STORMSHIELD

XDR

Mejora la cibereficacia operativa de su infraestructura

Ante unos ciberdelincuentes cada vez más profesionales y su modus operandi, las empresas se apresuran a desplegar productos de seguridad. El éxito recurrente de estos ataques demuestra la ineficacia de este planteamiento: la gran variedad de puntos de protección de redes y terminales, y la incoherencia de las políticas de seguridad, provocan una escasa capacidad de reacción ante estos ataques.

La proliferación de soluciones de detección requiere configuraciones cada vez más complejas, que generan numerosos y variados registros de log con patrones de comportamiento difíciles de interpretar y correlacionar por parte de los administradores. Esta falta de visibilidad limita la capacidad de reacción, lo que en la práctica se traduce en un menor nivel de protección.

El XDR **por Stormshield**

Stormshield es un actor de confianza en ciberseguridad con una nueva oferta para:

- Reducir el riesgo y mejorar la productividad operativa cibernética,
- Reducir los puntos ciegos inherentes a la integración de soluciones de seguridad de distinto fabricante,
- Proporcionar una solución completa para la seguridad de su infraestructura,
- Correlacionar los eventos notificados por la protección de red (SNS) y la protección de los endpoints (SES),
- Proporcionar alertas en tiempo real,
- Guiar los elementos de respuesta y remediación.

Controle toda la información de XDR

Gestione los incidentes de seguridad desde una ubicación centralizada

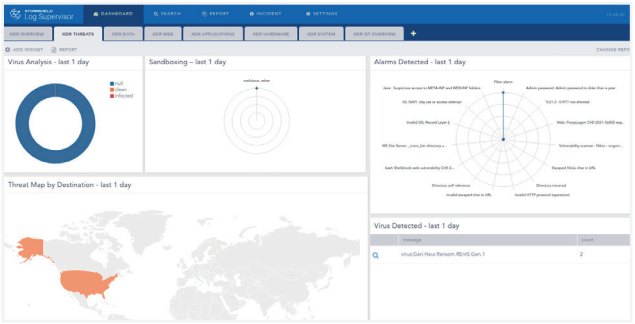
Mejore la seguridad y la cibereficacia operativa

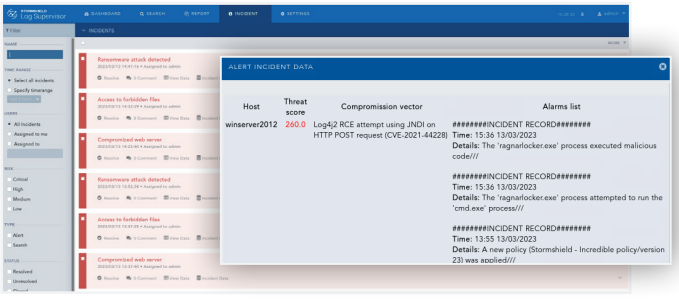
Una oferta de XDR **completamente integrada y controlada**

La combinación ideal de Stormshield Network Security para **proteger la red** y Stormshield Endpoint Security para **proteger los endpoints**, respaldada por la experiencia de Stormshield en ciberinteligencia para anticiparse a las amenazas.

Todo ello orquestado por Stormshield Log Supervisor para **alertarle en tiempo real** y **ofrecer una respuesta rápida y sostenible** tanto para la red como para los puestos de trabajo.

En resumen, una solución de protección que es 100% europea, 100% fiable.





Stormshield XDR

CONTROL • PRODUCTIVIDAD • COHERENCIA

#01
FICHERO MALICIOSO

Ataque

- Se recibe un fichero malicioso por correo electrónico y se abre
- Se ejecuta un instalador de malware (dropper)
- La carga viral se extrae y se lanza el ataque

Respuesta

- Se aplica la remediación a través del aislamiento de la red del endpoint
- Se detienen los procesos maliciosos en el terminal

#02
SERVIDOR WEB SOMETIDO A UN ATAQUE DDoS

Ataque

- El servidor es inundado con multitud de conexiones

Respuesta

- Restricción de conexiones solo a las confiables
- Activación del límite de conexiones en el servidor para proteger su integridad

#03
LLAVE USB MALICIOSA

Ataque

- Se introduce un instalador de malware en el PC
- Se establece una conexión con un servidor de mando y control (C2)
- Se descarga la carga viral del servidor
- Se intenta comprometer la estación de trabajo; el ataque se empieza a desplegar lateralmente

Respuesta

- Se detienen los procesos maliciosos en el terminal
- Se aplica la remediación aislando el endpoint de la red
- La llave USB se bloquea en otros endpoints
- La IP de C2 se bloquea en la protección de red

#04
DESCUBRIMIENTO DE LA RED INTERNA POR PARTE DEL ATACANTE

Ataque

- Escaneado de la red interna
- Descubrimiento de la red y de sus vulnerabilidades
- Prueba de exploits conocidos en servidores críticos (AD o Exchange)
- Intento de tomar el control de recursos críticos

Respuesta

- Aislamiento del endpoint comprometido
- Activación del IPS en conexiones críticas

Solución soberana

Como uno de los principales actores europeos de la ciberseguridad, ofrecemos soluciones que cumplen los requisitos legales europeos.

Certificaciones

Nuestras tecnologías están certificadas conforme a las normas europeas más exigentes, su garantía de una protección adaptada para la información estratégica o los datos más sensibles de su organización.

Ecosistema

Trabajamos con otros actores para desarrollar soluciones conjuntas, compartir información sobre amenazas y mejorar colectivamente las defensas de nuestros clientes.

www.stormshield.com

Stormshield: explore nuestras líneas de producto

Ciberseguridad para redes e infraestructuras TI

Las funciones básicas de las soluciones Stormshield Network Security proporcionan seguridad integral y protección de red de alto rendimiento. **Elija una seguridad eficaz y escalable.**

Ciberseguridad para los endpoints

Stormshield Endpoint Security es capaz de modificar **dinámicamente sus operaciones de seguridad en función del entorno** y, al mismo tiempo, analizar el acceso a aplicaciones y recursos corporativos en función de la ubicación del endpoint.

Ciberseguridad para datos sensibles

Mediante el cifrado de datos de extremo a extremo, nuestra solución Stormshield Data Security se posiciona como una oferta integral para **controlar los datos sensibles dentro de su organización** y garantizar la privacidad del correo electrónico.