Security Operations Center, una infraestructura como servicio

La ciberseguridad, una responsabilidad compartida

QUIÉN ES ENCRIPTIA

Grupo SVC seguridad

SVC

- Ingeniería
- Central Receptora Alarmas
- Vigilantes
- Auxiliares

Encriptia

- Consultoría
- Formación
- Ciberseguridad
- SOC
- Security Operation Center

QUIÉN ES ENCRIPTIA
MARCO CONCEPTUAL

Seguridad esférica

Security	Safety	Reputacional y Compliance
Seguridad Física	Seguridad Laboral	Seguridad de la información
Ciberseguridad	Seguridad Transporte	Imagen y marca
	Seguridad Alimentaria	Continuidad de negocio
	Seguridad medio - ambiental	

QUIÉN ES ENCRIPTIA
OBJETIVO Y PROCESO

Herramientas de Seguridad

Políticas de Seguridad

Continuidad de negocio

Asegurando la continuidad de negocio

QUIÉN ES ENCRIPTIA
EN LA CIBERSEGURIDAD

Auditoría de sistemas y web	Caja blanca o caja negra
	Análisis de vulnerabilidades
	Análisis de fugas y secuestro de información
Gestión de la seguridad	Elaboración e implantación de Planes Directores de la Seguridad de la información
	Integración de la ciberseguridad según RGPD/LOPD
	Integración de la ciberseguridad en el Plan de Prevención Penal
Periciales	Análisis forense de incidentes de seguridad
	Tasaciones y valoraciones
	Borrado seguro de datos
Formación	Concienciación en Ingeniería Social
	Prevención y Buenas prácticas en la Red
	Inteligencia en fuentes abiertas OSINT
e-SOC service	Detección y prevención de intrusiones
	Gestión de la infraestructura de seguridad de red
	Detección de conexiones no autorizadas a una red

QUÉ ES UN SOC

SECURITY OPERATIONS CENTER

Un centro de gestión de la ciberseguridad que abarca la monitorización, detección, aviso, análisis y neutralización basado en una herramienta de la que disponen las grandes corporaciones y que ponemos a disposición de las PYMES.

QUÉ ES UN SOC

- ENCRIPTIA ofrece **e-SOC service** para monitorizar y gestionar en tiempo real la ciberseguridad de las organizaciones y empresas.

- Operativo las 24 horas del día y los 365 días del año
- Atendido por personal altamente cualificado
- Funciones:
  - Monitorización y protección de los sistemas informáticos de las empresas
  - Verificación permanente de toda la actividad que genere un riesgo para el funcionamiento seguro de los sistemas IT/OT utilizadas por el cliente

VENTAJAS DE DISPONER DEL SERVICIO

Aseguramiento de la continuidad de negocio

1. Convertirse en un **proveedor seguro y responsable**
    1. Controlar la seguridad e integridad de la información
    2. Evitar **intrusiones** y **sabotajes** informáticos
    3. Detectar **fugas de información**
    4. Evitar instalación de programas no autorizados
    5. Controlar el uso de **USB**
    6. Descubrir **brechas de seguridad**
    7. Detección de **malware**
    8. Detección de funcionamiento anómalo del software y hardware (fallo de disco duro, errores de los programas…)
2. Herramienta para el cumplimiento de RGPD/LOPD
    1. Detección de escalada de privilegios
    2. **Accesos no autorizados**

A QUIÉN BENEFICIA

- **Las organizaciones y empresas** que contratan el servicio, porque se convierten en proveedores seguros de sus clientes ya que van a disponer de un instrumento que les facilitará, si lo desean, su certificación como tal.
- **La Sociedad** porque ponemos en manos de la **PYME** vasca una instrumento de ciberseguridad que hasta la fecha por su complejidad e inversión necesaria, sólo ha estado a disposición de las grandes corporaciones. Ofrecemos al tejido industrial y económico una ventaja competitiva así como un mejor posicionamiento en el mercado.

QUÉ PAPEL TIENE EL SOC

MONITORIZA

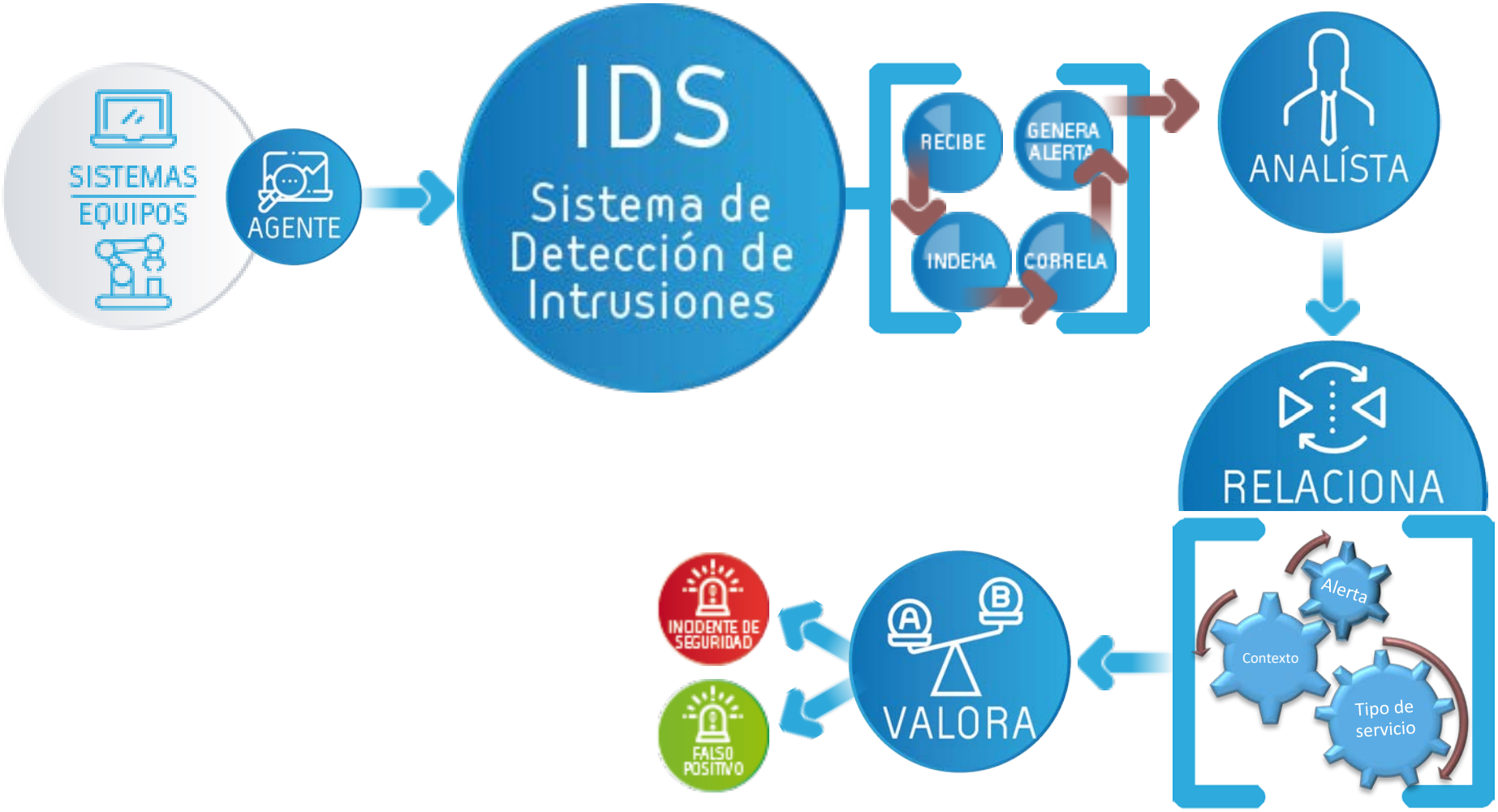
QUÉ PAPEL TIENE EL SOC
DETECTA Y ANALIZA

QUÉ PAPEL TIENE EL SOC
INFORMA

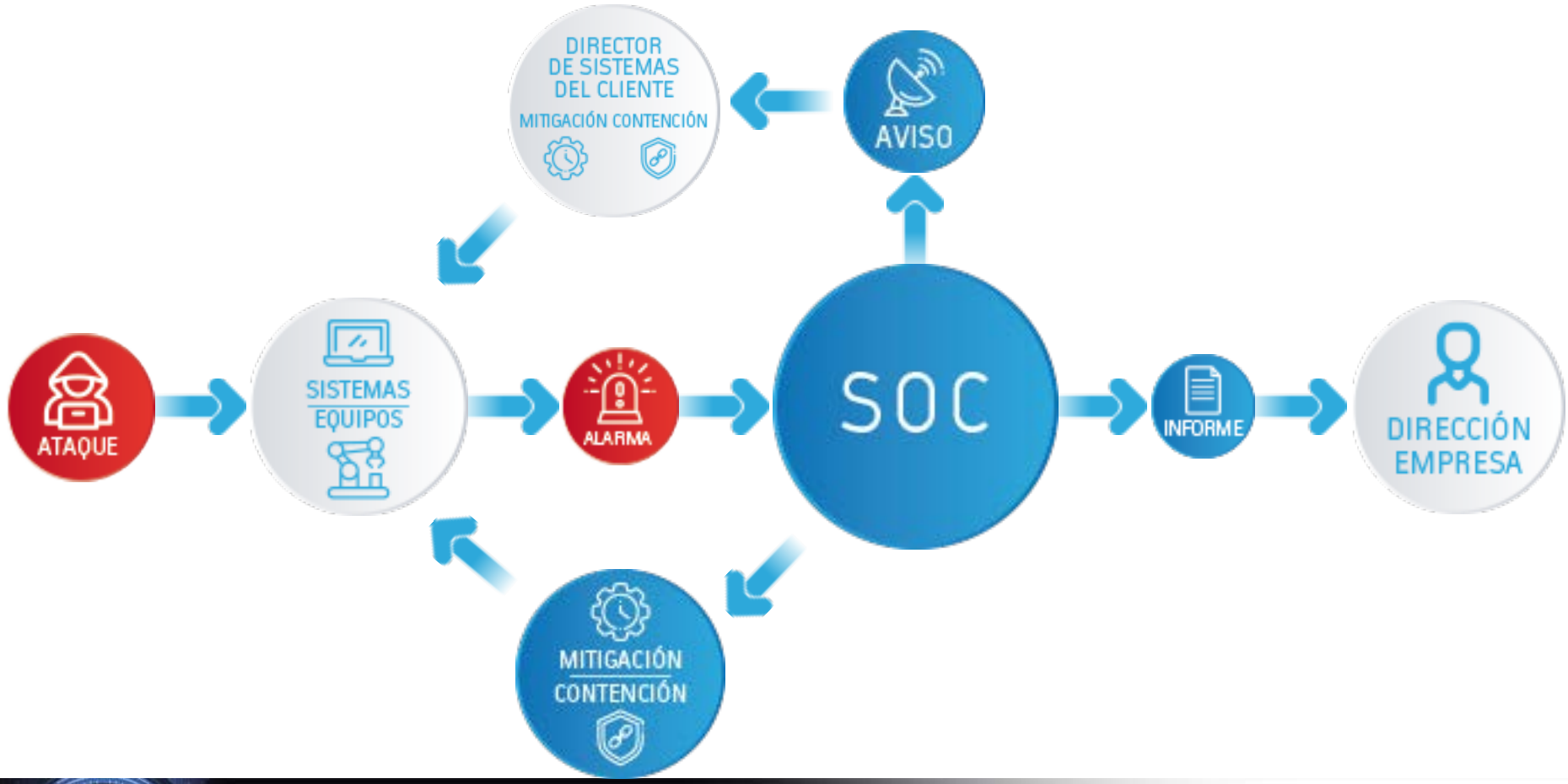
QUÉ PAPEL TIENE EL SOC

NEUTRALIZA

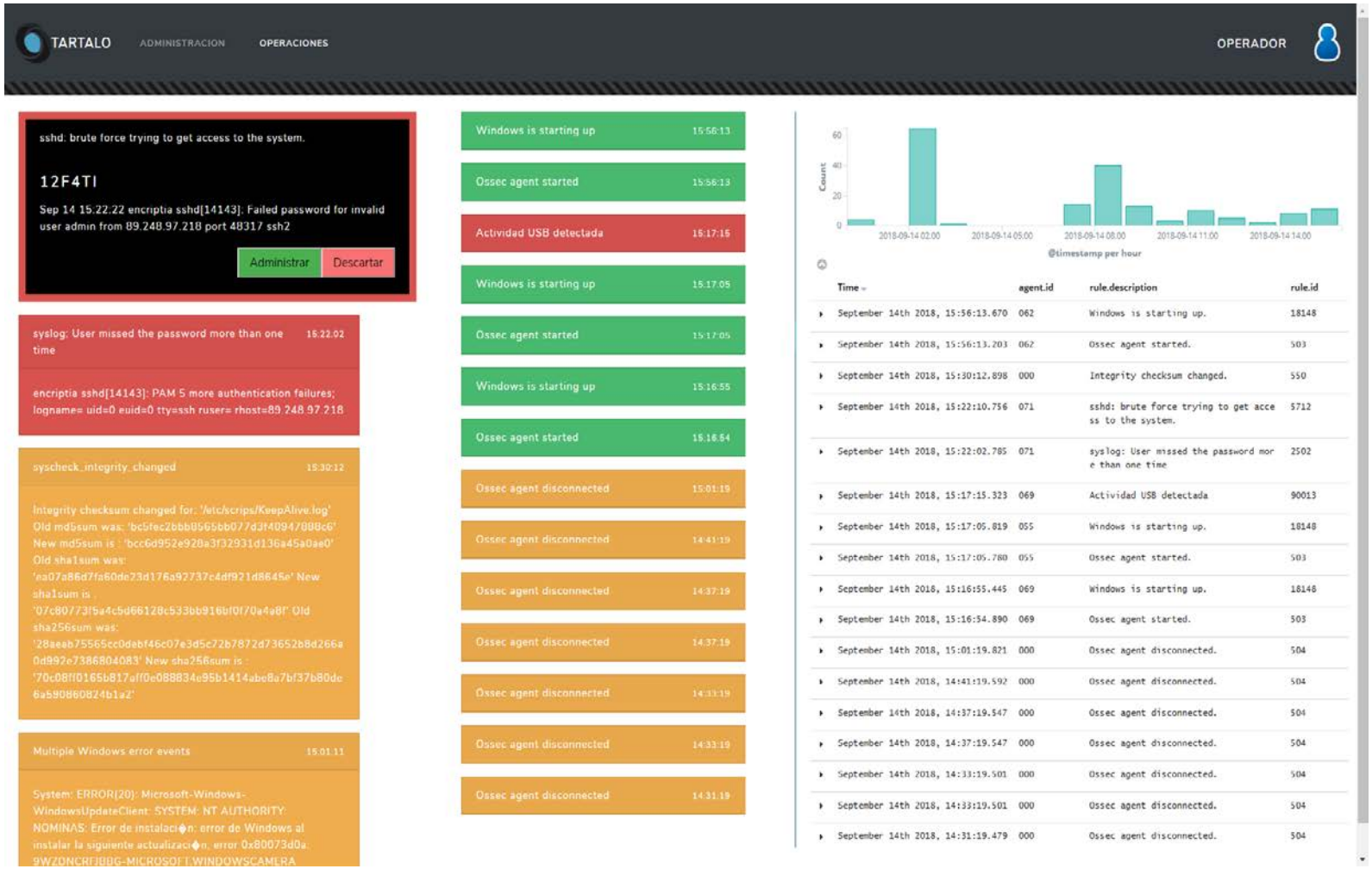
CÓMO TRABAJA EL SOC



CÓMO ES EL PROCESO DE "E-SOC SERVICE"



CÓMO SE DETECTA



EJEMPLOS DE ATAQUES RECIBIDOS

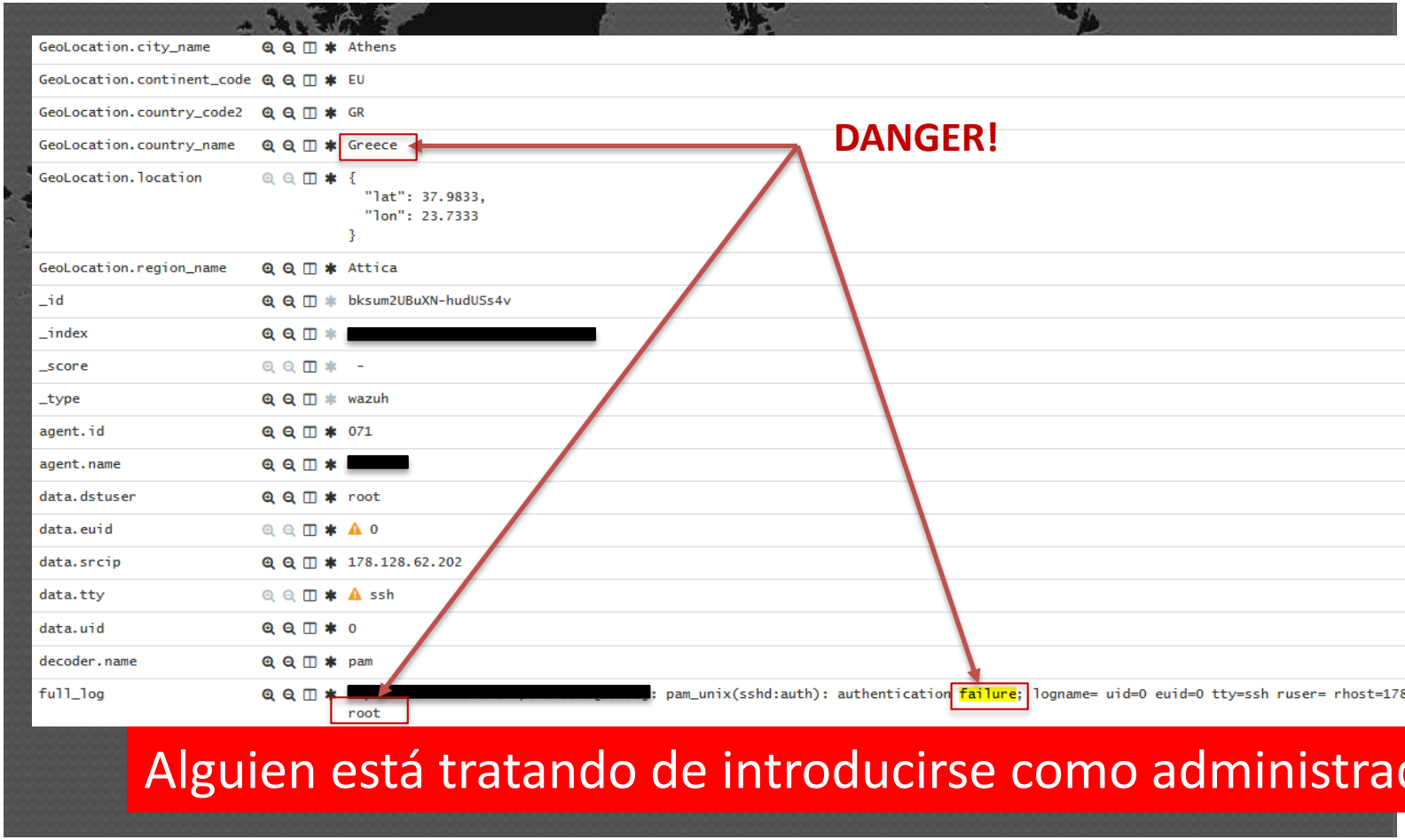
FUERZA BRUTA

Detectamos

de

s

el



Alguien está tratando de introducirse como administrador!!!

EJEMPLOS DE ATAQUES RECIBIDOS
USO NO AUTORIZADO DE USB

Se detecta actividad USB, de modo que nos ponemos a investigarla.

Espacio libre antes y después

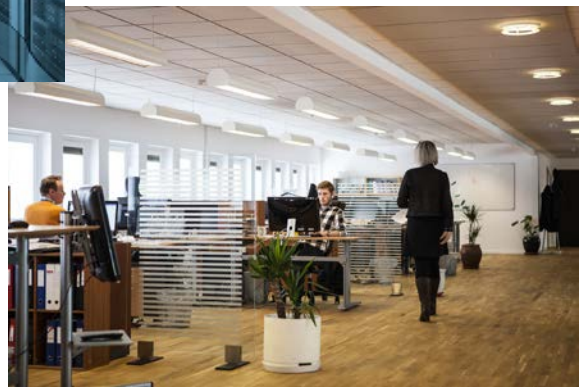
```
ossec: output: 'wmic logicaldisk where drivetype=2 list /format\list | findstr "FreeSpace VolumeName" & echo .':
FreeSpace=
VolumeName=
FreeSpace=15502254080
VolumeName=TOSHIBA
.

DELPHOS

1535619333.127793

wmic logicaldisk where drivetype=2 list /format\list | findstr "FreeSpace VolumeName" & echo .

DELPHOS

ossec: output: 'wmic logicaldisk where drivetype=2 list /format\list | findstr "FreeSpace VolumeName" & echo .':
FreeSpace=
VolumeName=
FreeSpace=15502213120
VolumeName=TOSHIBA
```

Alguien puede estar robando información!

A QUIEN VA DIRIGIDO
(POR SECTOR)

e-SOC service

UN SERVICIO PARA
PYMES



A QUIEN VA DIRIGIDO
(POR SU ESTRUCTURA)

Tipo de servicio	Dirigido a
Básico	Alto nivel de gestión de la infraestructura informática
Básico Pro	Alto nivel de gestión de la infraestructura informática, aviso telefónico 24 h
Avanzado	Medio nivel de gestión de la infraestructura informática
Avanzado Pro	Medio nivel de gestión de la infraestructura informática, aviso telefónico 24 h
Premium	Bajo nivel de gestión de la infraestructura informática
Premium Pro	Bajo nivel de gestión de la infraestructura informática, aviso telefónico 24 h

A MÁS, MENOS

FAQ

- ¿Afecta al funcionamiento de mis equipos?
  - No interfiere en nada porque solo lee información que ya existe, no la trata.
- ¿Cuánto ocupa el agente?
  - 15 mb, como cualquier app de un móvil,
- ¿Hasta donde puedes ver mis datos?
  - No se ven los datos que maneja el usuario, solo se ven los accesos a los datos
- ¿Si rescindo el servicio que tengo que hacer?
  - Nada, también se puede desinstalar el agente
- ¿Exige formar al usuario?
  - NO. Al SisAdmin si quiere sacar el máximo partido para su trabajo le podemos formar.
- ¿Si no tengo SisAdmin quién hace la instalación?
  - La instalación es muy sencilla y la puede hacer un usuario sin conocimientos porque se entrega con un manual, también la podemos hacer nosotros.
- ¿Aumenta la carga de trabajo del SisAdmin?
  - Todo lo contrario, le ayuda a depurar su sistemas

ASÍ DE FÁCIL

ESKERRIK ASKO