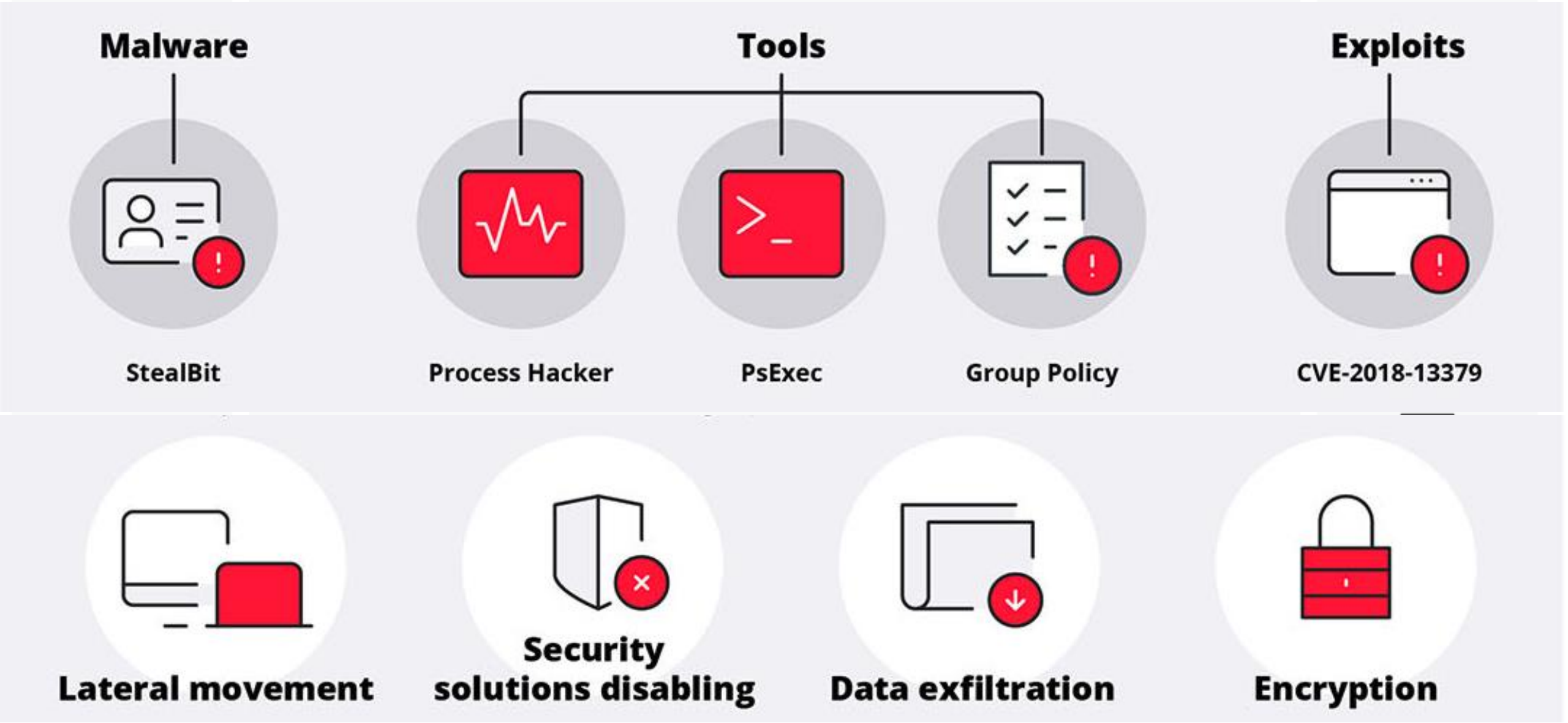
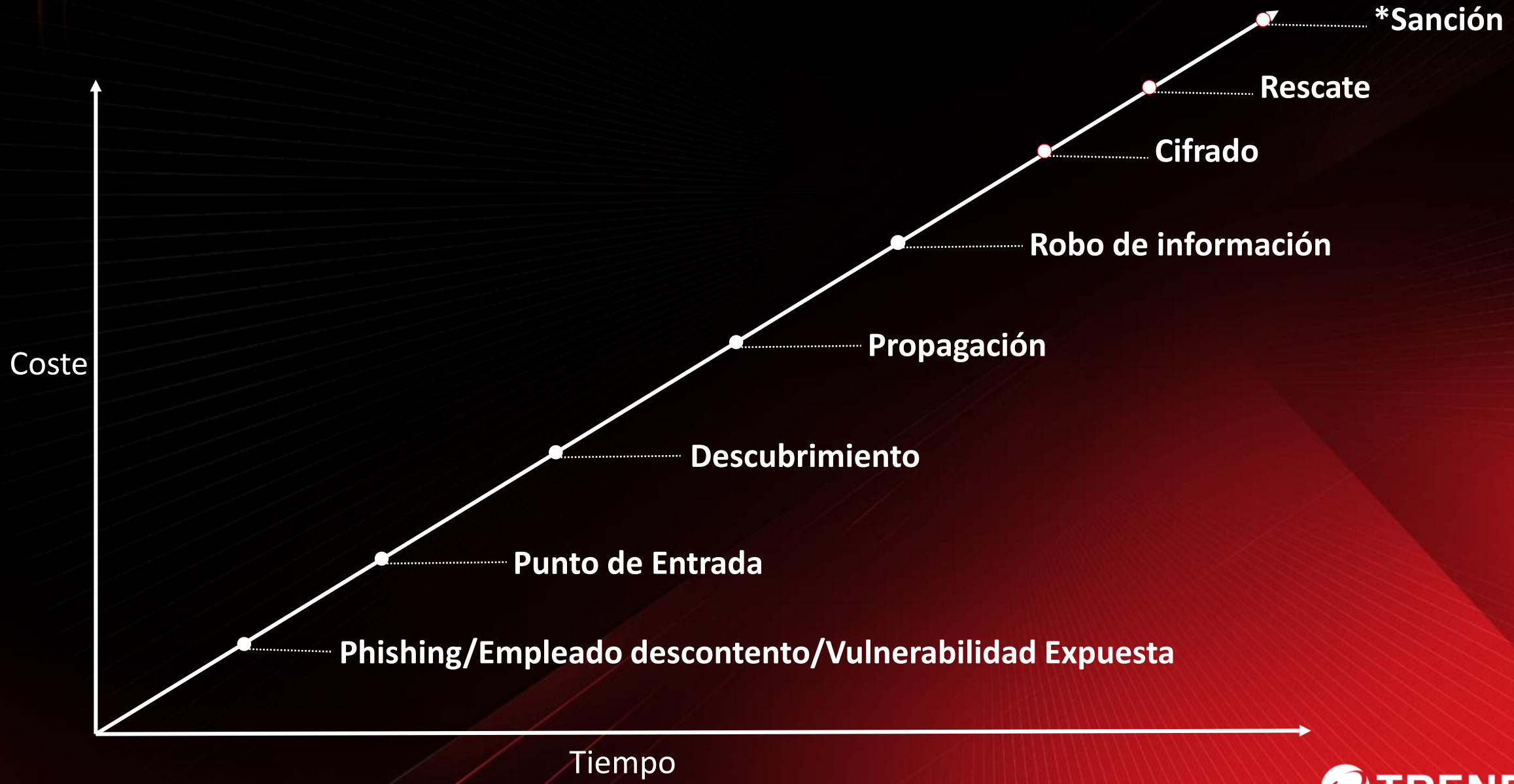
Uno para Todos
Todos para Uno

José de la Cruz González

Technical Director - Iberia


Malware
Tools
Exploits
StealBit
Process Hacker
PsExec
Group Policy
CVE-2018-13379
Lateral movement
Security solutions disabling
Data exfiltration
Encryption

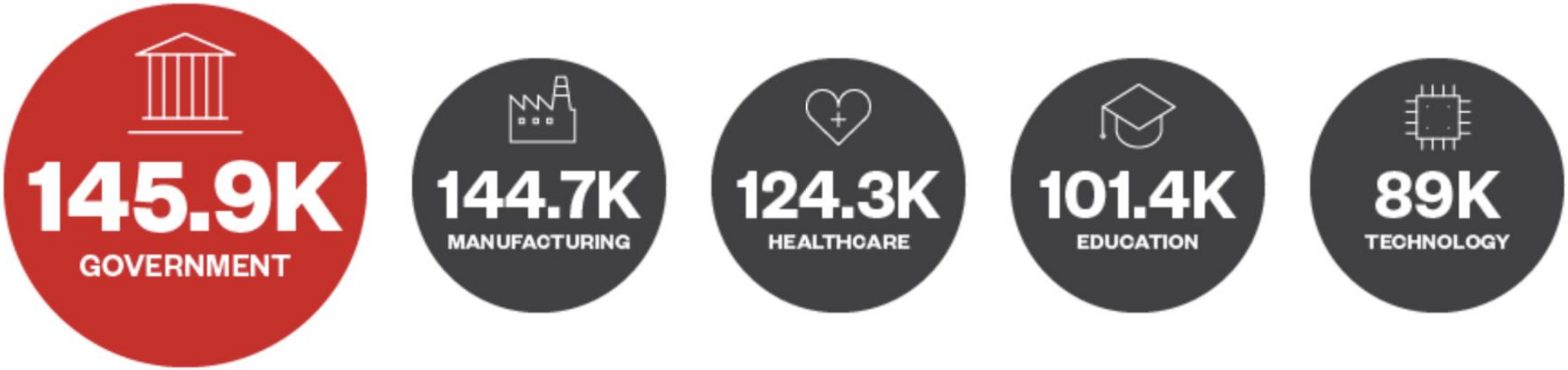
Coste = Cómo x Cuándo



Top 5 Industries

affected by malware campaigns

In the first half of 2023, malware campaigns targeted government organizations the most with 145,912 detections.



https://bit.ly/TrendMicroReport23

TREND MICRO

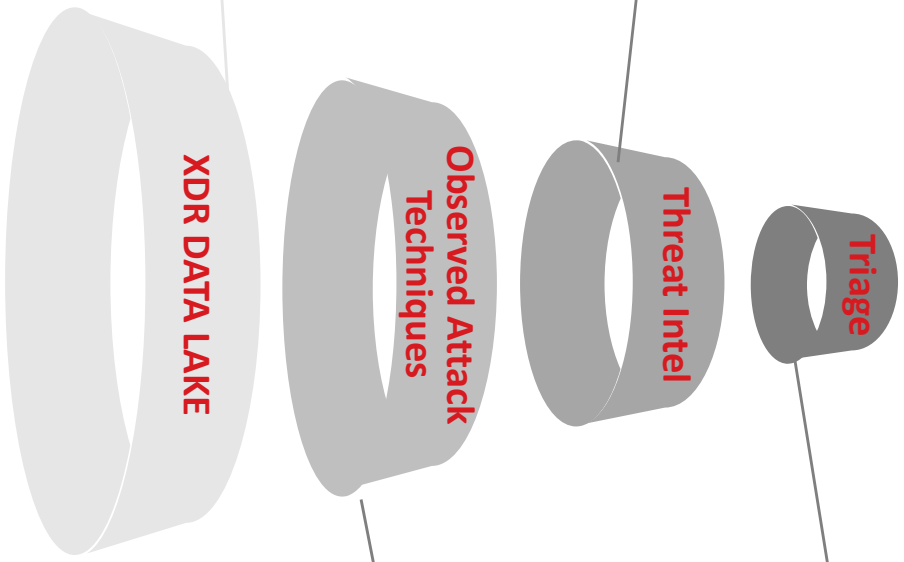
XDR - Detección temprana

- Endpoint
- Email
- Identity
- Cloud
- Network
- OT
- Data Access
- 3rd-Party

Activity Data Detections

XDR Data Lake

Detection and Activity Logs at Cloud Storage



Threat Intel Collaboration

Latest Threat campaigns (IOCs & STIX)

Few: High Fidelity Alerts

SIEM & SOC Analyst

Triage & Workbench

Detections – MITRE mapping

Líderes en XDR

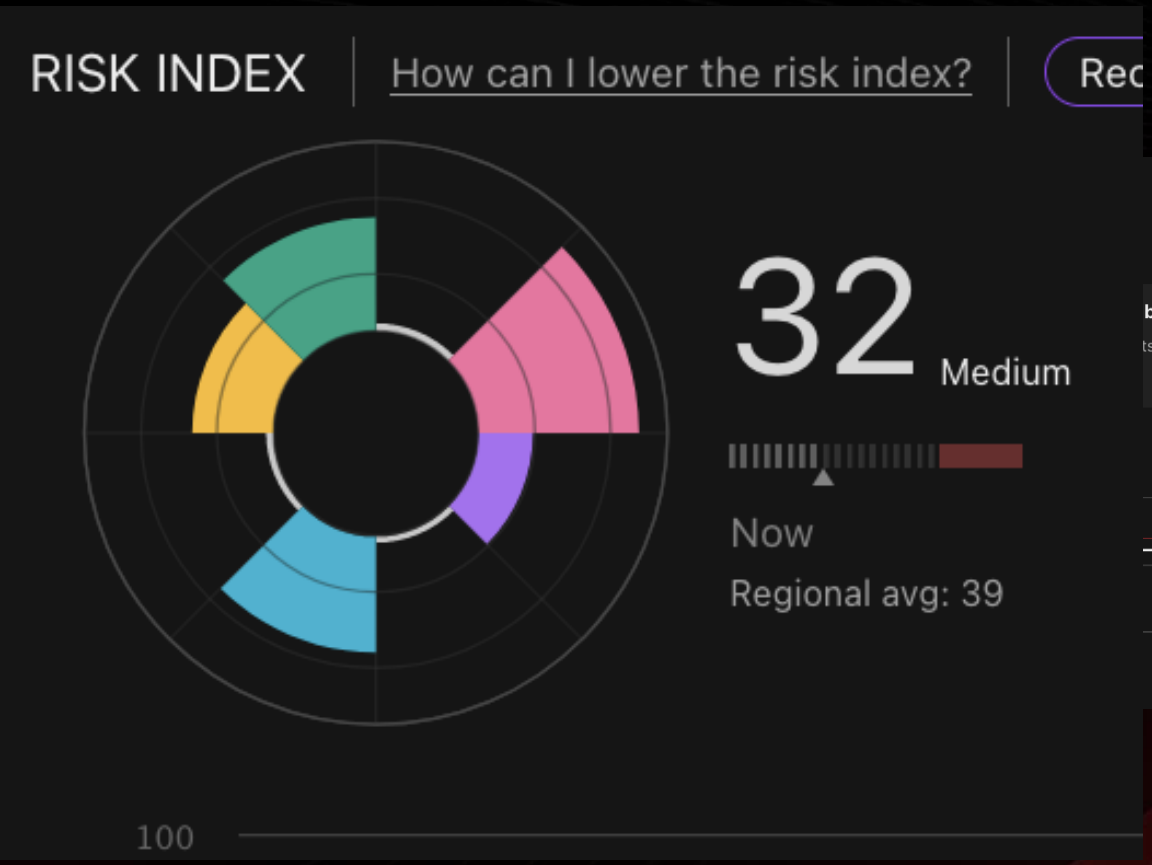
Ciberamenazas y Tendencias

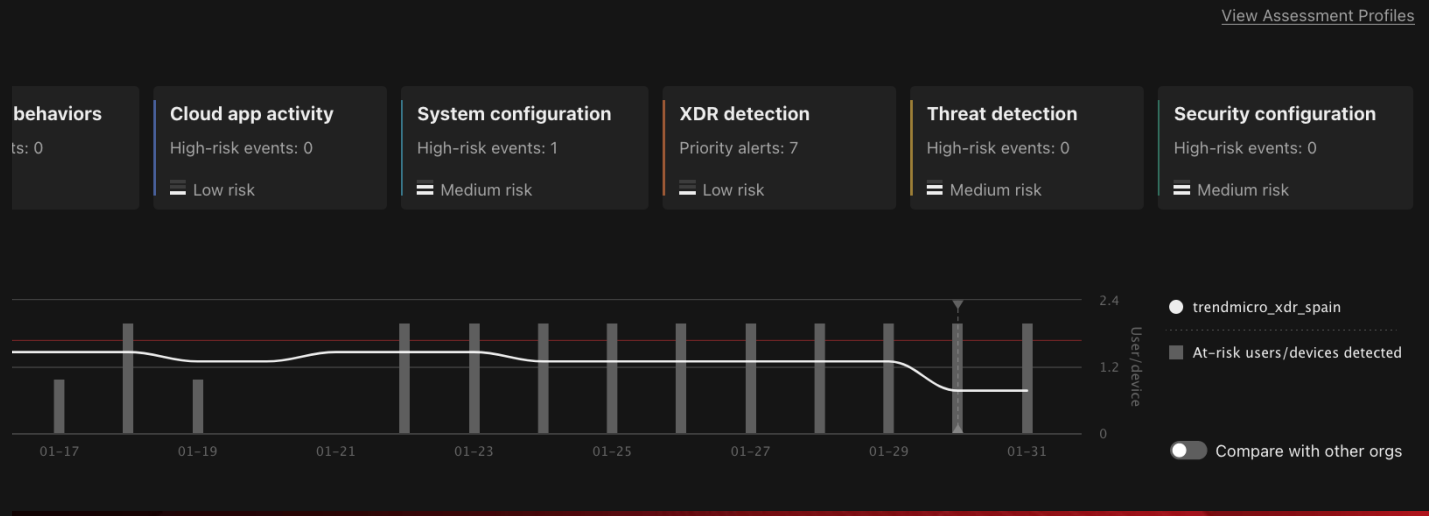
- Hacktivismo.
- Sofisticación del Ransomware.
- Vulnerabilidades.

https://bit.ly/InformeCCN2023

Análisis del Riesgo

Análisis de la postura de Seguridad.





Análisis de la postura de Seguridad.

Account compromise

High-risk events: 0

Events	Asset name	Asset risk score ↓
1	Pil[redacted]	66

Event Detected: 2024-01-23 11:55:49

[redacted]@[redacted].es information from breached domain detected (Domain: [redacted]; Breach date: 2023-12-13).

Remediation: Change the password immediately on this account and any other account where the same password is used.

dataSource:	Dark Web
detected:	2024-01-23 11:55:49
riskLevel:	Medium
compromisedFields:	password, email
mailBox:	[redacted]:ruz.es
leakedDate:	2023-12-12
domain:	[redacted]z.es
assetCriticality:	6
description:	In December 2023, a file containing aggregated exposed data, was found in the underground communities exposing 3972485
recommendation:	Update your password to the account associated to the exposure immediately and review any other services where you use th
breachDate:	2023-12-13
type:	stolenid breach
title:	Combo List 397M

Análisis de la postura de Seguridad.

System configuration

High-risk events: 1

Medium risk

Risk event	Data source / processor	Asset	Risk level
Deprecated OS Version Identified	Endpoint Sensor	WIN10ENTEN22	Medium

The device OS version Windows 10 Enterprise and Education Version 1709 (1709) is no longer supported.

Remediation: Upgrade the operating system.

riskLevel:	Medium
osVersionInternal:	10.0.16299
eosDate:	2020-10-13
osVersion:	1709
assetCriticality:	6
osName:	Windows 10 Enterprise and Education Version 1709

Análisis de la postura de Seguridad.

PUBLIC IP LIST (4777) Add

Assets marked with ★ are highly critical to your organization's ope

Public IP	Asset risk ... ↓	Host	Location	Host provider	Services	Ports	Highly exploit...
13.41.19.190	63	1	United Kingdom	Amazon	HTTPS, HTTP	443, 80	3
40.89.134.111	63	1	France	Azure	HTTPS, HTTP	22, 443, 80	2
49.13.14.21	63	1	Germany		HTTP, HTTPS	22, 80, 8000, ...	3
54.164.73.180	63	1	United States	Amazon	HTTP, HTTPS	80, 443	3

Análisis de la postura de Seguridad.

Vulnerabilities

At-risk vulnerabilities: 502

High risk

	Vulnerability ID	CVE im...	Global exploit...	OS/Application	Impact scope	Prevention rule	Explo
☐	CVE-2023-36025	84	High	Windows 10 Version 22H2 for x64-based Sy...	3	3	

Vulnerability (CVE-2023-36025) published on 2023-11-14 detected for Windows 10 Version 22H2 for x64-based Systems, Windows Server 2016, Windows Server 2019

Remediation: Apply the latest patch or upgrade the operating system version.

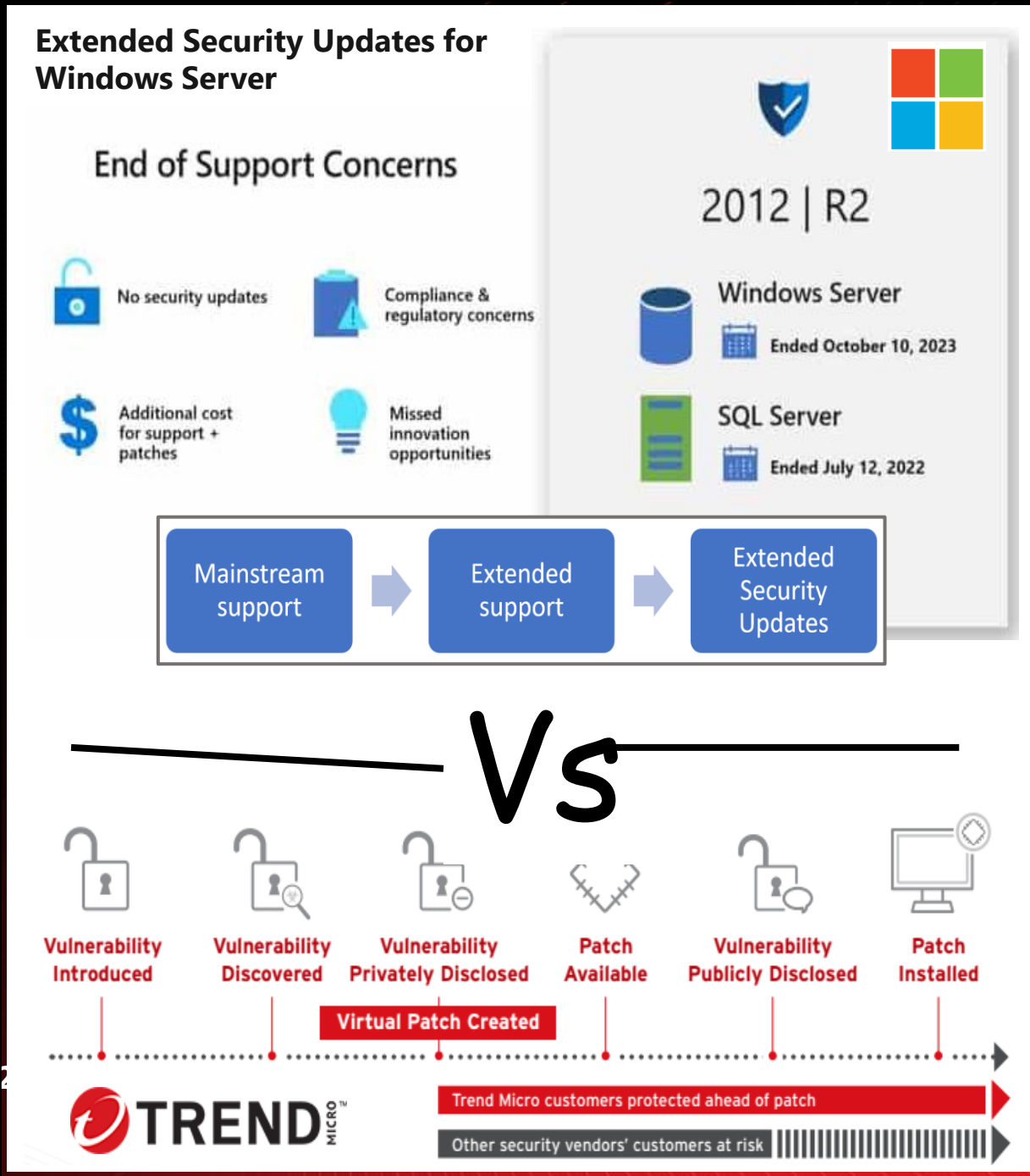
CVE ID:	CVE-2023-36025
CVE impact score:	84
Global exploit potential:	High
Publish date:	2023-11-14

☐	CVE-2019-1130	79	High	Windows Server 2016, windows_10, window...	1	0	
☐	CVE-2019-1315	79	High	Windows Server 2016, windows_server_200...	1	0	
☐	CVE-2019-1388	79	High	Windows Server 2016, windows_server_200...	1	0	
☐	CVE-2019-1405	79	High	Windows Server 2016, windows_server_200...	1	2	

Windows Server 2012 EOS

Incluido soporte para SO descontinuados por fabricante (Win 2000,

Extended Security Updates for Windows Server



CPSTIC

- **EPP/EDR.**
- **IDS.**
- **IPS.**
- **Industrial.**

TREND MICRO Vision One

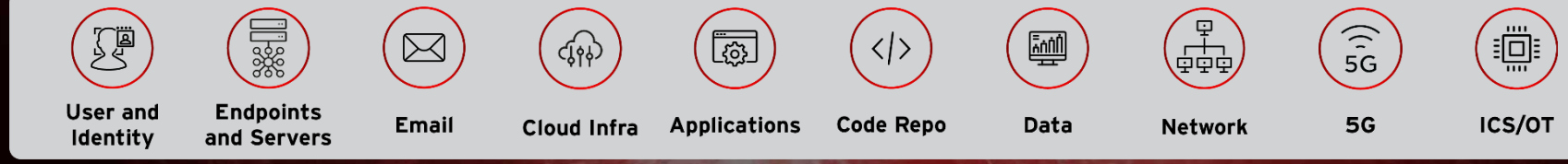
Cybersecurity Platform

Attack Surface Risk Management

Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Extended Detection and Response (XDR)



Email Security | **Endpoint Security** | **Workload Security** | **Network Security** | **Cloud Security**

Orchestration and Automation

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research | AI/ML | Big Data Analytics

Platform Foundations

Multi-Tenancy | Role-Based Access Control | Single Sign-On | Policy Decision Point

Managed Services

Ecosystem Integration

Gracias