NOTAS DE LA SOLUCIÓN

REFUERCE SU SIEM DE QRADAR CON DDI Y BLOXONE THREAT DEFENSE DE INFOBLOX

Vea más de su IBM Security QRadar con la visibilidad del DNS sin igual de Infoblox

El panorama de la ciberseguridad actual es complejo y está en constante evolución. Los ciberdelincuentes apuntan cada vez más a la infraestructura DNS para llevar a cabo ataques sofisticados, como campañas de phishing, distribución de software malicioso y exfiltración de datos. Los analistas de seguridad se hallan bajo una inmensa presión para identificar y responder a estas amenazas de manera oportuna. Sin embargo, las soluciones tradicionales de Gestión de Eventos e Información de Seguridad (SIEM) a menudo carecen de la profundidad de integración necesaria con los datos de seguridad del DNS para garantizar una investigación y una respuesta efectivas.

DESAFÍOS

Los equipos de seguridad se enfrentan a numerosos desafíos en el complejo panorama de amenazas actual:

- **Sobrecarga de alertas:** Los analistas de seguridad están inundados de continuas alertas procedentes de las diversas herramientas de seguridad, lo que les dificulta identificar y priorizar las amenazas más críticas.
- **Visibilidad limitada:** Las soluciones SIEM tradicionales a menudo carecen de la capacidad de capturar y analizar los datos de seguridad ampliados que generan por la infraestructura de DDI y BloxOne Threat Defense de Infoblox, lo que crea puntos ciegos y dificulta obtener una comprensión completa de los ataques basados en el DNS.
- **Flujos de trabajo ineficientes:** Investigar amenazas a menudo requiere alternar diferentes herramientas de seguridad, lo que malgasta tiempo y esfuerzo valiosos.

RÁPIDO RETORNO DE LA INVERSIÓN GRACIAS A UNA FÁCIL INTEGRACIÓN

Infoblox, líder en DNS, DHCP y gestión de direcciones IP (DDI) y en seguridad del DNS, junto con IBM Security QRadar, proveedor destacado de SIEM y SOAR, ofrece una integración sencilla capaz de mejorar las capacidades de cada solución y aumentar la eficiencia general de SecOps. Esta potente combinación mejora las capacidades de detección y respuesta a amenazas, lo que proporciona a su equipo de seguridad los conocimientos esenciales necesarios para proteger su organización de forma más eficaz.

Esta poderosa combinación capacita a los equipos de seguridad para:

- **Simplifique las investigaciones:** Optimice sus flujos de trabajo de seguridad utilizando los paneles de control prediseñados y las acciones de usuario disponibles en QRadar. Estas funciones proporcionan acceso rápido a información crítica sobre la actividad del DNS, threat intelligence y datos de red contextuales, reduciendo el tiempo necesario para investigar y responder a incidentes.

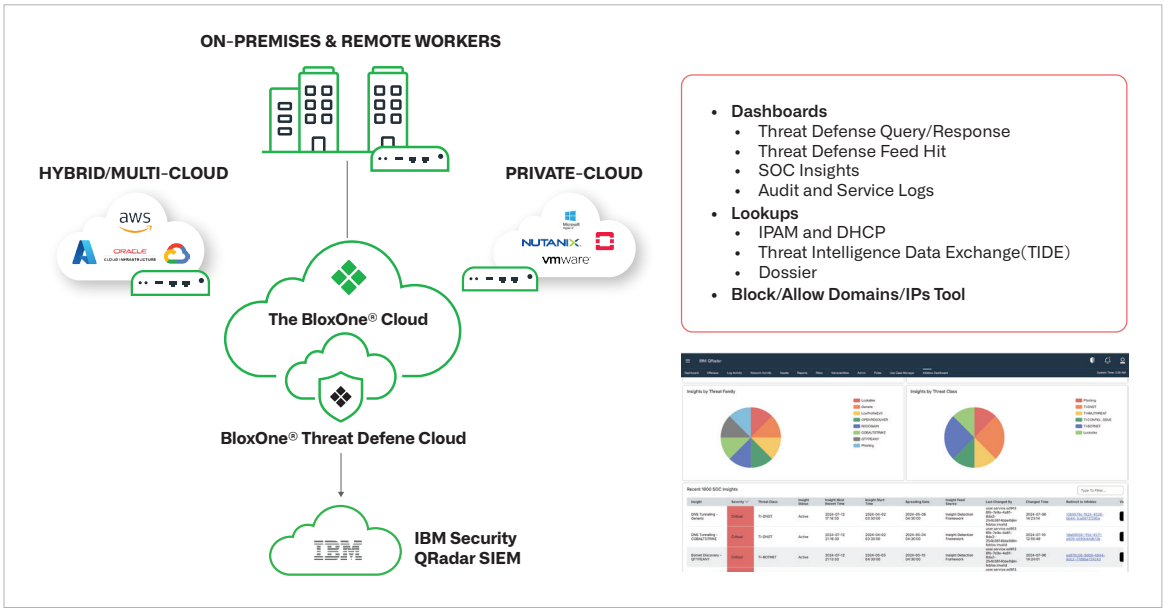
BENEFICIOS CLAVE

- **Visibilidad mejorada:** Obtenga información detallada sobre las actividades de DNS, DHCP e IPAM de su red, garantizando una visibilidad de red completa.
- **Respuesta acelerada:** Agilice la respuesta a incidentes, con acceso directo a threat intelligence de Infoblox y datos contextuales en QRadar.
- **Reducción de la fatiga causada por las alertas:** Céntrese en las amenazas críticas filtrando las alertas no esenciales, lo que reducirá la sobrecarga de sus analistas de seguridad.
- **ROI maximizado:** Amplifique el valor de su inversión en QRadar aprovechando la threat intelligence avanzada de Infoblox.

- **Unifique la Threat Intelligence:** Obtenga una visión integral de la actividad de su red por medio de correlacionar los datos de Infoblox, como eventos del DNS, asignaciones de DHCP, registros de auditoría y fuentes de threat intelligence, con otros eventos de seguridad recopilados por QRadar. Esta visión holística permite a los analistas identificar y comprender el alcance completo de las posibles amenazas.
- **Tome medidas decisivas:** Forme a sus analistas de seguridad para que puedan tomar medidas inmediatas contra amenazas directamente desde QRadar. La aplicación de Infoblox le permite bloquear dominios e IP maliciosos en un clic, lo que minimiza los posibles daños causados por un ataque.

Al implementar la aplicación de Infoblox para QRadar, los equipos de seguridad pueden transformar su posición de seguridad, puesto que obtienen una vista centralizada de la actividad de la red, agilizan las investigaciones y aceleran su respuesta ante las amenazas.

PRESTACIONES CLAVE



Configuración de la aplicación

- **Configuración sin contratiempos:** Configuración sencilla en QRadar para conectarse a los servicios de seguridad avanzados de Infoblox.

Paneles de control

- **Visión general de los eventos del DNS:** Ofrece una visualización clara de las actividades del DNS, lo que permite identificar rápidamente posibles amenazas.
- **Visión general de la asignación de DHCP:** Supervisa las asignaciones de DHCP para detectar conductas inusuales y posibles problemas de seguridad.
- **Visión general de los registros de auditoría:** Lleva a cabo un seguimiento de los cambios en la configuración de la red para garantizar cumplimiento normativo y seguridad.
- **Visión general de las solicitudes de DNS bloqueadas:** Analiza las solicitudes bloqueadas para prevenir y responder a las amenazas.
- **Visión general de SOC Insights:** Resume las perspectivas y alertas críticas de seguridad.

Acciones del Usuario

- **Búsqueda con Dossier:** Investigue rápidamente los dominios, las IP y otros indicadores de ataques con Infoblox Dossier.
- **Búsqueda con TIDE:** Acceda a threat intelligence detallada para tomar decisiones de seguridad fundamentadas.

- **Búsqueda de IPAM:** Recupere datos de direcciones IP para correlacionar las actividades de la red con posibles amenazas.
- **Búsqueda de asignaciones de DHCP:** Rastree las actividades del dispositivo a través de los registros de asignaciones de DHCP.
- **Bloqueo de dominios/IP:** Bloquee directamente o permita dominios e IP en QRadar para agilizar la mitigación de amenazas.

La aplicación de Infoblox para QRadar refuerza sus operaciones de seguridad con visibilidad avanzada, tiempos de respuesta mejorados y eficiencia optimizada para asegurarse de que su organización esté bien protegida contra amenazas emergentes.

INTEGRACIÓN GENERAL DE QRADAR E INFOBLOX

La integración de QRadar con Infoblox proporciona una solución de seguridad integral que mejora su infraestructura existente. Esta sinergia garantiza:

- **Eficiencia de SIEM:** Mantenga un rendimiento óptimo accediendo solo a la threat intelligence y los datos de red pertinentes.
- **Eficacia de SOAR:** Potencie la orquestación y automatización de su seguridad con datos ampliados y capacidades de filtrado avanzadas.
- **Simplicidad de integración:** La integración rápida y sencilla mediante métodos probados acorta el tiempo necesario para generar valor.
- **Productividad operativa:** Mejore la eficiencia de sus operaciones de seguridad proporcionando visibilidad avanzada y capacidades de filtrado avanzadas.
- **ROI de la inversión:** Aumente la rentabilidad de sus inversiones en SIEM y SOAR con las ventajas de seguridad adicionales de BloxOne Threat Defense.

CONCLUSIÓN

Gestionar las cargas de trabajo de seguridad, controlar los costes de almacenamiento y mantener una respuesta eficaz a las amenazas son retos significativos para los equipos de SecOps. La integración de Infoblox con QRadar mejora el valor de toda la pila de seguridad, al proporcionar threat intelligence ampliada y datos de red integrales. Esta combinación potencia la productividad de SecOps, mejora la eficiencia y garantiza un programa de seguridad más robusto y ágil. Al aprovechar la aplicación de Infoblox para QRadar, amplía las capacidades de seguridad de su organización y maximiza el retorno de sus inversiones en seguridad.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com

Versión: 20240703v1