PROTAAPP
PROTEGE LAS ADMINISTRACIONES PÚBLICAS
PRODUCTIONS

&

/Rooted CON
ENTERTAINMENT

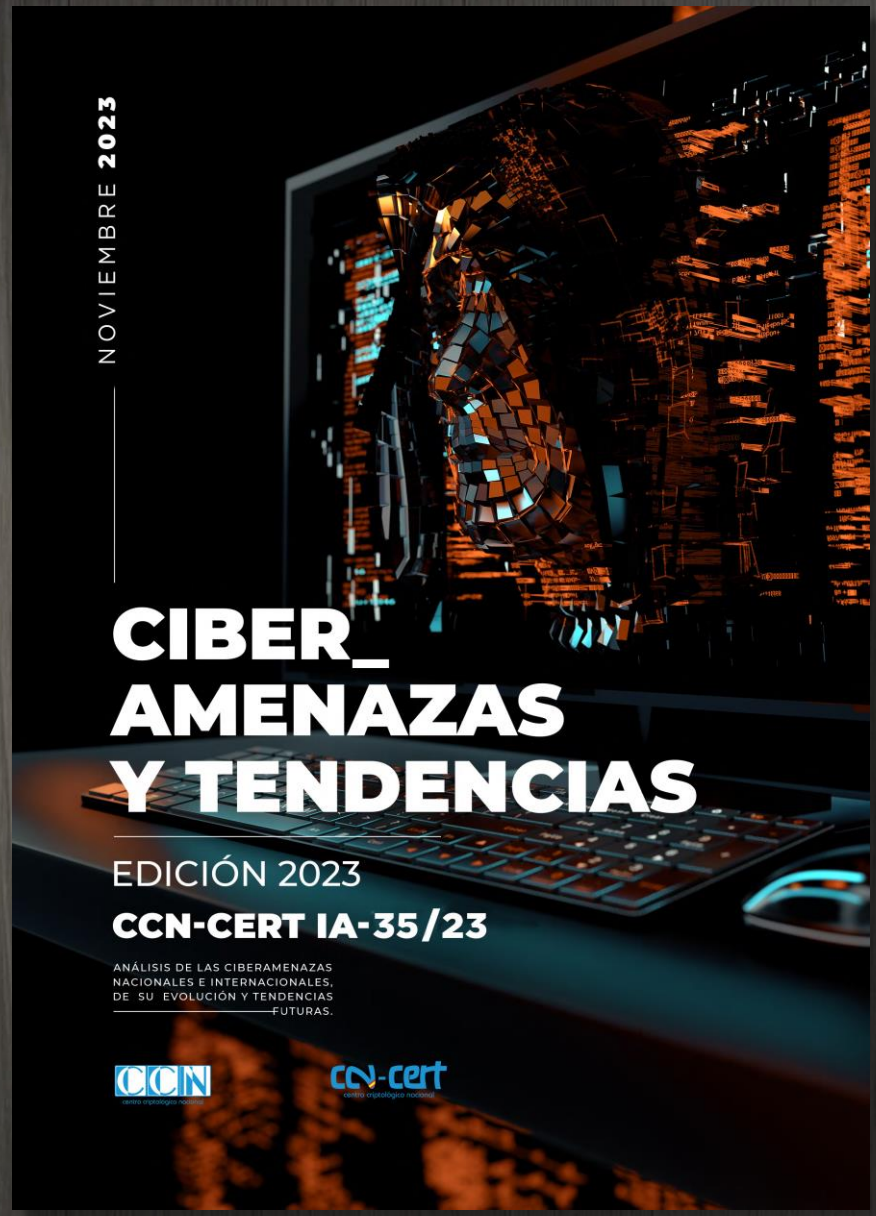
PRESENTAN

SOMOS LOS AGENTES DE LA T.I.A

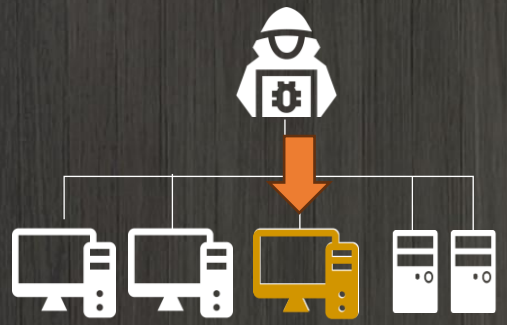
Así nos va

"Las operaciones de ransomware han seguido en aumento respecto a 2021 y las capacidades de postexplotación cada vez tienen mayor sofisticación y automatización, utilizando procedimientos y metodologías avanzadas comparable a los grupos APT de mayor madurez"

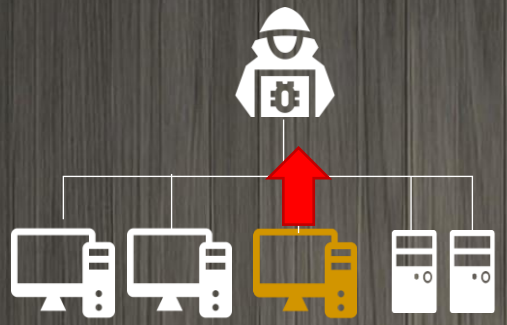
1.265% es el aumento porcentual de correos electrónicos maliciosos desde la llegada de ChatGPT (StormShield)



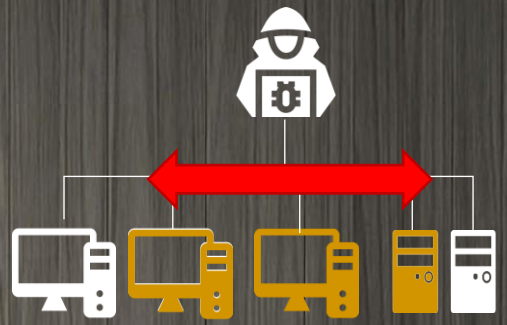
Y cada vez, más rápidos.



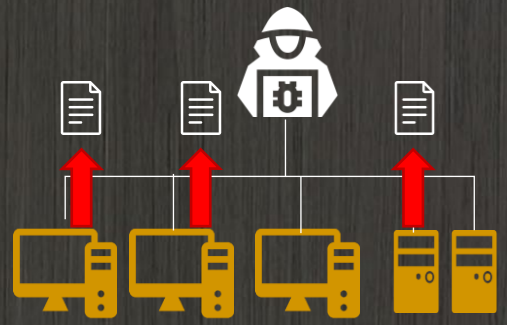
MENOS DE
1 MINUTO
INFRAESTRUCTURA DEL AGRESOR INSTALADA



MENOS DE
45 MINUTOS
COMUNICACIONES C2 SALIENTES OPERATIVAS



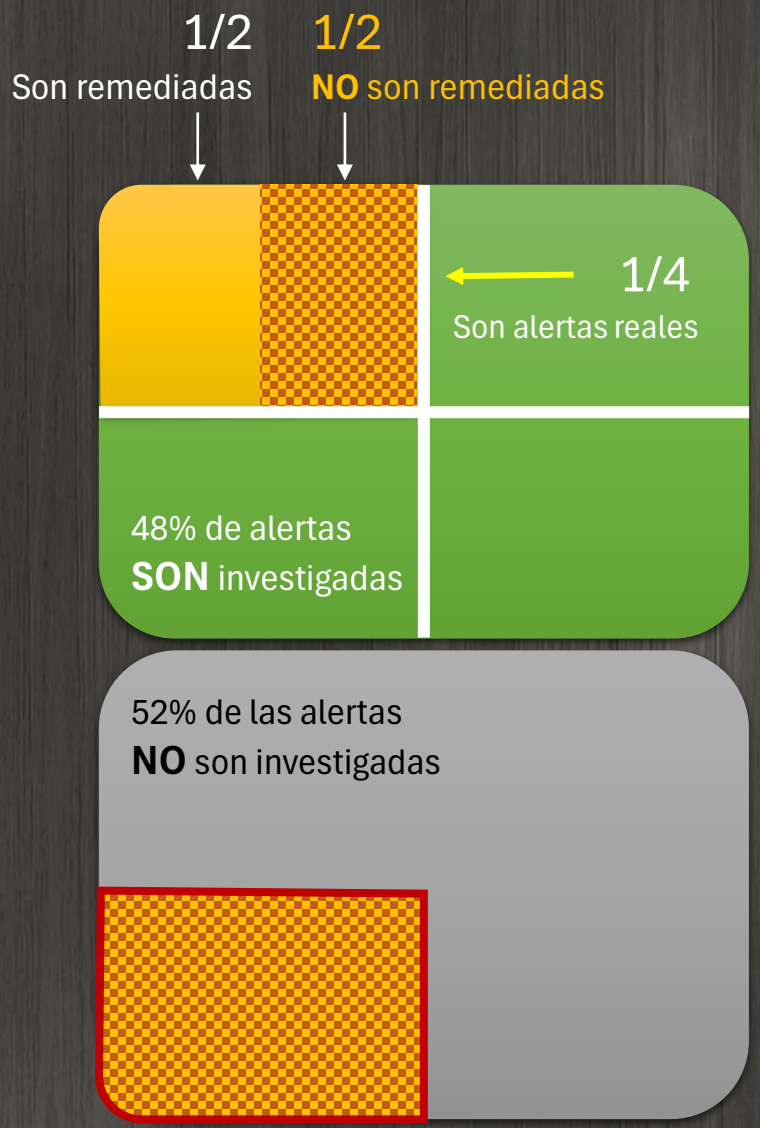
MENOS DE
1 HORA
CONTRASEÑAS DEL ADMINISTRADOR ADQUIRIDAS Y EL AGRESOR SE DESPLAZA LIBREMENTE POR EL ENTORNO DE LA VÍCTIMA



MENOS DE
2 HORAS
SE EXFILTRAN LOS DATOS

https://www.mandiant.es/resources/Infographics/how-stop-ransomware-attack

Nuestro problema: El abrumador volumen de las alertas (2)



Determinar si una alerta es relevante y urgente requiere recopilar información relacionada (contexto) de una amplia variedad de registros del sistema.

Por desgracia, los datos suelen ser difíciles de interpretar de forma aislada.

Somos incapaces de atender las alertas.

"2020 CISO Benchmark Study" de Cisco

TIME LINE Vul.

Pto. de vista Defensivo

Pto. de vista Adversario

Inicio de la vulnerabilidad →

Fabricante/ Investigador descubre la vulnerabilidad y se asigna un CVE.

Adversarios encuentran primero una vulnerabilidad (= ZERO DAY)

Fabricante/ Investigador comunica la vulnerabilidad (¿en Internet?).

Empieza la carrera

NIST's proporciona un 'initial assesment' de la vulnerabilidad

Adversarios monitorizan infraestructuras para explotar la vulnerabilidad

La comunidad de seguridad proporciona parches y/o alternativas

Adversarios identifican el impacto y se comunica vía foros, sitios de 'paste' y dark web

Fin de la vulnerabilidad →

Equipos Blue-Team aplican parches

Se desarrollan exploits y se venden o se comparten en Deep/Dark web

Finaliza la carrera

Defensores ganan

Si llegan primero

Adversarios ganan

Si llegan primero

TIME LINE Vul.

Pto. de vista
Defensivo

Inicio de la vulnerabilidad →

Fabricante/ Investigador descubre la vulnerabilidad y se asigna un CVE.

Fabricante/ Investigador comunica la vulnerabilidad (¿en Internet?).

Empieza la carrera

NIST's proporciona un 'initial assesment' de la vulnerabilidad

La comunidad de seguridad proporciona parches y/o alternativas

Fin de la vulnerabilidad →

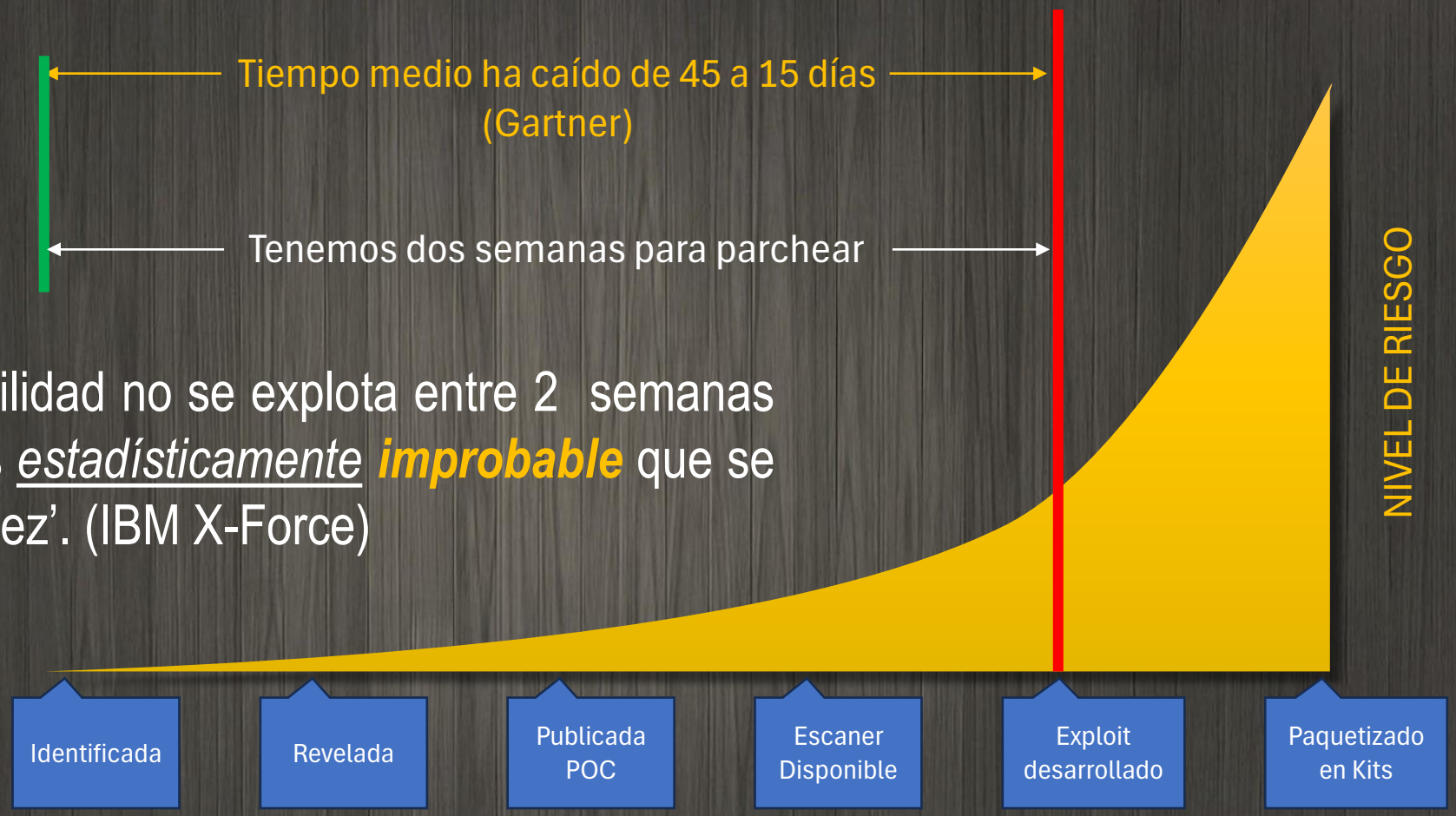
Equipos Blue-Team aplican parches

Finaliza la carrera

Defensores ganan

Si llegan primero

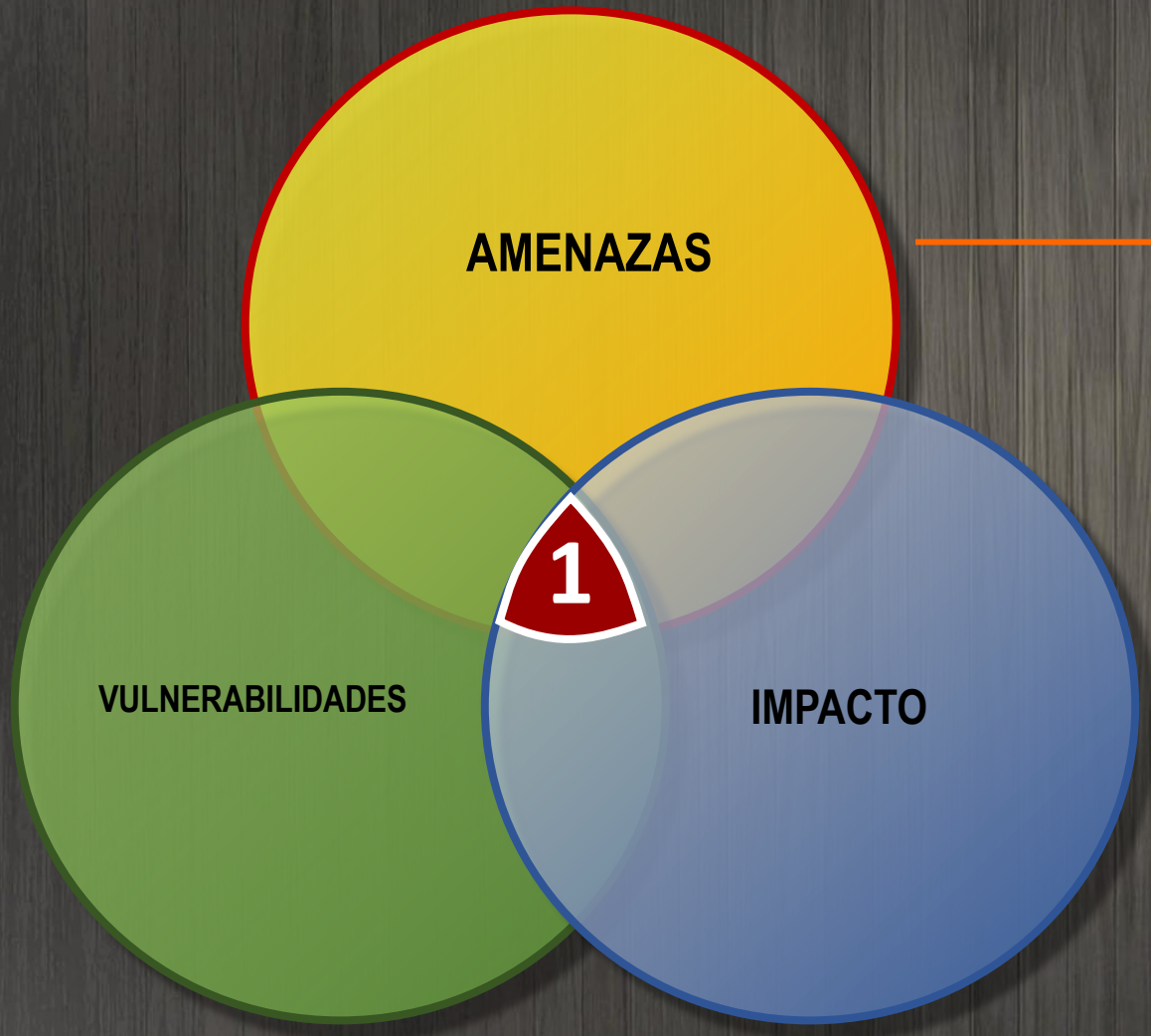
Incremento del riesgo



'Si una vulnerabilidad no se explota entre 2 semanas y tres meses, es *estadísticamente* ***improbable*** que se explote alguna vez'. (IBM X-Force)

El riesgo real aumenta drásticamente cuando las vulnerabilidades se convierten en un arma

RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



CAPACIDAD

Habilidad de un adversario para lograr el efecto deseado

OPORTUNIDAD

Momento para hacerlo: cuando pueda o cuando más daño haga

INTENCION

Objetivo o finalidad del adversario

Y AQUÍ ENTRAN NUESTROS AGENTES

T.I.A

Threat Intelligence – Inteligencia de amenazas

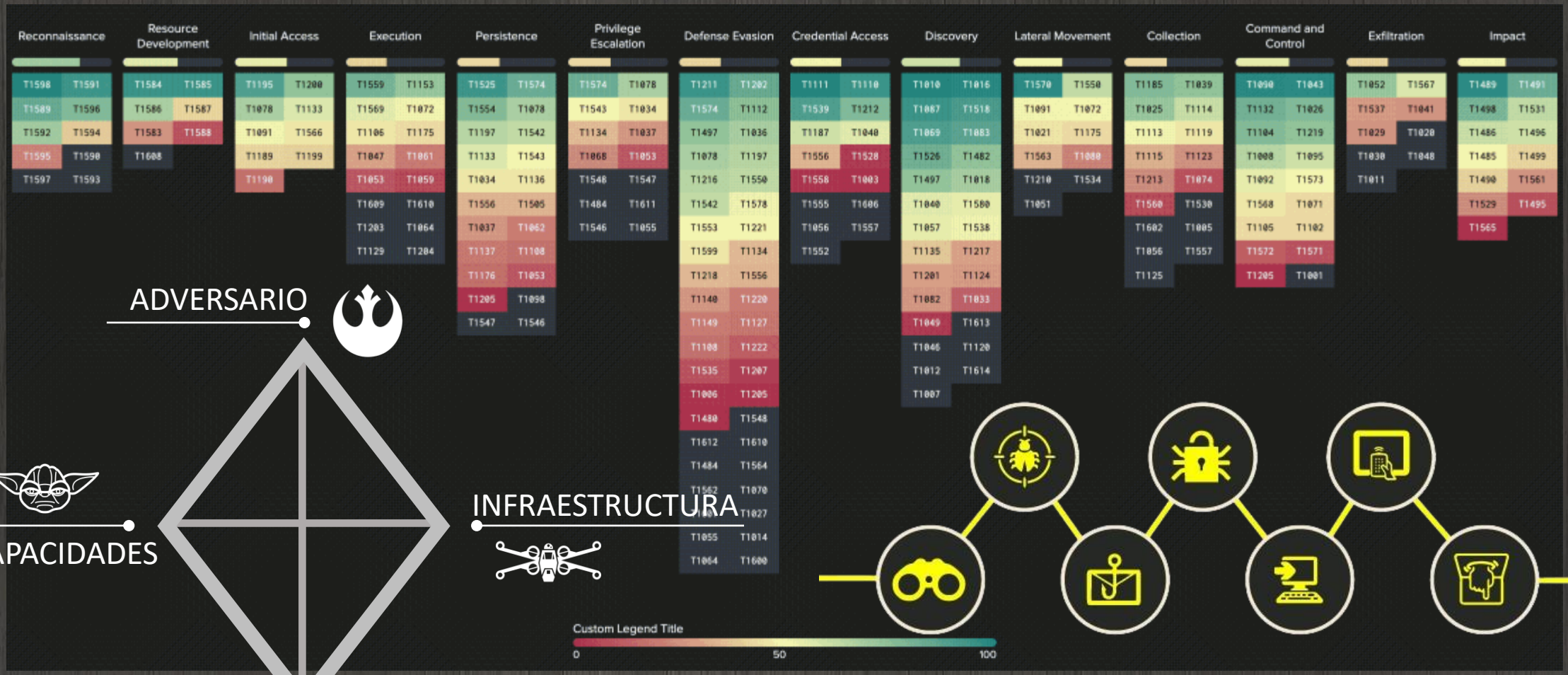
- “La inteligencia de amenazas es conocimiento basado en evidencia, que incluye contexto, mecanismos, indicadores, implicaciones y consejos prácticos, sobre una amenaza o peligro existente o emergente para los activos que puede usarse para informar decisiones sobre la respuesta del sujeto a esa amenaza o peligro”.

- “La Inteligencia de amenazas es información que ha sido agregada, transformada, analizada, interpretada y enriquecida, para proporcionar el contexto necesario para el proceso de toma de decisiones”.

- "La defensa basada en amenazas es la aplicación sistemática de un conocimiento profundo de las técnicas y la tecnología del adversario para mejorar las defensas".

(fuente: MITRE Engenuity Center for Threat-Informed Defense)

Frameworks centrados en amenazas

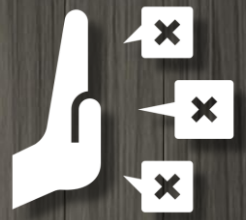


La pregunta del millón

entonces … ¿por qué todo el mundo apoya la seguridad centrada en las **amenazas**, pero tan pocos la practican?

NIVELES
de Seguridad

INTELIGENCIA
de baja calidad



Nula
FLEXIBILIDAD

Cultura de
CUMPLIMIENTO

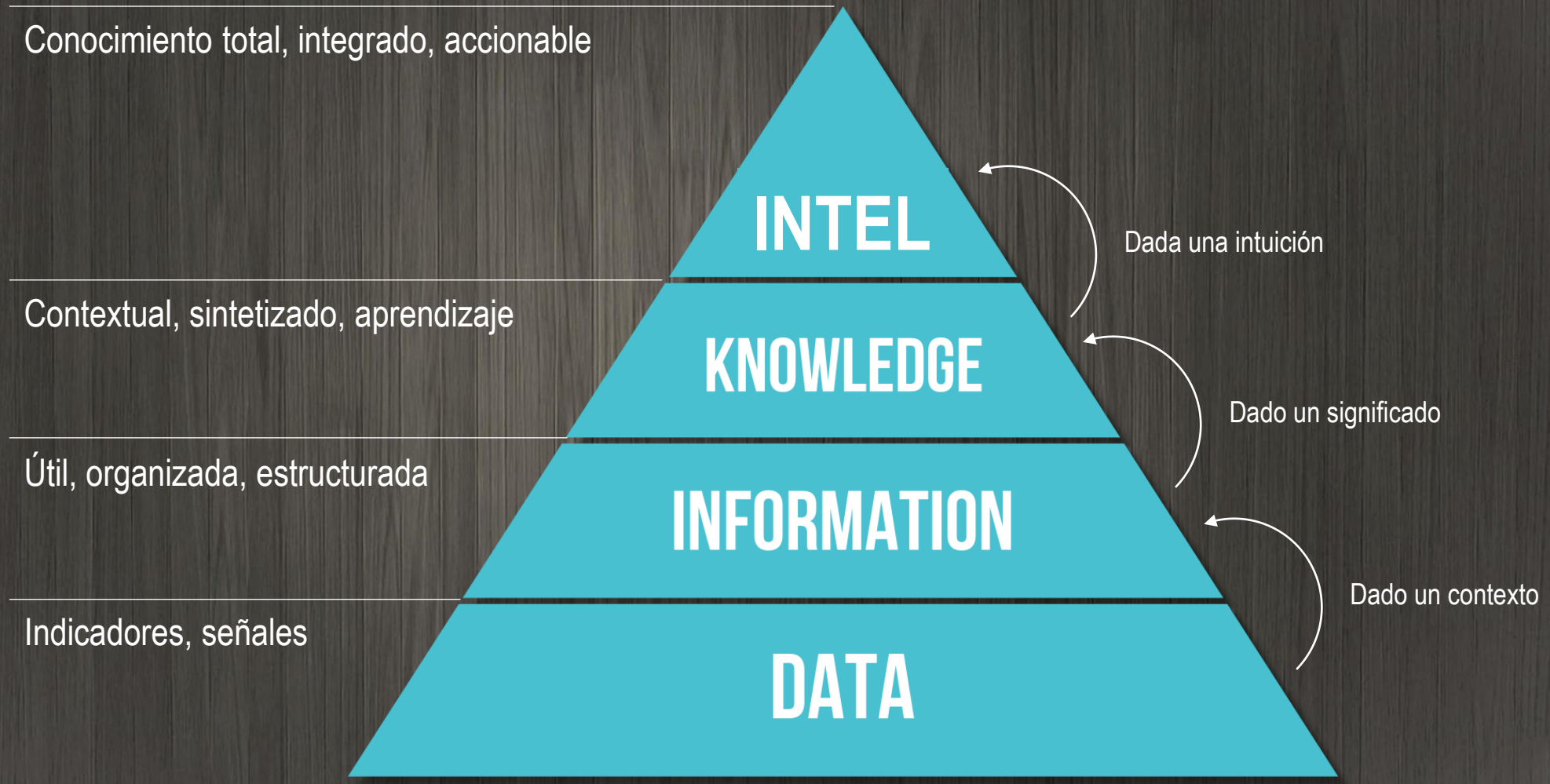
DESCONEXION
de las partes

Falta de
CAPACIDADES

Escasez
de RECURSOS

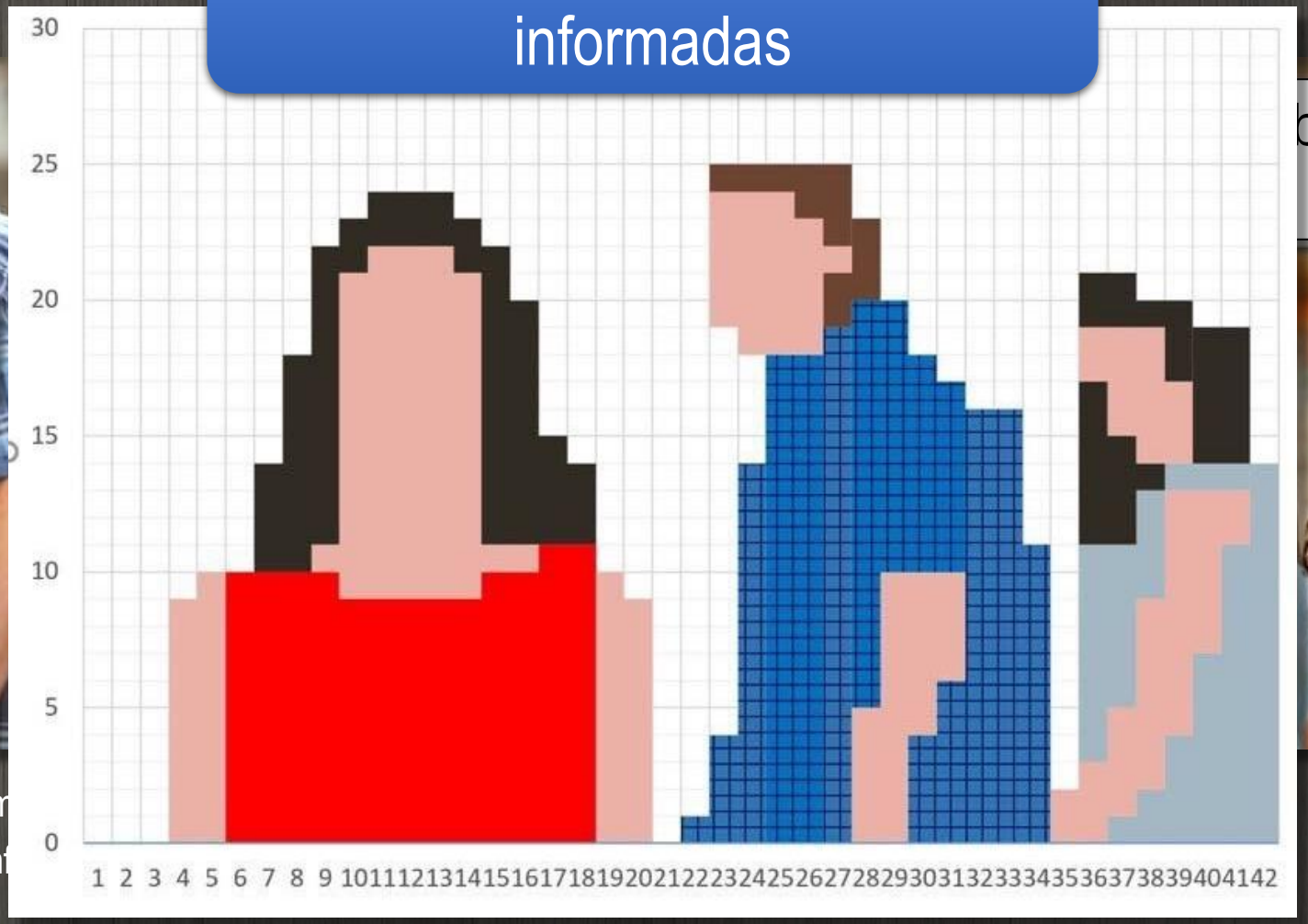
Falta de
MADUREZ

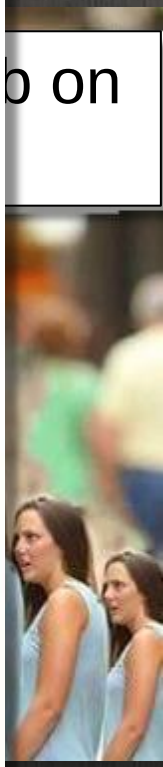
El modelo DIKWi



¿Soy yo o vosotros también?

se trata de tomar decisiones informadas

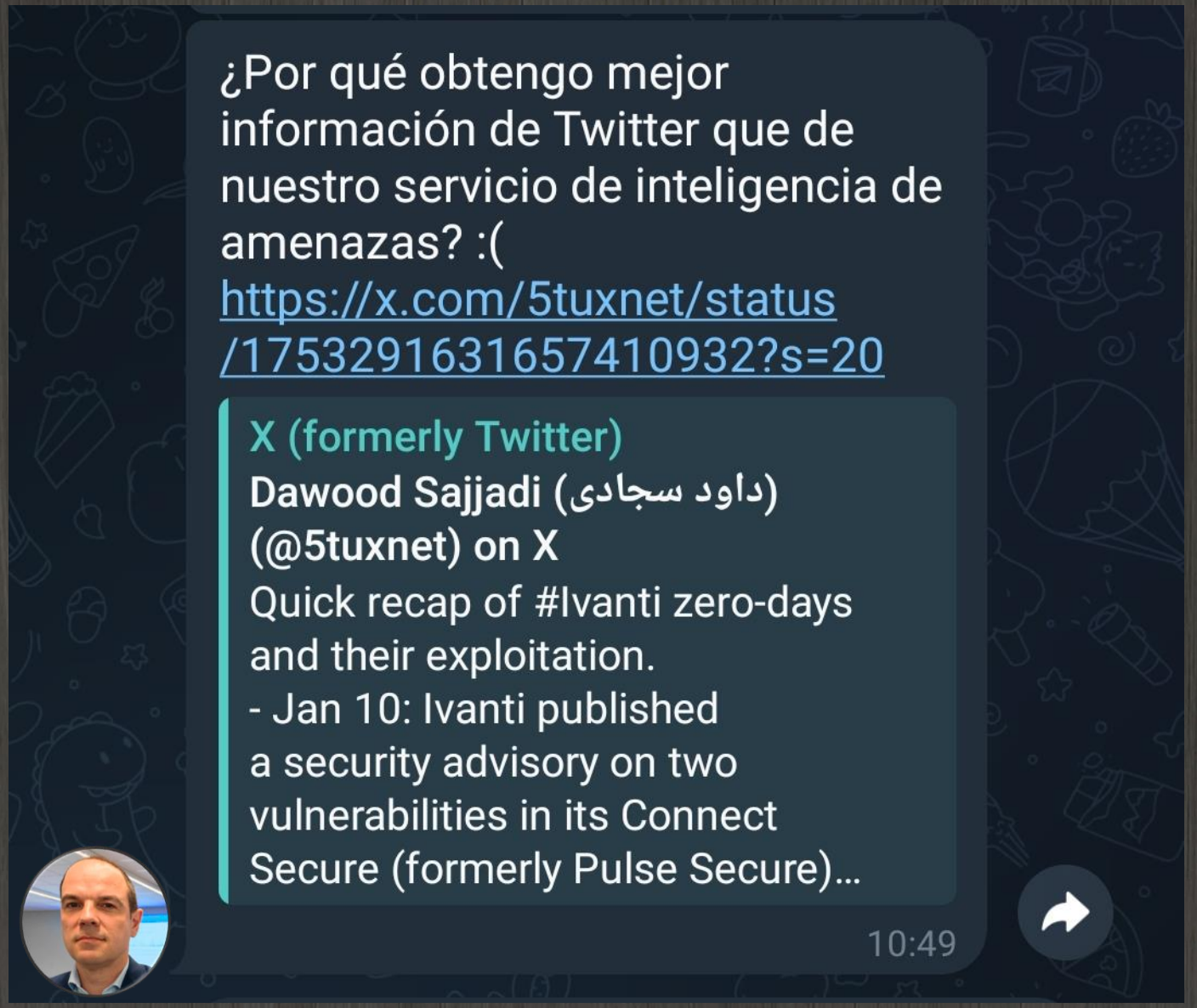




Las fuentes de datos que nunca se utilizan y los inform

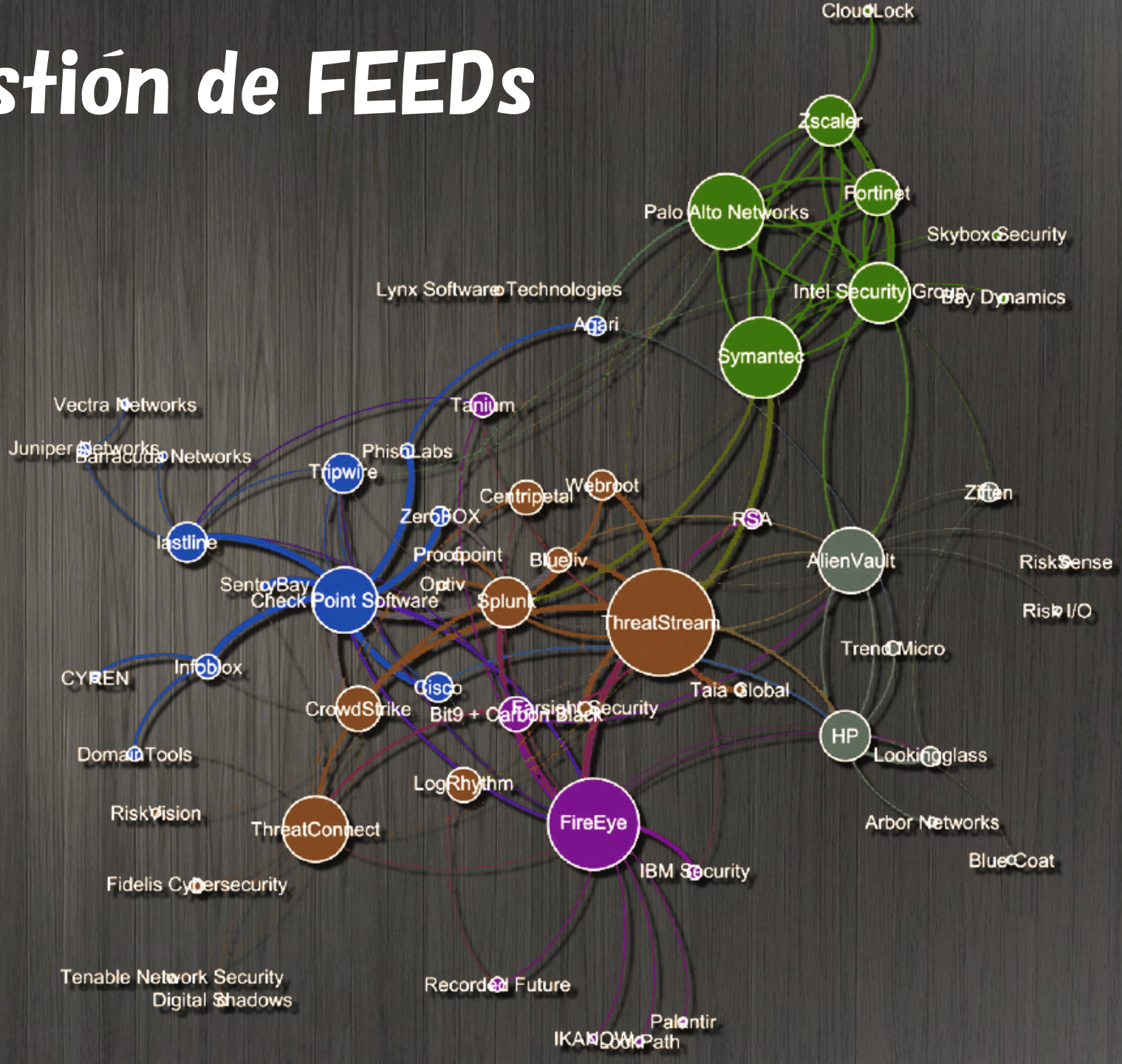
No se trata de obtener la mayor cantidad posible de in

LA QUEJA


¿Por qué obtengo mejor información de Twitter que de nuestro servicio de inteligencia de amenazas? :(
https://x.com/5tuxnet/status/1753291631657410932?s=20
X (formerly Twitter)
Dawood Sajjadi (داود سجادی) (@5tuxnet) on X
Quick recap of #Ivanti zero-days and their exploitation.
- Jan 10: Ivanti published a security advisory on two vulnerabilities in its Connect Secure (formerly Pulse Secure)...
10:49

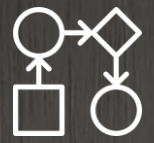
1. No es solo cuestión de FEEDs

- “Threat intelligence sharing between cybersecurity vendors”



2. Seguramente no tienes un plan de inteligencia

Modelo de madurez progresiva

	1	2	3	4
	Sin recursos	Algún recurso sin dedicación plena	Equipos IR, SecOps, … Using security inteligence	Equipo de analistas dedicado
	Sin feeds (solo Google)	Feeds gratuitos (mon. leaks y marca)	Feeds de pago. Inteligencia contextual	Múltiples proveedores de Inteligencia
	MSSP	SIEM y gestión de vulnerabilidades	Capacidad de IR	Plataforma de Inteligencia y capacidad de análisis
	N/A	Respuesta ad hoc	Integración con herramientas del SOC	Integración con múltiples herramientas

3. Y nadie dijo que fuera fácil

EL ‘WHITE PAPER’ DE ALGUNOS VENDORS

CUANDO TE LLEGA A CASA

La Inteligencia que nos haría falta

SecOps Intelligence

- Triaje
- Detección
- Prevención

Vulnerability Intelligence

- Priorización
- Monitorización de Vulnerabilidades

Attack Surface Intelligence

- Activos externos
- Monitorización de la superficie de ataque

Brand Intelligence

- Abuso de dominios
- Monitor. de activos
- Fugas de datos

Third-Party Intelligence

- Gestión Proveedores
- Gestión Adquisiciones
- Supply-Chain

Geopolitical Intelligence

- Visibilidad sobre acontecimientos de interés

Payment Fraud Intelligence

- Anticipación
- Mitigación

Cyber Threat Intelligence

- Investigación
- Detección
- Monitorización

Identity Intelligence

- Leaks de credenciales
- Identidad digital
- Identidad de terceros

La vigilancia digital es un 'must'

S2 GRUPO

22 May 2023 2 Minutos de lectura

Más de 65 millones de credenciales digitales han sido 'leakeadas' en 2023

it Digital Security

1 de cada 2 ciberataques en 2023 se iniciaron con el robo de credenciales

Actualidad 02 FEB 2024

AWS credentials found on Github and abused within 1 minute

https://s2grupo.es/mas-de-65-millones-de-credenciales-digitales-han-sido-leakeadas-en-2023/
https://www.itdigitalsecurity.es/actualidad/2024/02/1-de-cada-2-ciberataques-en-2023-se-iniciaron-con-el-robo-de-credenciales
https://www.comparitech.com/blog/information-security/github-honeypot/

Dónde encuentro esa Inteligencia?

Compartición de información

Sitios de Paste con info de leaks
(y otros indicadores de campañas)

IoCs asociados con actividad maliciosa

Repositorios de código

Monitorización en RR.SS. (anuncios, intenciones, …)

Información Geopolítica

Información propia publicada

Ciber HUMINT

Foros en Deep Web

Informes de malware (TTPs / IoCs)

Marketplaces en Dark Web

Apps de mensajería

No es fácil ...

DONDE

ACCESO

IDIOMA

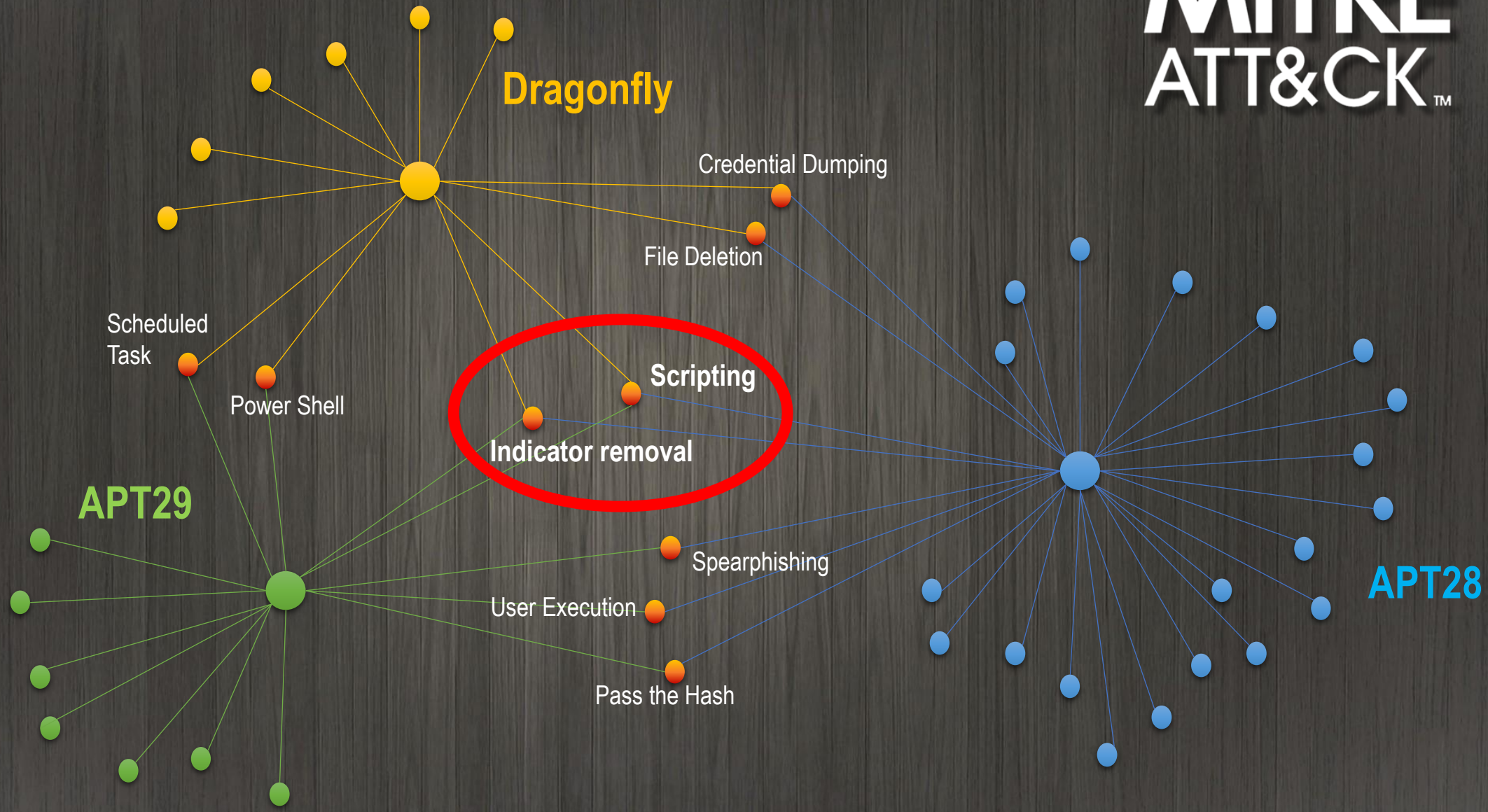
OFUSCACIÓN

SUSCEPTIBILIDAD

COMPLIANCE

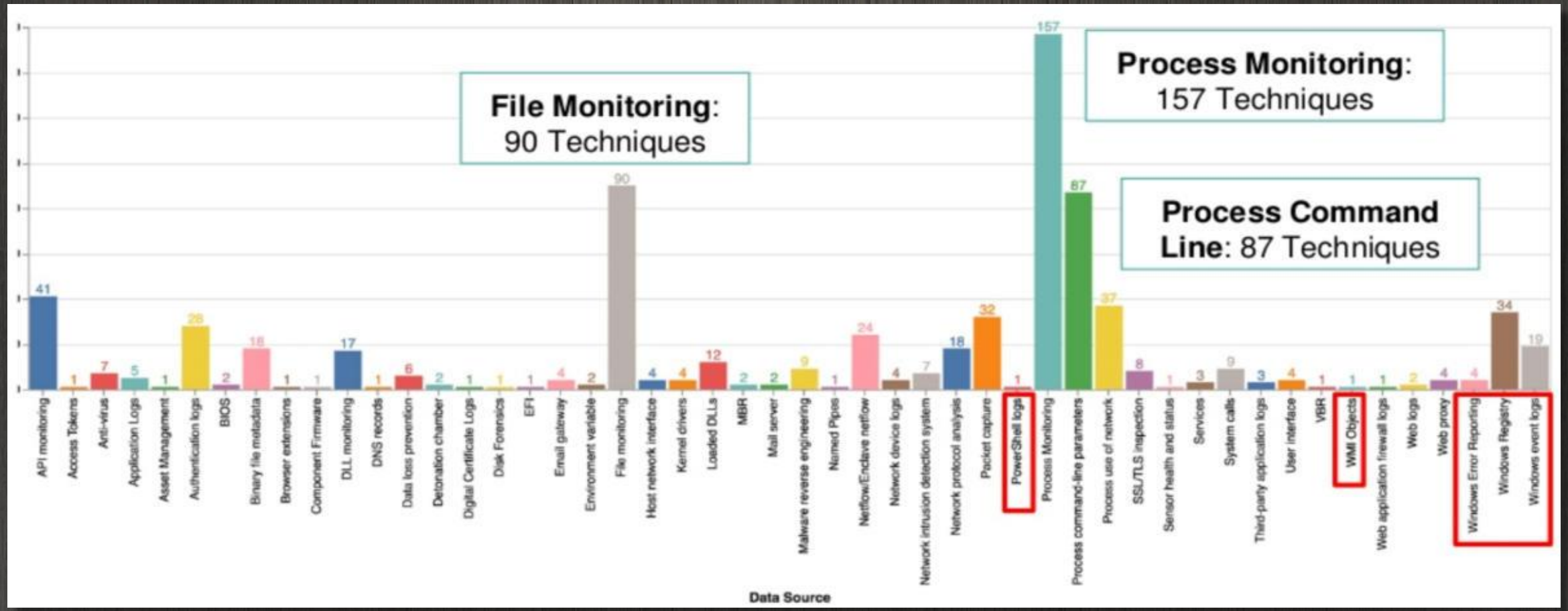
Priorizar !!

MITRE ATT&CK™



Priorizar más!!

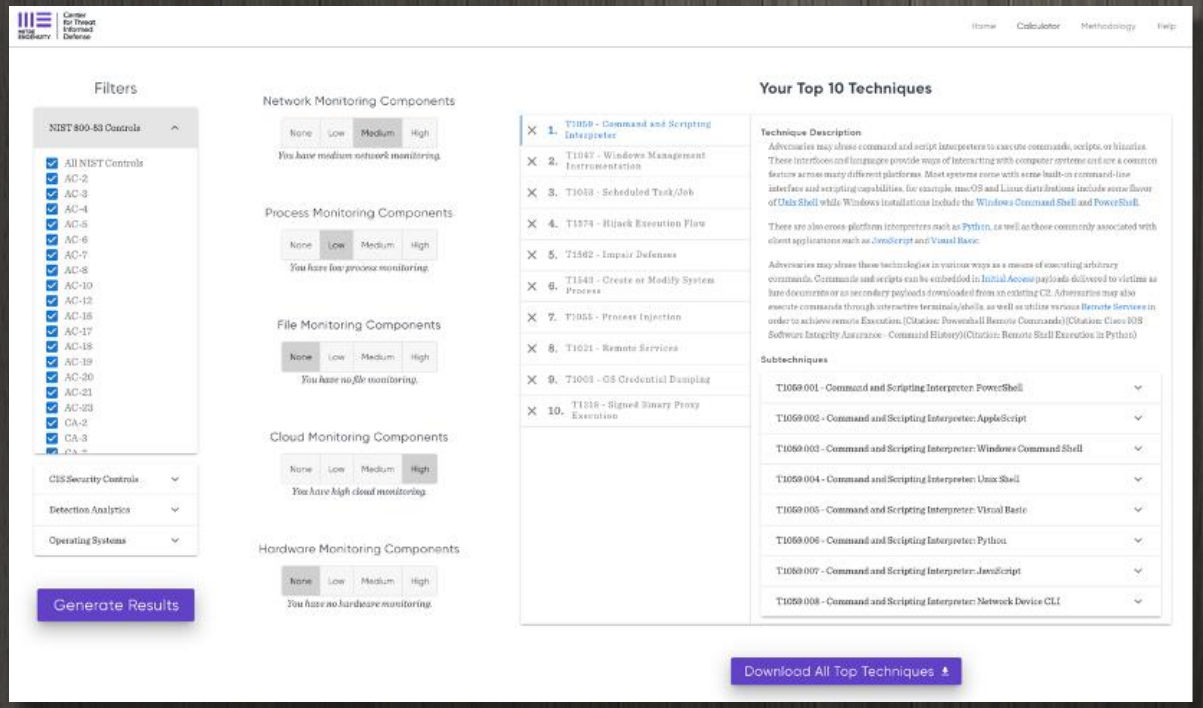
ATT&CK techniques vs Data Sources



Priorizar aún más!!

MITRE ENGENUITY

Tu Top-TEN personalizado



ATT&CK Calculator

O tirando de reports

TOP-TEN de Técnicas en 2023

1) T1059 Command and Scripting Interpreter
2) T1003 OS Credential Dumping
3) T1486 Data Encrypted for Impact
4) T1055 Process Injection
5) T1082 System Information Discovery
6) T1021 Remote Services
7) T1047 Windows Management Instrumentation
8) T1053 Scheduled Task/Job
9) T1497 Virtualization/Sandbox Evasion
10) T1018 Remote System Discovery

https://top-attack-techniques.mitre-engenuity.org/calculator

Center-for-threat-informed-defense/top-attack-techniques (github.com)

Soluciones Inteligentes OpenSource

+

The HIVE

+

Cortex

Open CTI

Software products heatmap

CERT-UE -Threat Landscape Report 2023

AI	Business intelligence	Cloud Services	Content management and collaboration tool	Compression	Data Backup and Recovery	Database Management	Development Languages	Development Tools and IDEs	Managed file transfer	Networking
ChatGPT	Qlik Sense	Amazon Web Services	3CX Desktop App	7zip	ConnectWise R1Soft Server Backup	Microsoft SQL server	GNU C library	Adobe ColdFusion	GoAnywhere	VMWare ESXi
		Google Cloud	Atlassian Confluence	WinRAR	Veeam Backup and Recovery	MySQL server	NPM library	Apache ActiveMQ	MOVEit	Cacti
		JumpCloud	Atlassian Jira		Veritas Backup Exec	Redis	Python library	Apache Strut	WS_FTP server	Cisco IOS XE
		Microsoft Azure	Joomla				Packagist	Docker		Cisco VPN
		Microsoft 365	Microsoft Streaming Service					Github		Citrix Netscaler ADC
		ownCloud	Microsoft Teams					JetBrains TeamCity		Citrix Netscaler Gateway
		VMware Cloud Foundation	Microsoft Exchange Server					Kubernetes		F5 BIG-IP
		Western Digital My Cloud	Oracle E-Business Suite					Microsoft Powerapps		Fortinet - FortiGate
			Roundcube					Mocky		Fortinet- FortiOS

Demo time !!

Hans On

The most interesting PDB string is the “4113.pdb,” which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that, with successful exploitation, would give any user SYSTEM access on the machine.

The malware component, test.exe, uses the Windows command "cmd.exe" /C whoami” to verify it is running with the elevated privileges of “System” and creates persistence by creating the following scheduled task:

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"
```

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00". The malware then requests a connection to 192.184.60.229 on TCP port 81 using the command "05 01 00 01 c0 b8 3c e5 00 51" and verifies that the first two bytes from the server are "05 00" (c0 b8 3c e5 is the IP address and 00 51 is the port in network byte order).

https://www.mandiant.com/resources/blog/operation-doubletap

Hans On

T1068 - Exploitation for Privilege Escalation

T1033 - System Owner/ User Discovery

T1059 - Command-Line Interface

The most interesting PDB string is the “4113.pdb,” which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that, with successful exploitation, would give any user SYSTEM access on the machine.

The malware component, test.exe, uses the Windows command "cmd.exe" /C whoami” to verify it is running with the elevated privileges of “System” and creates persistence by creating the following scheduled task:

schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00". The malware then requests a connection to 192.184.60.229 on TCP port 81 using the command "05 01 00 01 c0 b8 3c e5 00 51" and verifies that the first two bytes from the server are "05 00" (c0 b8 3c e5 is the IP address and 00 51 is the port in network byte order).

T1053 - Scheduled Task

T1095 - Standard Non-Application Layer Protocol

T1065 - Uncommonly Used Ports

T1104 - Multi-Stage Channels

https://www.mandiant.com/resources/blog/operation-doubletap

Lo que se puede hacer con ML

TRAM

THREAT REPORT ATT&CK MAPPER

INPUT → [BLACK BOX] → OUTPUT

- Informes DFIR
- Blogs
- Whitepapers
- Otro material escrito (html, json,…)

- Identificar Actores
- Identificar Herramientas
- Identificar técnicas
- Identificar relaciones

- Flujos de ataque
  - vectores
  - paths
- Timelines

Resumiendo

IN7ELLIG3NC3 I5 7H3 48ILI7Y 70
4D4P7 70 CH4NG3

- 573PH3N H4WKING -

Resumiendo

CONTROLES

CAPACIDADES

Un último ciberconsejo

Identity Intelligence

- Instalar 2FA en todas partes
- Cifrar todo lo que no esté anclado al suelo

Muchas gracias !!

MitreGator goodies

Mis páginas | Escuela de Calor | TTX | BAS | CTI

Compartir | Marcadores

Buscar en la web

Threat Intelligence Platforms

- OpenCTI-Platform/opencti
- eclecticiq - OPEN TAXII
- CISCO CSIRT - GOSINT
- TypeDB.com
- Te-k - HARPOON
- CRITs: Collaborative Research Into Threats
- Collective Intelligence Framework — CSIRT Gadgets, LLC
- Welcome to the Yeti documentation site!
- threatnote.io
- csirtgadgets - cif-v5

Mostrar todo (11)

Community Threat Exchange Platform

- MISP Communities and MISP Feeds
- IBM X-Force Exchange
- AlienVault Open Threat Exchange
- Docguard.io

FEEDS

- Index of /data/feed-osint/
- CINS Army Sentintel
- CyberCrime
- Green Snow
- Threat Intelligence

Black list

- SSLBL
- The Spamhaus Project

funny tools

- elceef/dnstwist

Report Repo

- CIRCL Publicaciones & Presentaciones
- The DFIR Report

Deep & Dark

APT | Crypto | Stuff | Research | Info Release | +

- Distributed Denial of Secrets
- WikiLeaks

Malware Sharing Sites

- VirusTotal
- AlienVault
- Malware Trends Tracker
- Koodous
- URLhaus
- MalwareBazaar
- MalShare
- InQuest Labs

Vulnerabilidades

- CIRCL CVE Search
- CVE Details
- CVE STALKER
- cve-search
- CWE
- Mitre CVE
- NIST - NVD

Threat Frameworks

- Cyber Kill Chain®
- diamond-model-influence-operations-analysis
- MITRE ATT&CK™
- diamond model for intrusion analysis
- The Unified Kill Chain

Tracking Botnets

- Feodo Tracker

OnLine Resources

- YARAify
- Cyber Threat Intelligence
- Threat-Informed Defense Ecosystem
- start.me/p/5vzX9A/cyber-threat-intelligence
- SANS Cyber Threat Intelligence Summit 2022

OPEN CTI

- OpenCTI-Platform/opencti
- demo.opencti.io/dashboard
- OpenCTI Documentation
- filigran-dark

Yara Rules

- abuse.ch

- Emilio Rico
- Security Advisor at trc
- Lector de comics

@Emilio_RR

Emilio Rico Ruiz

https://github.com/3MilioRR

#CyberDefence #CyberSecurity