NOTAS DE LA SOLUCIÓN

# INFORMACIÓN DEL SOC

**Aplique análisis basados en IA para convertir grandes cantidades de datos de inteligencia de eventos, red, ecosistema y DNS en información procesable para mejorar la eficiencia de SecOps**

## BARRERAS A LA EFICACIA DE LOS SECOPS

AAl igual que con otras funciones de empresas o organizaciones gubernamentales en la actualidad, el SOC moderno lucha por hacer más con los recursos disponibles. Según SANS 2023 SOC Survey[1], el 80 % de las 10 principales barreras SOC para hacer uso completo de las capacidades SOC se encuentran en 3 áreas:

- Comprensión y manejo de las alertas
- Integración o automatización limitada entre herramientas
- Realización de tareas clave con personal y habilidades disponibles

Pero la estadística más trágica puede ser que todas estas barreras han estado desafiando el SOC durante más de una década. Las mejoras incrementales derivadas de la simple priorización automática de incidentes basadas en clasificaciones de malware y otros filtros básicos no han podido seguir el ritmo del crecimiento de las alertas y otros eventos que puedan necesitar atención del analista SOC. Así que las cosas no han hecho más que empeorar.

## PERSPECTIVAS DE LA SOC IMPULSADAS POR LA AI

Las amenazas persistentes modernas dependen de la infraestructura flexible del atacante y de los sistemas C2 dinámicos para alojar e implementar las numerosas herramientas de prueba, exploit, cifrado y otras implicadas incluso en un único ataque. Esto los hace extremadamente dependientes del DNS y destaca una debilidad clave que los defensores pueden aprovechar para detectar e interrumpir estas amenazas.

El DNS detecta la actividad legítima y maliciosa independientemente del protocolo, la plataforma, el sistema operativo, la aplicación o incluso la ubicación. Con esta visibilidad única, un programa piloto bajo el Director de Ciberseguridad en el NSA reveló que proteger DNS puede reducir los ataques de malware en un 92 %[2].

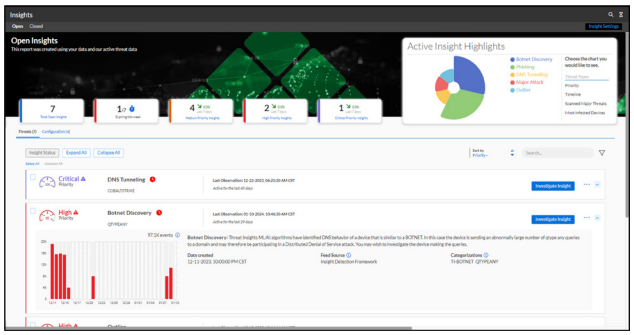


*Figura 1: La página Resumen de SOC Insights proporciona a los analistas acceso con un solo clic a lo que más importa.*

## FACTS & FIGURES

- El 60 % de los analistas de SOC afirma que sus **cargas de trabajo están creciendo** y puede que el **65 % cambie de trabajo** en el próximo año[4].
- El 55 % de los encuestados afirmó que **las alertas críticas se pierden** a menudo semanalmente e incluso a diario[5].
- El 64 % de los analistas afirma que **el trabajo manual consume más de la mitad de su tiempo**[6].
- La mala configuración es uno de los **3 factores principales en las infracciones relacionadas con errores**[3].
- 8 de las 10 principales **barreras que impiden la utilización completa de SOC** implican alertas, integración de herramientas y escasez de habilidades[1].
- El 77 % de los CEO están preocupados por la **disponibilidad de habilidades clave**[7].
- **El 92 % del malware y la actividad de C2 se pueden controlar en la capa de DNS** con la inteligencia y visibilidad de DNS adecuadas[2].

SOC Insights funciona con la solución de detección y respuesta DNS (DNSDR) de Infoblox, BloxOne Threat Defense, para ofrecer una oferta única Análisis impulsados por IA para detectar actividades de amenazas desconocidas que otras herramientas pasan por alto, aumentar la eficiencia del SOC y mejorar el ROI general de las inversiones en seguridad actuales.

## RESOLVER MÚLTIPLES PROBLEMAS CON UNA VARIEDAD DE CONOCIMIENTOS

Las investigaciones posteriores a incidentes o brechas a menudo revelan que los primeros indicadores de actividad maliciosa se pasaron por alto debido a errores de configuración, problemas de integración de herramientas de seguridad o una simple sobrecarga de alertas. SOC Insights aplica análisis basados en IA en una gran cantidad de datos para ayudar a abordar estos riesgos.

### Información de seguridad

El complemento Seguridad para SOC Insights está disponible para BloxOne Threat Defense "Business Cloud" o "Advanced", utiliza la IA para distorsionar grandes cantidades de eventos, redes, ecosistemas y visibilidad e inteligencia DNS en un conjunto manejable de información útil y de seguridad.

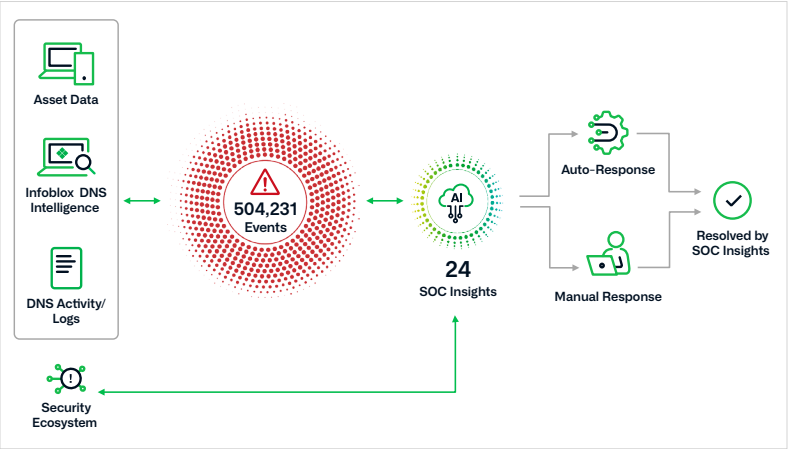


*Figura 2: Deje que SOC Insights elimine la sobrecarga de alertas, destilando montañas de eventos en un conjunto más manejable de percepciones significativas y procesables.*

- Amenaza persistente
- Propagación activa de amenazas
- Ataque mayor
- Descubrimiento de botnet
- Comunicación atípica
- Phishing
- Software malicioso
- Solucionador de DNS abierto
- Tunelización de DNS
- Actividad de pérdida de datos
- Ataque dirigido
- Errores de DNS excesivos
- Dominio similar supervisado

### Información sobre la configuración

La función de configuración de SOC Insights se incluye con BloxOne Threat Defense "Business Cloud" y "Advanced" para ayudar a los usuarios a garantizar que aprovechen al máximo las mejores prácticas actuales y a evitar errores comunes. Siga videos y otras guías para solucionar errores y debilidades, o desactive las advertencias innecesarias para las excepciones permitidas.

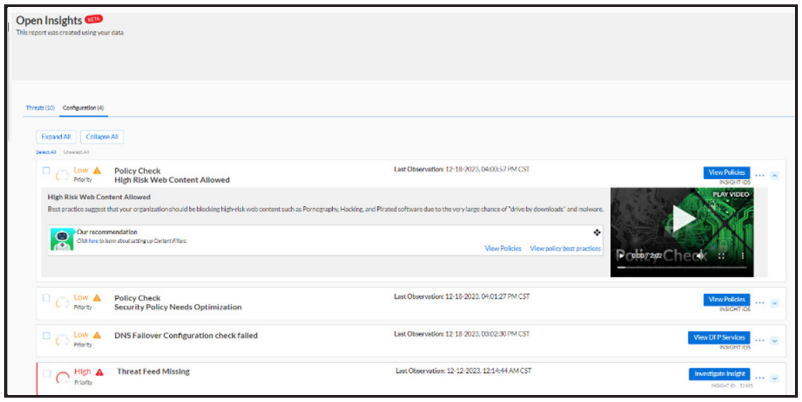


*Figura 3: Identificación proactiva de errores de configuración débiles o peligrosos para garantizar una capacidad óptima de defensa, investigación y respuesta.*

- Falta la fuente de amenazas DNS
- Falta la clave gratuita de VirusTotal
- La política de seguridad necesita optimización
- Error de comprobación de conmutación por error de DNS
- La acción de alimentación no coincide
- DFP ocultando detalles de activos
- Política de seguridad en modo de registro
- Filers de contenido web desactivados
- Contenido web de alto riesgo permitido

## UN IMPACTO FINANCIERO, OPERATIVO Y COMERCIAL POSITIVO

Mientras que la mayoría de las herramientas de seguridad pueden prometer poco más que "facilidad de uso" y "menos infracciones", SOC Insights puede hacer mucho más, desde reducir el estrés y la rotación de los analistas hasta reducir muchas preocupaciones de seguridad derivadas de la expansión, las fusiones y adquisiciones y otras iniciativas empresariales. Por ejemplo:

- La naturaleza del DNS facilita unificar una nueva ubicación o socio comercial en una infraestructura DNS común en cuestión de minutos en lugar de meses.
- Los análisis de configuración son altamente proactivos para ayudar a mitigar las violaciones de seguridad o la pérdida de datos debido a la "mala configuración", uno de los 3 principales factores notificados en las infracciones relacionadas con errores[3].
- La autocorrelación de "software malicioso", "phishing", "botnet" y otras actividades "importantes" o de "propagación" permite a los encargados de la respuesta hacer frente a muchas amenazas a la vez, lo que aumenta su eficacia.
- Pase a una postura de seguridad más proactiva con la capacidad de monitorear categorías de información como "valores atípicos", "túnel DNS" y "resolver abierto", así como características únicas de visibilidad de aplicaciones y similares de BloxOne Threat Defenses.
- La integración de inteligencia del ecosistema de seguridad mejora el retorno de la inversión de toda la pila de seguridad al ofrecer "información" procesable en lugar de solo registros y eventos sin procesar.
- SOC Insights recopila automáticamente datos relevantes y permite a los analistas ver y pivotar alrededor de esos datos para llegar a las conclusiones más rápido y con mayor confianza. Esto contribuye a reducir el estrés y a una mayor retención de profesionales de seguridad cualificados y experimentados.

## ELEVE SIEM, SOAR Y OTRAS PARTES DEL ECOSISTEMA CON INFORMACIÓN

SecOps conoce el valor y las limitaciones de compartir datos sin procesar en el ecosistema de seguridad. Esto ha convertido la experiencia en SIEM y SOAR en uno de los conjuntos de habilidades más desafiantes para la mayoría de las organizaciones. SOC Insights alivia la carga de estas otras herramientas y puede compartir la información resultante en toda la gama de seguridad para hacer que otras herramientas sean más eficaces y aumentar aún más la eficiencia general de SecOps.

---

1 "SANS 2023 SOC Survey", junio de 2023, por Chris Crowley, Barbara Filkins, John Pescatore

2 "NSA launches pilot program to secure defense contractors", 18 de junio, 2020, por Lauren C. Williams, NEXTGOV/FCW

3 "Verizon 2023 DBIR Report"

4 Voice of the SOC Analyst

5 The Orca Security 2022 Cloud Security Alert Fatigue Report

6 Voice of the SOC Analyst

7 https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

infoblox.

Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

**Sede corporativa**
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com



Versión: 20240104v1