NOTAS DE LA SOLUCIÓN

AUMENTE LA PRODUCTIVIDAD DEL SOC CON ALERTAS DE SEGURIDAD EN TIEMPO REAL EN MICROSOFT TEAMS

Envíe automáticamente mensajes de Microsoft Teams que contengan datos de seguridad basados en el DNS correlacionados y priorizados

El panorama de la ciberseguridad actual es complejo y está en constante evolución. Los ciberdelincuentes apuntan cada vez más a la infraestructura del 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 y no disponen del ancho de banda necesario para monitorizar y buscar de manera proactiva las múltiples aplicaciones de las que son responsables. Esta rutina de «silla giratoria» es altamente ineficiente y aumenta la necesidad de comunicarse y colaborar en una única herramienta familiar, que acelere tanto el tiempo medio de detección (MTTD) como el tiempo medio de respuesta (MTTR). Para las empresas que han adoptado las posibilidades de Microsoft Teams, Infoblox ha desarrollado una integración certificada, diseñada para ofrecer notificaciones de seguridad inmediatas y priorizadas directamente en Microsoft Teams, lo que permite tomar decisiones y medidas con rapidez en el centro de operaciones de seguridad.

DESAFÍOS

Los equipos de seguridad se enfrentan a numerosos retos 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 de seguridad tradicionales a menudo son incapaces de analizar fácilmente el contexto y el alcance de las amenazas y de determinar qué pasos deben darse.
- **Flujos de trabajo ineficientes:** Investigar amenazas a menudo requiere alternar diferentes herramientas de seguridad, lo que malgasta tiempo y esfuerzo valiosos.

RÁPIDA OBTENCIÓN DE VALOR MEDIANTE UNA INTEGRACIÓN SENCILLA: INFOBLOX + MICROSOFT TEAMS

La solución de detección y respuesta del DNS (DNSDR) de Infoblox, BloxOne Threat Defense, mejorada con SOC Insights, extrae automáticamente grandes cantidades de inteligencia sobre amenazas de DNS y datos de activos para correlacionar y priorizar respuestas procesables a las amenazas. La solución convierte grandes cantidades de datos de inteligencia sobre eventos, redes, ecosistemas y DNS en información procesable para mejorar la eficiencia de SecOps. Los extensos datos de seguridad generados por BloxOne Threat Defense con SOC Insights eliminan puntos ciegos y aumentan la capacidad de comprender plenamente los ataques basados en el DNS.

BENEFICIOS CLAVE

- **Comunicación y colaboración centralizadas:** Reciba notificaciones automáticas de alertas de seguridad priorizadas directamente en Microsoft Teams y reduzca la necesidad de monitorizar manualmente múltiples herramientas.
- **Respuesta acelerada:** Agilice la respuesta a incidentes, con acceso directo al contexto y datos de las amenazas para determinar rápidamente qué pasos deben seguirse.
- **Reducción de la fatiga causada por las alertas:** Reciba notificaciones solamente de amenazas críticas para reducir el ruido y la sobrecarga de los analistas de seguridad.
- **ROI maximizado:** Multiplique el valor de su inversión en Microsoft Teams, al optimizar los flujos de trabajo de seguridad y reducir el cambio de una aplicación a otra.

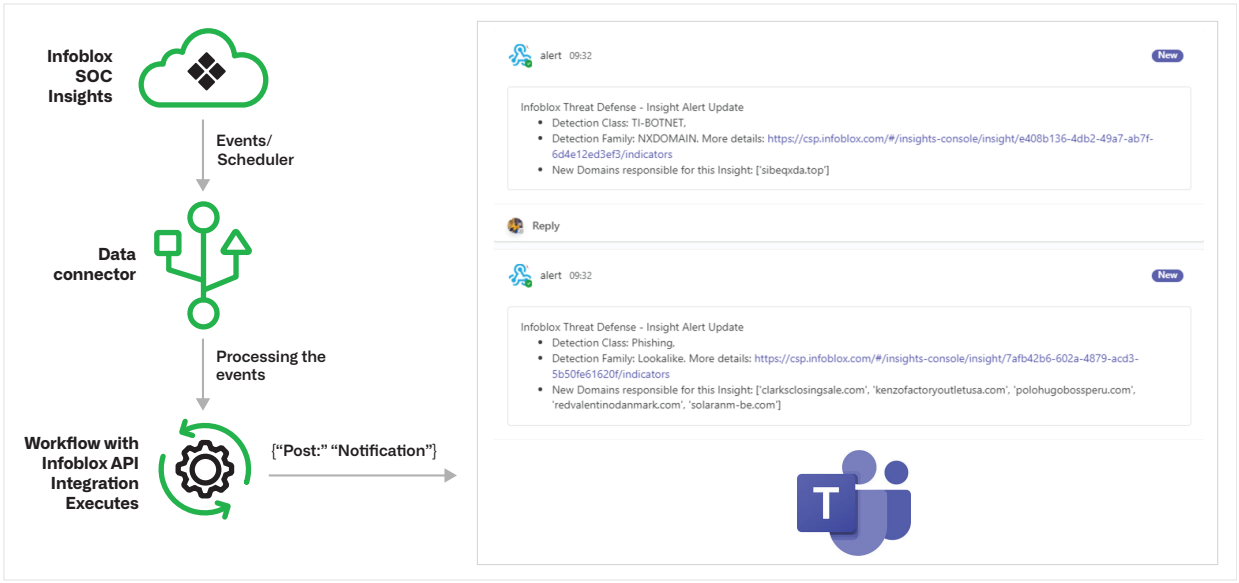
Para mejorar aún más la eficiencia general del centro de operaciones de seguridad, Infoblox ofrece una integración con Microsoft Teams con pocos requisitos de código, capaz de potenciar las ventajas de cada solución y reducir el coste de propiedad total. Esta potente combinación agiliza las capacidades de detección y respuesta a amenazas, proporcionando a los equipos de seguridad notificaciones inmediatas de los conocimientos críticos necesarios para proteger la organización.

Infoblox + Microsoft Teams capacita a los equipos de seguridad para:

- **Unificar alertas de amenazas:** Infoblox envía mensajes en tiempo real a través de Microsoft Teams para informar a los analistas de seguridad de las amenazas priorizadas, eliminando de inmediato la necesidad de efectuar tareas de monitorización manuales con múltiples herramientas. Las alertas se envían a un canal personalizado de Microsoft Teams, lo que permite a los analistas gestionar las alertas de forma centralizada, documentación histórica y seguimiento incluidos.
- **Simplificar las investigaciones:** Los mensajes en Microsoft Teams con la tecnología de Infoblox dan visibilidad al contenido crítico y ofrecen el contexto necesarios para clasificarlo y colaborar en los siguientes pasos. Solo hay que hacer clic en el enlace proporcionado en el mensaje para acceder directamente al Portal de Infoblox e investigar más a fondo.
- **Tomar medidas decisivas:** Provistos del contenido y el contexto adecuados que proporciona Infoblox, los analistas de seguridad pueden responder de manera eficiente y eficaz a las amenazas más significativas y actualizar el estado en el hilo de mensajes de Microsoft Teams a fin de mantener informado al equipo.

Al implementar Infoblox para Microsoft Teams, los equipos pueden transformar su posición de seguridad mediante una vista centralizada de las alertas críticas, que agiliza las investigaciones y acelera su respuesta a las amenazas.

CÓMO FUNCIONA



RENDIMIENTO SUPERIOR DEL SOC CON LA INTEGRACIÓN DE INFOBLOX Y MICROSOFT TEAMS

La integración de Infoblox con Microsoft Teams ofrece una solución de seguridad colaborativa que mejora la infraestructura existente. Esta sinergia garantiza:

- **La eficiencia del centro de operaciones de seguridad:** Mantenga un rendimiento óptimo, enviando de inmediato alertas de amenazas priorizadas a un canal de Microsoft Teams centralizado. Así se mejora la comunicación y se proporciona seguimiento histórico.
- **La eficacia del centro de operaciones de seguridad:** Apoye a los analistas de seguridad con contenido y contexto de amenazas directamente en el mensaje de alerta de Microsoft Teams para que puedan tomar medidas rápidas y apropiadas.
- **Productividad operativa/ROI:** Racionalizar los flujos de trabajo y reducir el cambio de una aplicación a otra puede mejorar la eficiencia de su equipo de SecOps y ahorrar tiempo y costes.
- **Simplicidad de integración:** Una integración con pocos requisitos de código, sencilla, probada y certificada acorta el tiempo necesario para generar valor.

CONCLUSIÓN

Automatizar las cargas de trabajo de seguridad, reducir los tiempos de detección y respuesta, y mantener comunicaciones y colaboración efectivas en la respuesta a amenazas son retos significativos para los equipos de SecOps. La integración de Infoblox con la mensajería de Microsoft Teams aumenta el valor de toda la pila de seguridad, al proporcionar una plataforma unificada donde transmitir comunicaciones de threat intelligence ampliadas. Esta combinación aumenta la productividad de SecOps, mejora la eficiencia y garantiza un programa de seguridad más robusto y ágil. Al utilizar Infoblox para Microsoft Teams, refuerza las capacidades de seguridad de su organización y maximiza el retorno de sus inversiones en seguridad.

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: 20240724v1