



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
Gestión del Riesgo	Gestión de activos y accesos	Seguridad de la cadena de suministro	Criptografía	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 gestión del riesgo

Gestión del Riesgo de Ciberseguridad

Escasez de profesionales y recursos

“Tenemos que hacer más con los mismos recursos ...”



RISCO

INFORMATION
SECURITY

RISC2

NIS2

CHIEF
INFORMATION
SECURITY
OFFICER

CYBER
SECURITY
OFFICER

RISCO
INFORMATION SECURITY

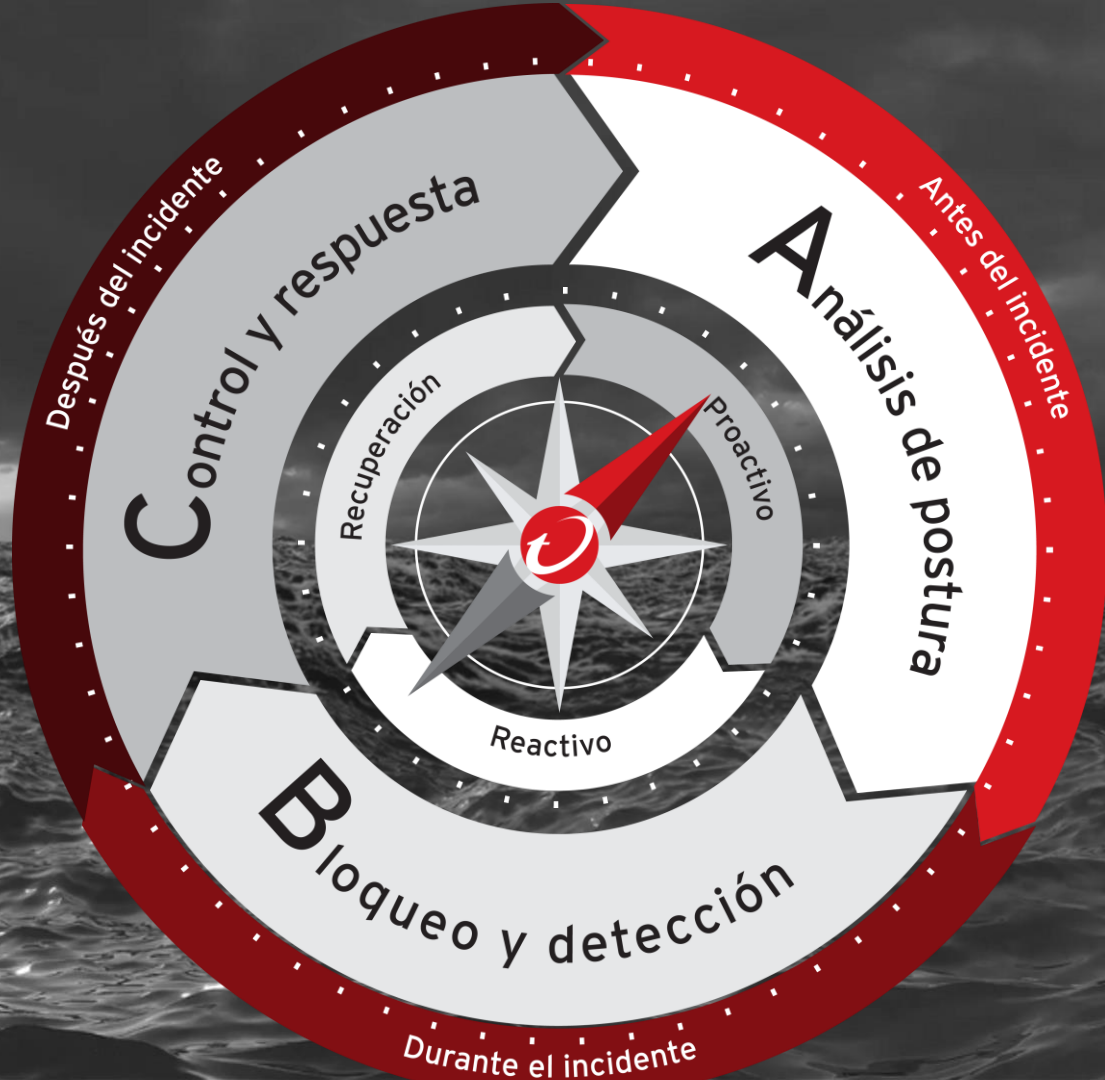
NIS2
GATAQUES

NIS2

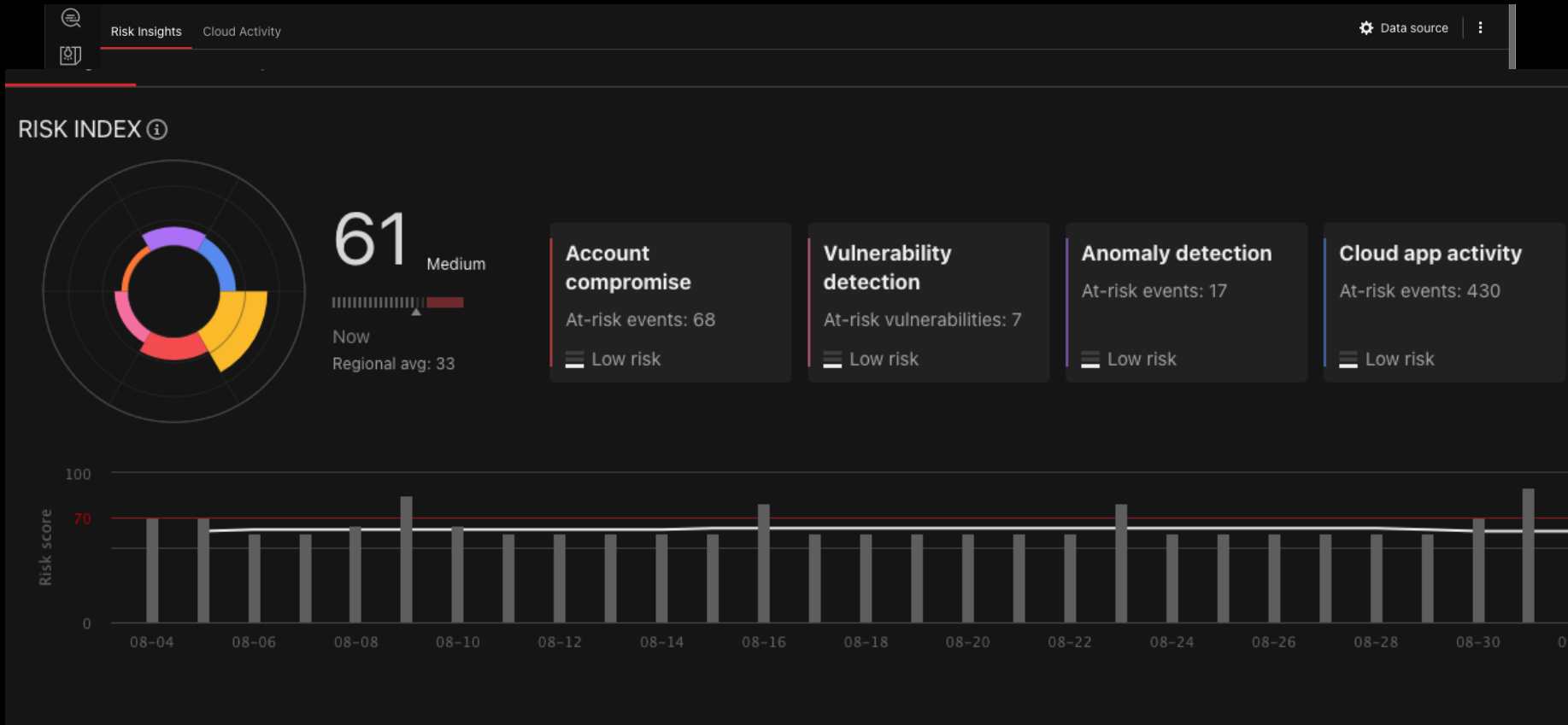
NIS2

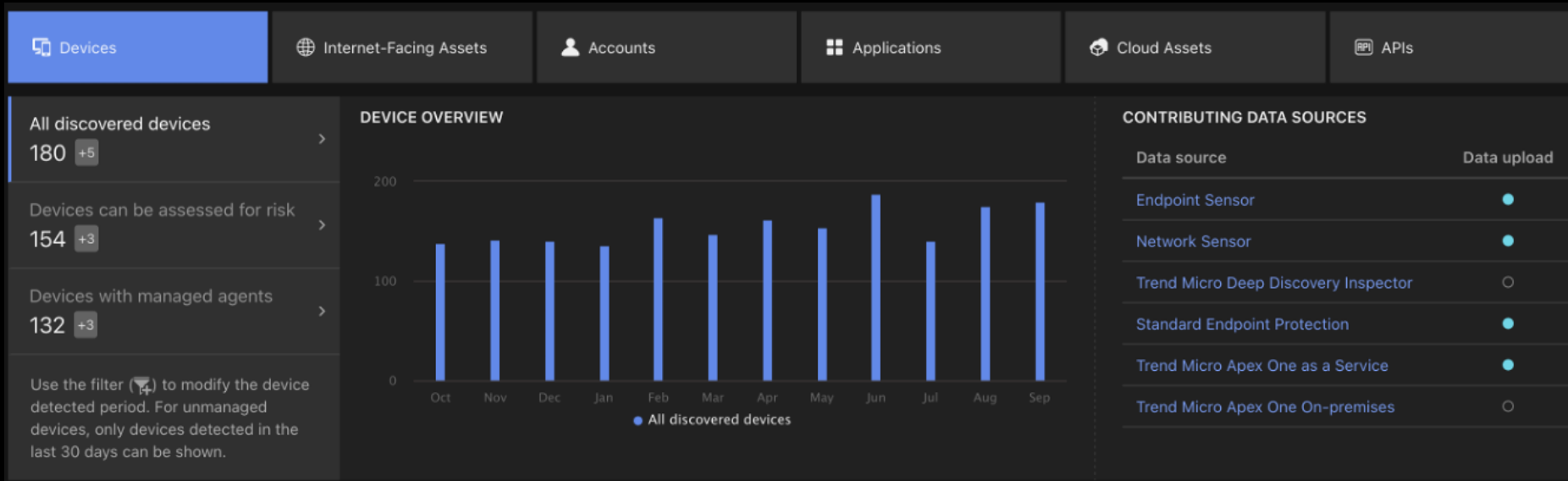


TREND
MICRO™



Posture Management. **A**nálisis





Usuarios, Infraestructuras, Aplicaciones y Datos

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

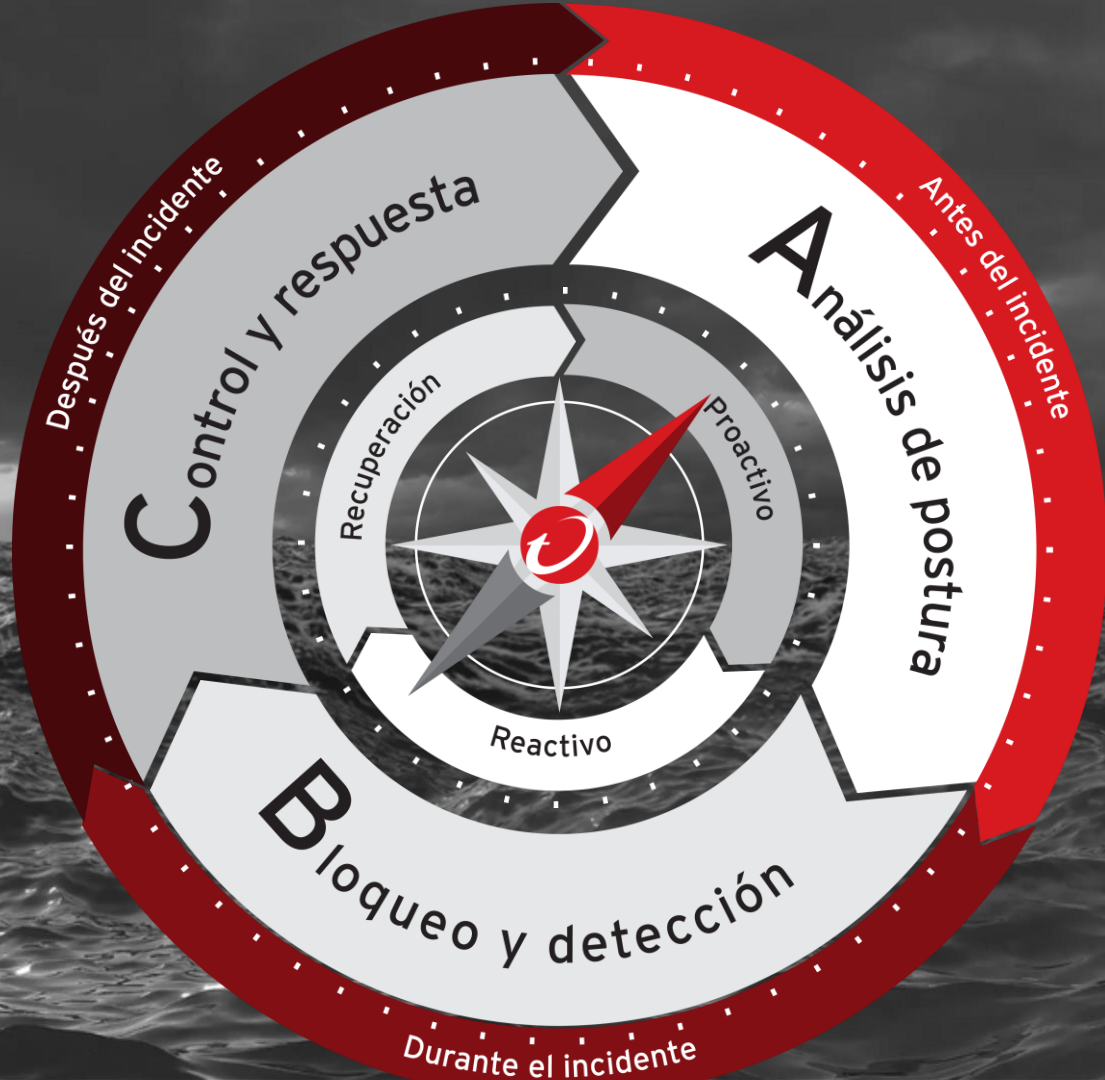


Network



Coste = Cómo x Cuándo







Score ⓘ

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

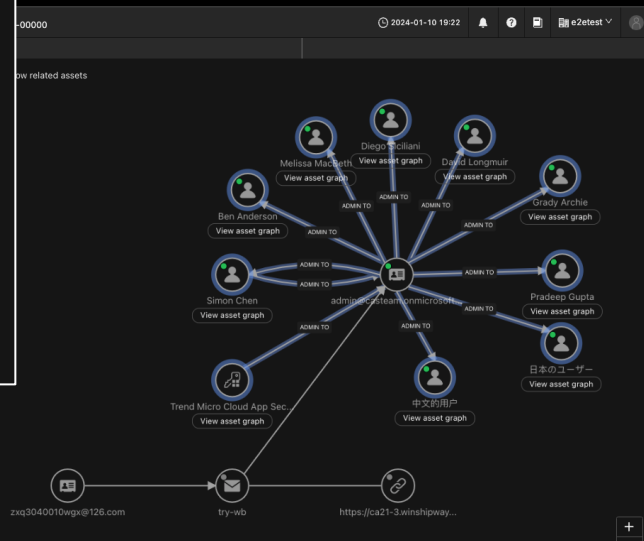
They may do this, for example, by retrieving account usernames or by using OS Credential Dumping . The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, 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

<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

Show related assets

XDR



Detect Patient Zero

Threat Hunting

Bloqueo y detección de inci

Trend Vision One™ Workbench > WB-30353-20231211-00001 2023-12-12 10:19

Summary

Case: Open new case Show related assets

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

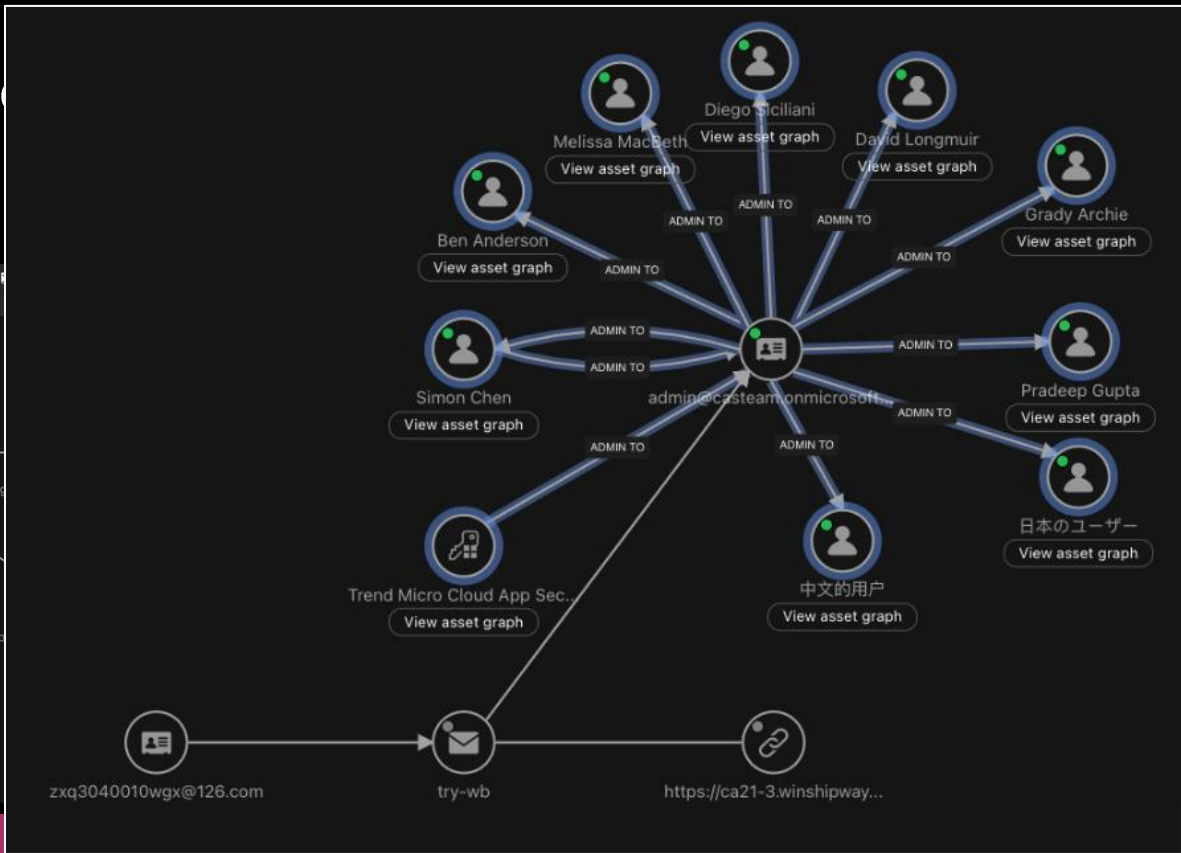
Spearphishing Link Addressed by RetroScan

Technique: T1566.002 - Spearphishing Link

Data source / Email Sensor processor:

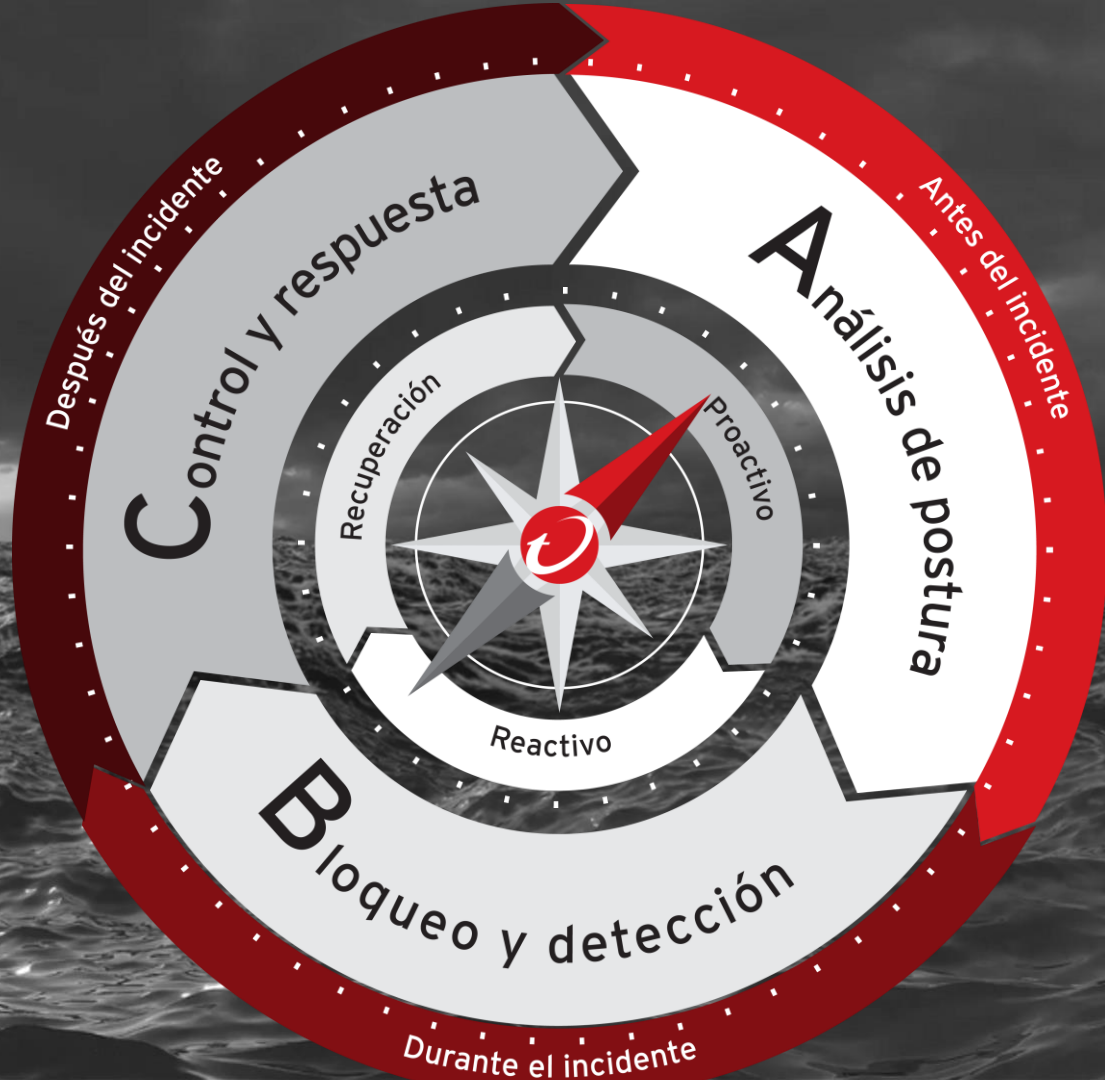
- 2023-12-11 14:35:22 | View event
- (msgUuid) AAAALgAAAAAHYQDEapmEc2b...
- (msgId) <CANmevUm=4ALXTW6MnmWYnQ...
- (mailMsgSubject) Fwd: Customer Reports 20...
- (highlightedRequest) https://drive.google.co...
- (user) juand7716@gmail.com
- diego_siciliani@visionarymomentum.com

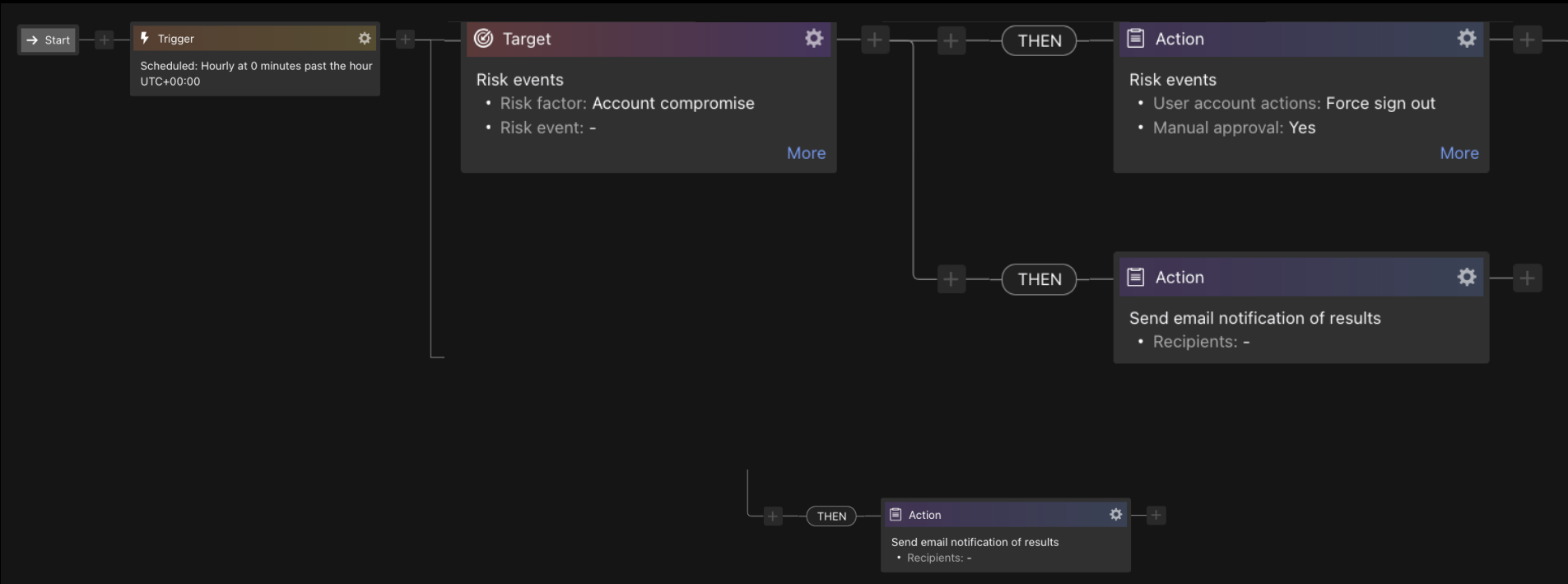
juand7716@gmail.com → Fwd: Customer Reports 202...

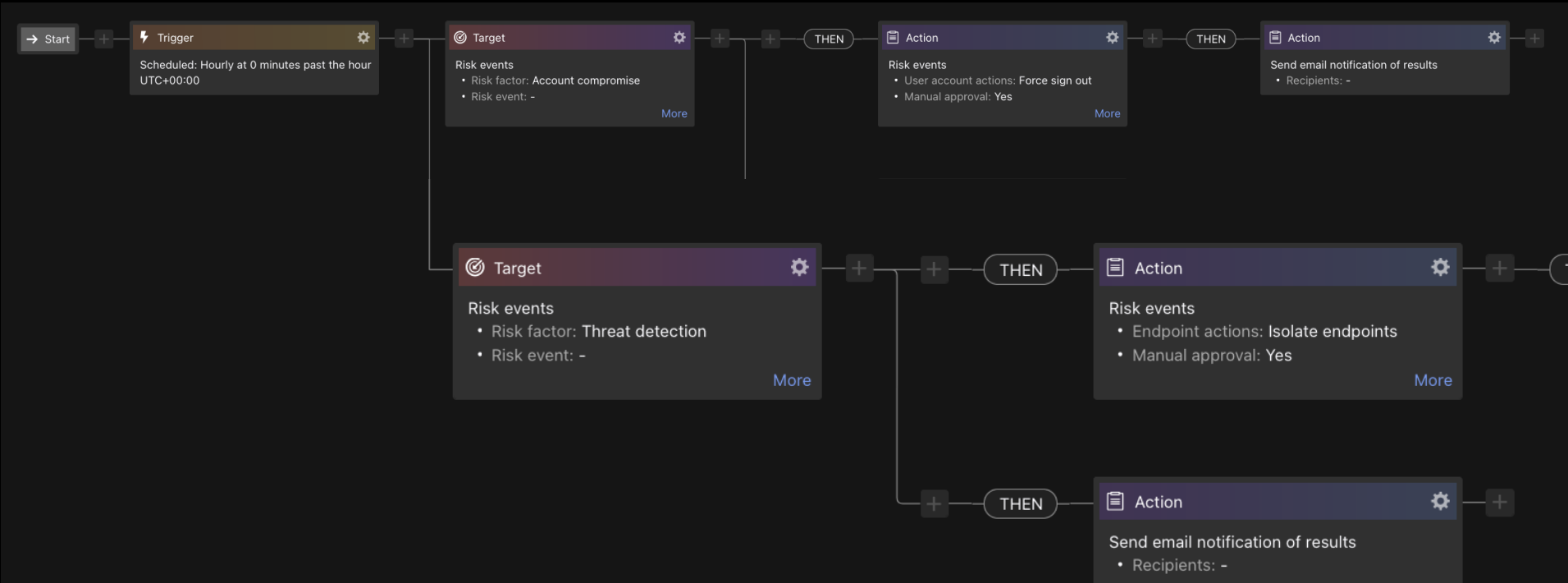


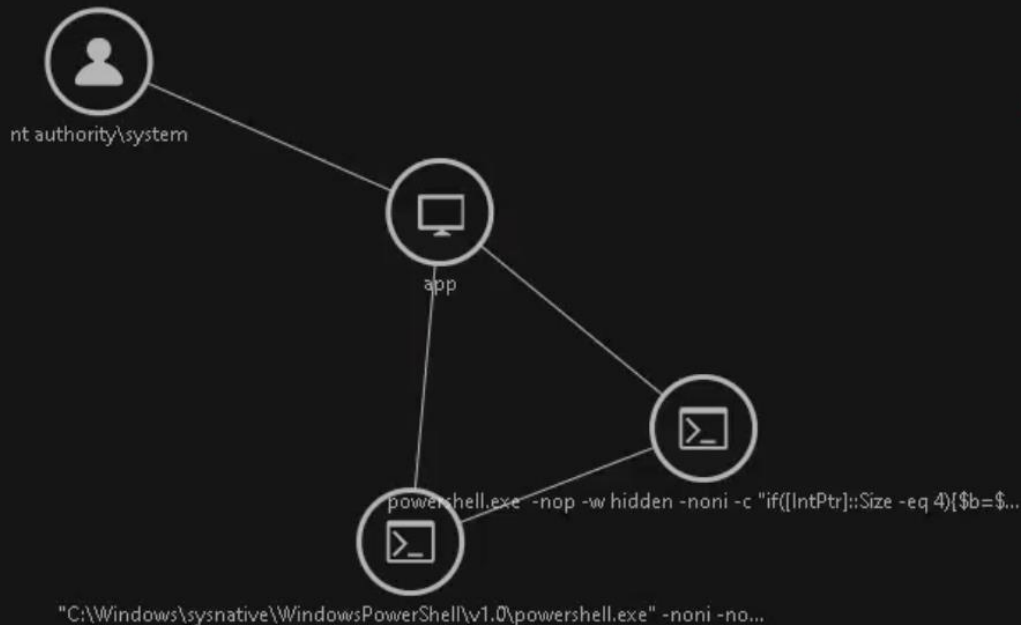
Detect Patient Zero

Threat Hunting









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.

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

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	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

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)



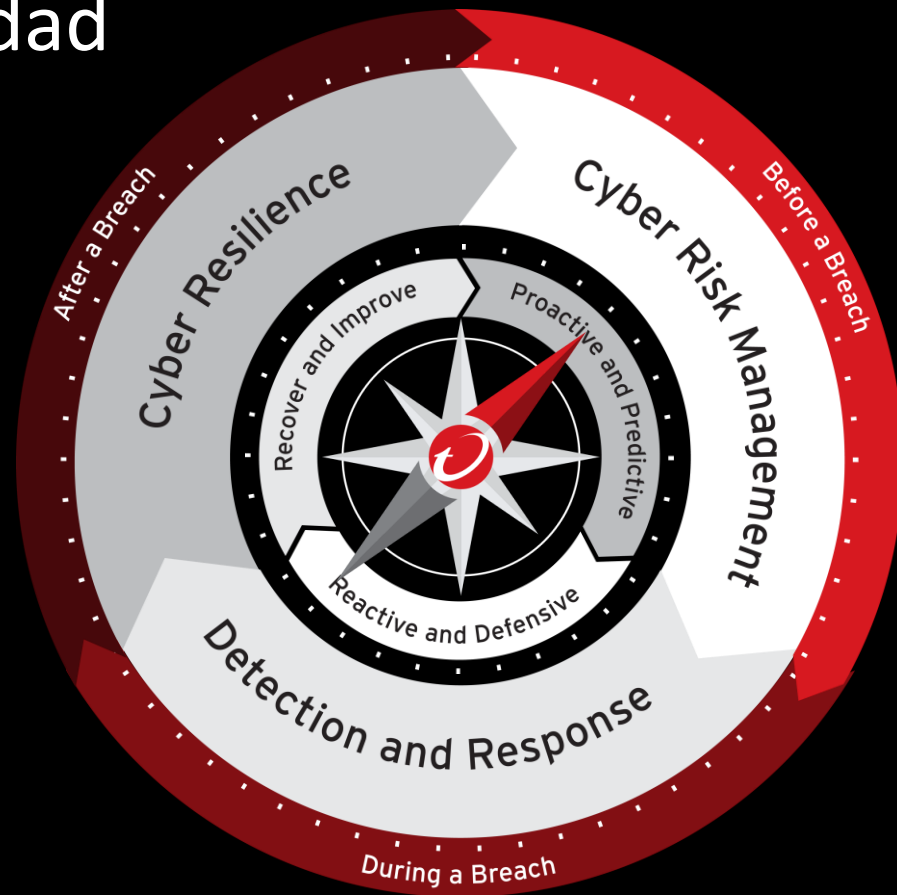
El ABC de la Ciberseguridad

La brújula del CISO

Análisis del riesgo

Bloqueo y detección del incidente.

Control & Respuesta.





¿Dudas?



Muchas gracias!!!



Raúl Guillén

Evangelizador de Estrategias de Ciberseguridad

