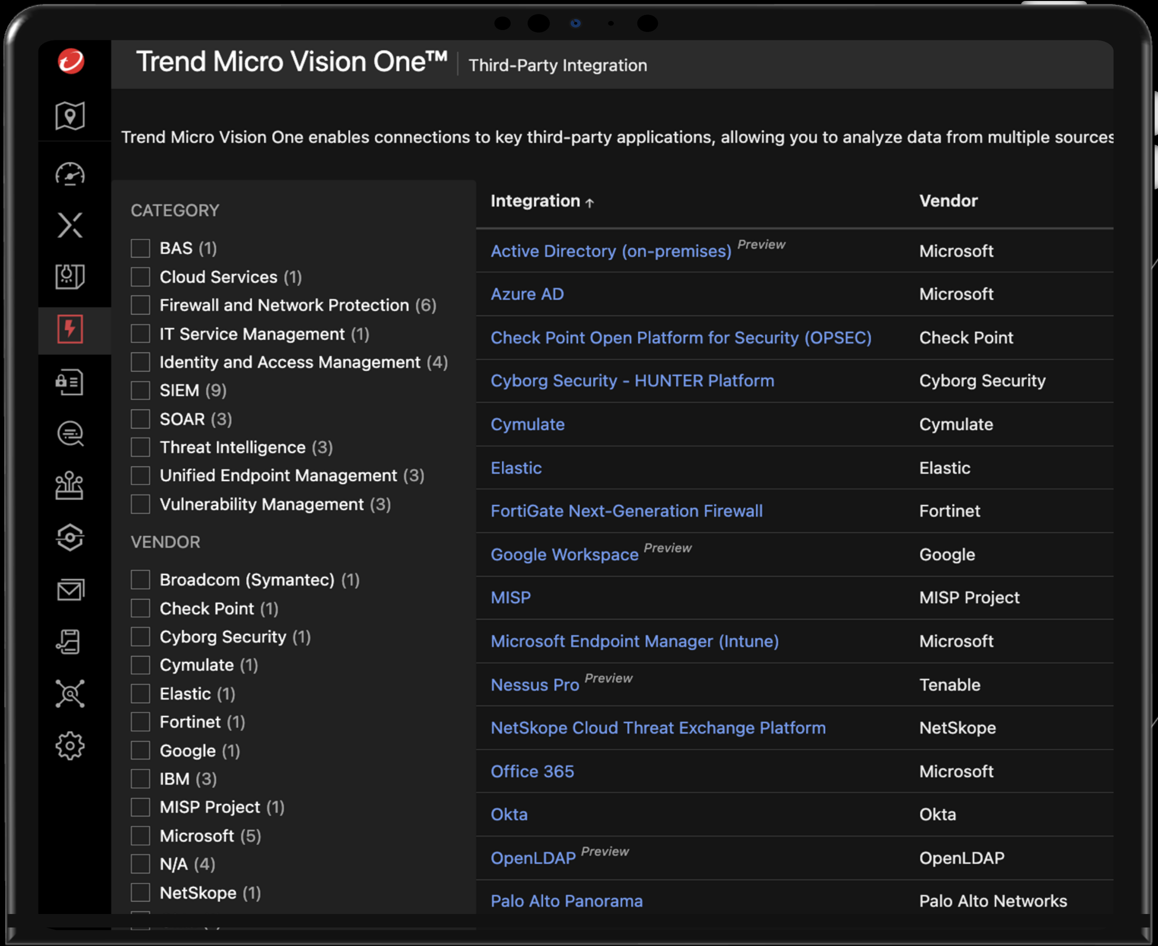
Con Terceros

IT, OT e IoT

(Industria,

Smart Cities,

Hospitales...)



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

- □ 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)

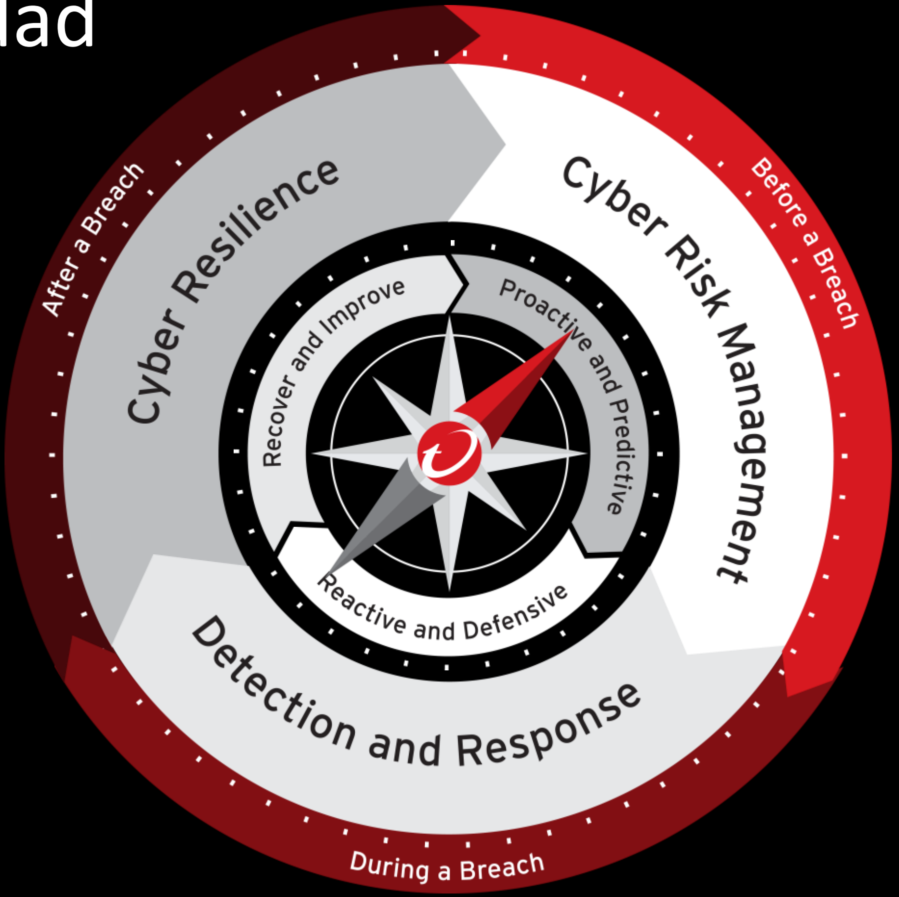
Integration ↑	Vendor
Active Directory (on-premises) *Preview*	Microsoft
Azure AD	Microsoft
Check Point Open Platform for Security (OPSEC)	Check Point
Cyborg Security - HUNTER Platform	Cyborg Security
Cymulate	Cymulate
Elastic	Elastic
FortiGate Next-Generation Firewall	Fortinet
Google Workspace *Preview*	Google
MISP	MISP Project
Microsoft Endpoint Manager (Intune)	Microsoft
Nessus Pro *Preview*	Tenable
NetSkope Cloud Threat Exchange Platform	NetSkope
Office 365	Microsoft
Okta	Okta
OpenLDAP *Preview*	OpenLDAP
Palo Alto Panorama	Palo Alto Networks

El **ABC** de la Ciberseguridad
La **brújula** del CISO

Análisis del riesgo

Bloqueo y detección del incidente

Control & Respuesta



¿Qué dicen los analistas?

Gartner

Leader in Endpoint Security
(Q3 2024)

FORRESTER

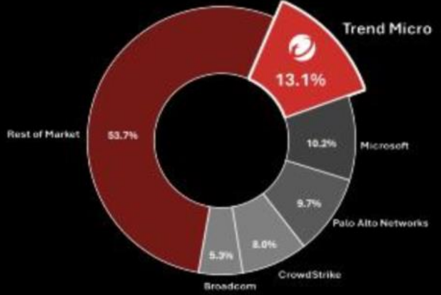
Leader in NDR
(Q2 2023)

FORRESTER

Leader in ASM
(Q3 2024)

IDC

Ranked #1 in CNAPP
Market Shares
(2023)

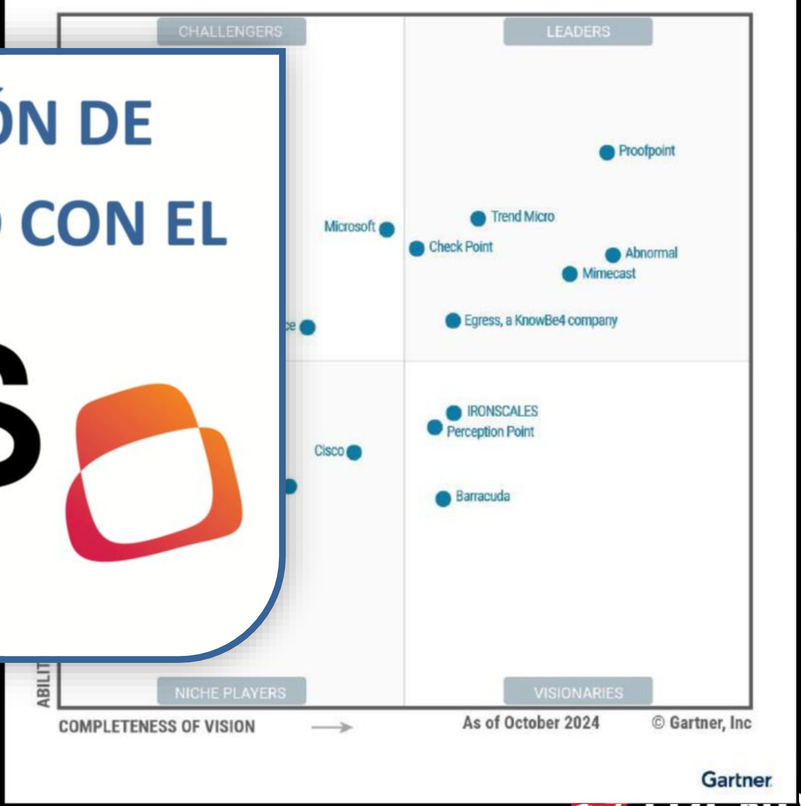


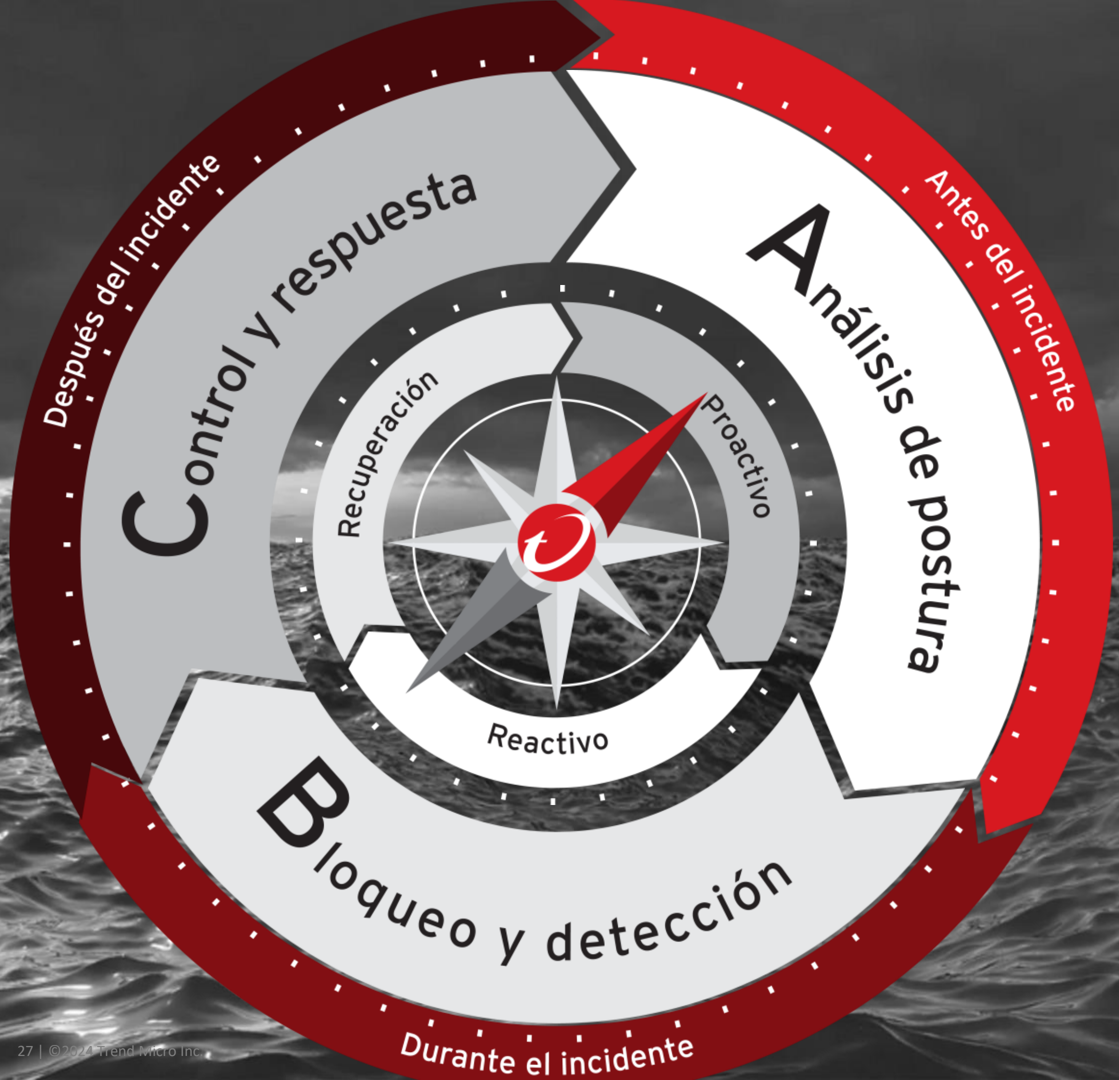
CERTIFICACIÓN DE CONFORMIDAD CON EL

_ens
Esquema Nacional de
Seguridad

Magic Quadrant

Figure 1: Magic Quadrant for Email Security Platforms





¿Dudas?

TREND MICRO

Conservas Guillén

Tu Podcast de ciberseguridad y tecnología

Raúl Guillén

Evangelizador de Estrategias de Ciberseguridad

TREND MICRO