NOTE DE SYNTHÈSE

Infoblox Threat Intel

Détectez, surveillez et bloquez les menaces à leur source - DNS

DÉFIS DE L'UTILISATION DE LA THREAT INTELLIGENCE AXÉE SUR LES MALWARES

La plupart des solutions de sécurité adoptent une approche centrée sur les malwares pour la threat intelligence, en s'appuyant sur un compromis avant de signaler un domaine comme malveillant. Cette approche post-incident signifie qu'ils jouent au chat et à la souris, en essayant de repérer les sites web malveillants à mesure qu'ils apparaissent et en les ajoutant aux flux de threat intel pour les bloquer.

C'est pourquoi, malgré les efforts du secteur de la sécurité, les attaques de type MFA (authentification multi-facteurs), les attaques de type domaine similaire et les attaques de phishing ciblées continuent d'avoir un impact sur les organisations, entraînant des violations de données et une atteinte à la réputation de l'entreprise. Il est nécessaire d'adopter une approche différente de la sécurité, qui permette de protéger les entreprises de manière proactive contre les criminels lorsqu'ils construisent leur infrastructure pour lancer des attaques.

INFOBLOX THREAT INTEL : POUR CONTRER LA CYBERCRIMINALITÉ À LA SOURCE

Infoblox Threat Intel allie une expertise avancée en matière de DNS à des techniques de pointe en science des données pour identifier l'infrastructure des cybercriminels avant qu'ils ne l'utilisent, et pour perturber les communications vers les domaines à haut risque. Infoblox Threat Intel est la première et la seule solution qui se concentre sur la détection des acteurs malveillants spécialisés dans le DNS et le suivi de leurs activités sur Internet, protégeant les clients de manière proactive contre les attaques émergentes : smishing, domaines similaires, domaines à haut risque, ransomwares, malwares, C&C, et bien plus encore. Infoblox Threat Defense utilise Infoblox Threat Intel pour détecter et neutraliser les menaces essentielles, des mois avant les autres systèmes de sécurité. Infoblox Threat Intel est spécialisé dans le DNS, il se charge de tout. Vous pouvez ainsi protéger votre réseau sans compromettre ses performances.

STATISTIQUES CLÉS :

Au premier trimestre 2024,

- 60 % des menaces ont été détectées avant la première requête DNS
- 82 % des menaces ont été détectées après une seule requête DNS
- 89 % des menaces ont été détectées dans les 48 premières heures

DES FAITS ET DES CHIFFRES

- Les attaques par MFA constituent l'incident le plus visible et le plus préoccupant de 2023, car elles combinent la vulnérabilité des employés (y compris les employés en télétravail) et l'utilisation de domaines similaires
- 75 % des organisations ont déjà été confrontées à des attaques par smishing (rapport State of Phish 2024 de Proofpoint)
- Dans de nombreuses attaques, les acteurs malveillants laissent vieillir leurs domaines pendant très longtemps, parfois même des mois après leur enregistrement.

DISPONIBILITÉ IMMÉDIATE D'INFOBLOX THREAT INTEL

Threat Defense, le produit de détection et de réponse DNS d'Infoblox, est disponible en quatre forfaits :

1. Threat Defense Essentials
2. Threat Defense Business On-Premises
3. Threat Defense Business Cloud
4. Threat Defense Advanced

Chaque forfait offre un accès à une gamme de données Infoblox Threat Intel via les « flux RPZ ». Le forfait Advanced inclut également un outil d'intégration et de distribution personnalisées de flux de menaces, appelé TIDE (Threat Intelligence Data Exchange), un portail de recherche sur les menaces appelé Dossier qui exploite ces données, et plus encore.

Voici les flux de menaces disponibles pour chaque forfait Threat Defense :

Flux	Essential	Business OnPrem	Business Cloud	Advanced
Base Infoblox	X	X	X	X
Infoblox Base IP		X	X	X
Infoblox à risque élevé				X
Infoblox à risque moyen				X
Infoblox à risque faible				X
Infoblox informatif		X	X	X
Noms d'hôtes publics du DoH	X	X	X	X
IP publiques du DOH	X	X	X	X
Bogon	X	X	X	X
DHS_AIS_Domain	X	X	X	X
DHS_AIS_IP	X	X	X	X
EECN IPS		X	X	X
L'OFAC américain sanctionne les IP				X
L'OFAC américain sanctionne les IP de haut niveau		X	X	X
L'OFAC américain sanctionne les IP moyennes		X	X	X
Noms d'hôtes et domaines pour les cryptomonnaies		X	X	X
IP des nœuds de sortie TOR		X	X	X

DESCRIPTION SOMMAIRE DES FLUX

Infoblox Base : le flux Infoblox Base permet une protection contre les domaines malveillants ou compromis connus. Cela inclut les malwares, les ransomwares, les APT, les kits d'exploitation, les serveurs de noms malveillants, les failles, etc. Nous vous recommandons de les bloquer pour tous les utilisateurs.

Infoblox Base IP : le flux Infoblox Base IP offre une protection contre les adresses IP malveillantes ou compromises connues. Ces adresses IP sont des infrastructures connues pour héberger des menaces qui peuvent agir sur un système ou le contrôler par le biais de téléchargements de malwares C&C et de sites de phishing actifs. Nous vous recommandons de les bloquer pour tous les utilisateurs.

Infoblox à risque élevé : le flux Infoblox à risque élevé comprend des domaines qui ne sont pas encore confirmés mais qui sont très suspects. Il est très probable qu'ils soient utilisés dans un acte malveillant à un moment ou à un autre. Ces domaines, bien que non confirmés, présentent une menace élevée et un niveau de confiance élevé, c'est pourquoi nous recommandons à la plupart des utilisateurs de les bloquer. Il s'agit de domaines suspects, de domaines similaires et de domaines émergents nouvellement observés (NOED) dont le score combiné de menace et de niveau de confiance est élevé.

Infoblox à risque moyen : le flux Infoblox à risque moyen comprend des domaines qui ne sont pas encore confirmés mais qui présentent un risque moyen. Il s'agit de domaines suspects dont le score combiné de menace et de confiance est inférieur à celui du flux « risque élevé », mais supérieur à celui du flux « risque faible ». Il est toujours possible qu'ils soient utilisés dans le cadre d'un acte malveillant, c'est pourquoi nous recommandons à la plupart des utilisateurs de les bloquer. Il s'agit de domaines suspects, de domaines similaires et de NOED (Newly Observed Emergent Domains) suspects dont le score combiné des niveaux de menace et de confiance est moyen.

Infoblox à risque faible : le flux Infoblox à risque faible comprend des domaines dont le danger n'est pas confirmé, mais qui restent suspects. Il est possible qu'ils soient utilisés à des fins malveillantes. Ces domaines sont associés à un score combiné de menace et de confiance moins élevé. Nous recommandons à la plupart des utilisateurs de les surveiller avec l'option Allow-WithLog et de les passer en mode blocage dans les environnements sensibles. Ce flux inclut les domaines suspects, les domaines similaires et les domaines émergents nouvellement observés (NOED, Newly Observed Emergent Domains), associés à un score combiné de menace et de confiance moins élevé.

Infoblox Informatif : le flux Infoblox Informatif comprend des domaines avec de faibles niveaux de menace et de confiance. Ceux-ci sont à titre informatif conformément à la politique et à la sensibilité de l'environnement. Cette alimentation porte des domaines émergents nouvellement observés (NOED). Il est recommandé de surveiller avec l'option Allow-WithLog pour la plupart des utilisateurs et de l'avoir en mode blocage pour les environnements sensibles (car les nouveaux domaines ne sont pas critiques pour la plupart et il est préférable de les activer lorsqu'ils sont établis pour une période plus longue).

Bogon : les adresses IP bogon sont souvent les adresses à l'origine des attaques DDoS. Le terme « bogon » est un nom informel donné à un paquet IP sur l'Internet public qui prétend provenir d'une zone de l'espace d'adressage IP réservé mais pas encore alloué, ou qui prétend être alloué par l'IANA (Internet Assigned Numbers Authority) ou par un registre Internet régional (RIR) délégué. Les zones d'un espace d'adressage non attribué sont appelées des « espaces bogon ». De nombreux FAI et pare-feu d'utilisateurs finaux filtrent et bloquent les adresses bogon parce qu'elles n'ont pas d'utilisation légitime et sont généralement le résultat d'une mauvaise configuration accidentelle ou malveillante.

IP DHS AIS et domaine DHS AIS (2 flux) : le programme AIS (Automated Indicator Sharing) du ministère de la sécurité intérieure (DHS) permet l'échange d'indicateurs de cybermenaces entre le gouvernement fédéral et le secteur privé. Le programme AIS s'inscrit dans le cadre des efforts déployés par le DHS pour créer un écosystème dans lequel, dès qu'une entreprise ou une agence fédérale observe une tentative de compromission, l'indicateur est partagé avec les partenaires du programme AIS, dont Infoblox. Les indicateurs IP contenus dans ce flux ne sont pas validés par le DHS car ils mettent l'accent sur la vitesse et le volume. Infoblox ne modifie ni ne vérifie les indicateurs. Cependant, les indicateurs du programme AIS sont classés et normalisés par Infoblox pour en faciliter la consommation.

Les données incluses dans ces flux IP AIS et nom d'hôte AIS comprennent des données AIS soumises à la législation américaine. Les conditions d'utilisation du partage automatisé des indicateurs du DHS sont disponibles à l'adresse www.us-cert.gov/ais et doivent être traitées conformément aux conditions d'utilisation. Avant de continuer à distribuer les données AIS, il peut vous être demandé de signer et de soumettre les conditions d'utilisation disponibles à l'adresse www.us-cert.gov/ais. Pour de plus amples informations, veuillez envoyer un e-mail à ncciccustomerser vice@hq.dhs.gov.

Noms d'hôtes publics du DoH et IP publiques du DoH (2 flux) : ce flux basé sur une politique contient les noms de domaine et les adresses IP des services DoH (DNS over HTTPS) de tiers. Les organisations qui souhaitent appliquer une politique de sécurité par le biais du DNS peuvent souhaiter empêcher le contournement des politiques de sécurité du DNS par l'utilisation de serveurs DoH tiers.

IP des nœuds de sortie Tor: les nœuds de sortie Tor sont les passerelles où le trafic Tor crypté atteint l'Internet. Cela signifie qu'un nœud de sortie peut surveiller le trafic Tor (après qu'il ait quitté le réseau). Le réseau Tor est conçu pour qu'il soit difficile de déterminer la source du trafic.

Noms d'hôtes de cryptomonnaies : ce flux contient des menaces qui permettent à des acteurs malveillants de mener des activités illégales et/ou frauduleuses, des « coinhives » qui permettent aux propriétaires de sites d'intégrer un logiciel de minage de cryptomonnaies dans leurs pages web pour remplacer la publicité normale, du « cryptojacking » qui permet aux propriétaires de sites de miner des cryptomonnaies sans le consentement du propriétaire, et des « cryptocurrency mining pools » (groupements de minage de cryptomonnaies).

IP EECN : ce flux basé sur les politiques contient des adresses IP de pays d'Europe de l'Est et de Chine non membres de l'UE qui sont souvent à l'origine de cyberattaques visant la propriété intellectuelle ou d'autres données sensibles ou classifiées, ainsi que le vol de cartes de crédit ou d'informations financières.

L'OFAC américain sanctionne les IP : ce flux basé sur des politiques contient les adresses IP de pays sanctionnés par les USA répertoriés par l'OFAC (Office of Foreign Assets Control), un organisme dépendant du Département du Trésor des États-Unis qui administre et applique les sanctions économiques imposées par le pays aux états étrangers. Pour en savoir plus, consultez la page « Sanctions Programs and Country Information » à l'adresse suivante : www.treasury.gov/resource-center/ sanctions/Programs/Pages/Programs.aspx.

L'OFAC américain sanctionne les IP (risque élevé) : ce flux inclut tous les indicateurs à haut risque des pays sanctionnés. Les indicateurs des pays suivants sont inclus dans le flux : Biélorussie, Cambodge, Centrafrique, Chine, Corée du Nord, Cuba, Iran, Iraq, Libye, Macao, Myanmar, République démocratique du Congo, Russie, Syrie, Venezuela et Yémen.

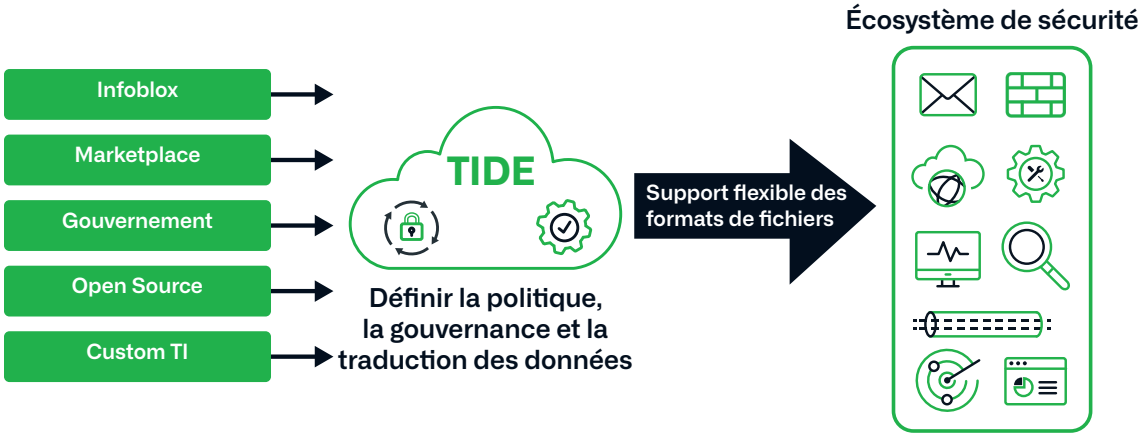
L'OFAC américain sanctionne les IP (risque moyen) : ce flux comprend tous les indicateurs de risque moyen des pays sanctionnés. Les indicateurs des pays suivants sont inclus dans le flux : Biélorussie, Cambodge, République centrafricaine, Chine, Cuba, RD Congo, Iran, Irak, Libye, Macao, Myanmar, Corée du Nord, Russie, Somalie, Soudan du Sud, Soudan, Syrie, Venezuela, Yémen et Zimbabwe.

OPPORTUNITÉS SUPPLÉMENTAIRES POUR OPTIMISER VOTRE UTILISATION D'INFOBLOX THREAT INTEL

Threat Defense Advanced offre deux fonctionnalités uniques qui accéléreront les enquêtes sur les menaces et la réponse aux incidents, faciliteront la détection des menaces et amélioreront de nombreuses autres activités SecOps.

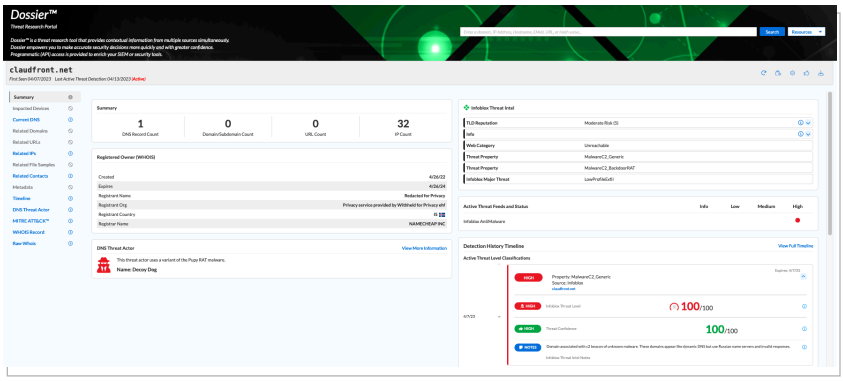
TIDE (THREAT INTELLIGENCE DATA EXCHANGE)

TIDE est une plateforme qui peut automatiser l'intégration, la gestion et la distribution d'Infoblox Threat Intel, en utilisant des flux supplémentaires provenant du gouvernement et de l'industrie, de sources ouvertes, de prestataires tiers de la Threat Intelligence (TI), de fournisseurs de sécurité générale ou même de vos propres renseignements internes sur les menaces.



DOSSIER

Dossier fournit aux analystes une vue centrée sur le DNS de la Threat Intelligence, qui inclut l'impact au sein de leur propre réseau et un historique complet des verdicts d'un indicateur. Les indicateurs associés et les informations sur les acteurs malveillants sont mis en évidence pour faciliter les évaluations des menaces persistantes. Les enrichissements comprennent les scores de réputation d'Infoblox, les informations d'enregistrement, la catégorisation du contenu, les liens de publication et d'autres informations actuelles sur les DNS. Une API permet une intégration programmée avec les produits SIEM.



FLUX DE MENACES TIERS DISPONIBLES POUR INFOBLOX THREAT DEFENSE ADVANCED

Threat Defense Advanced offre aux clients la possibilité de compléter les nombreuses options d'Infoblox threat intelligence par des données supplémentaires sur les menaces provenant de sources tierces. Alors que les fonctionnalités TIDE de Threat Defense peuvent automatiser l'intégration et le partage d'informations sur les menaces, certains partenaires proposent une fonctionnalité d'intégration rapide et facile du BYOL (Bring Your Own License). Après avoir acheté les licences appropriées auprès des partenaires suivants, les clients saisissent simplement leur licence sur la page BYOL dans Threat Defense Advance pour activer l'intégration prête à l'emploi, et ils sont opérationnels ; certains partenaires ont travaillé avec Infoblox pour simplifier le processus d'intégration du client. Les partenaires suivants proposent une assistance prête à l'emploi :

FireEye iSight Threat Intelligence : son adresse IP et son nom d'hôte fournissent aux entreprises des analyses stratégiques, opérationnelles et tactiques issues de son équipe mondiale d'experts. Un abonnement à ThreatScape fournit les informations nécessaires pour aligner un programme de sécurité sur les objectifs de gestion des risques de l'entreprise et pour se défendre de manière proactive contre les cybermenaces nouvelles et émergentes. Bien que les clients doivent acheter le flux iSight directement auprès de FireEye, Infoblox peut aider à « activer » le flux sur la plateforme TIDE.

Farsight Security Newly Observed Domains (NOD) Feed : Ce flux DomainTools offre une protection supplémentaire contre l'exfiltration de données par les malwares, le détournement de marque et les attaques par spam ayant pour origine ou pour destination des domaines nouvellement lancés.

VirusTotal est la plateforme de Threat Intelligence collaborative la plus riche et la plus exploitable au monde. En fournissant un contexte complet, il aide les équipes de sécurité à être confrontées fréquemment à des fichiers/URL/domaines/adresses IP inconnus pour tenter de comprendre une attaque. L'intégration de la Threat Intelligence de VirusTotal dans Threat Defense permet aux analystes de sécurité de tirer facilement parti de ce contexte unique en analysant les données relatives aux appareils, aux événements et aux menaces afin de se faire une idée rapide d'un incident.

Remarque : Ceci est un résumé marketing des capacités de Threat Intelligence des offres Threat Defense. Il est mis à jour périodiquement mais, s'agissant d'un produit SaaS, les capacités réelles du produit peuvent varier par rapport à ce qui est indiqué dans le présent document.

Infoblox unifie le réseau et la sécurité pour offrir des performances et une protection sans égales. Reconnu par les entreprises listées au classement Fortune 100 et les innovateurs émergents, nous offrons une visibilité et un contrôle en temps réel sur les personnes et les appareils se connectant au réseau d'une organisation afin d'accélérer son fonctionnement et d'arrêter les menaces plus tôt.

Siège social
2390 Mission College Boulevard, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version : 20251902v2