PROTAAAPP
PROTEGE LAS ADMINISTRACIONES PÚBLICAS
PRODUCTIONS

&

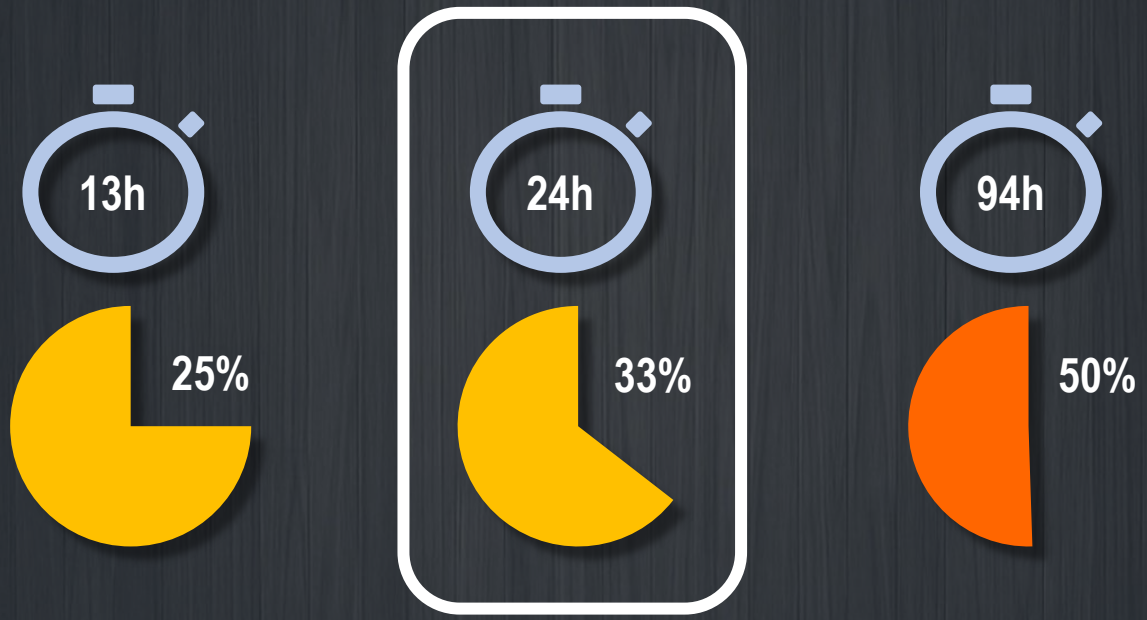
/Rooted CON
ENTERTAINMENT

PRESENTAN

Pero … ¿Qué me estás contando?

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

https://www.itdigitalsecurity.es/

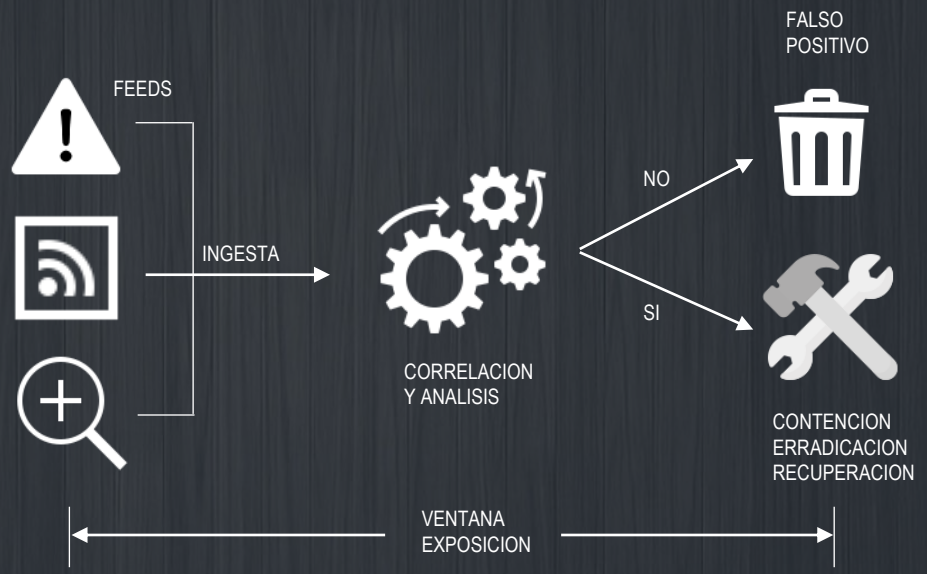


https://www.itdigitalsecurity.es/

1

AUMENTAR LA CAPACIDAD DE

DETECCION



2

COMPARTIR

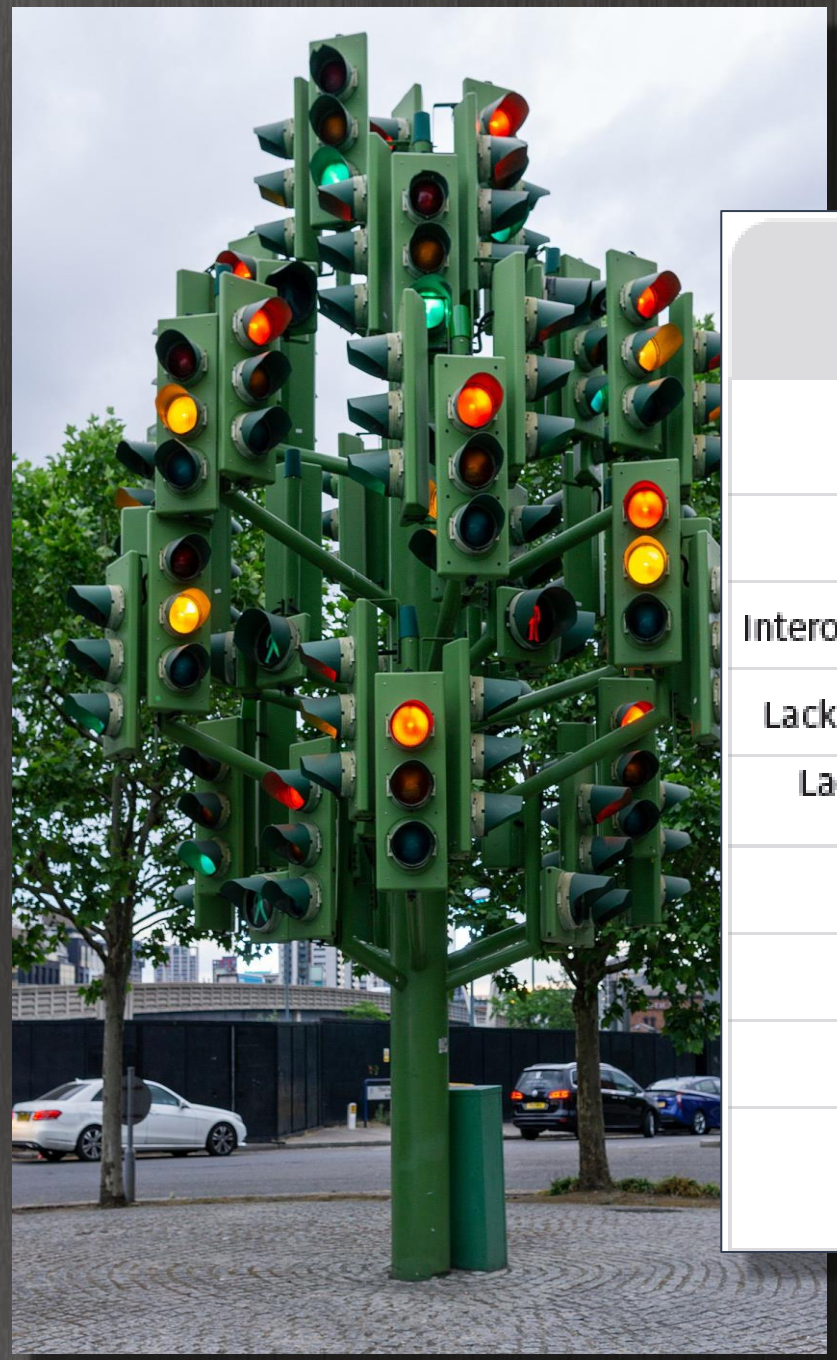
44% % de los analistas de amenazas que hacen públicos sus descubrimientos

52% % de analistas que trabajan en inteligencia de amenazas (o ciberseguridad) y no pueden compartir sus hallazgos

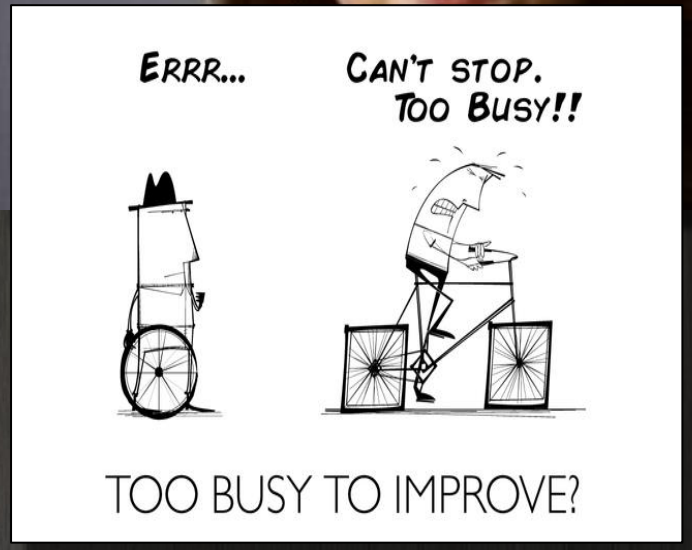
77% % de analistas que comparten información en empresas donde SÍ se permite la colaboración

.....

IT security economics part 4: managing your IT security team | Kaspersky official blog



SANS Survey (2019): The Evolution of Cyber Threat Intelligence


ERRR...
CAN'T STOP.
TOO BUSY!!
TOO BUSY TO IMPROVE?

Compartir: Qué?

IOC,s

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

IOC,s

Indicadores conductuales

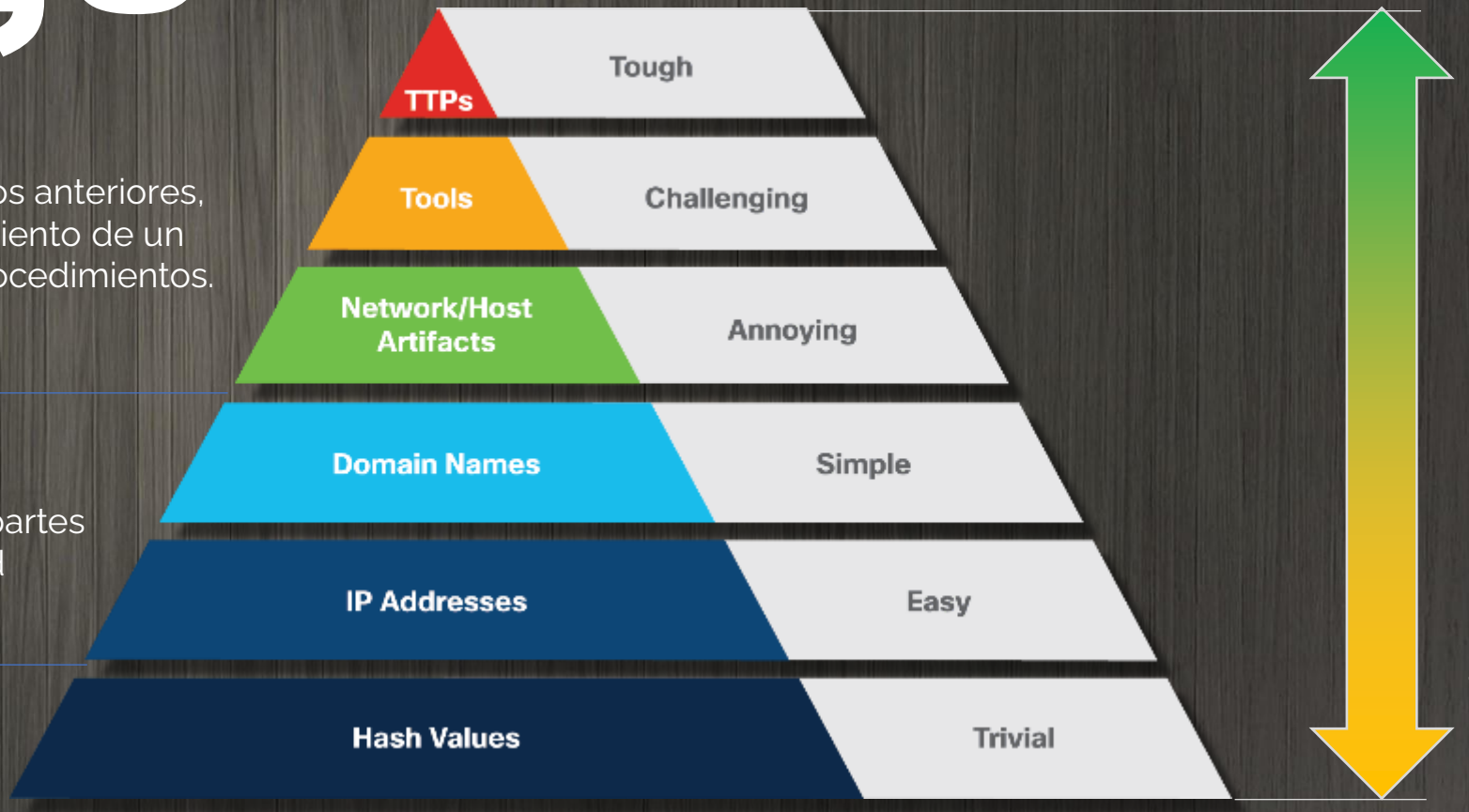
los que a partir del tratamiento de los anteriores, permiten representar el comportamiento de un atacante, sus tácticas, técnicas y procedimientos.

Indicadores atómicos

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

Indicadores calculados

se derivan de datos implicados en un incidente



The Pyramid of Pain | Enterprise Detection & Response (detect-respond.blogspot.com)

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)

CAMPAÑAS
INCIDENTES A IC

CISO, CIO, CTO, ...

Inteligencia Operacional
Aborda el **cómo**

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

TTPs — Tough
Tools — Challenging
Network/Host Artifacts — Annoying

Comportamientos

Threat Hunters

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

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

Domain Names — Simple
IP Addresses — Easy
Hash Values — Trivial

Huellas

SEC-ADMINS

Detecta comportamiento anómalo
Anomalías de comportamiento
del Sistema (IOABs)

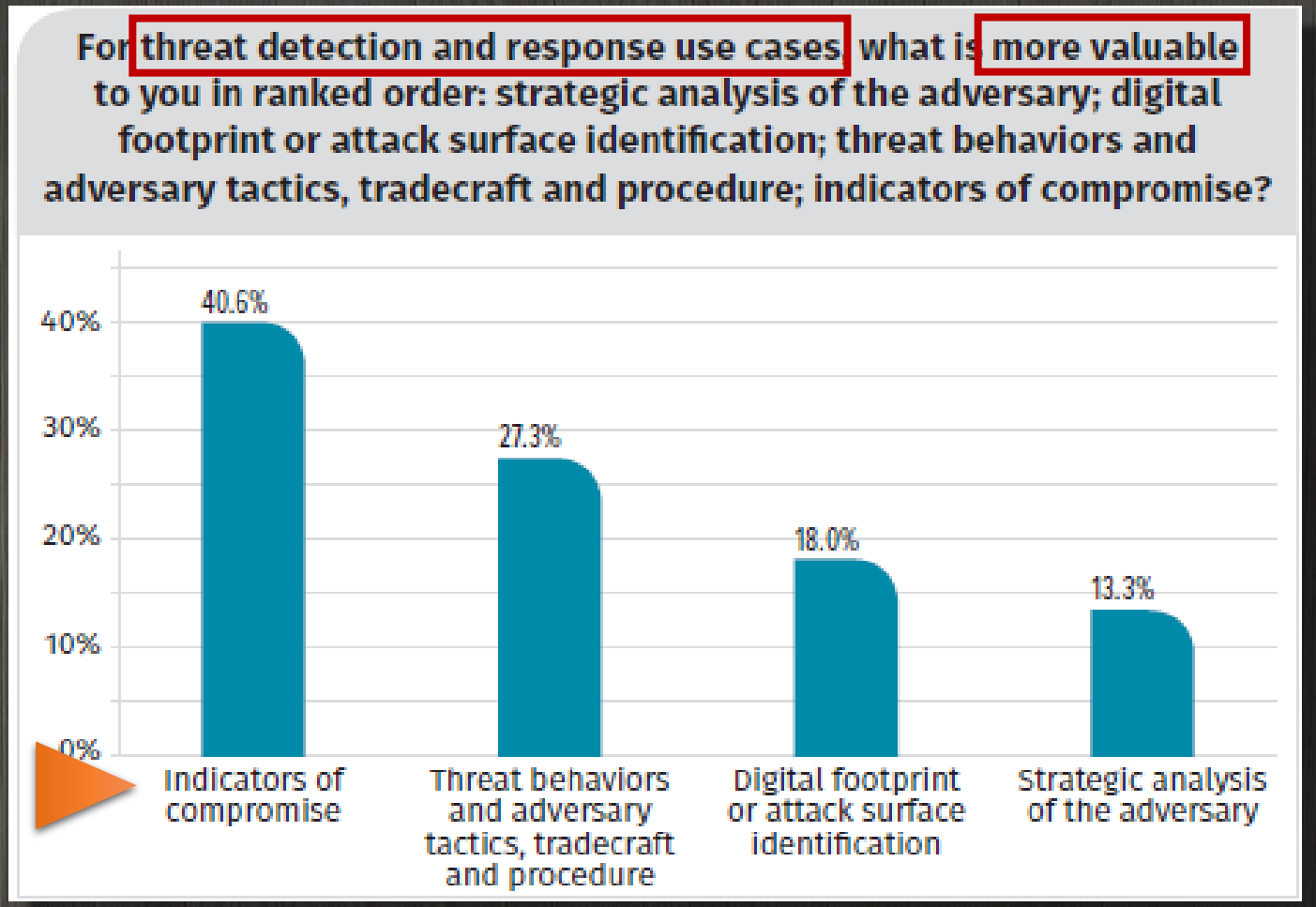
Peticiones DNS unusuales
Cambio de numero de alertas
Actividades fuera de horario

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

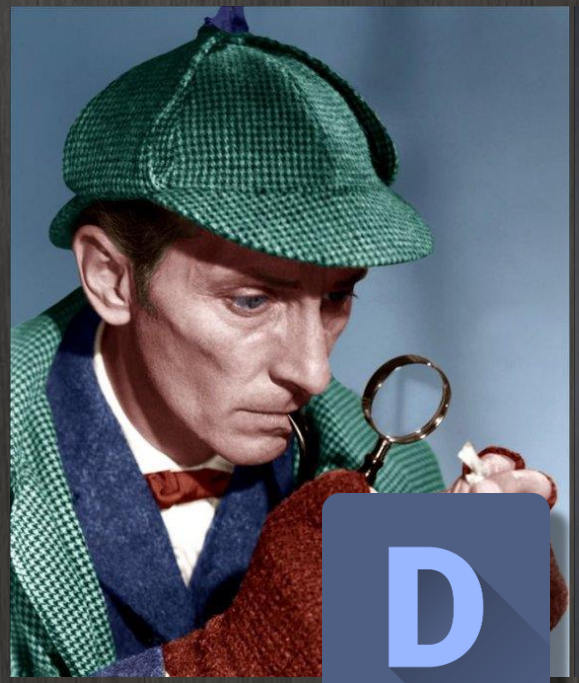
IOC,s

IOA,s

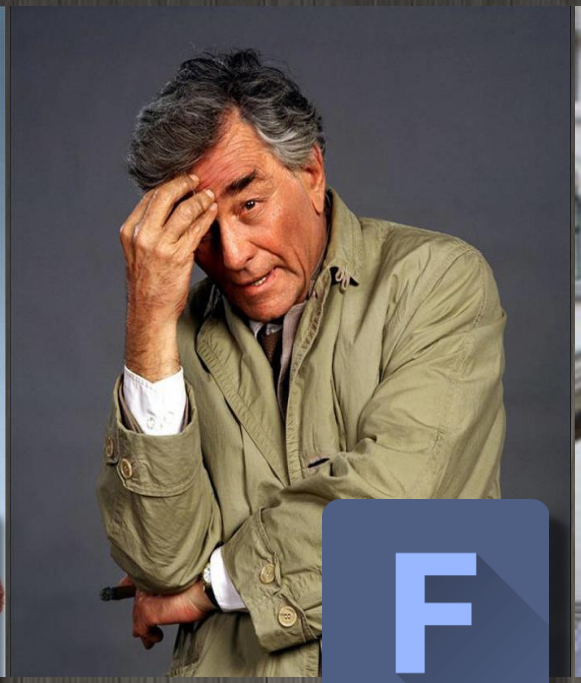


SANS Survey (2019): The Evolution of Cyber Threat Intelligence

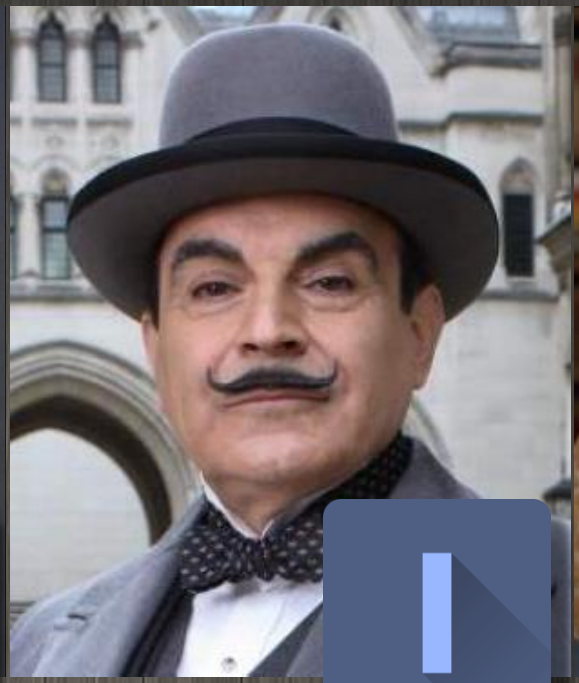

¿QUÉ PRODUCE MAYOR VALOR? (promedio)
1. Información Contextualizada
2. Inteligencia Procesada
3. Datos en Crudo
4. Otros Consejos y Opiniones
5. Apoyo Técnico
6. Apoyo Emocional
INCIDENT RESPONSE
1. Datos en Crudo
2. Inteligencia Procesada
3. Otros Consejos y Opiniones
4. Apoyo Técnico
5. Información Contextualizada
6. Apoyo Emocional
SECURITY OPERATIONS
1. Información Contextualizada
2. Inteligencia Procesada
3. Apoyo Técnico
4. Otros Consejos y Opiniones
6. Datos en Crudo
EXECUTIVE LEADERSHIP
1. Inteligencia Procesada
2. Información Contextualizada
3. Otros Consejos y Opiniones
4. Apoyo Emocional
5. Datos en Crudo
6. Apoyo Técnico



D



F



I

R

PRECISA

CONFIABLE

OPORTUNA

RELEVANTE

ACCIONABLE

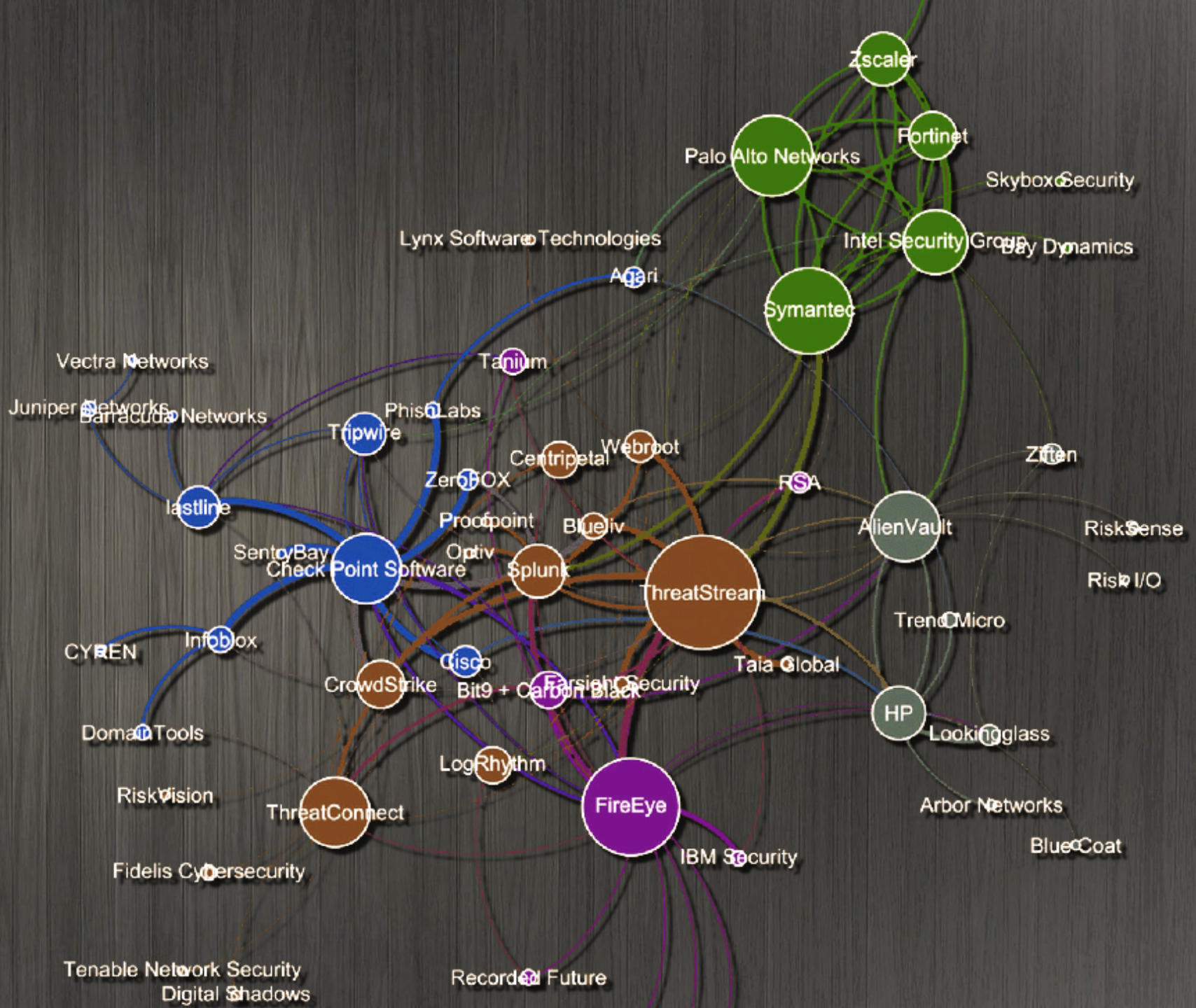
CTIs

...How to??

FEEDS

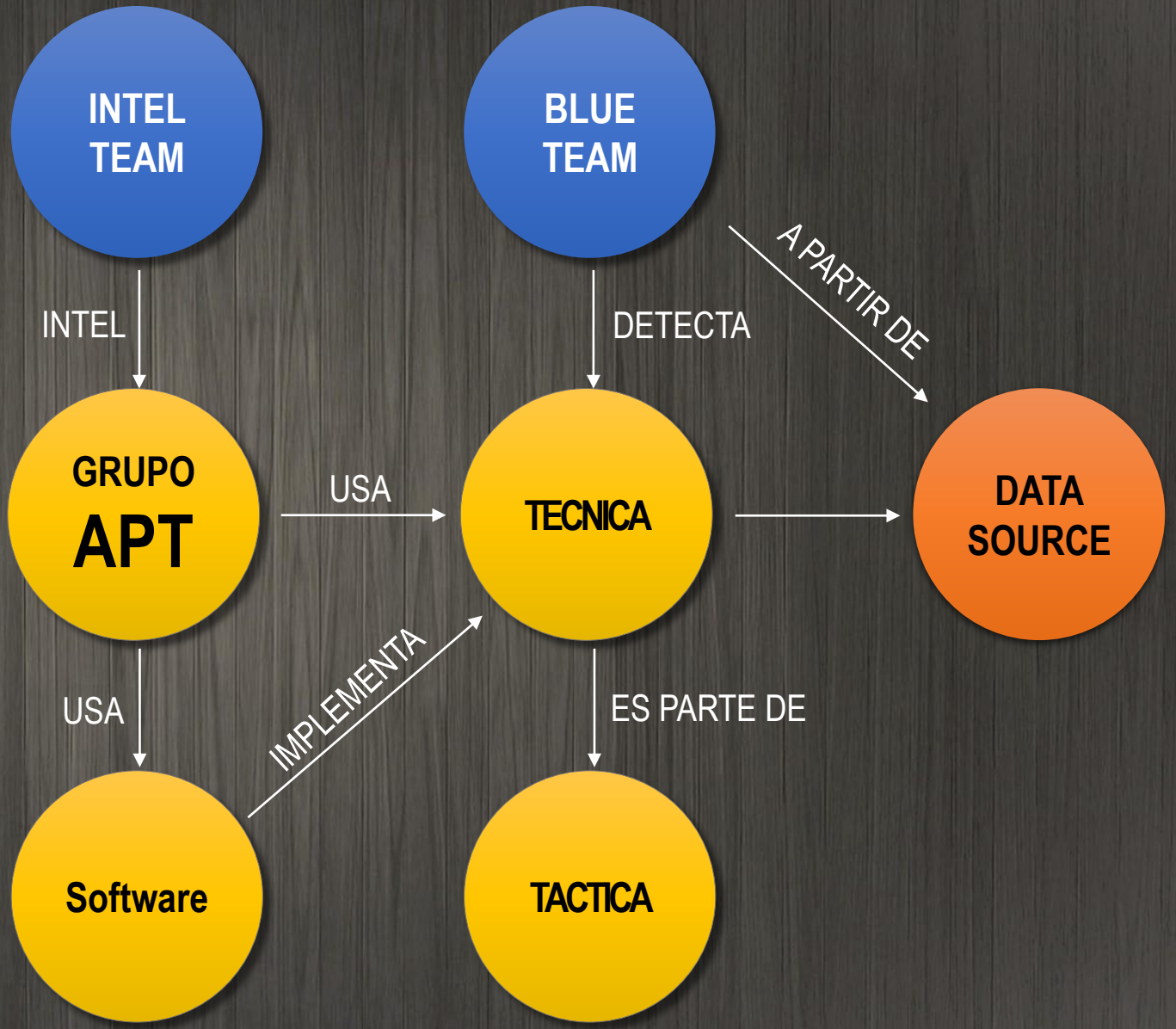
TIP

“Threat intelligence sharing between cybersecurity vendors”




ALL YOU
NEED IS
LOGS
2 APROXIMACIONES
TODO
VS

DATA SOURCES

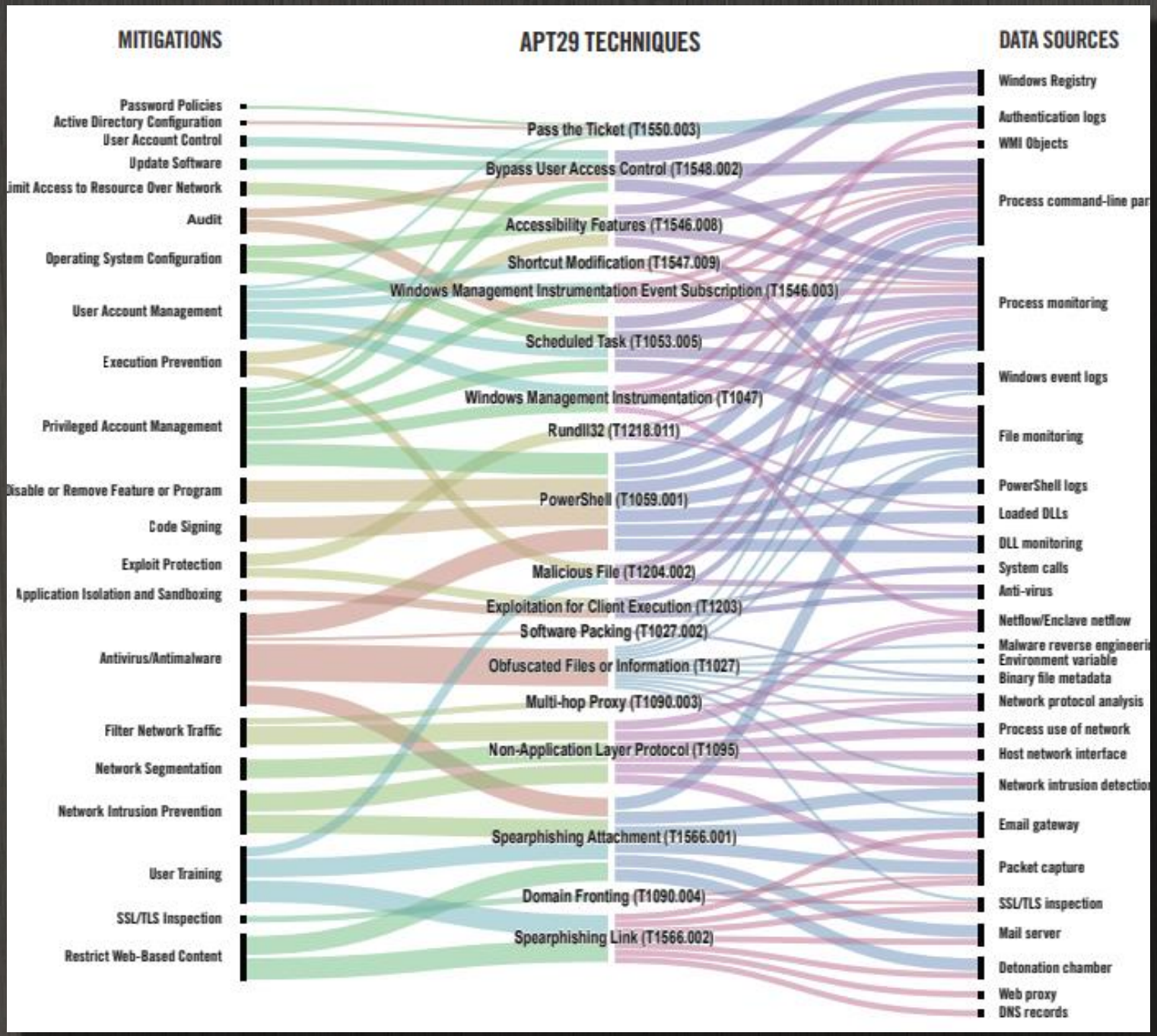


MITRE

DeTT&CT

MITIGAR

DETÉCTAR



ATT&CK-Folding-Map-Feb-2020-FINAL-for-Web (mitre.org)

compartir

...TOOLS ??

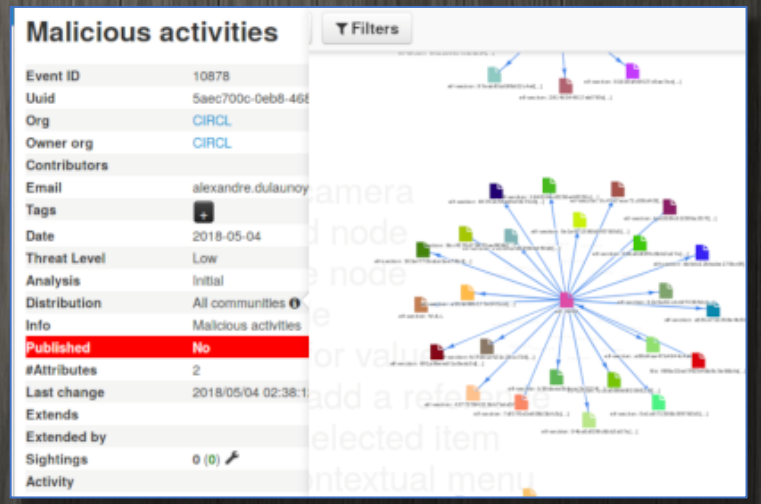
EL MODELADO DE AMENAZAS

Structured Threat Information eXpression

18 STIX Domain Objects

Trusted Automated Exchange of Intelligence Information

SERVER SERVER O CLIENT



MISP Threat Sharing

Malware Information Sharing Platform

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


compartir ... a/de QUIEN ??

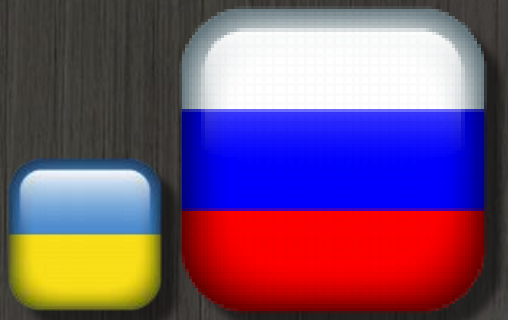
CERT-CSIRT
SHARING ORGANIZATIONS

Compartir, Cooperar, Divulgar

MUNDO

TF-CSIRT
Trusted Introducer
EUROPA

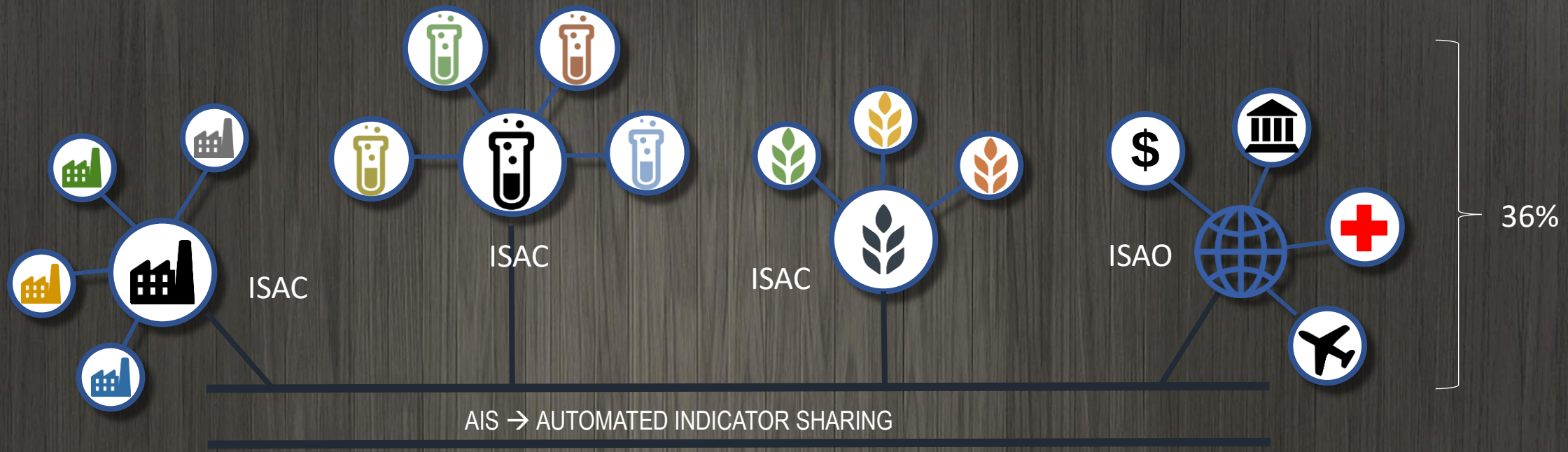
ESPAÑA



CRISIS

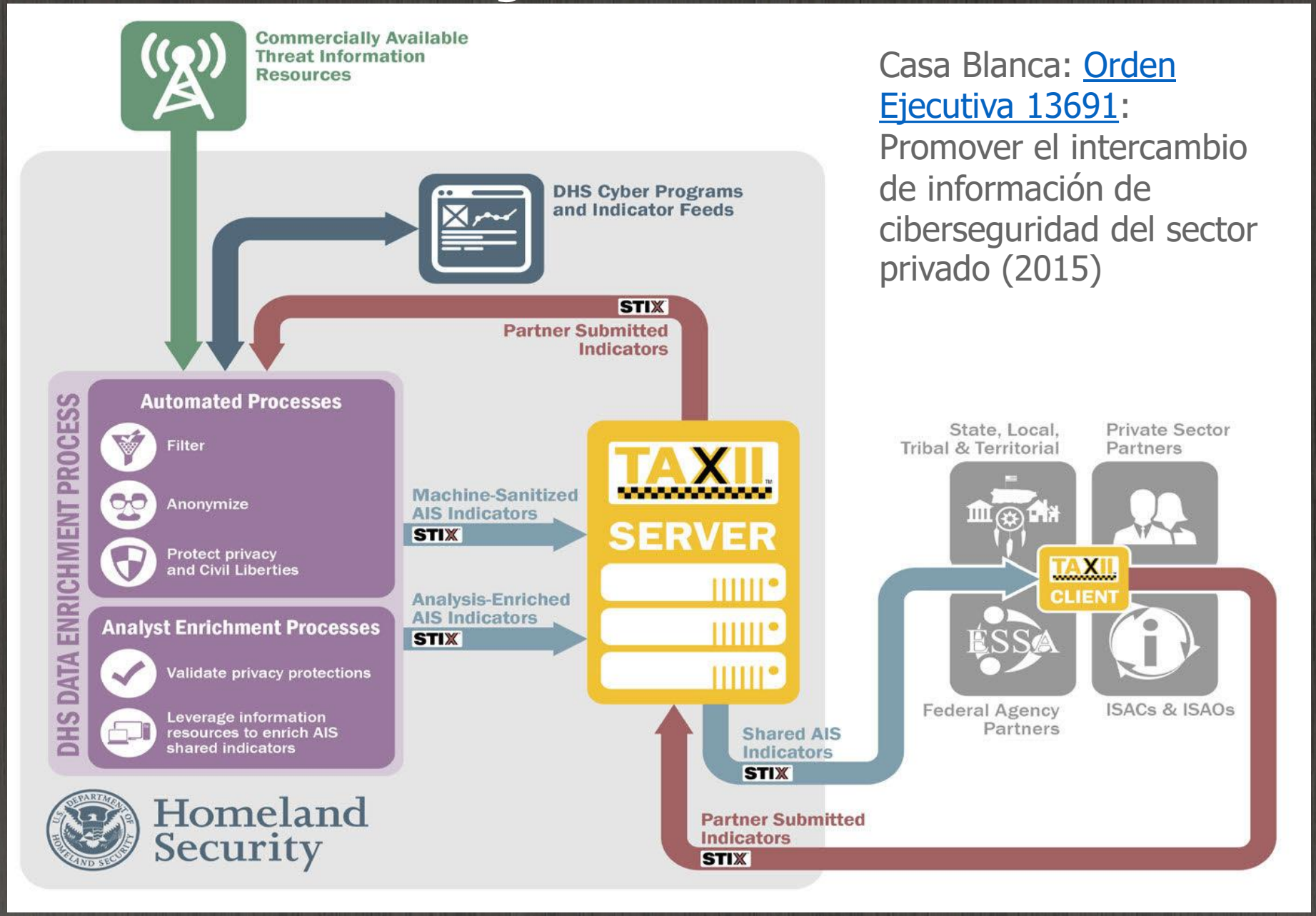
USA → CISA → CISCP

CISCP: CYBER INFORMATION SHARING AND COLLABORATION PROGRAM



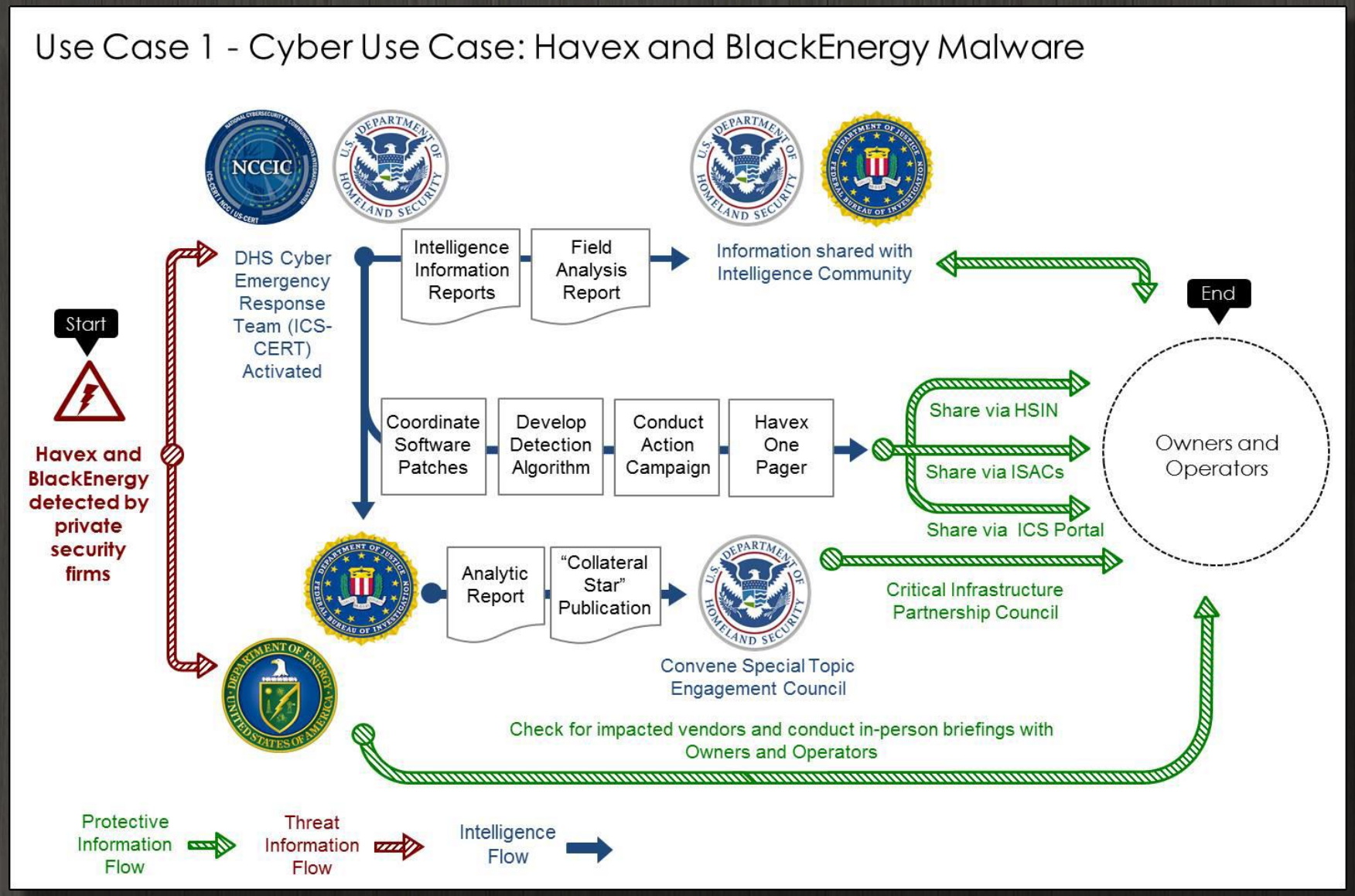
ISAC Information Sharing and Analysis Center
ISAO: Information Sharing and Analysis Organization

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



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

https://www.ccn-cert.cni.es/soluciones-seguridad/reyes.html

RNS: la obligación de compartir

CCCS Centro de Operaciones de Ciberseguridad


SOC Ministeriales


CERT- SOC Autonómicos


SOC Entidades locales


SOC Sectoriales


SOC Privados

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

https://www.ccn.cni.es/index.php/es/soc/red-nacional-de-soc

BENEFICIOS DE COMPARTIR

SEC AWARENESS

OK READY

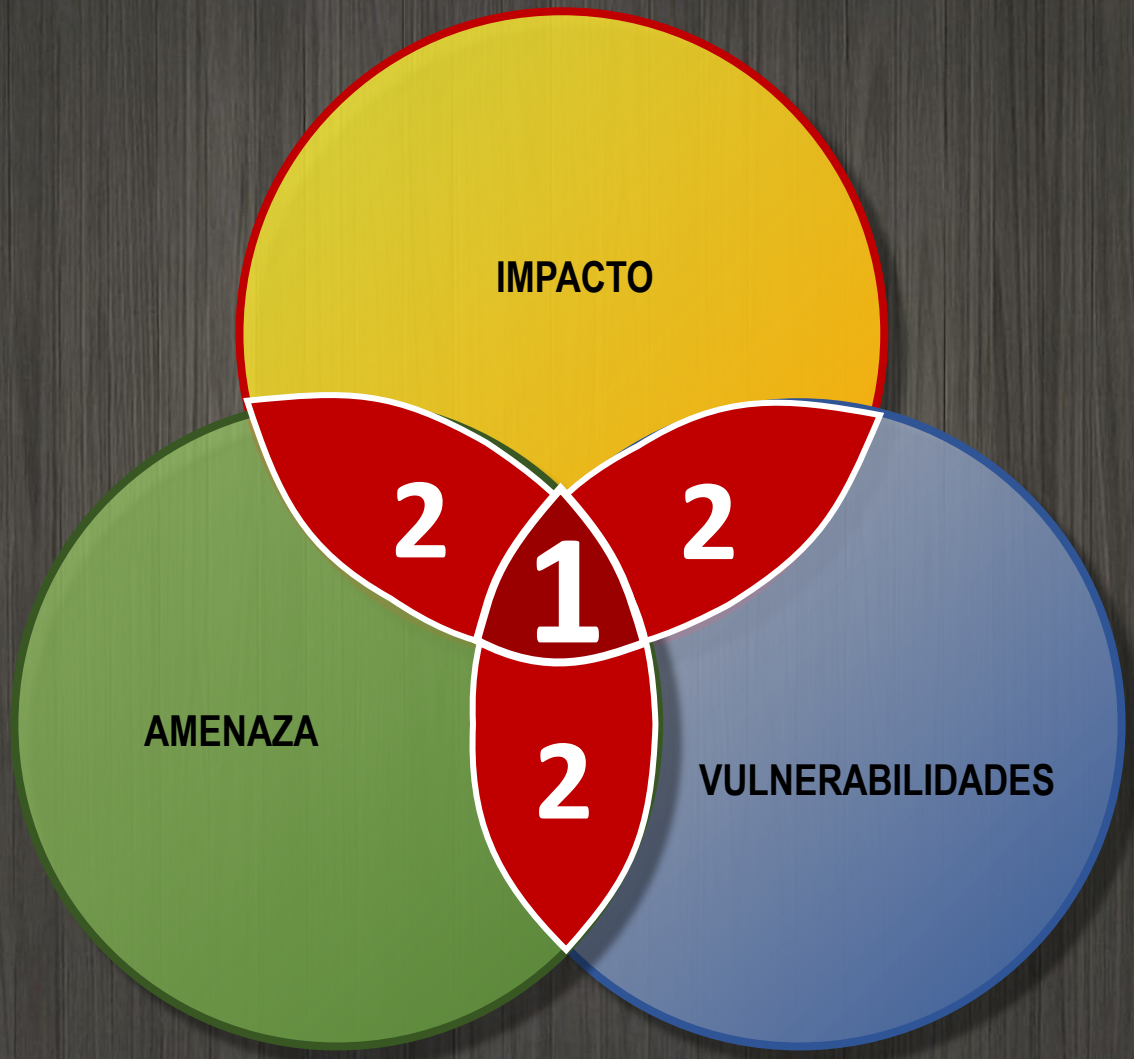
SELECT PEOPLE WHERE…

< COSTES

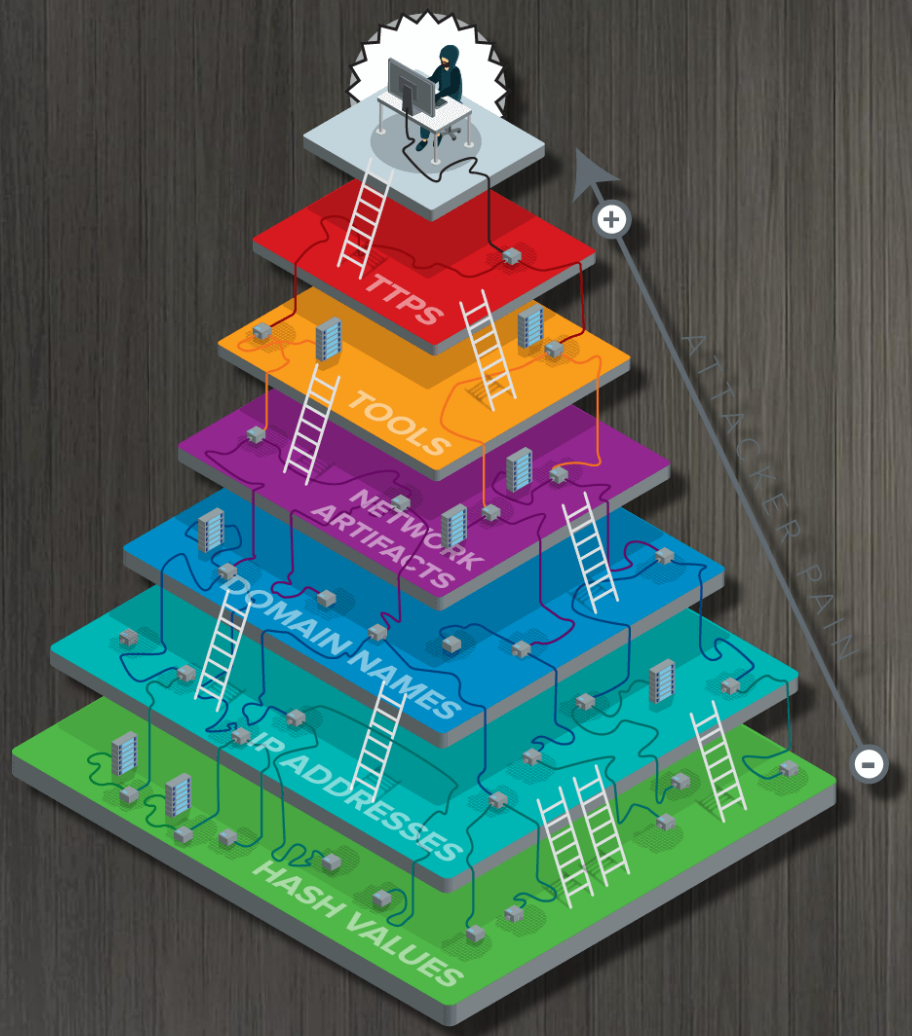
compartir

CONCLUYENDO

RIESGO = VULNERABILIDADES * AMENAZA * IMPACTO



RECAPITULANDO: SOC - CTI - INTEL



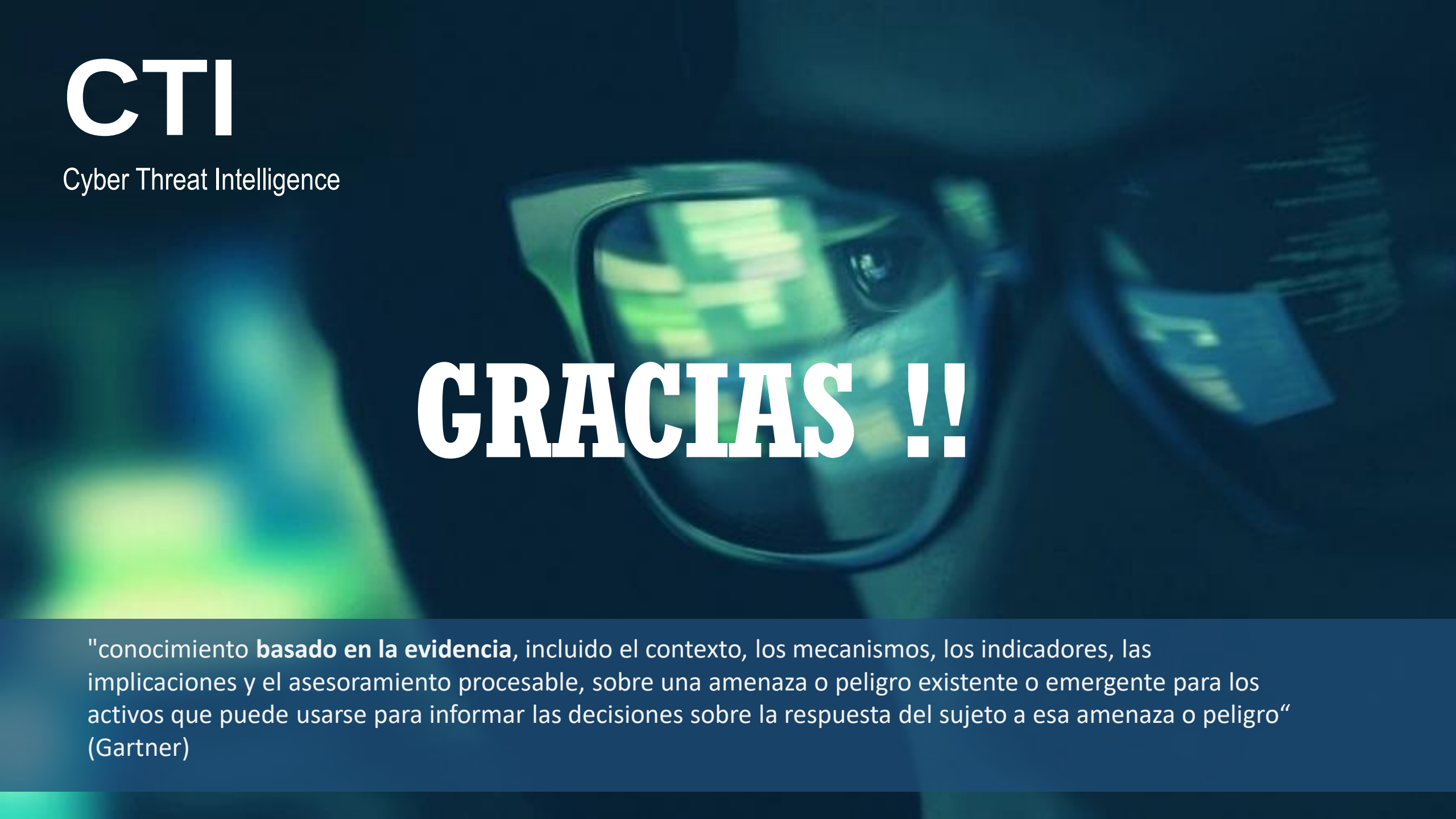
- Los Centros de Operaciones de Seguridad (SOC / COS) son la piedra angular en la lucha contra el cibercrimen.
- CTI no es la respuesta a todas las preguntas, pero la CTI debe ser parte fundamental de la ciber defensa
- La Inteligencia de Amenazas hace a los Equipos de Seguridad **un 33% mas eficaces**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

XV JORNADAS STIC CCN-CERT

CIBER_SEGURIDAD 360°. IDENTIDAD Y CONTROL DEL DATO.

Akamai

Red Nacional de SOC. Funcionamiento

SOBREINFORMACIÓN

SOC Privados

COCS Administración General del Estado (AGE)

SOC Ministeriales

CERT / SOC Autonómicos

Red Nacional de SOC

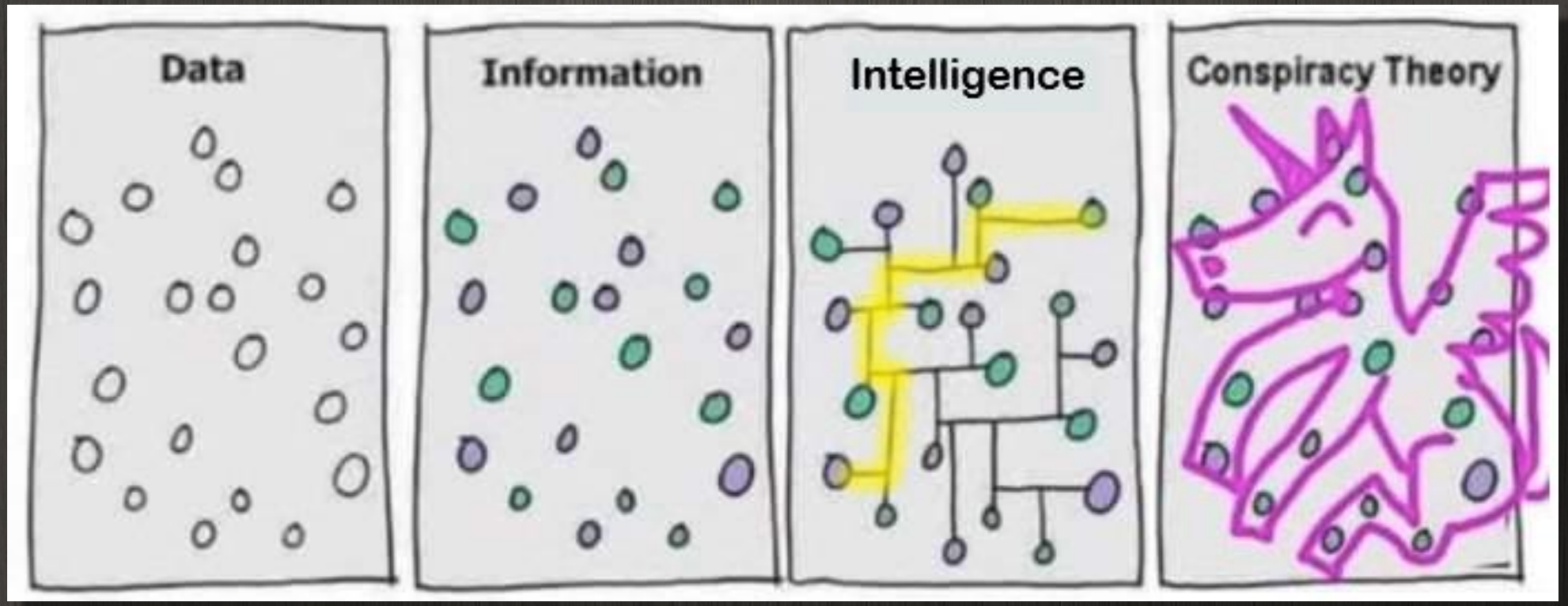
#XVJORNADASCCNCERT

ccn-cert

#XVJORNADASCCNCERT

ccn-cert

CICLO INFORMAL DE INTELIGENCIA



Procesos automatizados → Análisis → Cervezas

Cliffor Stoll, autor de ‘El huevo del cuco’

BIBLIOGRAFIA

ENCUESTAS

- 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

ESTUDIOS E INFORMES

- 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

GUÍAS

- CCN-STIC 423 - Indicadores de Compromiso
- CCN-STIC 424 - INTERCAMBIO DE INFORMACIÓN DE CIBERAMENAZAS (2015)

```
<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>
```