



& /Rooted[®]CON
ENTERTAINMENT

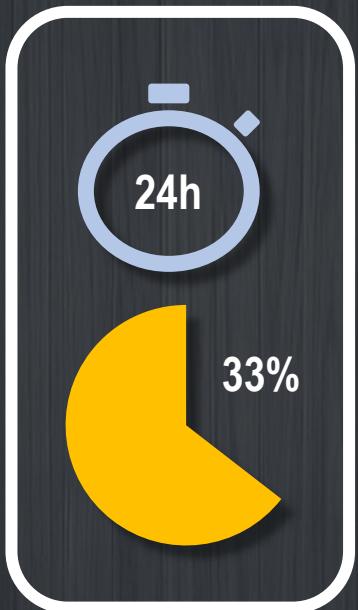
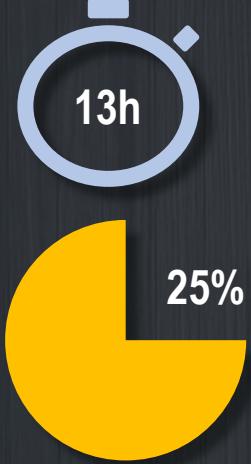
PRESENTAN

Pero ... ¿Qué me estás contando?



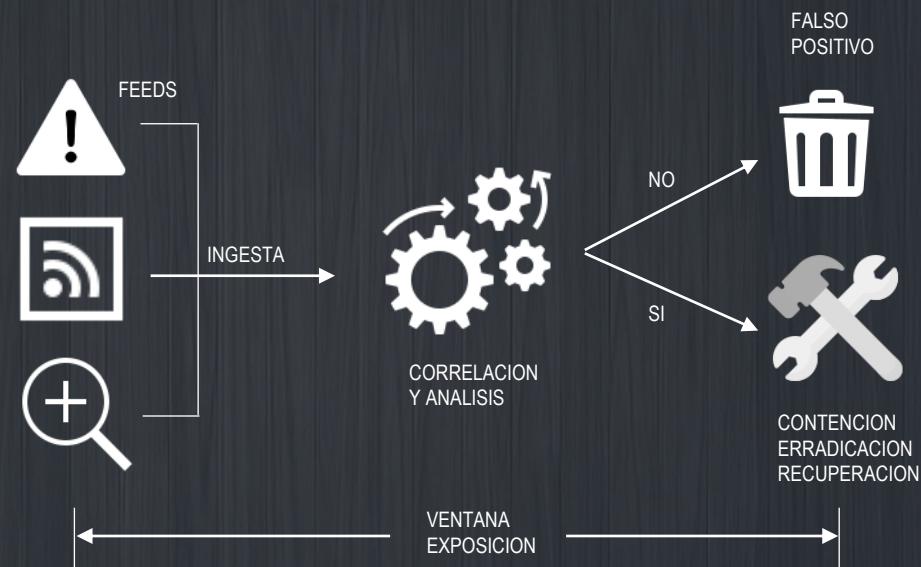


(07/01/2022)
un tercio de las páginas
de phising dejan de
estar activas el primer
día



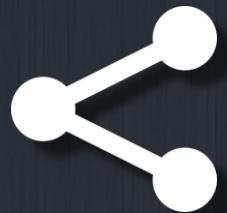
1

AUMENTAR LA CAPACIDAD DE DETECCION



2

COMPARTIR





44%

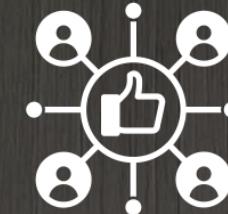
% de los analistas de amenazas que hacen públicos sus descubrimientos

52%

% de analistas que trabajan en inteligencia de amenazas (o ciberseguridad) y no pueden compartir sus hallazgos

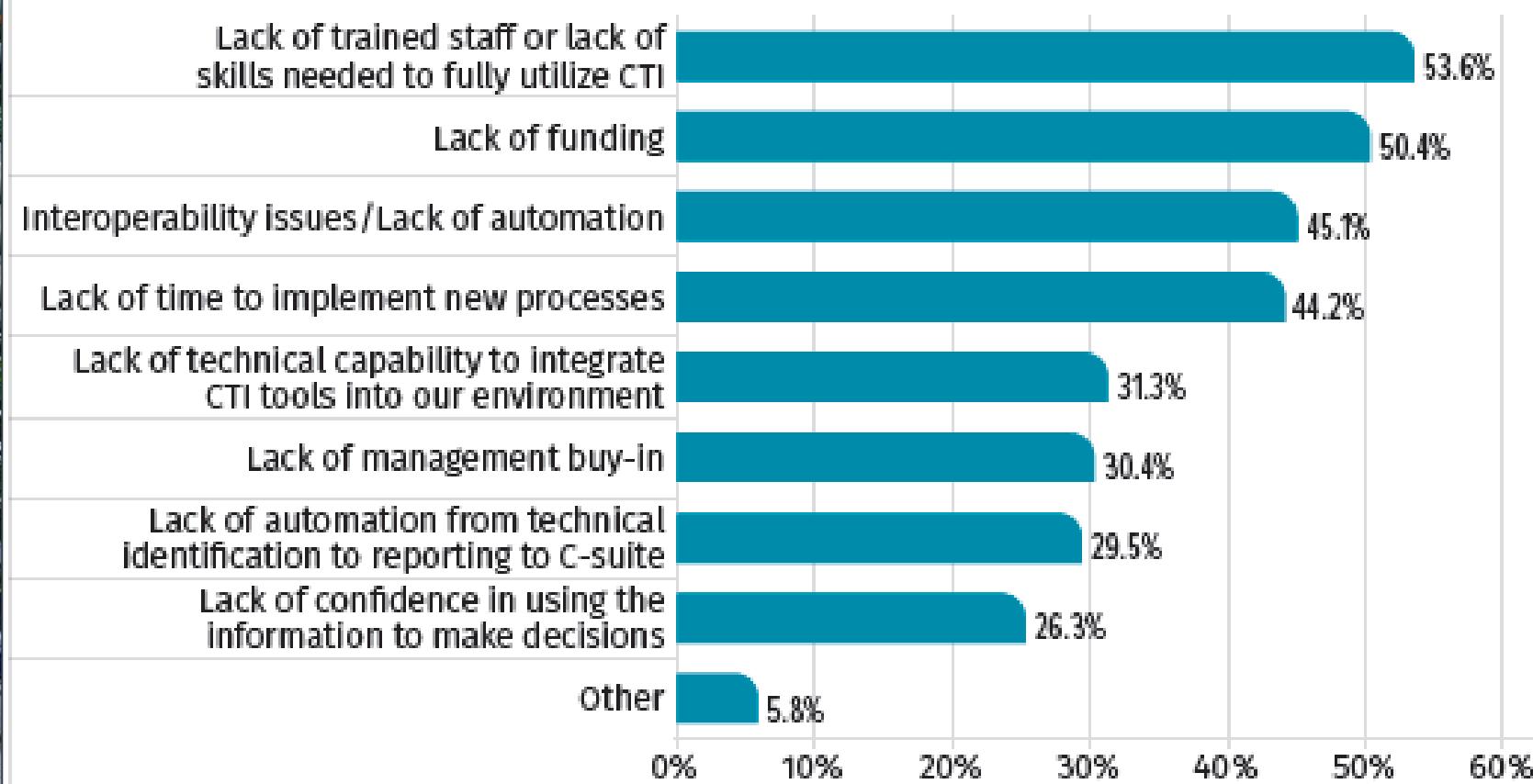
77%

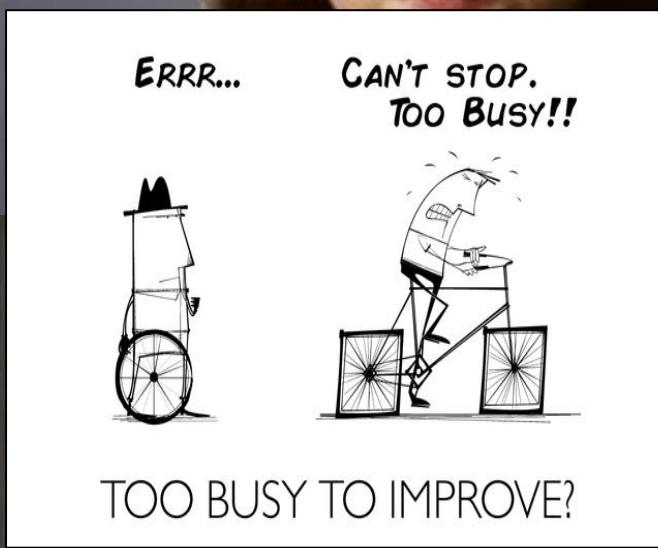
% de analistas que comparten información en empresas donde SÍ se permite la colaboración





What inhibits your organization from implementing CTI effectively? Select all that apply.





Compartir: Qué?

IOC,s

piezas de información que pueden utilizarse para identificar un posible compromiso. de un entorno

IOCs

Indicadores conductuales

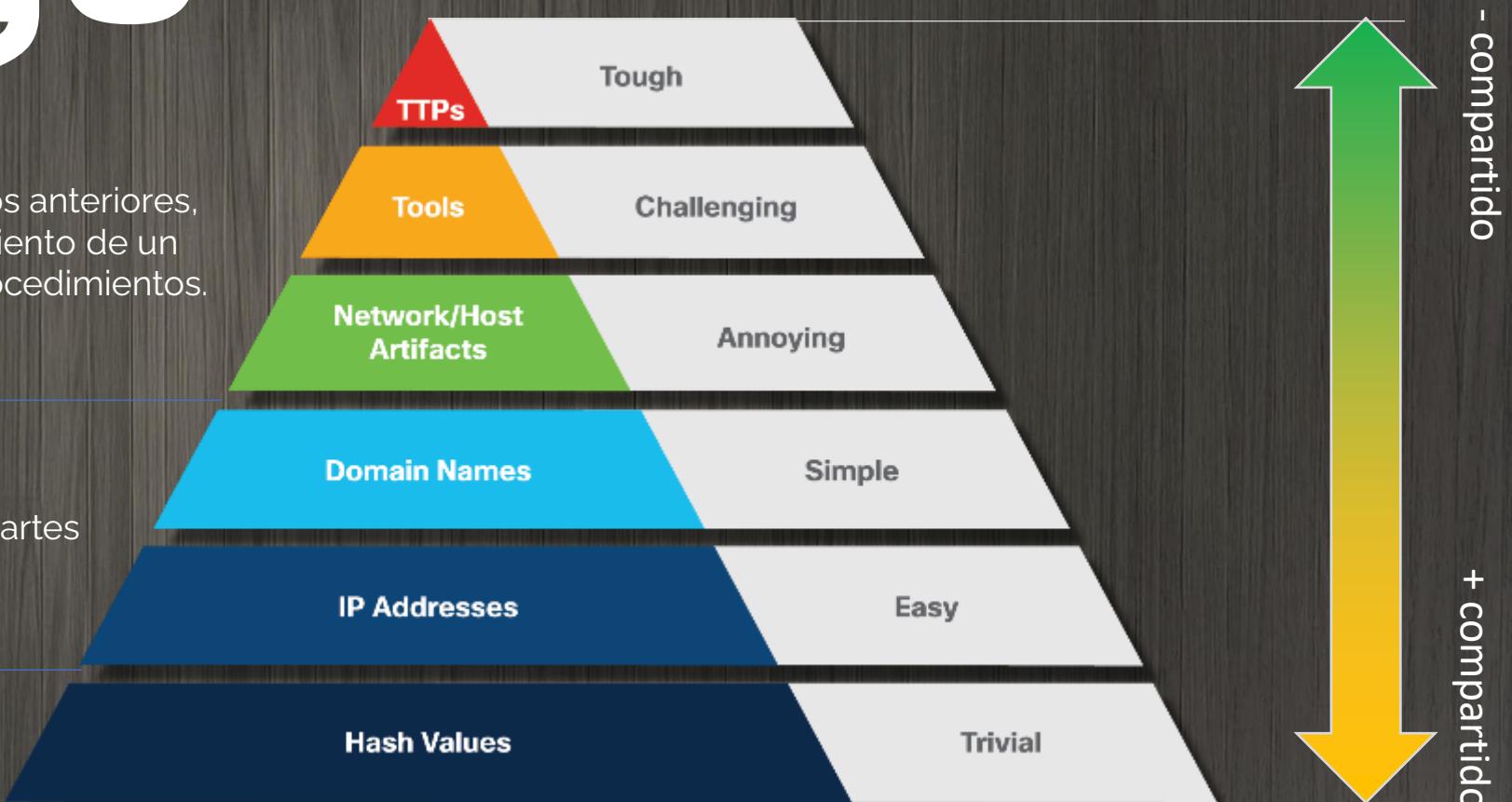
los que a partir del tratamiento de los anteriores, permiten representar el comportamiento de un atacante, sus tácticas, técnicas y procedimientos.

Indicadores atómicos

no pueden ser descompuestos en partes más pequeñas sin perder su utilidad

Indicadores calculados

se derivan de datos implicados en un incidente



Inteligencia Estratégica Identifica el **quién** y el **por qué**

Detecta variaciones de actividad
(comparación del histórico de nº de Incidentes y campañas)
Indicadores de actividad (IOAs)

CISO, CIO, CTO, ...



Inteligencia Operacional Aborda el **cómo**

Detecta comportamiento (TTPs) del enemigo
Indicadores de Comportamiento (IOBs)

Threat Hunters



Inteligencia Táctica Se centra en el **qué** y **dónde**

Detecta HUELLAS del enemigo
Indicadores de Compromisos (IOCs) que conocemos del enemigo

Detecta comportamiento anómalo
Anomalías de comportamiento del Sistema (IOABs)

Domain Names

Simple

IP Addresses

Easy

Hash Values

Trivial

SEC-ADMINS



Peticiones DNS unusuales
Cambio de numero de alertas
Actividades fuera de horario

Variación anormal de flujos de trafico (tipo, origen y destino)
Tráfico denegado por firewalls o IPS
Entradas de registro o cambios en ficheros de sistema.

Anomalías

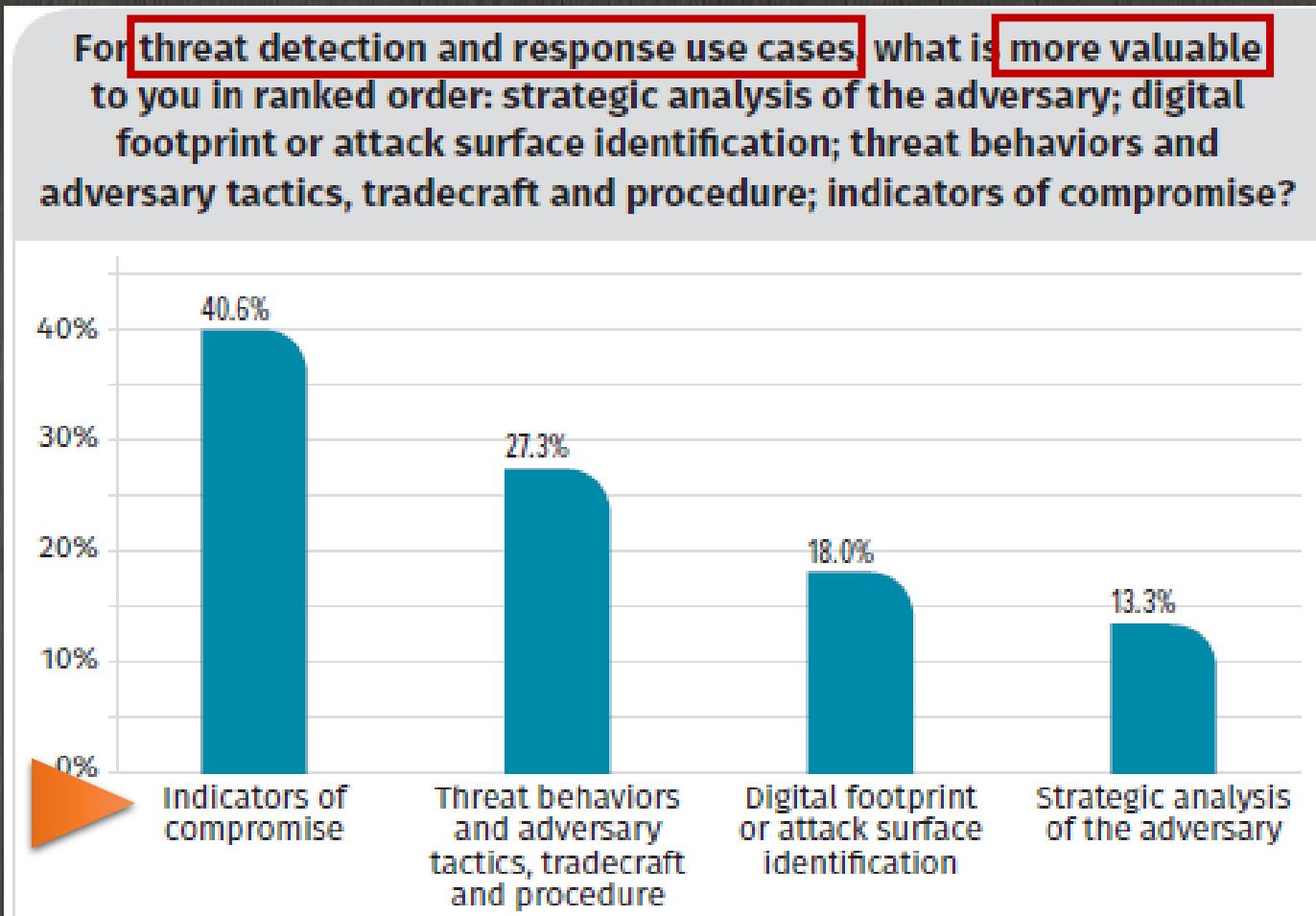
Comportamientos

Huellas

IOC,s

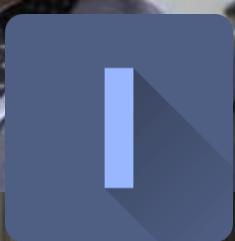
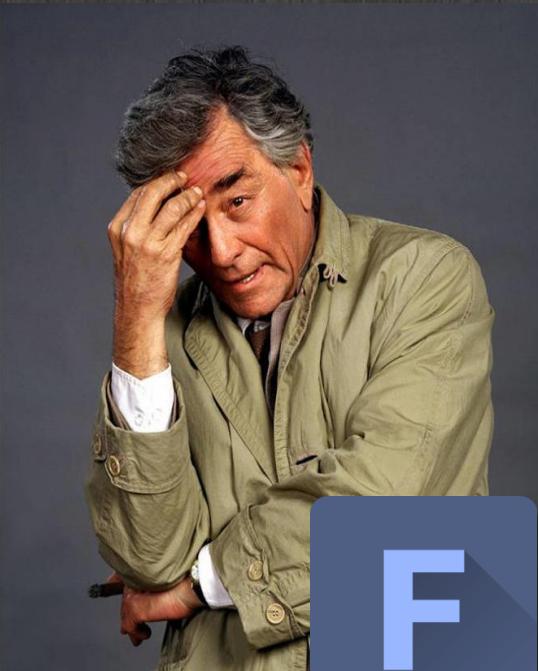


IOA,s



¿QUÉ PRODUCE MAYOR VALOR? (promedio)





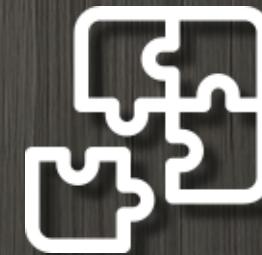
PRECISA



CONFIALBE



OPORTUNA



RELEVANTE



ACCIONABLE

CTIs ...How to??



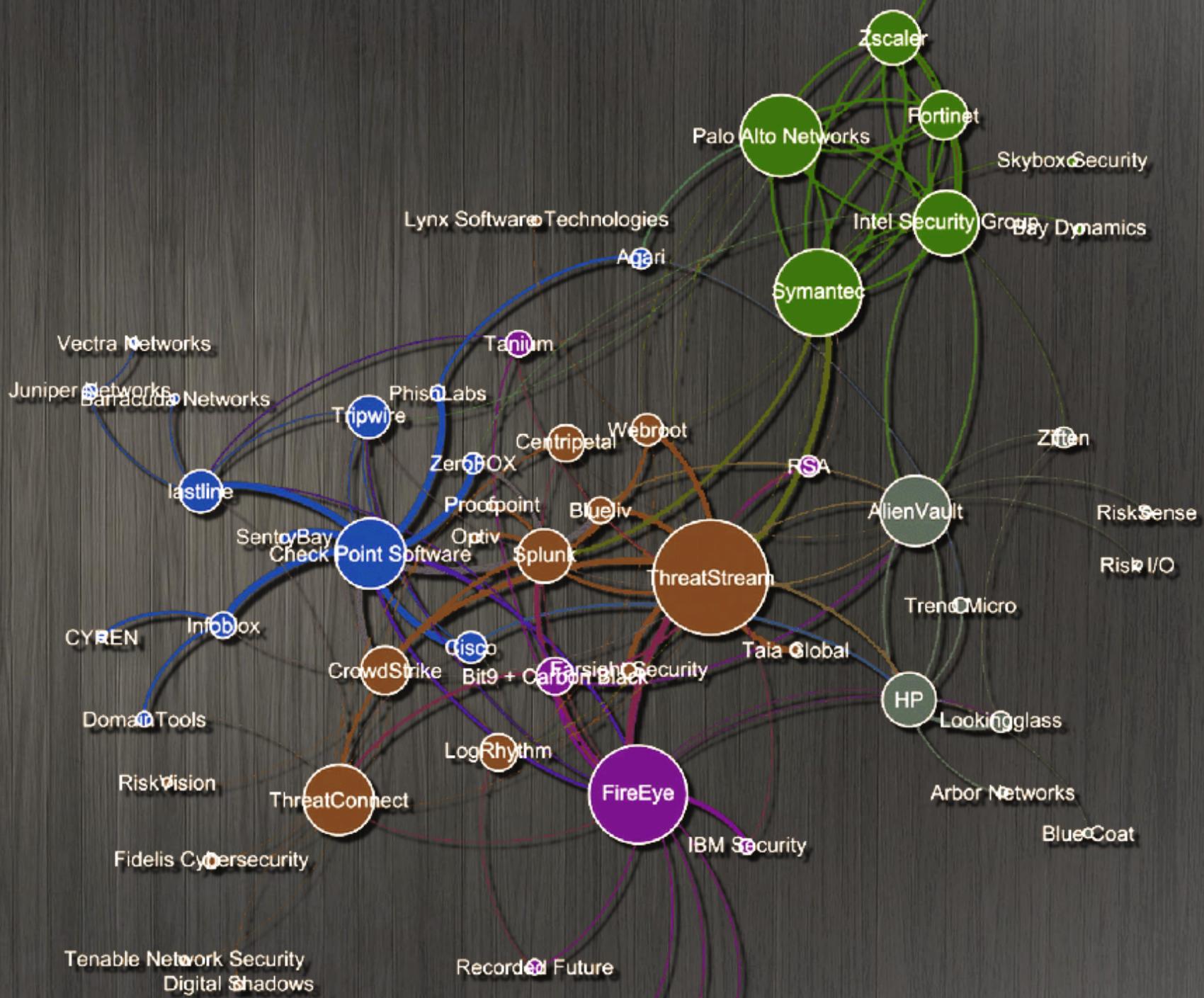
FEEDS



TIP



“Threat intelligence sharing
between cybersecurity
vendors”



ALL YOU
NEED IS
LOGS

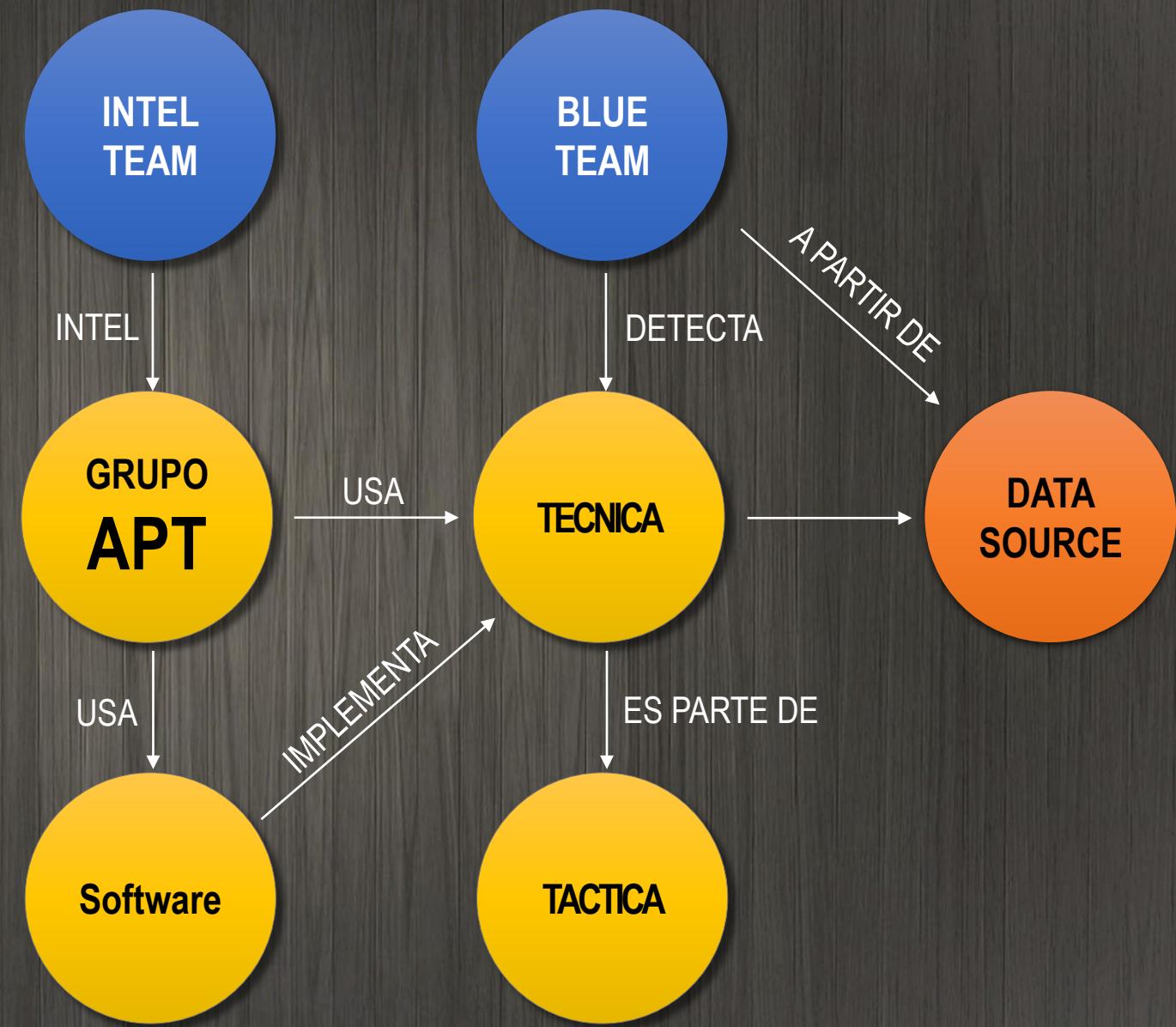
2 APROXIMACIONES

TODO

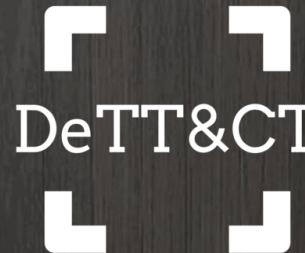
vs



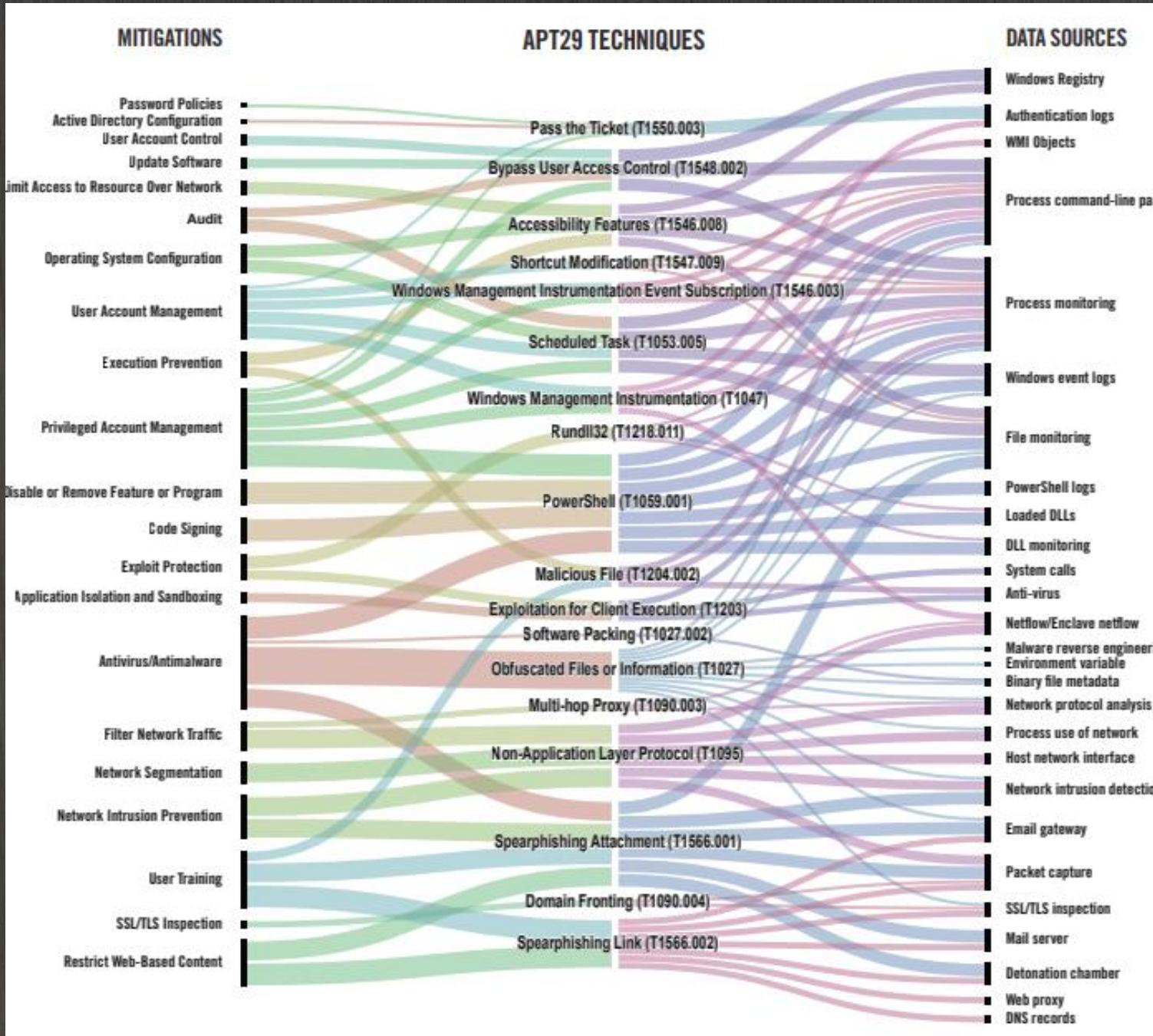
DATA SOURCES



MITRE



MITIGAR



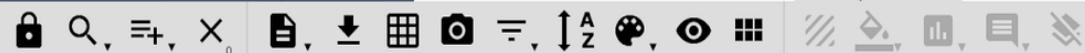
DÉTECTAR

compartir

...TOOLS ??



EL MODELADO DE AMENAZAS



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	Accessibility Features	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Data Encrypted	Data Transfer Size Limits	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	Credentials in Files	Data from Information Repositories	Data Transfer Size Limits	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	CMSTP	Credentials in Registry	Exploitation of Remote Services	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Network Share Discovery	Pass the Hash	Data from Removable Media	Data from Removable Media	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Hooking	Network Sniffing	Pass the Ticket	Exfiltration Over Other Network Medium	Domain Fronting	Fallback Channels
Trusted Relationship	Graphical User Interface	Browser Extensions	Dylib Hijacking	Component Object Model Hijacking	Input Capture	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Multi-hop Proxy
Valid Accounts	InstallUtil	Change Default File Association	Exploitation for Privilege Escalation	Control Panel Items	Input Prompt	Peripheral Device Discovery	Remote File Copy	Email Collection	Exfiltration Over Physical Medium	Multi-stage Channels
	Launchctl	Component Firmware	Extra Window Memory Injection	DCShadow	Kerberoasting	Replication Through Removable Media	Remote Services	Input Capture	Input Capture	Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	File System Permissions Weakness	Deobfuscate/Decode File or Information	Keychain	Man in the Browser	Replication Through Removable Media	Scheduled Transfer	Scheduled Transfer	Multilayer Encryption
	LSASS Driver	Create Account	File System Permissions Weakness	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Permission Groups Discovery	Screen Capture	Screen Capture	Screen Capture	Port Knocking
	Mshta	DLL Search Order Hijacking	Hooking	DLL Search Order Hijacking	Network Sniffing	Process Discovery	Shared Webroot	Video Capture	Video Capture	Remote Access Tools
	PowerShell	Dylib Hijacking	Image File Execution Options Injection	DLL Side-Loading	Password Filter DLL	Remote System Discovery	Taint Shared Content	Third-party Software	Third-party Software	Remote File Copy
	Regsvcs/Regasm	External Remote Services	Launch Daemon	Exploitation for Defense Evasion	Private Keys	Security Software Discovery	Windows Admin Shares	Windows Admin Shares	Windows Admin Shares	Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	New Service	Extra Window Memory Injection	Securityd Memory	System Information Discovery	Windows Remote Management	Windows Remote Management	Windows Remote Management	Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Path Interception	Two-Factor Authentication Interception	System Network Configuration Discovery	System Network Configuration Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Plist Modification	File Deletion	File Permissions Modification	System Network Configuration Discovery				Uncommonly Used Port
	Scripting	Image File Execution Options Injection	Port Monitors	File System Logical Offsets	Gatekeeper Bypass	System Network Connections Discovery				Web Service
	Service Execution	Hypervisor	Process Injection	Hidden Files and Directories	Hidden Users	System Network Connections Discovery				
	Signed Binary Proxy Execution	Kernel Modules and Setuid	Scheduled Task	Hidden Users	Hidden Window	System Owner/User Discovery				
	Signed Script Proxy Execution	Setuid	Service Registry Permissions Weakness							

Structured Threat Information eXpression
18 STIX Domain Objects



Trusted Automated
Exchange of Intelligence
Information



SERVER



SERVER O CLIENT

A screenshot of a web-based interface titled "Malicious activities". On the left is a sidebar with details about an event:

- Event ID: 10878
- Uuid: Saec700c-0eb8-468
- Org: CIRCL
- Owner org: CIRCL
- Contributors: alexandre.dulaunoy
- Email: alexandre.dulaunoy
- Tags: [empty]
- Date: 2018-05-04
- Threat Level: Low
- Analysis: Initial
- Distribution: All communities
- Info: Malicious activities
- Published: No
- #Attributes: 2
- Last change: 2018/05/04 02:38:1
- Extends:
- Extended by:
- Sightings: 0 (0)
- Activity:

On the right is a network graph visualization showing various nodes connected by lines, representing relationships between malicious activities.



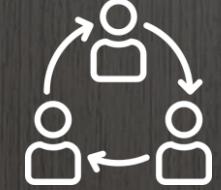
Malware Information
Sharing Platform



compartir ... a/de QUIEN ??



CERT-CSIRT SHARING ORGANIZATIONS



Compartir, Cooperar, Divulgar



MUNDO



TF-CSIRT
Trusted Introducer
EUROPA



CSIRT.es

ESPAÑA

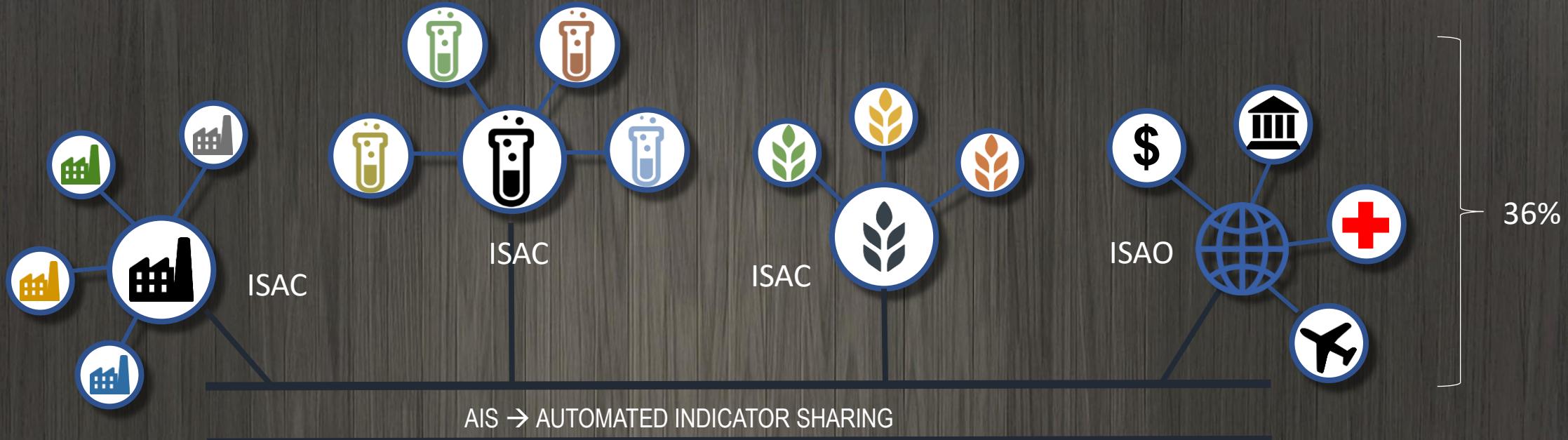


CRISIS



USA → CISA → CISCP

CISCP: CYBER INFORMATION SHARING AND COLLABORATION PROGRAM

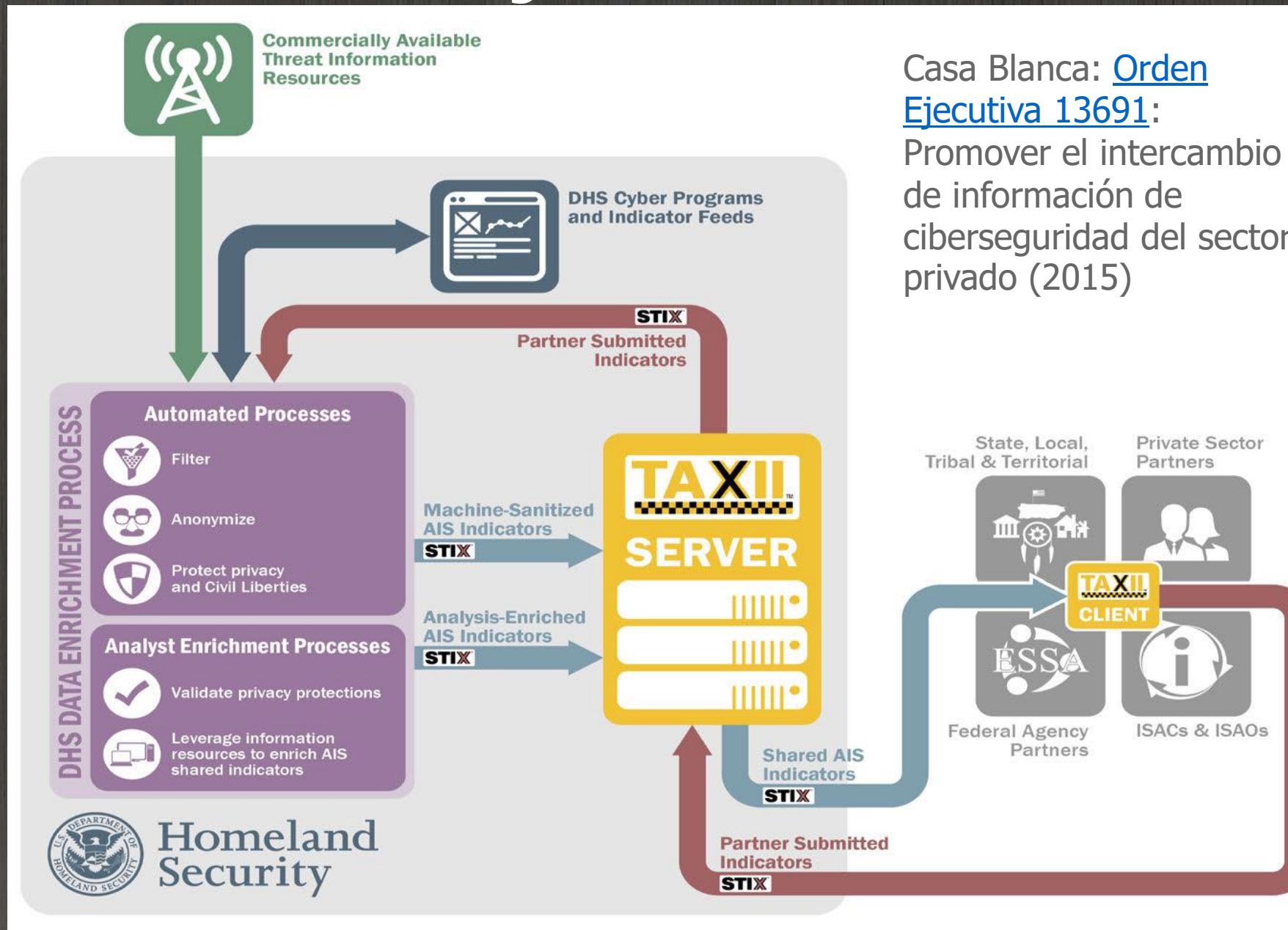


ISAC: Information Sharing and Analysis Center

ISAO: Information Sharing and Analysis Organization



CISCP → FLUJO DE CTIs → AIS



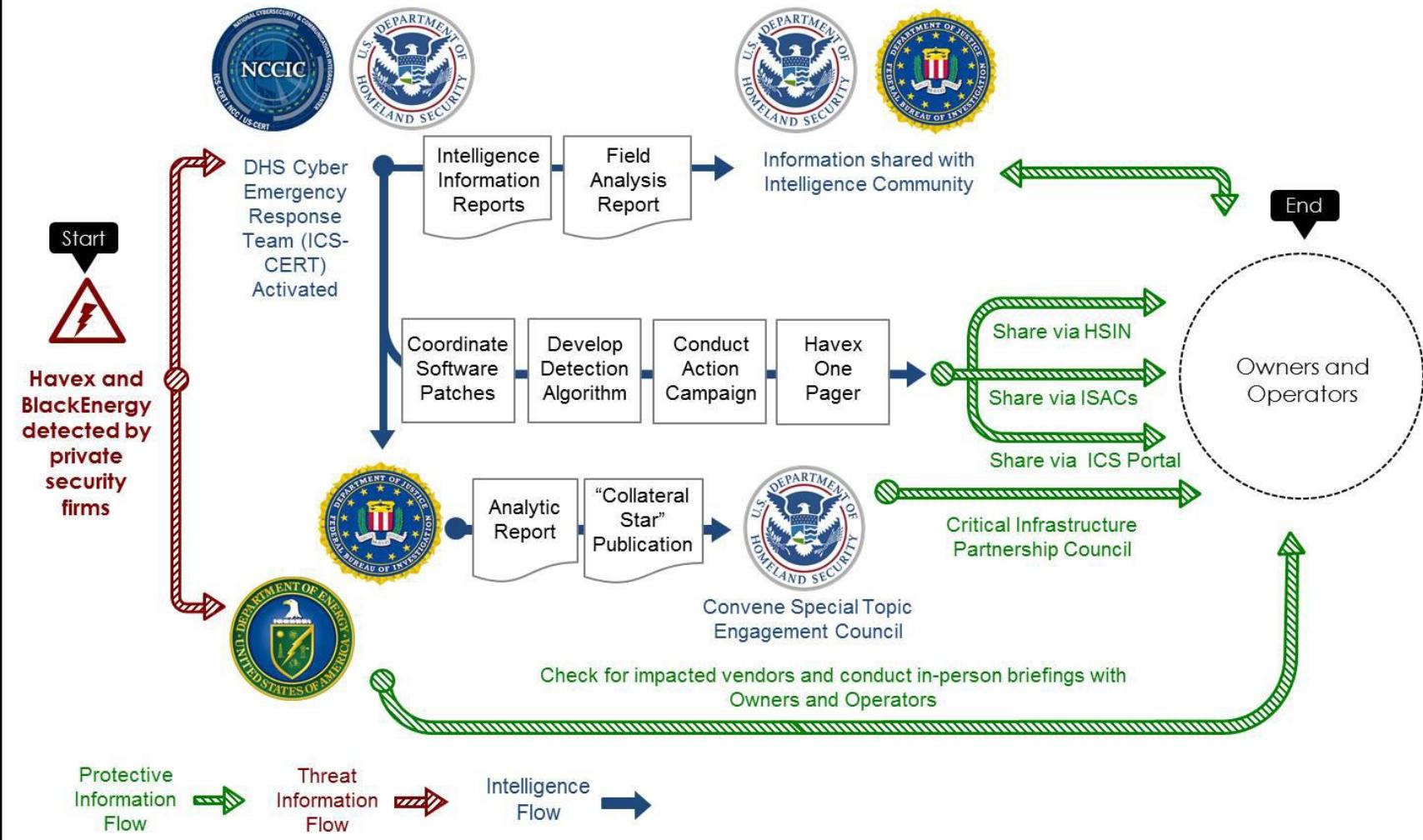
Casa Blanca: [Orden Ejecutiva 13691](#):

Promover el intercambio de información de ciberseguridad del sector privado (2015)



CISCP → CASOS DE USO

Use Case 1 - Cyber Use Case: Havex and BlackEnergy Malware





El modelo ESPAÑOL

Real Decreto 43/2021, de 26 de enero - desarrolla el RDL 12/2018, de seguridad de las redes y sistemas de información
→ Artículo 11. Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes



Guía CCN-STIC-423 Indicadores de Compromiso
Guía CCN-STIC-424 Intercambio de Información de Ciberamenazas. STIX-TAXII



CCN-CERT → REYES



Feeds



MISP
Federados



Feeds

Comunidad
CCN





RNS: la obligación de compartir



**Red
Nacional de
SOC**

- Vulnerabilidades e incidentes
- Reglas de detección
- Listas negras
- Listas blancas
- TTP de nuevas amenazas
- Reglas de detección
- Casos de uso
- Almacenamiento de Inteligencia
- IOA para investigaciones conjuntas



BENEFICIOS DE COMPARTIR

SEC AWARENESS



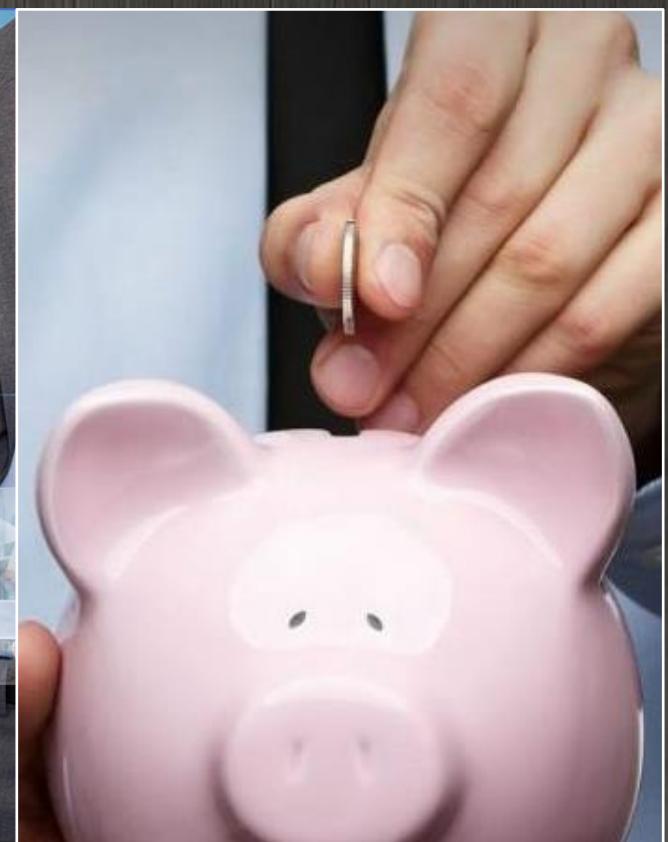
OK READY



SELECT PEOPLE WHERE...



< COSTES

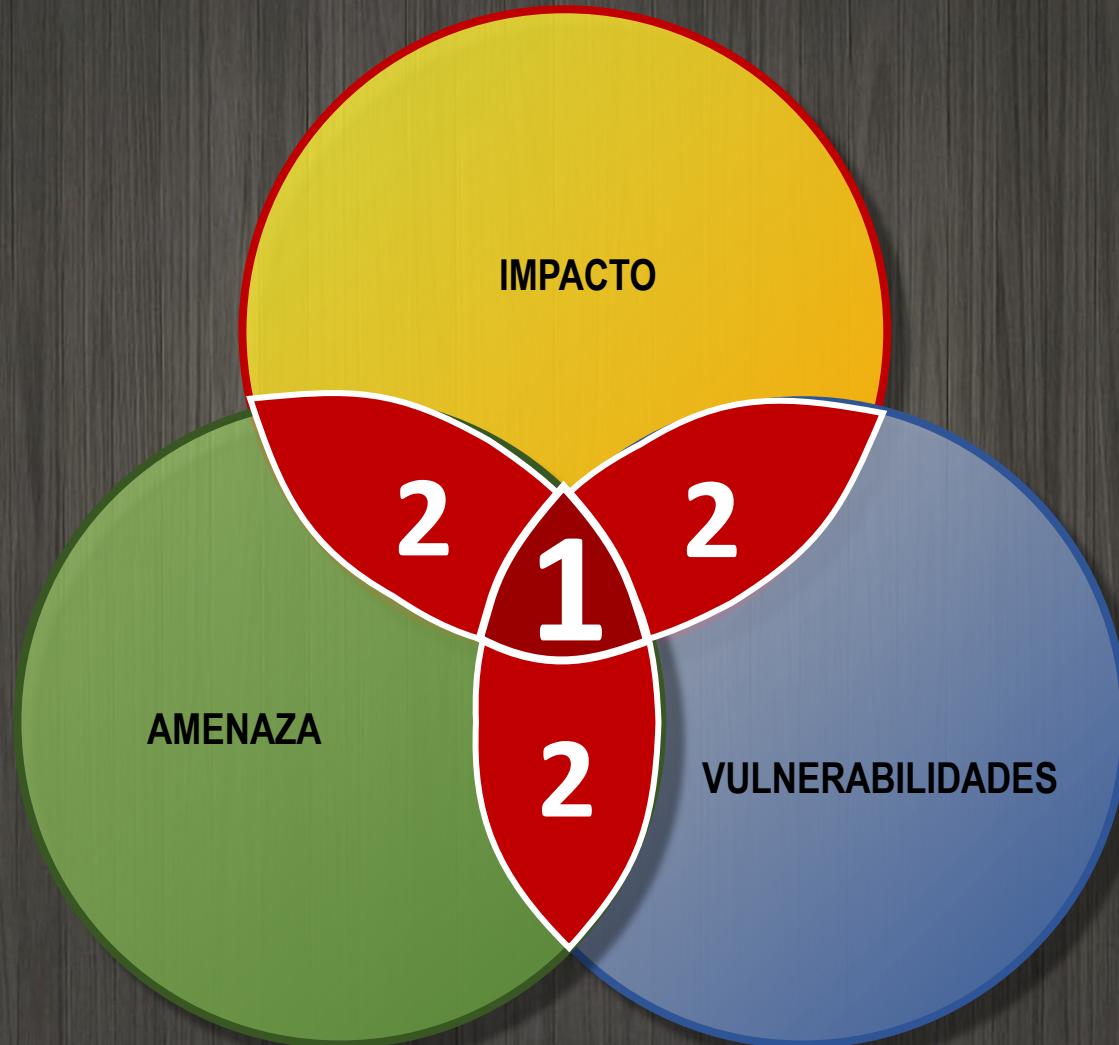


compartir

CONCLUYENDO



RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



RECAPITULANDO: SOC - CTI - INTEL



- Los Centros de Operaciones de Seguridad (SOC / COS) son la piedra angular en la lucha contra el cibercrimen.
- CTI no es la respuesta a todas las preguntas, pero la CTI debe ser parte fundamental de la ciber defensa
- La Inteligencia de Amenazas hace a los Equipos de Seguridad **un 33% mas eficaces**
- **LA INTELIGENCIA VALE MUCHO MAS SI SE COMPARTE**



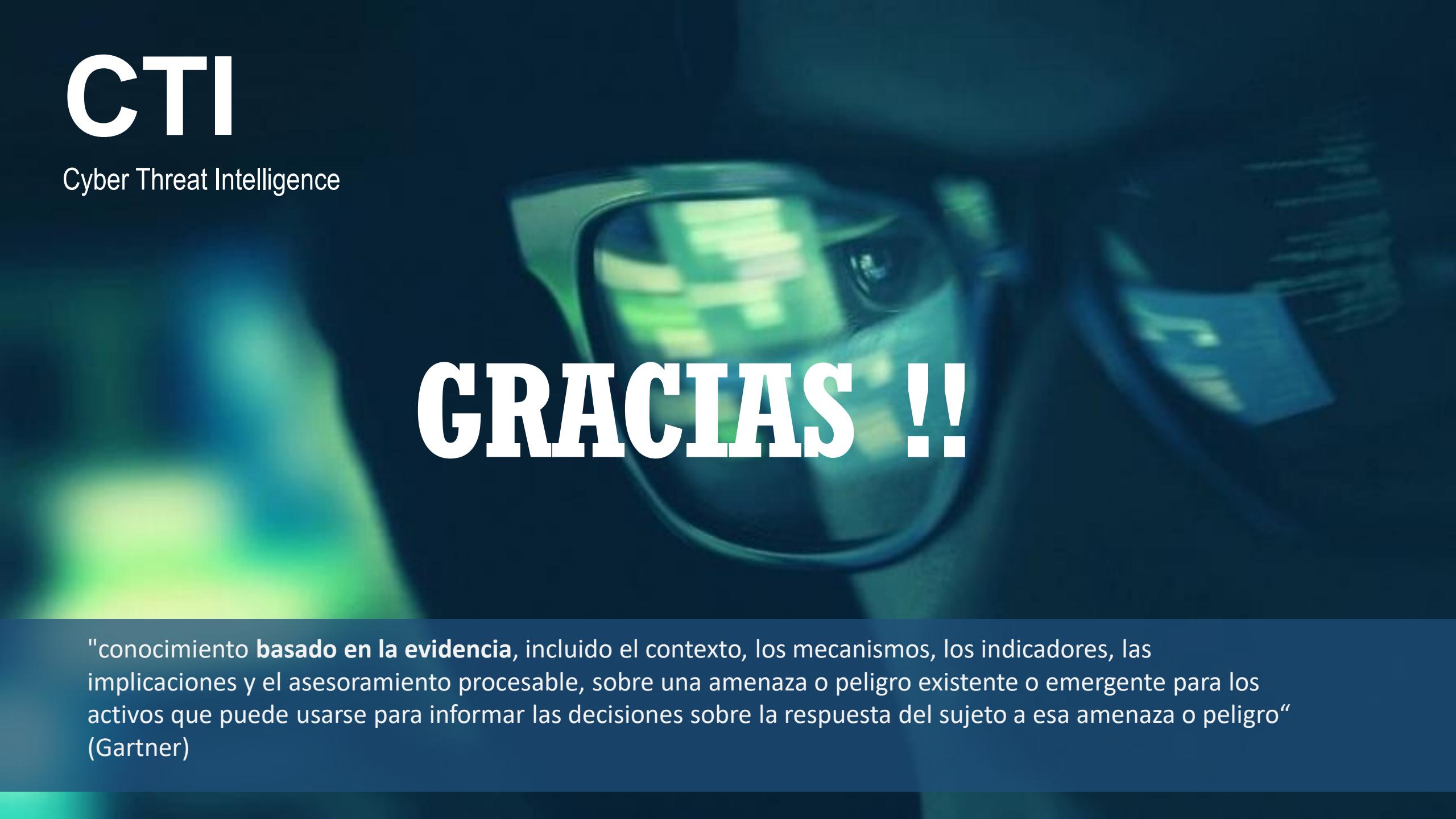
CIBER CONSEJO

NO SUBVALORAR LA AMENAZA !!
El adversario superará tus defensas
y terminará por escalar privilegios



CTI

Cyber Threat Intelligence



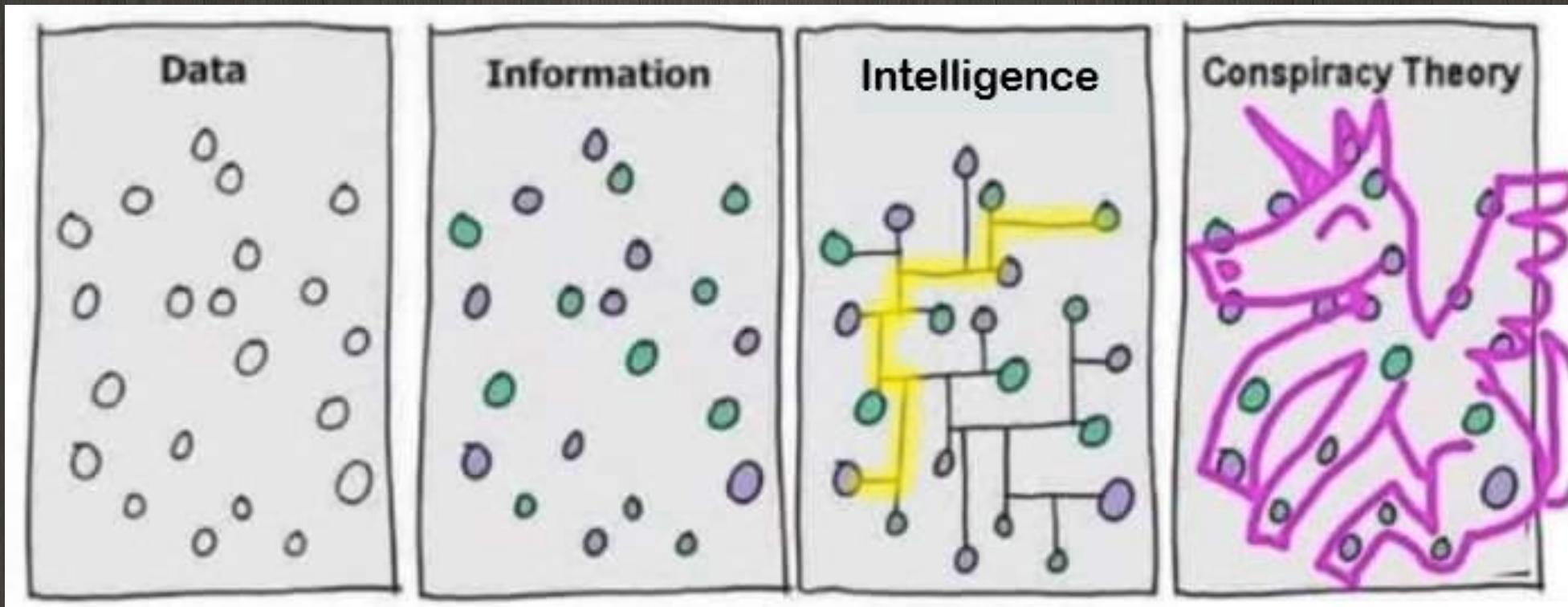
GRACIAS !!

"conocimiento **basado en la evidencia**, incluido el contexto, los mecanismos, los indicadores, las implicaciones y el asesoramiento procesable, sobre una amenaza o peligro existente o emergente para los activos que puede usarse para informar las decisiones sobre la respuesta del sujeto a esa amenaza o peligro"
(Gartner)

LA SOLUCIÓN AL INTERCAMBIO DE CTIs

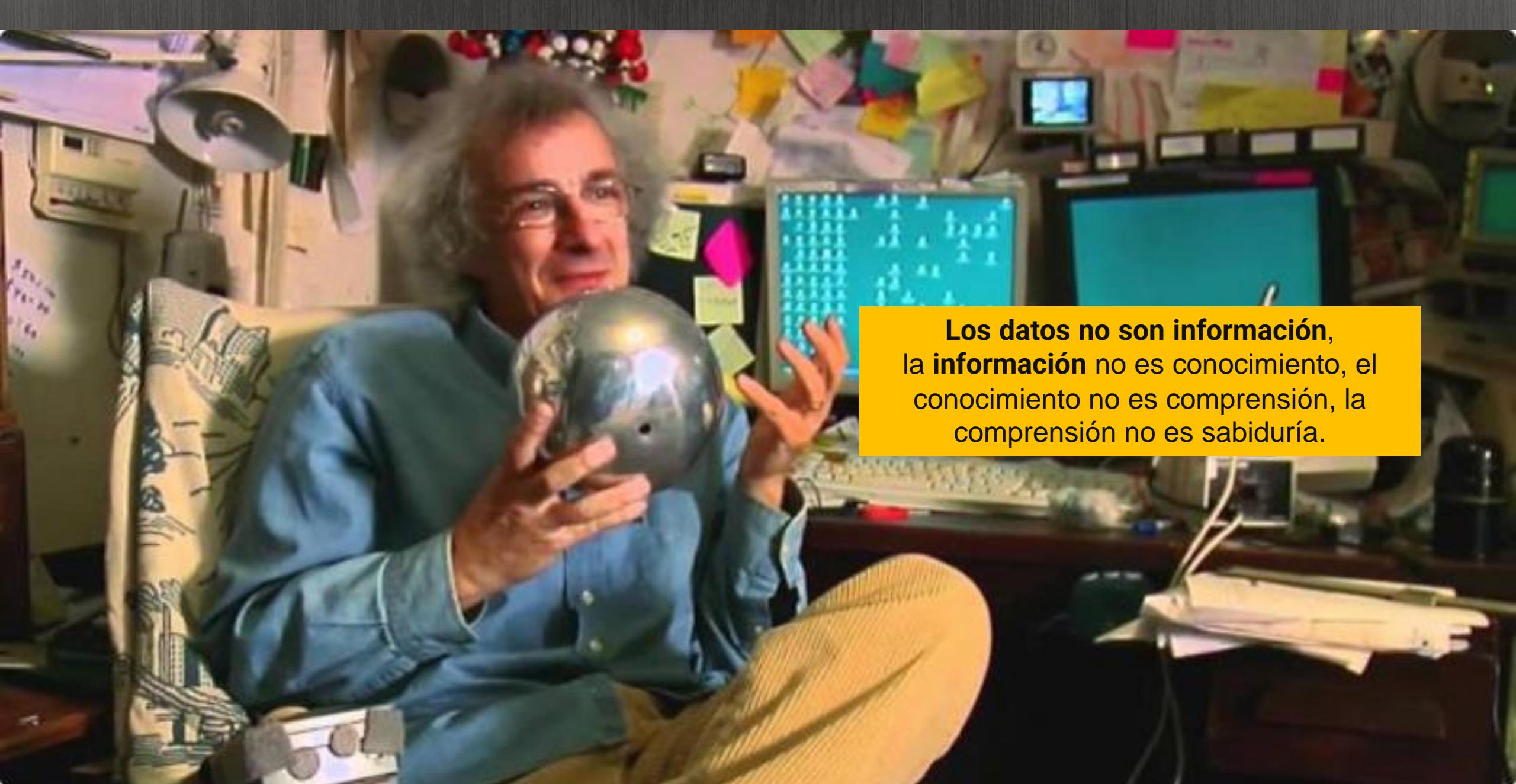


CICLO INFORMAL DE INTELIGENCIA



← Procesos automatizados → Análisis → Cervezas →





**Los datos no son información,
la información no es conocimiento, el
conocimiento no es comprensión, la
comprensión no es sabiduría.**

Clifford Stoll, autor de 'El huevo del cuco'

BIBLIOGRAFIA

ENQUETAS

- IS SHARING CARING? - Grace Chi
- 2021 SANS Cyber Threat Intelligence (CTI) Survey
- 2022 SANS Cyber Threat Intelligence (CTI) Survey
- 2019 Ponemon - Value of Threat Intelligence
- Cybersecurity Information Sharing Incentives and Barriers - Priscilla Koepke
- INFORMATION SHARING FOR CYBER THREATS - Vasil RIZOV
- NCIA - MISP Pre-CC20 Training - OTAN
- D2.2 Threat sharing methods comparative analysis - Cyber-Trust
- Critical Infrastructure Threat Information Sharing Framework - Homeland Security
- CTI Capability Maturity Model - ENISA (MARCO LOURENCO 2018)
- CTI Model An Evaluation of Taxonomies Sharing Standards and Ontologies
- Guide to CTI Sharing - NIST
- ODNI - Cyber Threat Framework Overview
- MITRE - Building a National Cyber Information-Sharing Ecosystem, 2017
- Cuaderno de Estrategia 185 - IEEE
- CCN-STIC 423 - Indicadores de Compromiso
- CCN-STIC 424 - INTERCAMBIO DE INFORMACIÓN DE CIBERAMENAZAS (2015)

ESTUDIOS E INFORMES

GUÍAS



```
<profile>
  <name>Emilio Rico</name>
  <prompt>FOCE@MCCE:~# </prompt>
  <SecMode>/RootedCON ON</SecMode>
  <jobs>
    <day>Analista de Seguridad</day>
    <night> Reader, ProtAAPP follower</night>
  </jobs>
  <![CDATA[
    Twitter: @Emilio_RR
    #CyberDefence #CyberSecurity
    Interested in C-
  ]]>
</profile>
```

