

## Ter-Soc Servicio de Monitorización de Red

DESCRIPCIÓN DEL SERVICIO

El exclusivo servicio de monitorización de red de Efimatica, permite analizar a fondo y de forma automatizada los riesgos de seguridad de su red y aportar soluciones a cada amenaza.

Mediante la instalación de un sensor en la red, todo el tráfico es capturado y analizado en tiempo real, por una batería de softwares específicos que obvian todo el tráfico lícito e inspeccionan a fondo todo comportamiento sospechoso o tramas de red de dudosa procedencia, y todo ello, sin penalización de velocidad o ancho de banda. Esta solución se traduce en una muy sustancial mejora de la seguridad de la organización y un elevado ahorro en costes. Esto se realiza de forma transparente sin penalización en el rendimiento de la red o los equipos.

Un servicio creado por especialistas en seguridad, que cubrirá de forma global todas sus necesidades operativas y normativas.

### Principales características



Profundo y automatizado control y análisis de los riesgos de seguridad de red.



De forma transparente y sin penalización en el rendimiento de la red o equipos.



Identifica las IP que sufren intentos de ataque y las distribuidoras de malware.



Identifica amenazas de todo tipo: phishing, malware y actividades sospechosas.



Hace fácilmente visible el uso de aplicaciones de los usuarios.



Máxima seguridad del dato: la información recopilada no sale de la infraestructura de la empresa.



Capacidad DFIR (Digital Forensic & Incident Response).

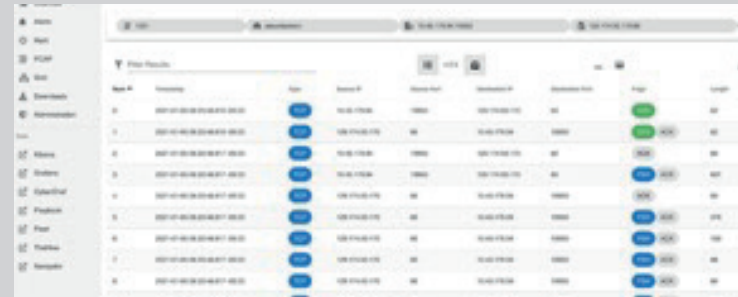
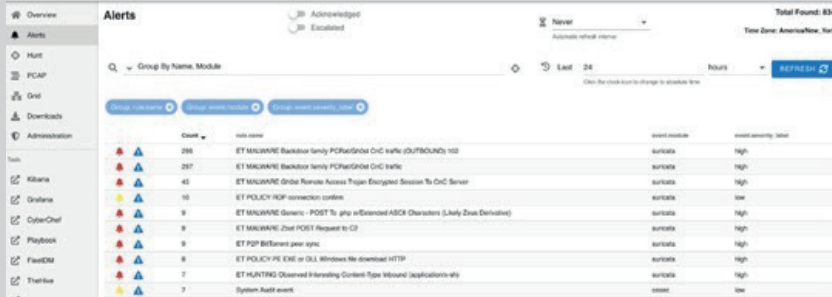


Integración con otras soluciones de monitorización o ciberseguridad como EDR o SIEM.

### El componente humano como Clave de la Eficacia: Procesos automatizados atendidos por técnicos especialistas

Los analistas de Efimatica comprueban periódicamente el estado de la red. Reciben todas las alertas que se generan y las documentan con sus correspondientes recomendaciones con medidas oportunas en cada caso.

Las alertas son comunicadas en función de su gravedad al cliente a través del Panel de Incidencias exclusivo para cada cliente. La periodicidad de comprobación dependerá de la modalidad de servicio contratada



efimatica

Ter-Soc  
Servicio de  
Monitorización  
de Red

DESCRIPCIÓN DEL SERVICIO

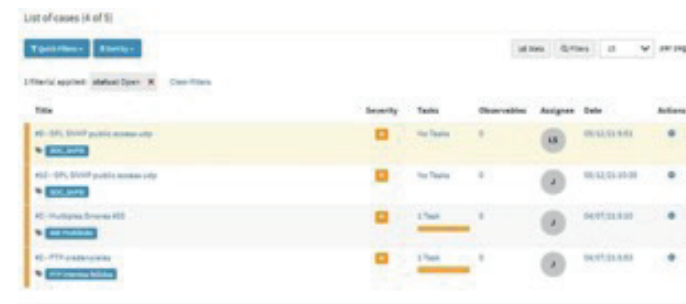
## Registro Total

Tras el estudio de las evidencias, el analista crea una notificación en el que explica y muestra los eventos que generaron la amenaza, reflejando cuando fue creada la alerta y el tiempo en el que fue resuelta.

## Intervención humana en el análisis

El analista estudia la alerta mediante diferentes herramientas que le permite profundizar en los detalles para notificar al cliente la amenaza concreta.

**¡Adiós a los falsos positivos!**



## Completas Notificaciones

En cada notificación el cliente encontrará los detalles para mitigar la amenaza o problema de seguridad, el sistema genera estadísticas de resolución de incidentes que permitirá estudiar y mejorar los tiempos de respuesta todos los actores involucrados en las notificaciones.

## Complemento ideal

La herramienta de monitorización complementa el firewall en la protección del tráfico malicioso ya que analiza el tráfico entre dispositivos internos. Está orientada a la detección y prevención de ataques (IPS/IDS) efectuados desde Internet hacia nuestra red interna o desde el propio interior de la red a otro dispositivo de la misma red.

## Gestión y modelo de servicio e intervención personalizado

Ponemos a su entera disposición el modelo de gestión de intervención que considere más adecuado para su organización. Desde sistemas desatendidos para que sea su departamento IT quien autogestione totalmente el servicio hasta una intervención de gestión exhaustiva por parte de nuestro personal de SOC.

## Modelos de servicio totalmente adaptables a todas las necesidades:

- Desatendido,
- Híbrido
- Gestionado