NOTAS DE LA SOLUCIÓN

THREAT INTELLIGENCE DATA EXCHANGE (TIDE)

Impulse la eficiencia de SecOps mediante la gestión y automatización de inteligencia sobre amenazas

LA EFICACIA EN SEGURIDAD DEPENDE DE UNA INTELIGENCIA SOBRE AMENAZAS DIVERSA Y PRECISA

Durante décadas, muchas de las empresas más grandes y seguras del mundo han adoptado un enfoque de seguridad multiproveedor, partiendo de la idea de que ningún proveedor por sí solo puede ofrecer una protección lo suficientemente completa frente a un panorama de amenazas en constante evolución. Para lograrlo, orquestaban sus defensas de forma que los ataques tuvieran que atravesar múltiples soluciones de distintos fabricantes, con la esperanza de que al menos uno contara con el conocimiento necesario para detectar alguna fase del ataque a lo largo de la cadena de eliminación.

En los últimos años, diversos estudios han validado y puesto en valor este enfoque al revelar la escasa superposición entre los distintos feeds de amenazas disponibles, ya sean de proveedores comerciales, de código abierto o comunitarios. En uno de estos estudios, la comparación entre dos proveedores de inteligencia sobre amenazas mostró apenas un 11 % de coincidencia, lo que indica que el 89 % de los datos eran únicos para cada uno.

Esto ha impulsado la búsqueda de la combinación óptima de inteligencia sobre amenazas que permita a las organizaciones maximizar el retorno de su inversión en seguridad. Sin embargo, este esfuerzo ha incrementado la carga de los equipos de SecOps, que deben identificar, recopilar, normalizar y distribuir distintos tipos de datos provenientes de decenas de fuentes, para luego proporcionar la combinación adecuada a cada herramienta de seguridad. Como resultado, la mayoría se ve obligada a trabajar con una mezcla de herramientas comerciales y soluciones internas, conectadas mediante API, scripts y macros, en un intento por lograr cierto grado de éxito.

TIDE DE INFOBLOX OPTIMIZA Y SIMPLIFICA LA GESTIÓN DE INTELIGENCIA SOBRE AMENAZAS

BloxOne Threat Defense Advanced de Infoblox incluye una funcionalidad clave: TIDE (Threat Intelligence Data Exchange), pensada para simplificar la recopilación y gestión de inteligencia sobre amenazas. Además de incluir hasta 30 fuentes de amenazas con BloxOne Threat Defense, TIDE permite incorporar inteligencia sobre amenazas de fuentes externas y controlar cómo se distribuye esa información en toda la pila de seguridad, para que cada herramienta sea lo más eficaz posible.

DATOS Y CIFRAS

Según la encuesta de SANS sobre Inteligencia de Ciberseguridad (CTI) de 2021:

- **2 de cada 3 encuestados tienen dificultades** para distribuir la información de CTI por correo electrónico o mediante documentos
- Más de la mitad de los encuestados señalan **la falta de personal, habilidades o financiación** como principales barreras para una CTI efectiva
- Los autores de la encuesta de SANS concluyen que **la automatización es fundamental para que la CTI sea eficiente y escalable**

Los beneficios clave de TIDE incluyen:

- Recopile y gestione inteligencia sobre amenazas seleccionada en tiempo real desde múltiples fuentes en una única plataforma abierta y flexible
- Apoye una investigación y respuesta más rápidas a las amenazas con el contexto de más de 300 áreas distintas de clasificación de amenazas
- Mejore la eficiencia de SecOps y la efectividad de toda la infraestructura de seguridad mediante inteligencia sobre amenazas que se puede compartir fácilmente
- Observe y controle actividades de amenazas altamente evasivas a nivel de DNS con la ayuda de BloxOne
- Threat Defense, que permite identificar riesgos como puertas traseras, comunicaciones con servidores de comando y control (C2), túneles de datos o exfiltración mediante DNS

TIDE de Infoblox está diseñado para mantener actualizadas en tiempo real las soluciones de seguridad como BloxOne Threat Defense de Infoblox y el resto del ecosistema de ciberseguridad frente a amenazas nuevas y en evolución. Puede combinar hasta 30 fuentes distintas de inteligencia provistas por Infoblox con otras fuentes comerciales, gubernamentales, del sector, de código abierto o incluso datos internos del cliente. Gracias a sus capacidades de automatización y compatibilidad con múltiples formatos de archivo, TIDE ayuda a los clientes a recopilar y distribuir la combinación adecuada de inteligencia sobre amenazas hacia distintas herramientas dentro de su ecosistema: firewalls, SIEM, SWG, SOAR, escáneres de vulnerabilidades y más.

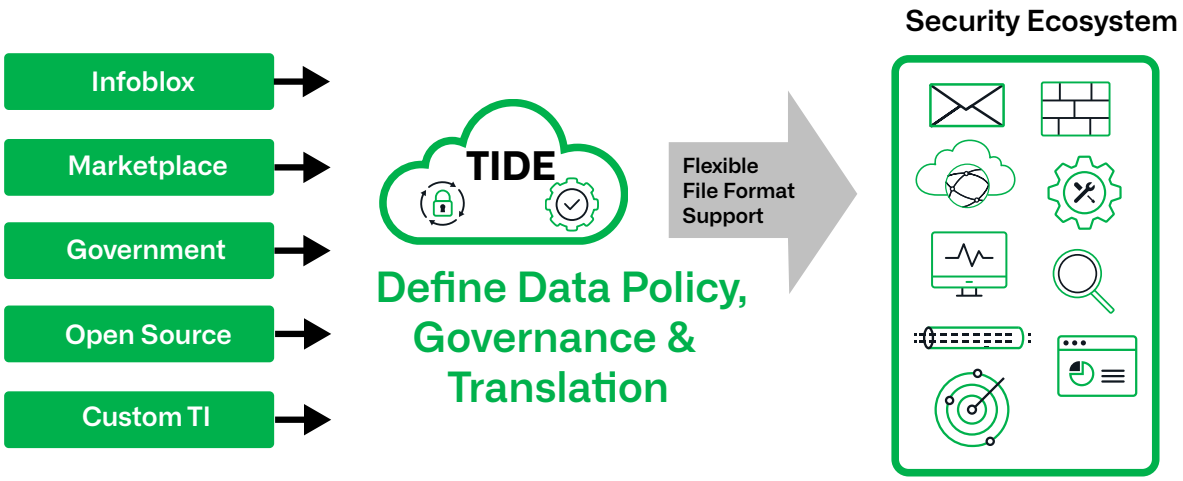

Figura 1: TIDE facilita el intercambio de inteligencia sobre amenazas en todo el ecosistema de seguridad, mejorando las defensas y la generación de informes.

SOLO UNA DE LAS MUCHAS CARACTERÍSTICAS VALIOSAS DE BLOXONE THREAT DEFENSE

TIDE es una de las funcionalidades integradas en BloxOne Threat Defense, una solución de seguridad nativa en la nube para proteger contra el software malicioso moderno, el ransomware, las comunicaciones C&C, la exfiltración de datos y otras amenazas avanzadas utilizando el DNS como primera línea de defensa. Incluye herramientas que mejoran toda la pila de seguridad y hacen más eficientes las operaciones de seguridad, al acelerar las investigaciones de amenazas y permitir una respuesta más rápida y fiable. Es la primera solución de seguridad de la industria pensada para la realidad híbrida actual, que ofrece protección integral en todo momento y lugar para todos los dispositivos de la red, incluidos los dispositivos BYOD y los de IoT/OT.

OPTIMICE LA BÚSQUEDA, INVESTIGACIÓN Y RESPUESTA FRENTE A AMENAZAS

BloxOne Threat Defense Advanced también incorpora una funcionalidad que permite a los analistas acceder y explorar todo el panorama de inteligencia sobre amenazas desde una única vista llamada Dossier. Dossier permite acceder bajo demanda a información sobre la gravedad de amenazas, datos WHOIS, referencias al marco MITRE ATT&CK, muestras de archivos, direcciones IP, URL y dominios relacionados, perfiles de actores de amenazas, cronologías de actividad y mucho más. Permite a los analistas moverse con libertad por los datos según su experiencia, de modo que puedan llegar a conclusiones seguras de forma más rápida.

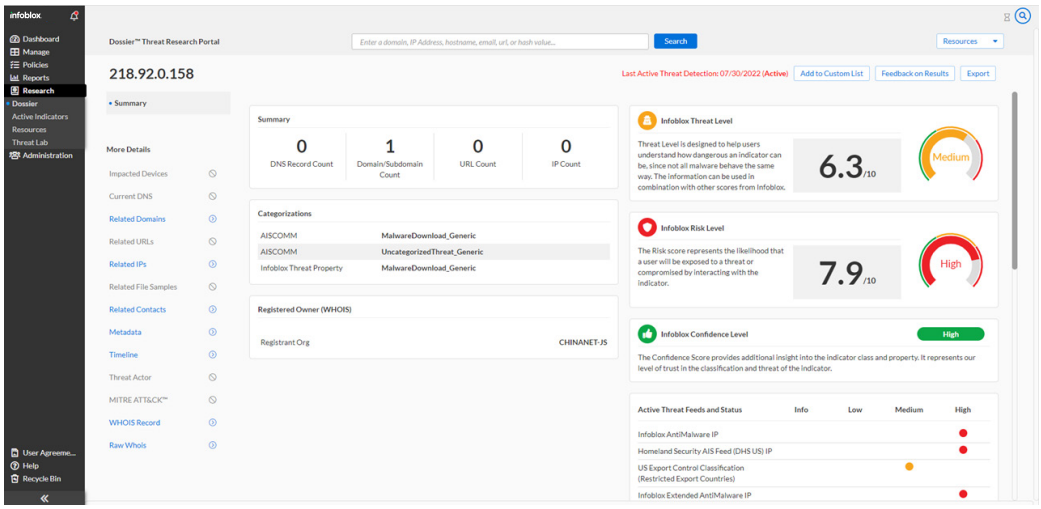

Figura 2: Panel de control de Dossier con la capacidad de profundizar y analizar bajo demanda.

INTEGRACIONES LISTAS PARA USAR: FUENTES DE AMENAZAS DE TERCEROS

Aunque la función TIDE de BloxOne Threat Defense puede simplificar y automatizar el proceso de integración de casi cualquier fuente de inteligencia sobre amenazas, y distribuirla a prácticamente cualquier herramienta de seguridad, algunos socios han colaborado con Infoblox para facilitar el proceso de incorporación de clientes.

Los siguientes socios ya son compatibles con la función TIDE:

CrowdStrike: proveedor líder de protección de endpoints de nueva generación, inteligencia sobre amenazas y servicios asociados. La inteligencia de nombres de host e IP de CrowdStrike Falcon permite a las organizaciones evitar daños por ataques dirigidos, detectar y atribuir malware avanzado y actividades de actores maliciosos en tiempo real, así como realizar búsquedas en todos los endpoints de manera eficiente, reduciendo el tiempo total de respuesta ante incidentes.Los clientes deben adquirir este feed directamente a través de CrowdStrike, pero Infoblox puede asistir en la «activación» del feed dentro de la plataforma TIDE.

FireEye iSIGHT Threat Intelligence: ofrece inteligencia cibernética de IP y nombres de host, basada en análisis estratégicos, operativos y tácticos realizados por un equipo global de expertos. Una suscripción a ThreatScape proporciona la inteligencia necesaria para alinear los programas de seguridad con los objetivos de gestión de riesgos empresariales y defenderse de forma proactiva frente a amenazas cibernéticas nuevas y emergentes. Los clientes deben adquirir este feed directamente desde FireEye, pero Infoblox puede facilitar su activación dentro de la plataforma TIDE.

Además, los suscriptores de BloxOne Threat Defense Advanced pueden aprovechar las siguientes fuentes de proveedores externos (requiere una suscripción adicional) en formato RPZ (sin coste adicional) para aumentar su cobertura de amenazas en el plano de control DNS:

Fuente de dominios recién observados (NOD) de Farsight Security: esta fuente ofrece una capa añadida de defensa para combatir la exfiltración de malware, el abuso de marca y los ataques basados en spam que se originan o terminan en dominios recién activados.

Fuente de reputación de direcciones IP y dominios de Proofpoint Emerging Threats (ET): esta fuente proporciona datos procesables sobre la reputación de IP y dominios, basados en observaciones de comportamientos reales de actores de amenazas y en información directa del equipo de ET de Proofpoint. Gracias a un proceso exclusivo que aprovecha uno de los mayores intercambios activos de malware del mundo, la emulación de víctimas a gran escala, tecnología de detección propia y una red global de sensores, Proofpoint ET Intelligence se actualiza en tiempo real para proporcionar información útil frente a las amenazas emergentes actuales.

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: 20231030v1