NOTAS DE LA SOLUCIÓN

OPTIMICE SU SPLUNK SIEM Y SOAR CON INFOBLOX

Optimice su inversión en SIEM y SOAR de Splunk Enterprise mediante una visión detallada del DNS.

DESAFÍOS

Los equipos de seguridad confían en las herramientas SIEM y SOAR para investigar y responder eficazmente ante eventos de seguridad. A medida que los ataques se vuelven más sigilosos y difíciles de detectar, las organizaciones se han visto obligadas a aumentar la supervisión, lo que implica la incorporación de cada vez más registros en sus plataformas de monitoreo de seguridad. Este proceso aumenta los requisitos de almacenamiento, así como la cantidad de alertas generadas e investigaciones realizadas, lo que a menudo puede derivar en fatiga e incluso desgaste para los analistas de seguridad.

Además, suele resultar difícil acceder y correlacionar la inteligencia sobre amenazas con datos relevantes de red y dispositivos, lo que dificulta la automatización eficaz y la obtención de conclusiones precisas. Sin esta información contextual, las capacidades de los manuales de estrategias se ven seriamente limitadas.

RESULTADOS INMEDIATOS GRACIAS A UNA INTEGRACIÓN SENCILLA

Infoblox, líder en infraestructura y seguridad DNS, y Splunk, proveedor líder en soluciones SIEM y SOAR, ofrecen integraciones sencillas que pueden mejorar las capacidades de cada solución y potenciar la eficiencia general de los equipos de SecOps.

Splunk Cloud Platform y Splunk Enterprise Security ofrecen servicios híbridos en la nube con mecanismos tanto proactivos como reactivos para el consumo de datos externos. Basándose en esos datos, los equipos de seguridad pueden buscar, analizar, visualizar y actuar de forma más efectiva.

BloxOne® Threat Defense de Infoblox, junto con SOC Insights, se integra con las soluciones de Splunk para proporcionar información priorizada y exclusiva, además de datos relacionados con eventos, mediante herramientas como Threat Intelligence Data Exchange (TIDE) y Dossier de Infoblox. Cada funcionalidad puede proporcionar datos priorizados a Splunk para reducir los requisitos de almacenamiento y optimizar las tareas de investigación, automatización y otras actividades clave de los analistas de seguridad.

VISUALICE LOS DATOS DE INTELIGENCIA SOBRE AMENAZAS DE INFOBLOX EN SPLUNK ENTERPRISE SECURITY Y EN LA PLATAFORMA EN LA NUBE

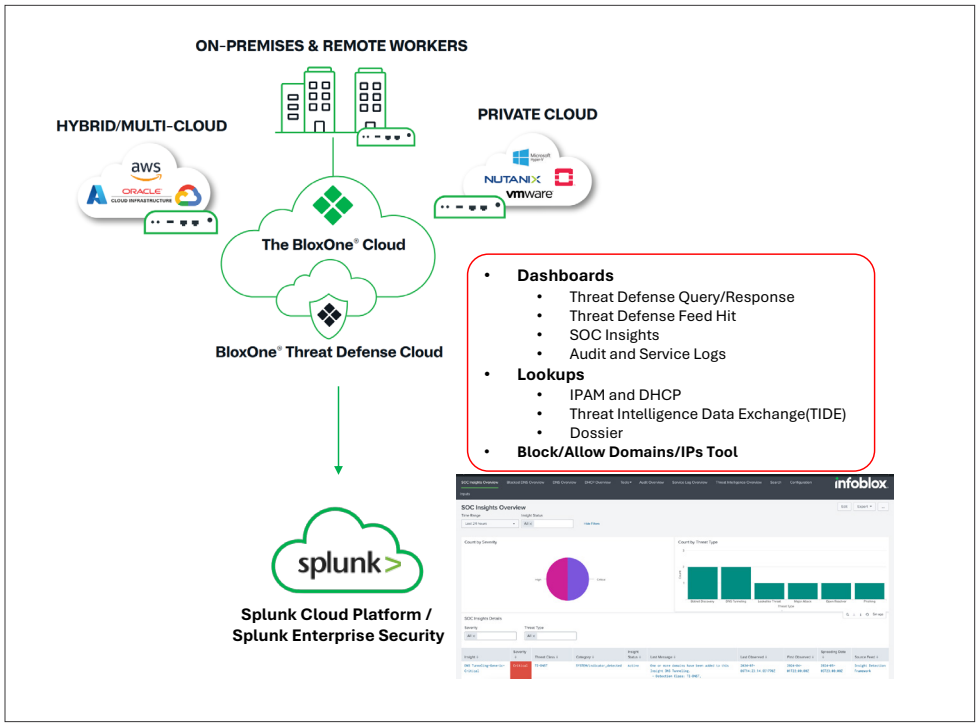
TIDE de Infoblox proporciona inteligencia sobre amenazas de alta precisión en formato legible por máquina a Splunk, lo que permite a los equipos de seguridad detectar actividad maliciosa y reducir el tiempo de permanencia de las amenazas. En conjunto, la solución integrada de Infoblox y Splunk contribuye a reducir los tiempos de investigación y a mejorar la visibilidad, respaldando así los entornos de red híbridos modernos.

PRESTACIONES CLAVE

La integración de Infoblox con Splunk Cloud Platform, Splunk Enterprise Security y Splunk SOAR mejora el rendimiento de Splunk y amplía la visibilidad sobre los eventos y la inteligencia sobre amenazas, lo que acelera las investigaciones y permite una respuesta más eficiente. Gracias a esta integración, los equipos de seguridad y respuesta ante incidentes pueden aprovechar al máximo la potencia de SIEM y SOAR, ya sea en entornos locales o en la nube de Splunk, combinándola con eventos de seguridad DNS, metadatos de gestión de direcciones IP (IPAM) e información sobre amenazas proporcionada por Infoblox.

Las capacidades de Splunk SIEM, mejoradas por Infoblox TIDE, permiten a los equipos de seguridad:

- Acceso a datos detallados de dispositivos y red para obtener mayor contexto
- Optimización de los requisitos de almacenamiento mediante filtrado inteligente de datos
- Correlación de inteligencia sobre amenazas priorizada e integral relacionada con los eventos



PRESTACIONES CLAVE

- Acceda a datos detallados de dispositivos y red (incluidos dominios, direcciones IP y otras solicitudes DNS) que ofrecen un contexto invaluable sobre los eventos para facilitar una toma de decisiones más inteligente.
- Relacione eventos con inteligencia sobre amenazas priorizada y exhaustiva para proporcionar a los analistas información clave que acelere los procesos de investigación y respuesta.
- Optimice los requisitos de almacenamiento mediante el filtrado inteligente de datos, para maximizar el rendimiento de Splunk y garantizar que los analistas dispongan, bajo demanda, de los datos «correctos».
- Genere resúmenes de incidentes de seguridad en función de los indicadores de compromiso (IoC) y realice un seguimiento del panorama de amenazas a lo largo del tiempo, clasificado por nivel de gravedad, gracias a los datos disponibles en la herramienta Dossier de Infoblox.
- Priorice los eventos de mayor riesgo y acelere la respuesta con acceso a una amplia variedad de fuentes de inteligencia sobre amenazas.
- Supervise la actividad de los dispositivos y las tendencias en toda la plataforma con una visibilidad consolidada.

IMPULSE LA PRODUCTIVIDAD DE SOAR A TRAVÉS DE LA HERRAMIENTA DOSSIER DE INFOBLOX

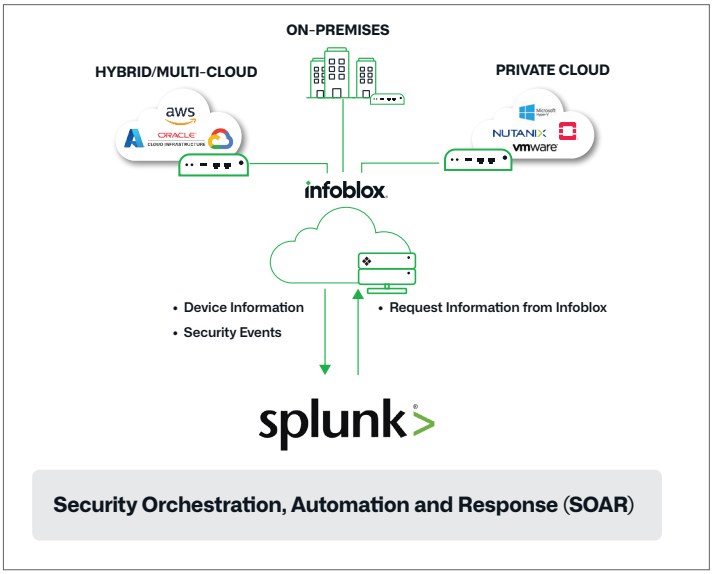
Además de eventos, contexto y metadatos de red y dispositivos, Dossier ofrece acceso a inteligencia sobre amenazas en profundidad. Esto ayuda a los analistas a investigar, valorar riesgos, activar respuestas automatizadas y reforzar la eficacia de los manuales de estrategias.

Las capacidades de Splunk SOAR, mejoradas por Infoblox Dossier, permiten a los analistas de seguridad:

- Acceso directo a la inteligencia sobre amenazas de Infoblox para detectar actividad maliciosa
- Automatización de respuestas eficaces ante amenazas con metadatos completos de dispositivos
- Manuales de estrategias más eficaces gracias a una visión integral de amenazas y red

PRESTACIONES CLAVE

- Acceda directamente a los indicadores de compromiso (IoC) de Infoblox Threat Intelligence para la detección y el bloqueo de amenazas y actividad sospechosa
- Automatice el aislamiento eficaz de dispositivos y otras respuestas a amenazas con amplia visibilidad y metadatos de dispositivos
- Proporcione a los administradores acceso a información adicional sobre amenazas y red para mejorar sus manuales de estrategias de SOAR
- Automatice y acelere la respuesta con un conjunto completo de API de inteligencia sobre amenazas
- Agilice la respuesta con información más precisa sobre amenazas y enfocándose en los eventos de seguridad de mayor riesgo



BENEFICIOS GENERALES DE LA INTEGRACIÓN DE SPLUNK E INFOBLOX

- **Eficiencia de SIEM:** mantenga un rendimiento óptimo accediendo solo a inteligencia sobre amenazas y a los datos de red relevantes.
- **Eficacia de SOAR**: amplíe la capacidad de sus manuales de estrategias con información consolidada sobre amenazas y datos clave de dispositivos.
- **Simplicidad en la integración:** aproveche fácilmente las aplicaciones de Splunk ya disponibles para acelerar el tiempo de obtención de valor.
- **Productividad de SecOps:** mejore la visibilidad y utilice capacidades avanzadas de filtrado para incrementar la eficiencia de sus operaciones de seguridad.
- **Retorno de inversión:** obtenga más valor de su inversión en SIEM y SOAR, junto con los beneficios de seguridad únicos que ofrece BloxOne Threat Defense.

CONCLUSIÓN

Los equipos de SecOps suelen tener dificultades para gestionar la carga de trabajo, controlar los costos de almacenamiento y sacar el máximo provecho de las herramientas disponibles para investigar y responder a incidentes de seguridad. La integración de Splunk Enterprise SIEM y SOAR con inteligencia sobre amenazas depurada, junto con metadatos de dispositivos y red, mejora tanto la efectividad de estas soluciones como la eficiencia de los equipos de seguridad. La combinación de Infoblox con Splunk aporta mayor valor a toda la infraestructura, impulsa la productividad de SecOps y refuerza su capacidad de respuesta ante amenazas.

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 (EE. UU.)

+1.408.986.4000
www.infoblox.com

Versión: 20240724v4