Estrategias de monitoreo de seguridad a nivel nacional

José Callero - jose.callero@cert.uy

Uruguay Presidencia | agesic | CERTuy

¿Qué hacemos en AGESIC en Seguridad de la Información?

Gestión de Riesgos y Continuidad Op.

- Buenas prácticas, metodologías y estándares
- Auditoria
- Gestión de riesgos
- Cooperación y relacionamiento
- MC

Gestión y Auditoría

Fortalecer el Ecosistema

- Difusión y entrenamiento
- Asesoramiento
- Gestión de incidentes
- Monitoreo y análisis
- Gestión de vulnerabilidades

CERTuy (CERT+SOC)

Universalizar la eID

- Firma Digital
- Identificación Digital

Identidad Digital

Adecuación del Marco Normativo

- Impulsar el desarrollo del marco normativo nacional en la materia
- Protección de datos personales

¿Porqué CERTuy está priorizando el monitoreo y detección de amenazas?

“Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas”

John T. Chambers
JC2 Ventures

Top 5 Ciberamenazas (Splunk)

- Entornos cloud mal configurados
- Phishing mas baratos y mas eficientes
- Malware a la carta
- Problemas de compliance
- Vulnerabilidades conocidas

https://www.splunk.com/en_us/blog/security/top-5-cybersecurity-threats-to-watch-in-2020.html

Ejemplo: Target Corp

Septiembre	15 Noviembre	27 Noviembre	30 Noviembre	2 Diciembre	12 Diciembre	15 Diciembre
• Compromeeten Fazio Mechanical Services	• Ingresan a la red de Target y prueban el malware en los POS	• Comienza la colección de informacion de tarjetas de credito	• POS malware operativo 100% • Instalan software para exfiltrar datos • Symantec / Fireeye disparan alertas	• Comienza el exfiltrado de información • Fireeye dispara alertas adicionales	• Depto. de justicia notifica a Target	• El malware es removido

https://arxiv.org/pdf/1701.04940.pdf

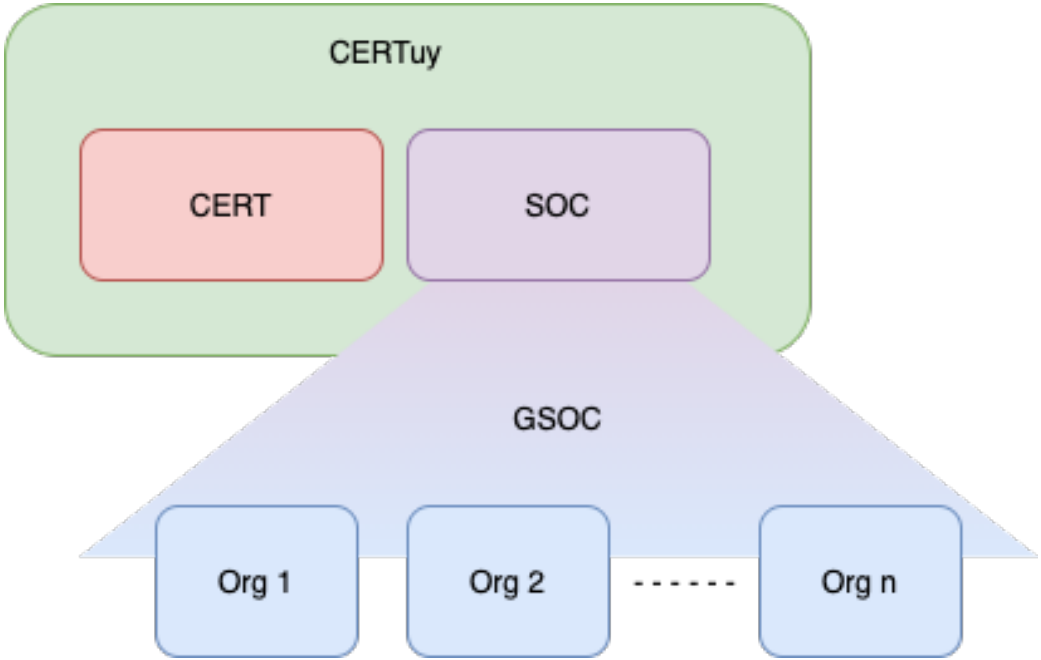
Tiempo de permanencia (dwell time)

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019
All	416	243	229	205	146	99	101	78	56
Internal Detection	—	—	—	—	56	80	57.5	50.5	30
External Notification	—	—	—	—	320	107	186	184	141

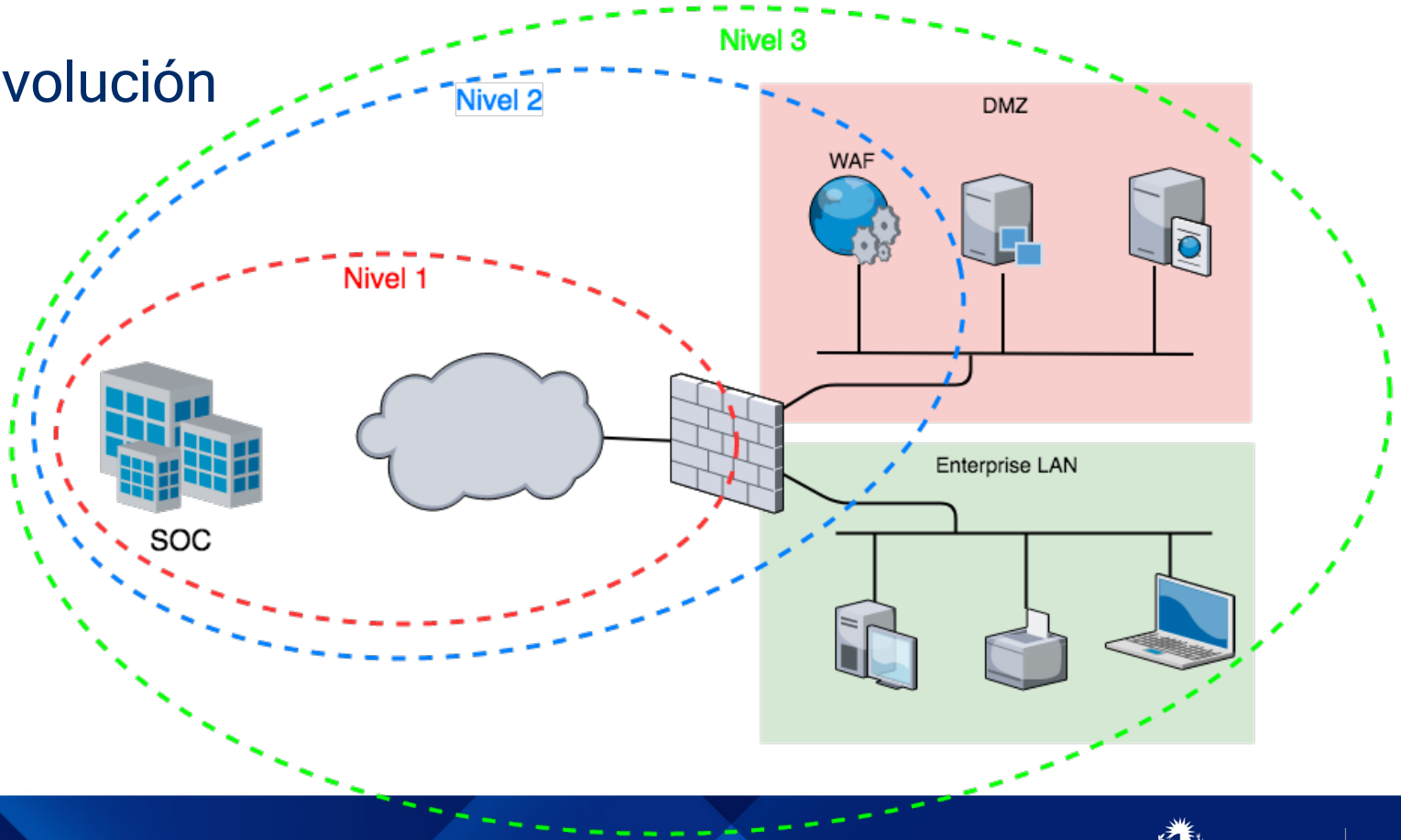
https://www.fireeye.com/content/dam/collateral/en/mtrends-2020.pdf

FIREEYE MANDIANT

CERTuy 3.0 y el servicio GSOC

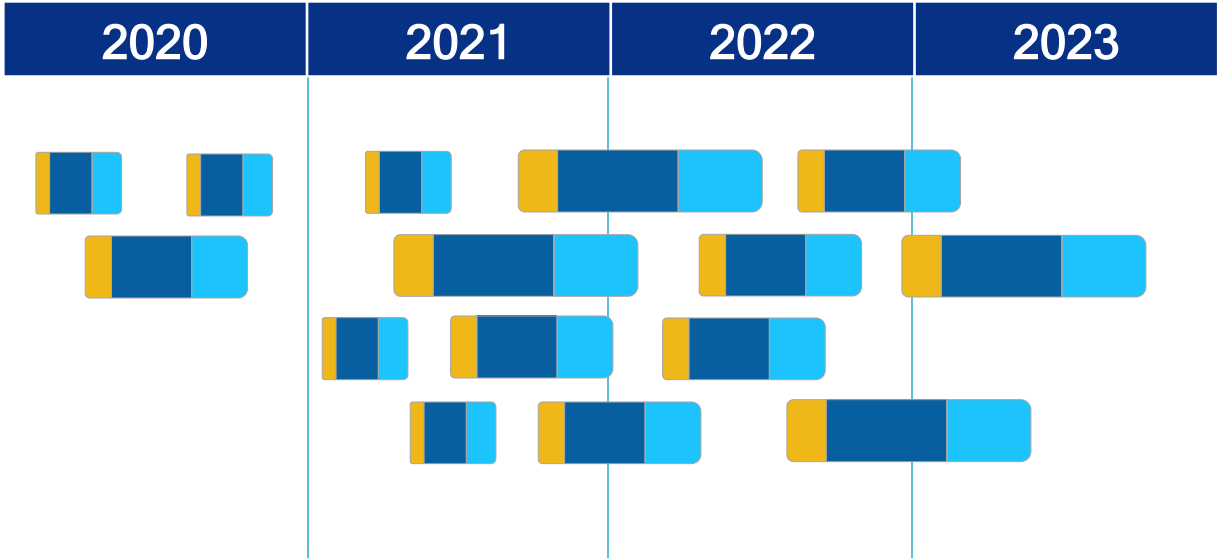


Evolución

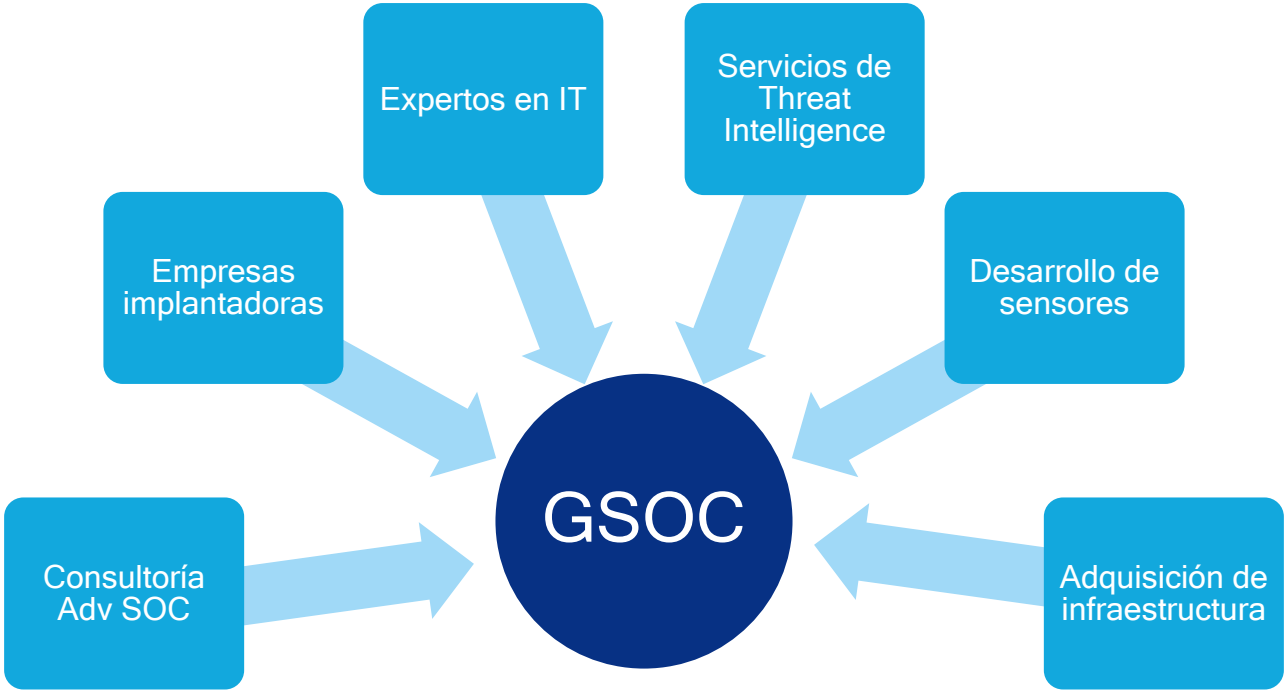


Programa GSOC

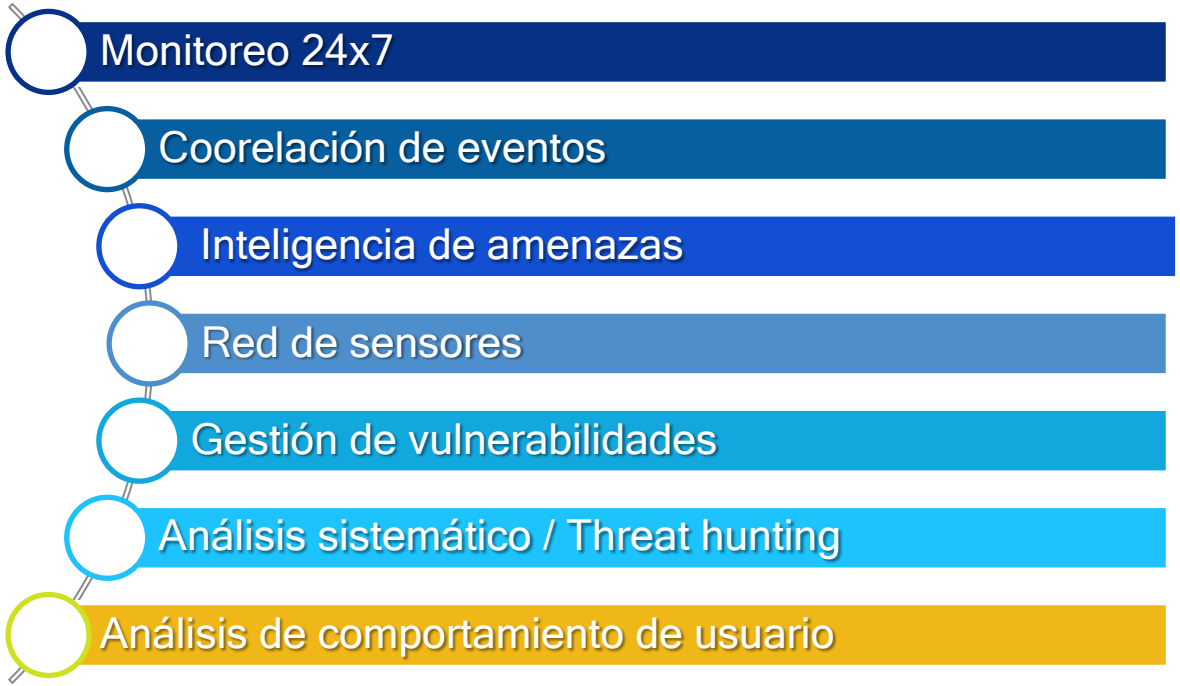
- **2** empresas implantadoras.
- **15** nuevos organismos.
- Más de **5.000** horas de servicios profesionales de alta especialización.
- Disponibilización de infraestructura

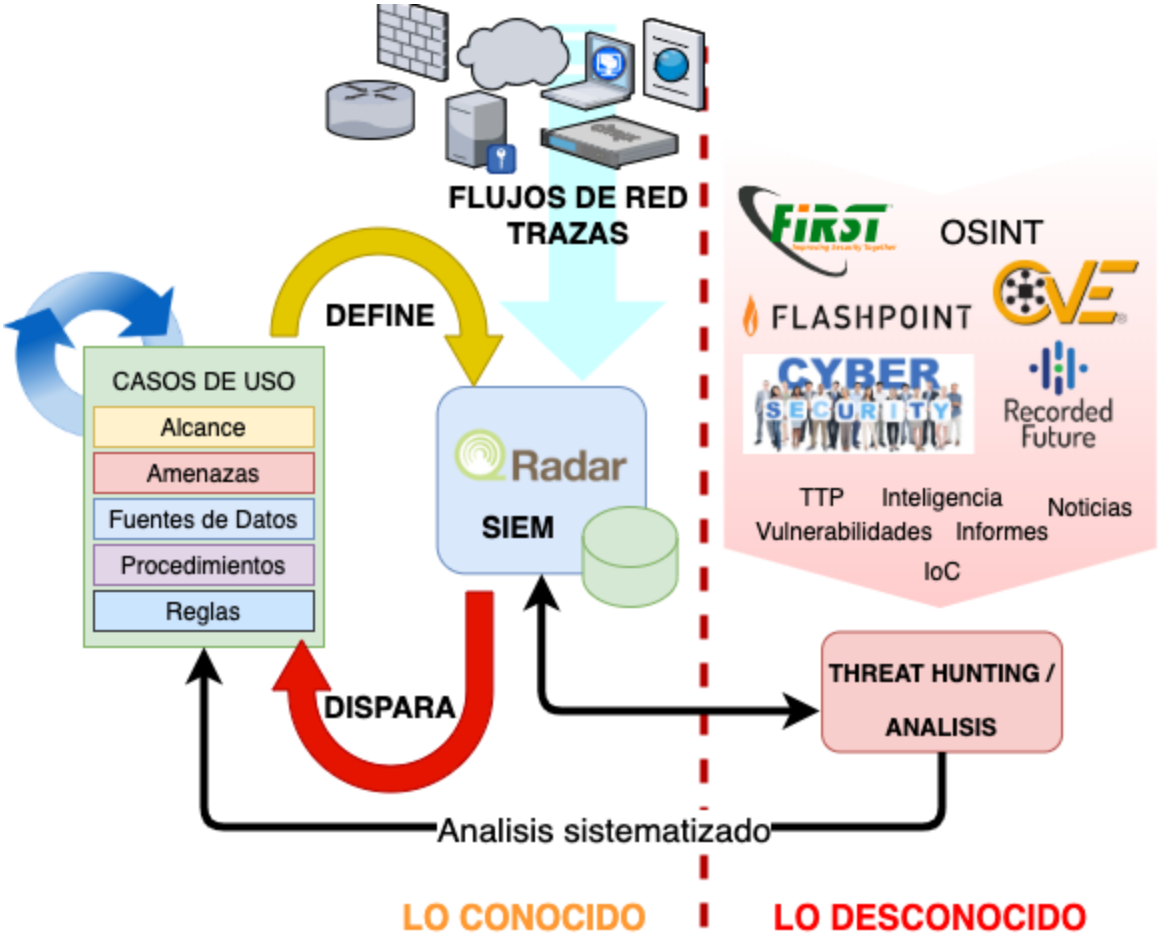


Proyectos relacionados

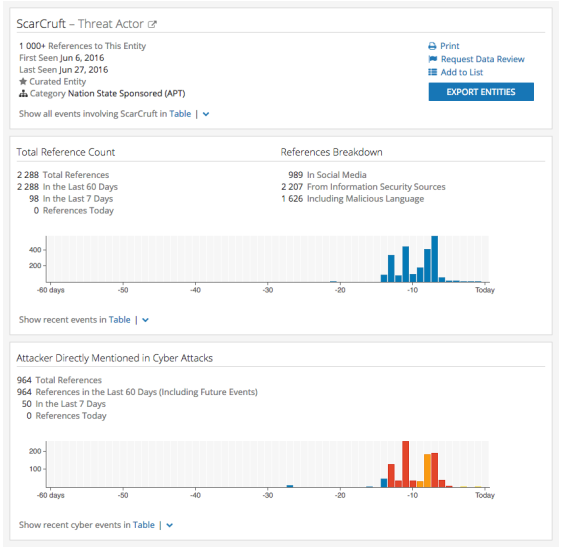


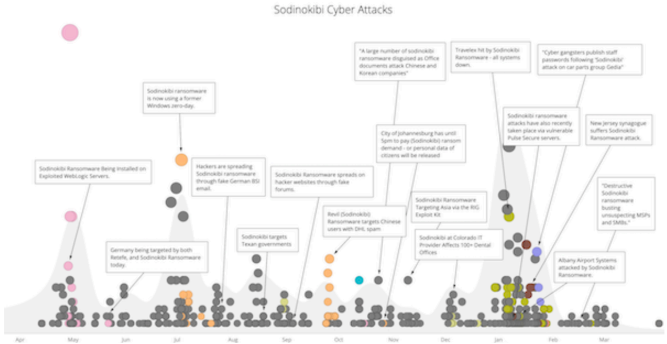
Servicios


Monitoreo 24x7
Coorelación de eventos
Inteligencia de amenazas
Red de sensores
Gestión de vulnerabilidades
Análisis sistemático / Threat hunting
Análisis de comportamiento de usuario

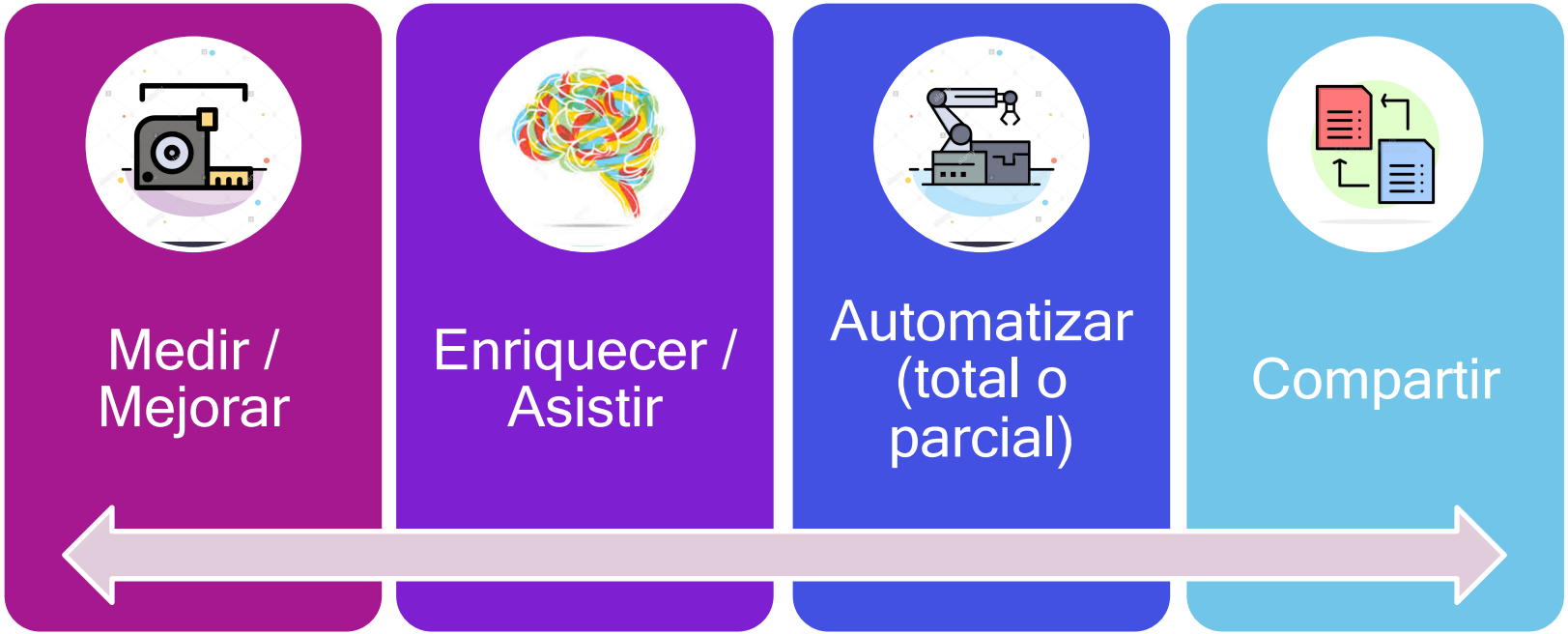

FLUJOS DE RED
TRAZAS
DEFINE
CASOS DE USO
Alcance
Amenazas
Fuentes de Datos
Procedimientos
Reglas
Radar
SIEM
DISPARA
OSINT
FLASHPOINT
CYBER SECURITY
Recorded Future
TTP
Inteligencia
Noticias
Vulnerabilidades
Informes
IoC
THREAT HUNTING / ANALISIS
Analisis sistematizado
LO CONOCIDO
LO DESCONOCIDO

Inteligencia de amenazas





Futuro próximo



Uruguay Presidencia | agesic | CERTuy

www.gub.uy/cert