La brújula de la Ciberseguridad

Raúl Guillén

Evangelizador de Estrategias de Ciberseguridad

Profesionalización del Cibercrimen

Cybercrime as a Service

hacktivismo

+ Recursos

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.

(*) La transposición de la NIS2 se ha retrasado pendiente de fecha definitiva.

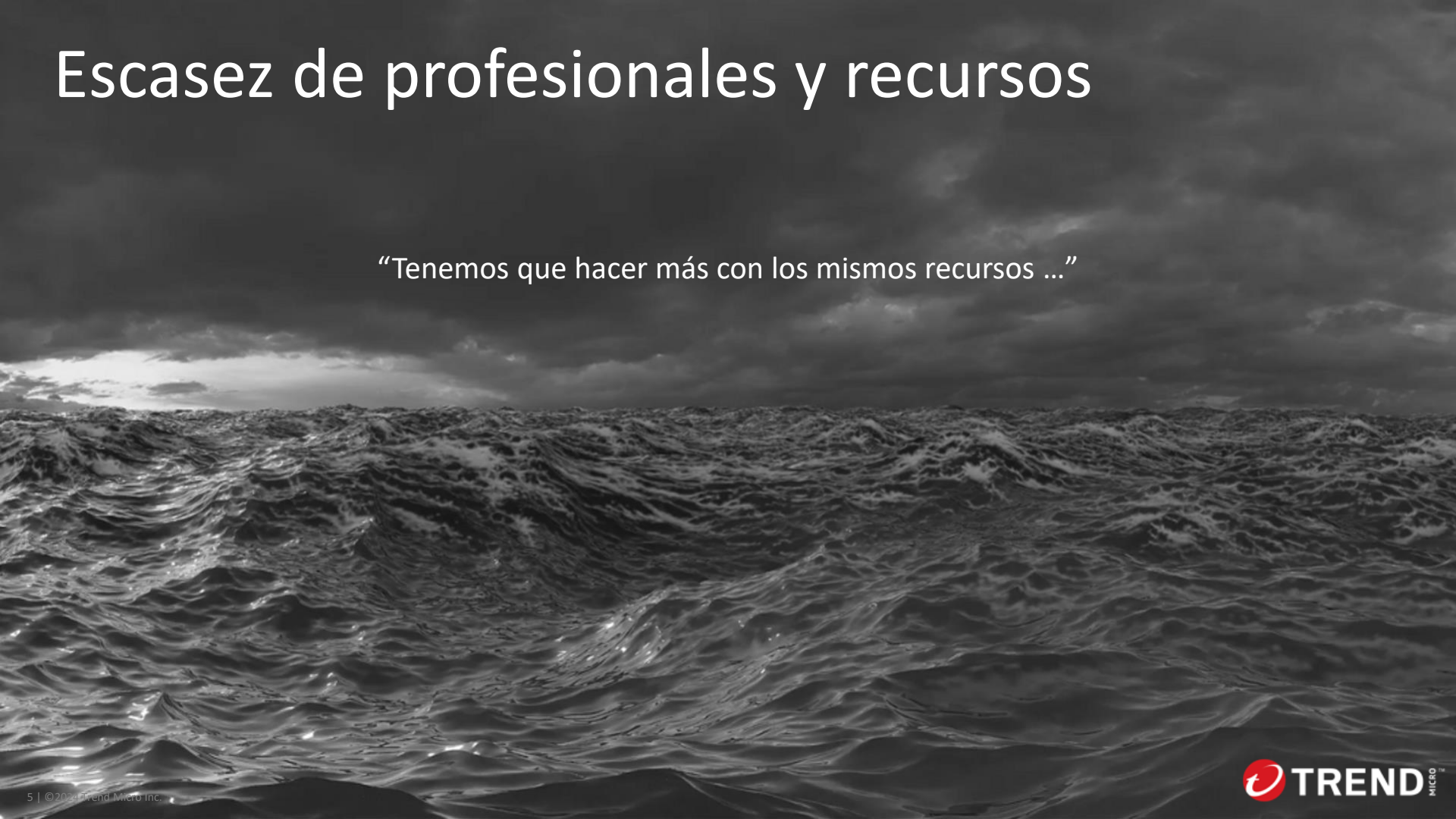
NIS 2

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 Concienciación	Seguridad en Recursos Humanos	Continuidad de Negocio	Seguridad Física

La clave de NIS2 es la gestion del riesgo

Gestión del Riesgo de Ciberseguridad

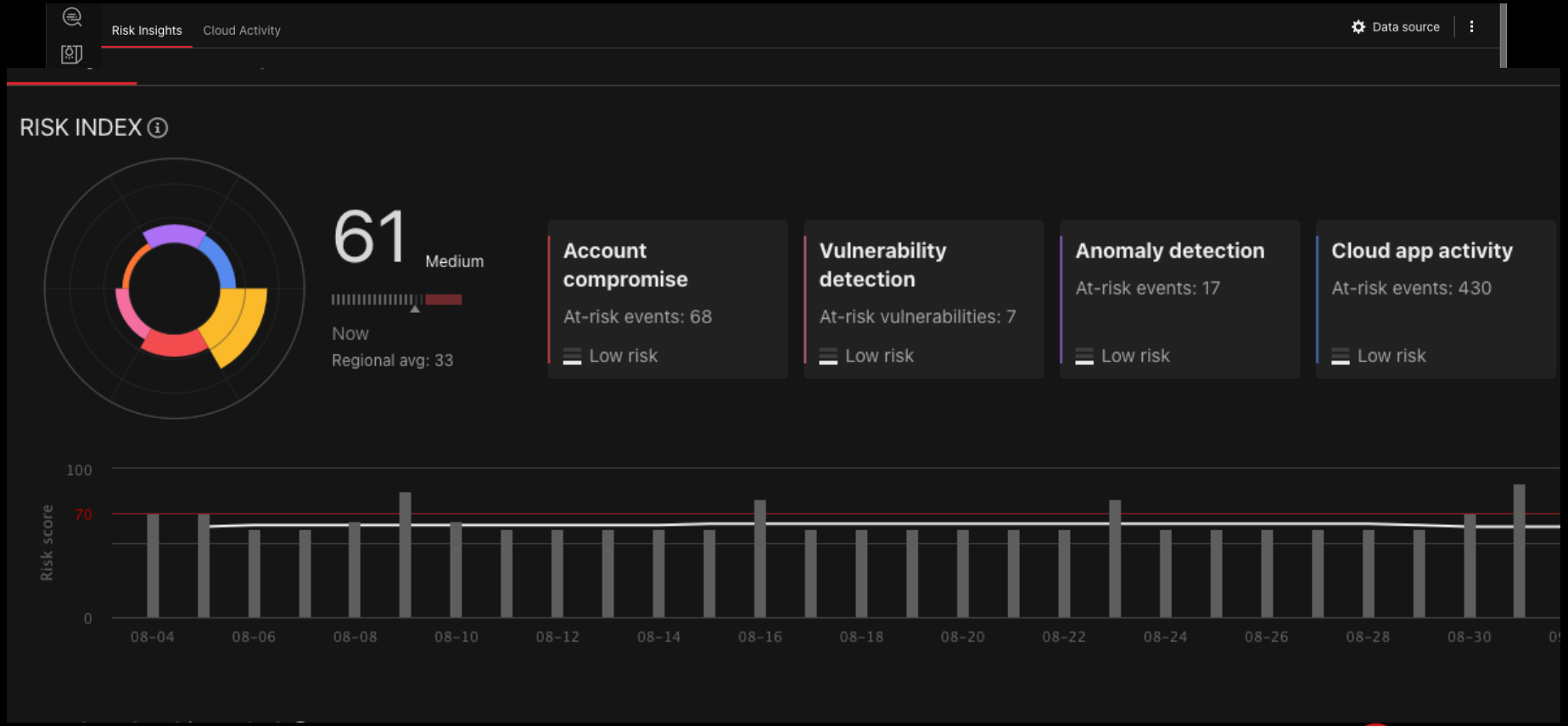
Escasez de profesionales y recursos




RISCO
INFORMATION SECURITY
RISC2
NIS2
CHIEF INFORMATION SECURITY OFFICER
RISCO
NIS2
NIS2
NIS2
TREND MICRO

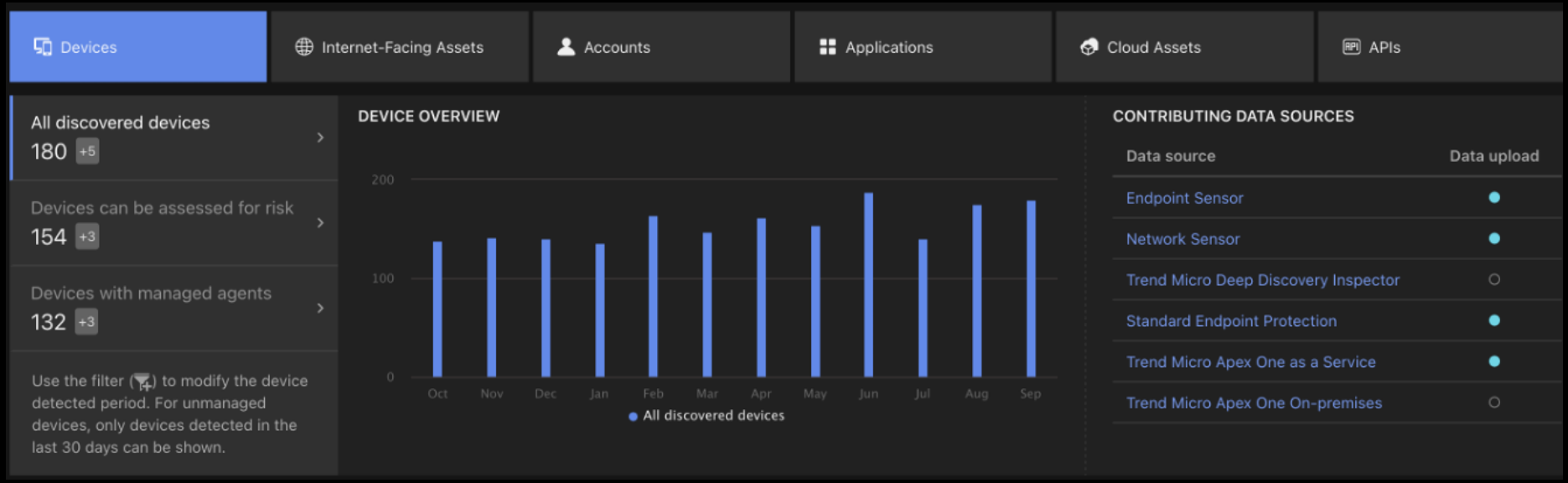

Después del incidente
Antes del incidente
Durante el incidente
Control y respuesta
Análisis de postura
Bloqueo y detección
Recuperación
Proactivo
Reactivo

Posture Management. Análisis



Posture Management. Análisis

Visibilidad



Usuarios, Infraestructuras, Aplicaciones y Datos

Posture Management. Análisis

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

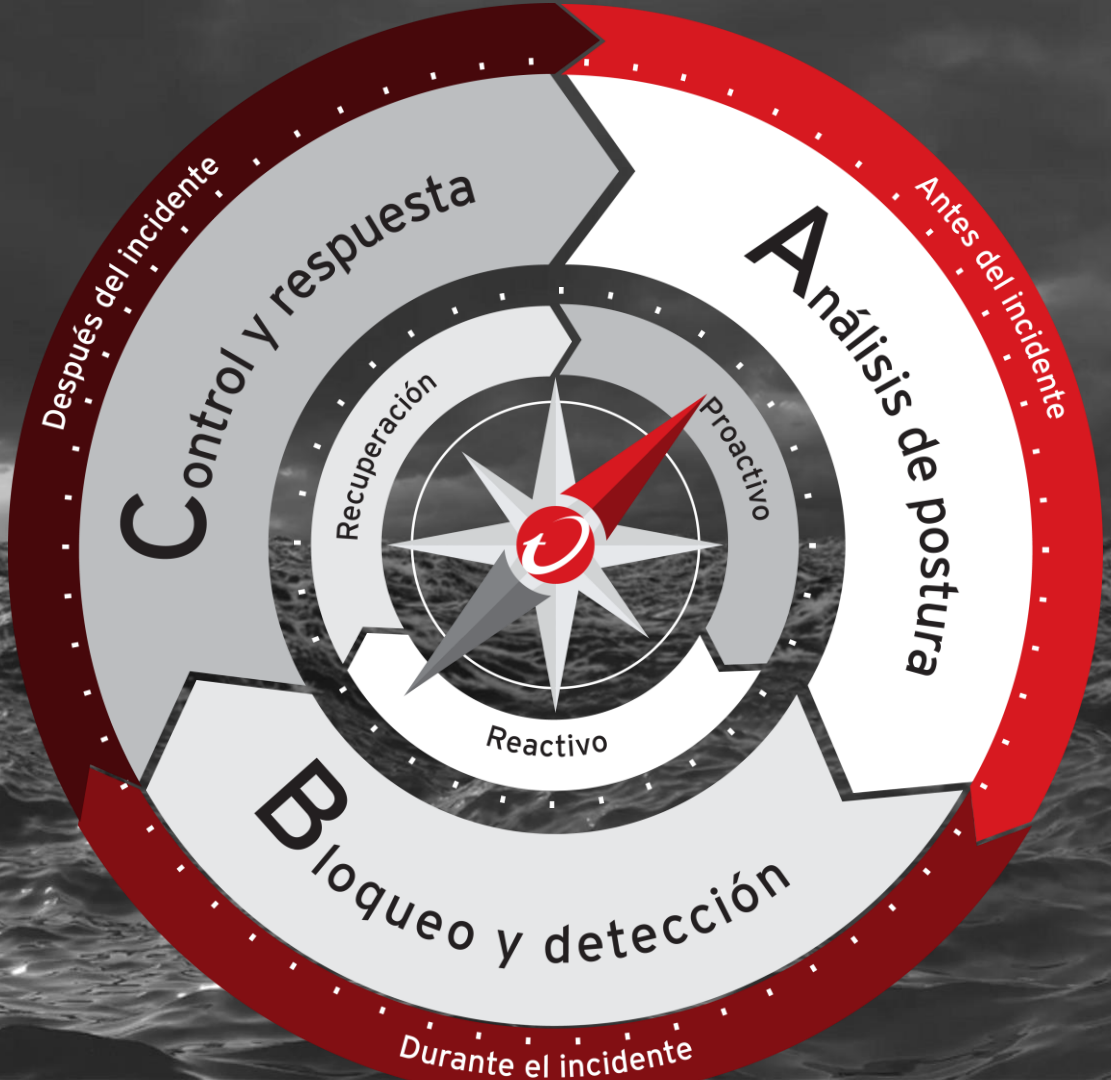
Identity Threat Detection and Response (ITDR)

- 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

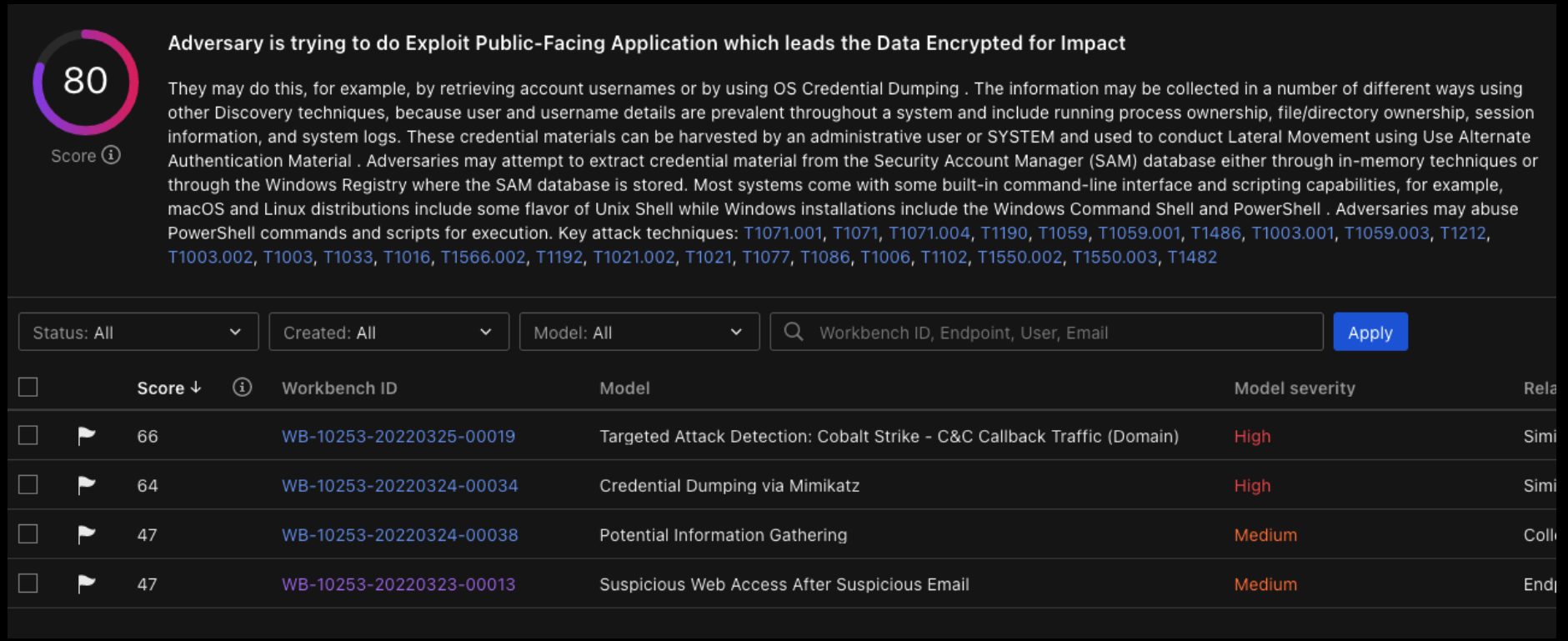
- **Endpoint**
- **Email**
- **SaaS Apps**
- **Web Traffic**
- IAM
- Network

Coste = Cómo x Cuándo

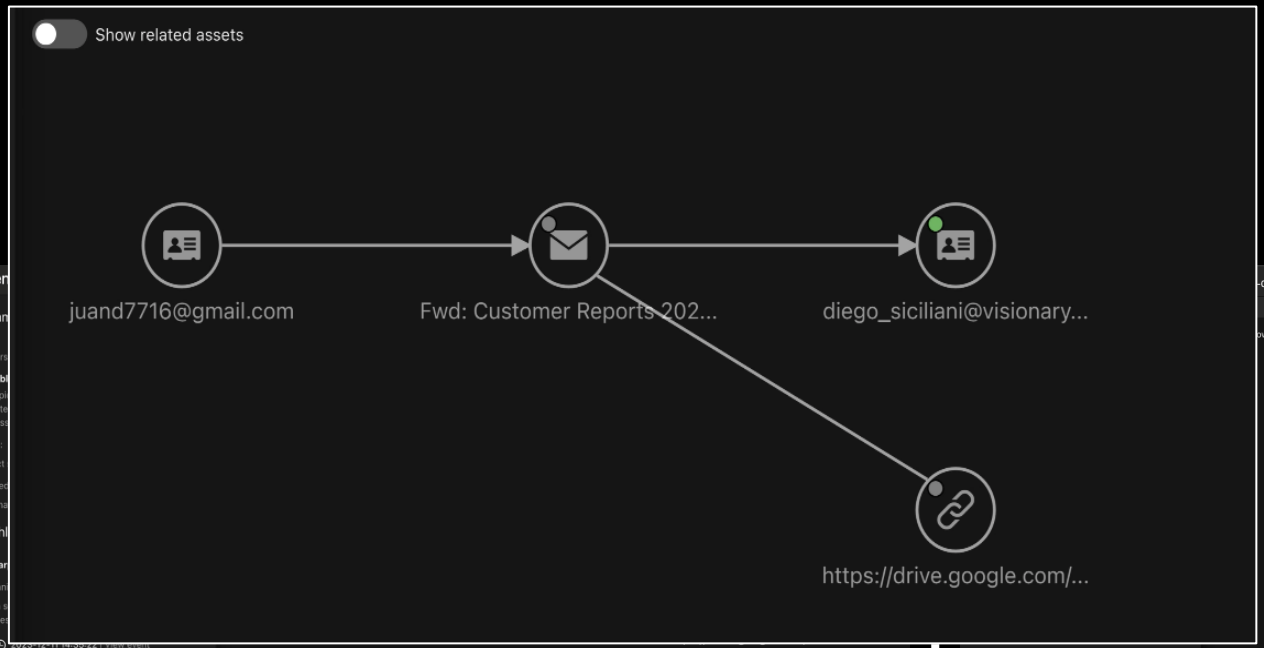

Después del incidente
Antes del incidente
Durante el incidente
Control y respuesta
Análisis de postura
Bloqueo y detección
Recuperación
Proactivo
Reactivo

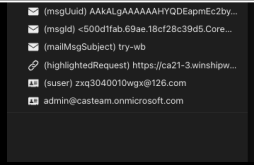
Bloqueo y detección de incidentes

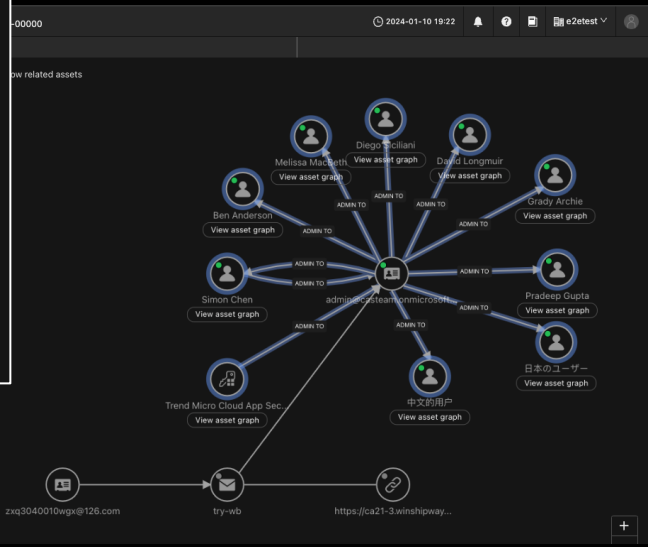
XDR



XDR



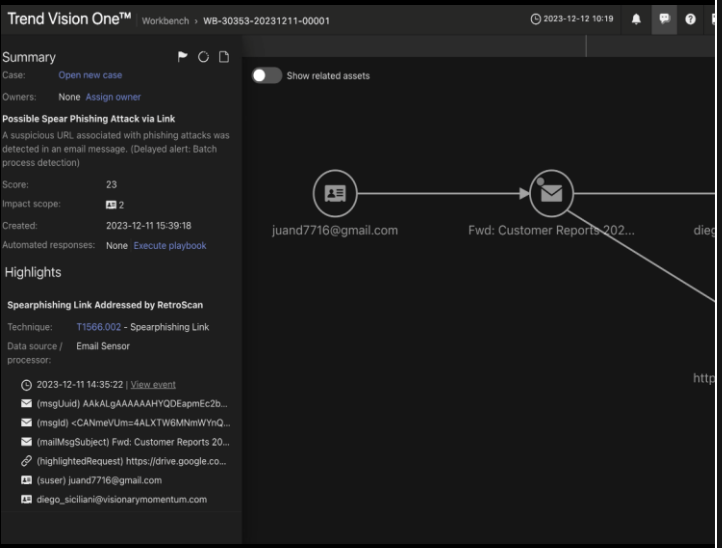


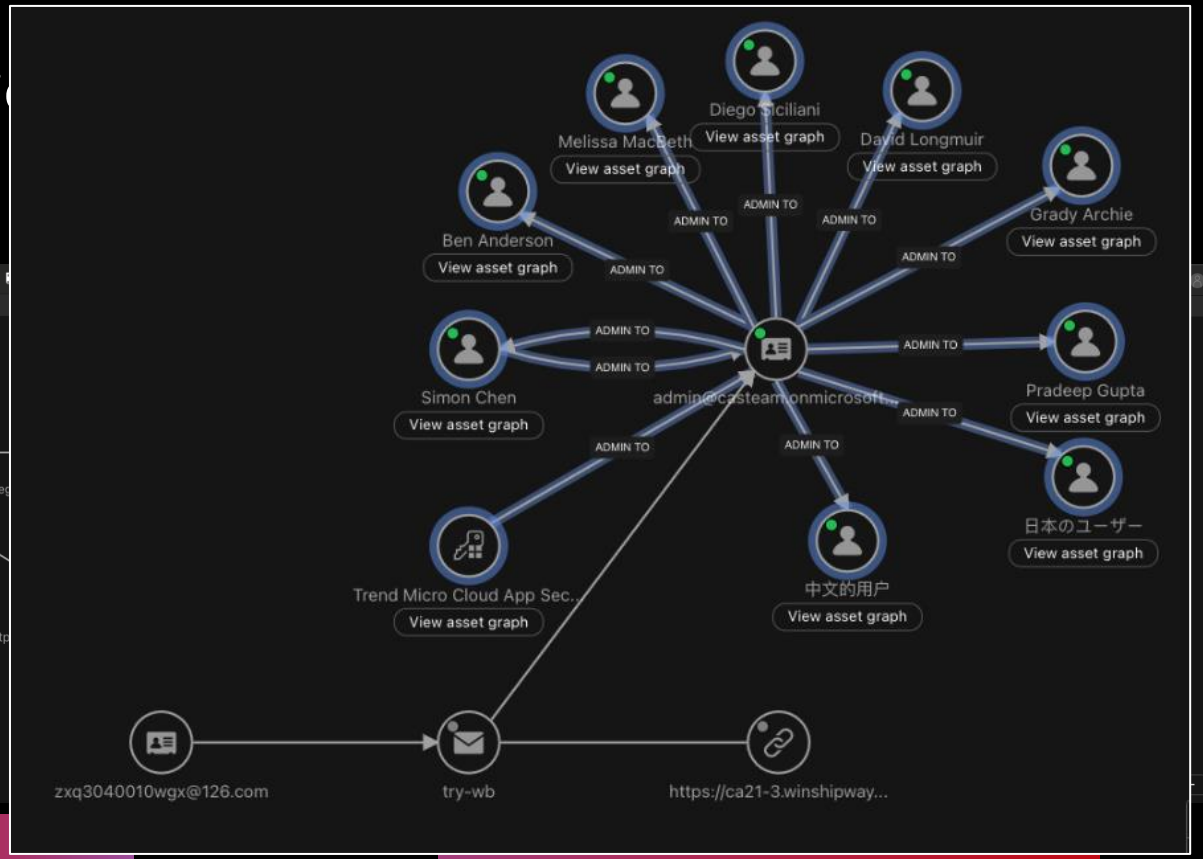


Detect Patient Zero

Threat Hunting

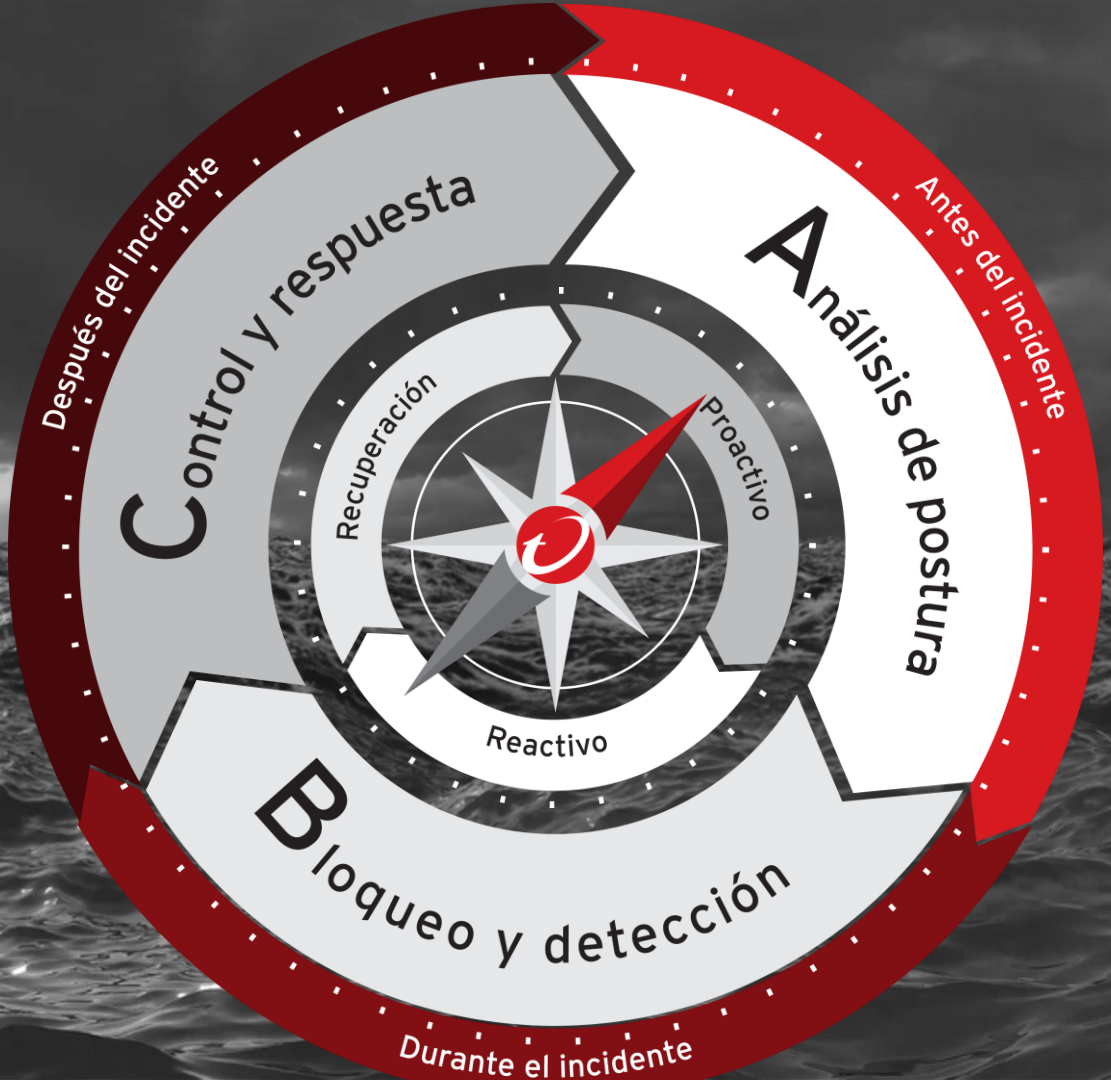
Bloqueo y detección de inci





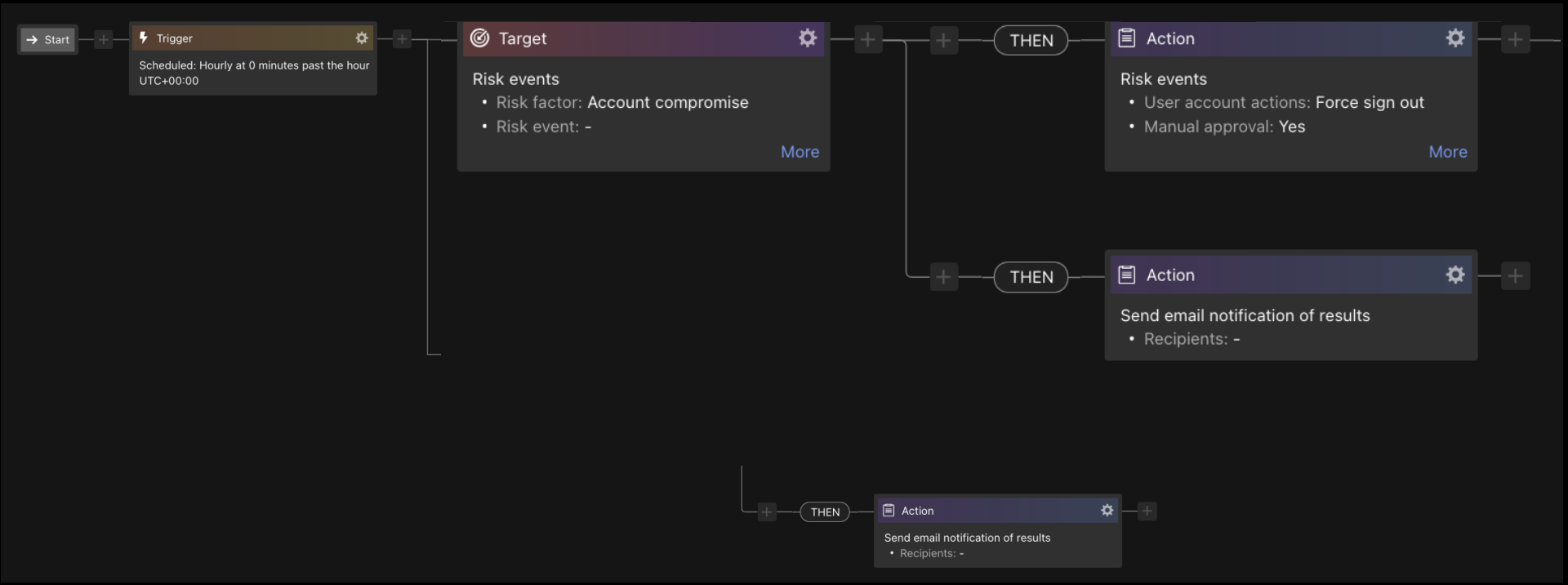
Detect Patient Zero

Threat Hunting



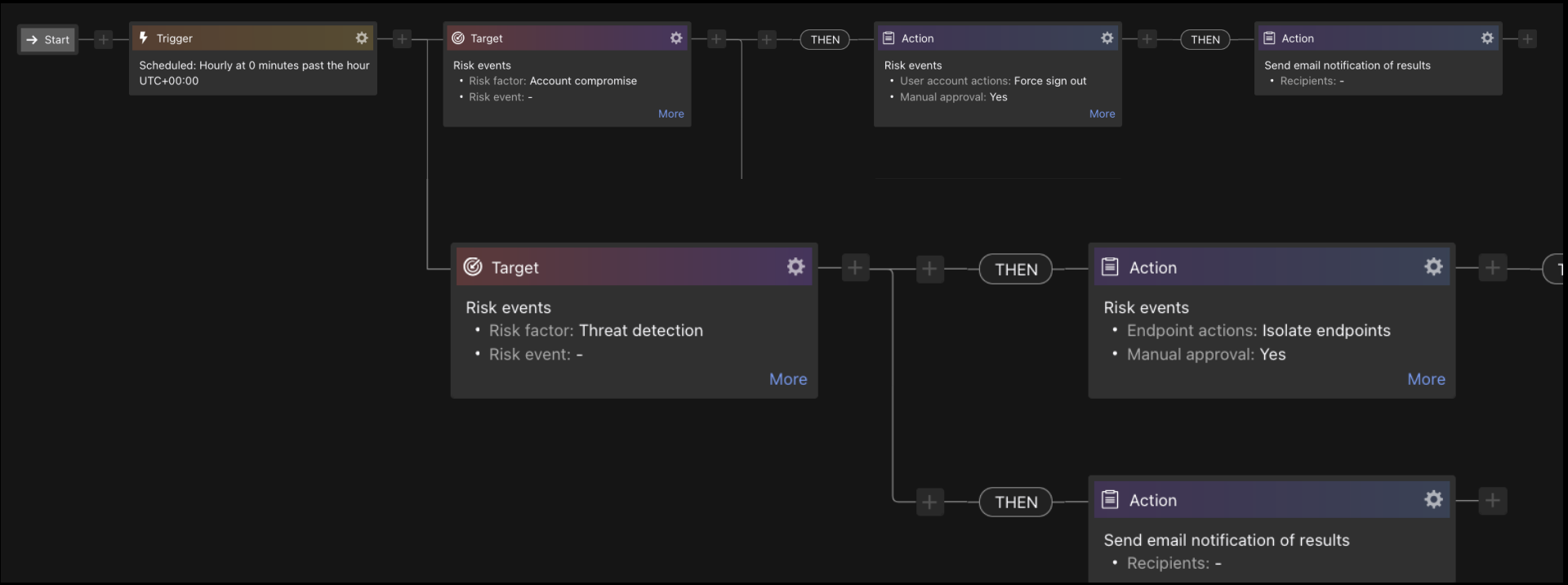
Control & Respuesta

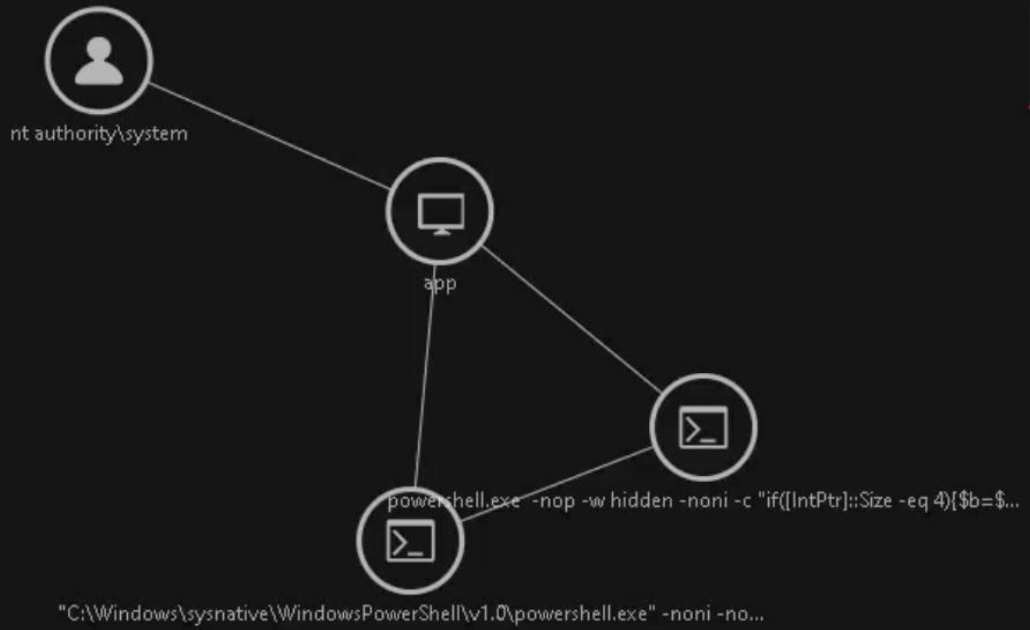
Automatización



Control & Respuesta

Automatización





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

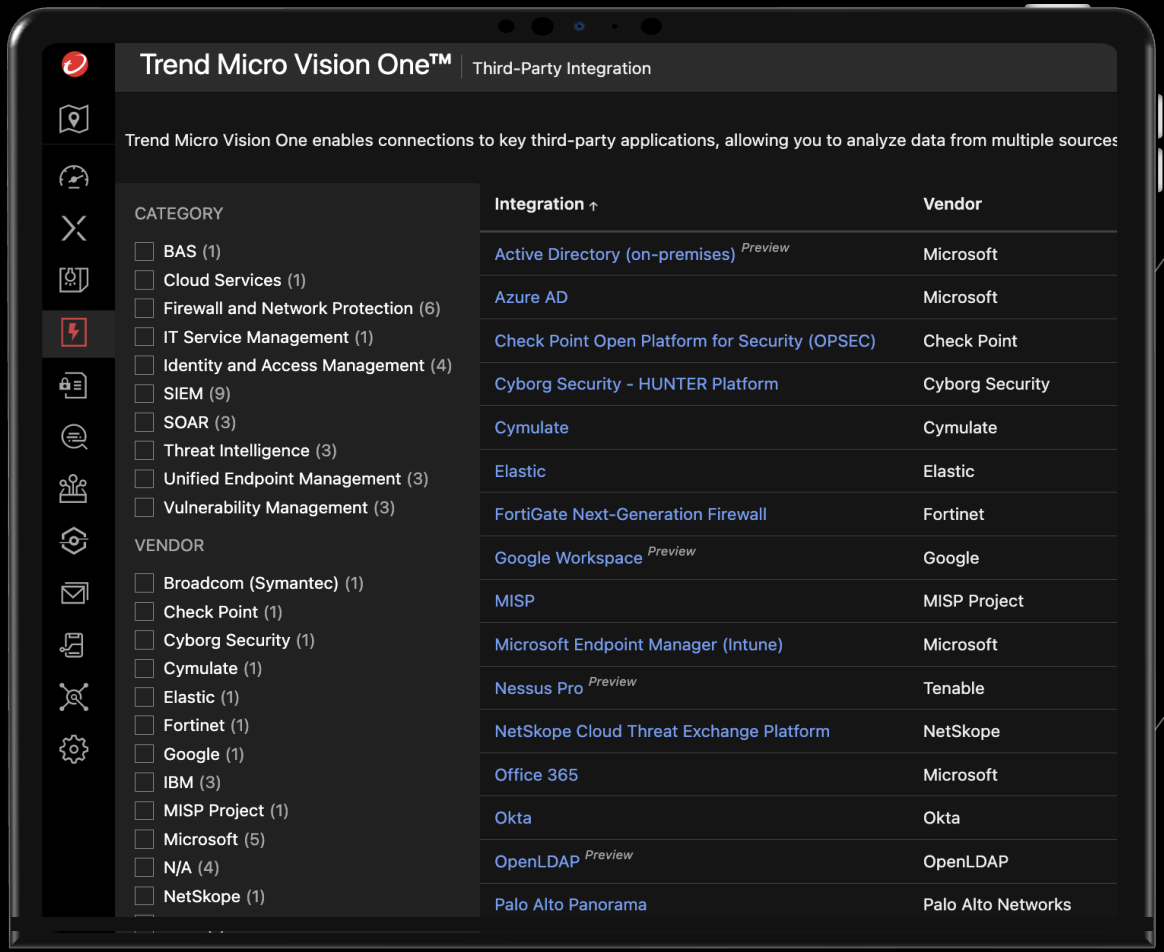
Type your question here

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 los resultados de la búsqueda de amenazas, y mejorar el tiempo medio de detección y respuesta.

Integración Expansiva Con Terceros

IT, OT e IoT (Industria, Smart Cities, Hospitales…)



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

Análisis del riesgo

Bloqueo y detección del incidente.

Control & Respuesta.

¿Dudas?

Muchas gracias!!!

Raúl Guillén

Evangelizador de Estrategias de Ciberseguridad