LÖSUNGSHINWEIS

Infoblox Threat Intel

Bedrohungen aufspüren, verfolgen und stoppen, wo sie beginnen – DNS

HERAUSFORDERUNGEN BEIM EINSATZ VON MALWARE-ZENTRIERTER THREAT INTELLIGENCE

Die meisten Sicherheitslösungen verfolgen einen Malware-zentrierten Ansatz für Threat Intelligence und kennzeichnen eine Domäne somit erst dann als bösartig, nachdem bereits eine Kompromittierung erfolgt ist. Dieser Post-Incident-Ansatz bedeutet, dass sie in gewisser Weise „Hau den Maulwurf“ spielen: Sie versuchen, bösartige Websites zu verfolgen, sobald sie auffallen, um sie zu Threat-Intelligence-Feeds hinzuzufügen und zu blockieren.

Trotz aller Bemühungen der Sicherheitsbranche wirken sich MFA-Angriffe, Lookalike-Domain-Angriffe und gezielte Phishing-Angriffe daher weiterhin negativ auf Unternehmen aus und verursachen Datenschutzverletzungen und Rufschädigungen der betroffenen Marken. Ein anderer Sicherheitsansatz ist notwendig, der Unternehmen proaktiv vor kriminellen Akteuren schützen kann, während diese noch ihre Infrastruktur aufbauen, um einen Angriff vorzubereiten.

CYBERKRIMINALITÄT AN DER WURZEL PACKEN – MIT INFOBLOX THREAT INTEL

Infoblox Threat Intel kombiniert marktführende DNS-Expertise mit modernster Datenwissenschaft, um Infrastruktur von Bedrohungsakteuren noch vor deren Einsatz zu identifizieren und die Kommunikation mit diesen Hochrisikodomänen zu unterbrechen. Infoblox Threat Intel ist die erste und einzige Lösung, die sich darauf konzentriert, DNS-Bedrohungsakteure und ihre Aktivitäten im Internet zu verfolgen und Kunden proaktiv vor aufkommenden Angriffen zu schützen, einschließlich Smishing, Lookalike-Domains, Hochrisiko-Domains, Ransomware, Malware-C&C und mehr. Infoblox Threat Defense verwendet Infoblox Threat Intel, um kritische Bedrohungen schon Monate vor anderen Sicherheitssystemen zu erkennen und zu stoppen. Infoblox Threat Intel ist auf DNS spezialisiert, damit Sie es nicht sein müssen und Ihr Netzwerk schützen können, ohne dessen Performance zu gefährden.

WICHTIGE STATISTIKEN:

Hier einige Zahlen aus dem ersten Quartal 2024:

- 60 % der Bedrohungen wurden vor der ersten DNS-Abfrage erkannt
- 82 % der Bedrohungen wurden nach nur einer DNS-Abfrage erkannt
- 89 % der Bedrohungen wurden innerhalb der ersten 48 Stunden erkannt

ZAHLEN UND FAKTEN

- MFA-Angriffe sind der mit Abstand sichtbarste und bedrohlichste Angriff des Jahres 2023, der die Anfälligkeit von Mitarbeitern (einschließlich Home-Office-/Remote-Mitarbeitern) mit der Verwendung von Lookalike-Domains kombiniert.
- 75 % der Unternehmen sahen sich bereits mit Smishing-Angriffen konfrontiert („State of the Phish“-Bericht für 2024 von Proofpoint).
- Bei vielen dieser Angriffe lassen die Bedrohungsakteure ihre Domänen sehr lange altern, manchmal sogar Monate nach deren Registrierung.

SOFORT EINSATZBEREITES INFOBLOX THREAT INTEL

Threat Defense, das Infoblox-Produkt für DNS-Erkennung und -Reaktion, ist in vier Paketen erhältlich:

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

Jedes Paket bietet über „RPZ-Feeds“ Zugriff auf eine Reihe von Infoblox Threat Intel-Daten. Das Advanced-Paket enthält außerdem das Tool TIDE (Threat Intelligence Data Exchange) für die Einspeisung und Verteilung benutzerdefinierter Bedrohungs-Feeds, das Portal Dossier zur Untersuchung von Bedrohungen, das diese Daten nutzt, und mehr.

Hier sind die Bedrohungs-Feeds, die für jedes Threat Defense-Paket verfügbar sind:

Feeds	Essential	Business OnPrem	Business Cloud	Erweitert
Infoblox Base	x	x	x	x
Infoblox Base IP		x	x	x
Infoblox Hohes Risiko				x
Infoblox Mittleres Risiko				x
Infoblox Niedriges Risiko				x
Infoblox Informativ		x	x	x
Öffentliche DoH-Hostnamen	x	x	x	x
DOH Public IPs	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
US OFAC Sanctions IPs				x
US OFAC Sanctions High IPs		x	x	x
US OFAC Sanctions Med IPs		x	x	x
Hostnamen und Domains von Kryptowährungen		x	x	x
TOR Exit Node IPs		x	x	x

KURZBESCHREIBUNGEN DER FEEDS

Infoblox Base: Der Infoblox Base-Feed ermöglicht den Schutz vor bekannten bösartigen oder kompromittierten Domänen. Dazu gehören bekannte Malware, Ransomware, APTs, Exploit-Kits, bösartige Nameserver, Sinklöcher usw. Wir empfehlen, sie für alle Benutzer zu blockieren.

Infoblox Base IP: Der Infoblox Base IP-Feed ermöglicht den Schutz vor bekannten bösartigen oder kompromittierten IP-Adressen. Diese IP-Adressen sind eine bekannte Infrastruktur zum Hosten von Bedrohungen, die über C&C-Malware-Downloads und aktive Phishing-Seiten auf ein System einwirken oder es kontrollieren können. Wir empfehlen, sie für alle Benutzer zu blockieren.

Infoblox High Risk: Der Infoblox High Risk-Feed enthält Domänen, die noch nicht bestätigt, jedoch höchst verdächtig sind. Es ist sehr wahrscheinlich, dass diese irgendwann für böswillige Zwecke verwendet werden. Auch wenn die Bösartigkeit dieser Domänen bisher nicht bestätigt wurde, stellen sie jedoch mit hoher Sicherheit eine große Bedrohung dar. Aus diesem Grund empfehlen wir, sie für die meisten Benutzer zu blockieren. Der Feed umfasst verdächtige Domänen, verdächtige Lookalikes und verdächtige NOED (Newly Observed Emergent Domains) mit einem hohen kombinierten Bedrohungs- und Konfidenzniveau.

Infoblox Medium Risk: Der Infoblox Medium Risk-Feed enthält Domänen, die noch nicht bestätigt sind, aber dennoch ein mittleres Risiko darstellen. Es handelt sich dabei um verdächtige Domänen, deren kombinierte Bewertung aus Bedrohungs- und Konfidenzniveau niedriger ist als beim High Risk-Feed, aber höher als beim Low Risk-Feed. Sie könnten mit guter Wahrscheinlichkeit für böswillige Zwecke verwendet werden, weshalb wir empfehlen, sie für die meisten Benutzer zu blockieren. Sie umfassen verdächtige Domänen, verdächtige Lookalikes und verdächtige NOED (Newly Observed Emergent Domains) mit einer mittleren kombinierten Bewertung aus Bedrohungs- und Konfidenzniveau.

Infoblox Low Risk: Der Infoblox Low Risk-Feed enthält Domänen, die noch nicht bestätigt wurden, aber dennoch verdächtig sind. Es ist möglich, dass sie für bösartige Zwecke verwendet werden könnten. Diese Domänen weisen eine niedrigere kombinierte Bewertung aus Bedrohungs- und Konfidenzniveau auf. Wir empfehlen, dass die meisten Benutzer sie mit der Option „Allow-WithLog“ überwachen und in sensiblen Umgebungen den Blockiermodus für sie aktivieren. Der Feed umfasst verdächtige Domänen, verdächtige Lookalikes und verdächtige NOED (Newly Observed Emergent Domains) mit einer niedrigeren kombinierten Bewertung aus Bedrohungs- und Konfidenzniveau.

Infoblox Informational: Der Infoblox Informational-Feed enthält Domänen mit niedrigem Bedrohungs- und Konfidenzniveau. Sie dienen zu Informationszwecken gemäß den Richtlinien und der Sensibilität der Umgebung. Dieser Feed enthält Newly Observed Emergent Domains (NOED). Es wird empfohlen, ihn für die meisten Benutzer mit der Option „Allow-WithLog“ zu überwachen und in sensiblen Umgebungen den Blockiermodus für ihn zu aktivieren (da neue Domänen meist nicht unternehmenskritisch sind und es am besten ist, sie zu aktivieren, sobald sie bereits länger etabliert sind).

Bogon: Bogon-IPs sind oft die Quelladressen von DDoS-Angriffen. „Bogon“ ist eine informelle Bezeichnung für ein IP-Paket im öffentlichen Internet, das behauptet, aus einem Bereich des IP-Adressraums zu stammen, der zwar reserviert, aber noch nicht von der Internet Assigned Numbers Authority (IANA) oder einem delegierten Regional Internet Registry (RIR) zugewiesen oder delegiert wurde. Die Bereiche nicht zugewiesenen Adressraums werden als „Bogon-Raum“ bezeichnet. Viele ISPs und Endbenutzer-Firewalls filtern und blockieren Bogons, da sie keine legitime Verwendung haben und in der Regel das Ergebnis einer versehentlichen oder böswilligen Fehlkonfiguration sind.

DHS AIS IP und DHS AIS Domain (2 Feeds): Das Programm Automated Indicator Sharing (AIS) des Department of Homeland Security (DHS) ermöglicht den Austausch von Cyberbedrohungsindikatoren zwischen der Bundesregierung und dem privaten Sektor. AIS ist Teil der Bemühungen des DHS, ein Ökosystem zu schaffen, in dem, sobald ein Unternehmen oder eine Bundesbehörde einen Kompromittierungsversuch beobachtet, der Indikator mit den Partnern des AIS-Programms, darunter auch Infoblox, geteilt wird. Die in diesem Feed enthaltenen IP-Indikatoren sind nicht vom DHS validiert, da dieses Geschwindigkeit und Volumen priorisiert. Infoblox verändert oder verifiziert die Indikatoren nicht. Die Indikatoren aus dem AIS-Programm werden jedoch von Infoblox klassifiziert und normalisiert, um die Nutzung zu erleichtern.

Die in diesen AIS IP- und AIS Hostname-Feeds enthaltenen Daten enthalten AIS-Daten, die den Nutzungsbedingungen des DHS der USA für Automated Indicator Sharing unterliegen, welche unter www.us-cert.gov/ais verfügbar sind, und müssen in Übereinstimmung mit den Nutzungsbedingungen gehandhabt werden. Bevor Sie die AIS-Daten weiterverbreiten, müssen Sie möglicherweise die Nutzungsbedingungen unter www.us-cert.gov/ais unterschreiben und einreichen. Senden Sie für weitere Informationen eine E-Mail an ncciccustomerservice@hq.dhs.gov.

DoH Public Hostnames und DoH Public IPs (2 Feeds): Dieser richtlinienbasierte Feed enthält Domänennamen und IPs von DoH-Diensten (DNS over HTTPS) von Drittanbietern. Unternehmen, die die Durchsetzung von Sicherheitsrichtlinien über DNS bereitstellen möchten, möchten möglicherweise die Umgehung von DNS-Sicherheitsrichtlinien verhindern, indem sie DoH-Server von Drittanbietern verwenden.

Tor Exit Node IPs: Tor Exit Nodes sind die Gateways, durch die verschlüsselter Tor-Traffic auf das Internet trifft. Das bedeutet, dass ein Exit-Node den Tor-Traffic überwachen kann (nachdem er das Onion-Netzwerk verlassen hat). Das Tor-Netzwerk ist so konzipiert, dass es schwierig ist, seine Datenverkehrsquelle zu bestimmen.

Cryptocurrency Hostnames: Dieser Feed enthält Bedrohungen, die es böswilligen Akteuren ermöglichen, illegale und/oder betrügerische Aktivitäten durchzuführen, Coinhives, die es Website-Eigentümern ermöglichen, Kryptowährungs-Mining-Software in ihre Webseiten einzubetten, um normale Werbung zu ersetzen, Cryptojacking, das es Website-Eigentümern ermöglicht, ohne Zustimmung des Eigentümers nach Kryptowährung zu schürfen, und Kryptowährungs-Mining-Pools.

EECN IPs: Dieser richtlinienbasierte Feed enthält IPs von Nicht-EU-Ländern in Osteuropa und China, die häufig Quellen von Cyberangriffen sind, die auf geistiges Eigentum oder andere sensible oder geheime Daten sowie den Diebstahl von Kreditkarten- oder Finanzinformationen abzielen.

US OFAC Sanctions IPs: Dieser richtlinienbasierte Feed enthält IPs von Ländern, gegen die die USA Sanktionen verhängt haben. Diese werden vom U.S. Treasury Office of Foreign Assets Control (OFAC) gelistet, das die von den Vereinigten Staaten gegen andere Länder verhängten Wirtschaftssanktionen verwaltet und durchsetzt. Weitere Informationen finden Sie auf der Seite „Sanctions Programs and Country Information“, die Sie hier finden: www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.

US OFAC Sanctions IPs (High Risk): Dieser Feed enthält alle Hochrisikoindikatoren aus sanktionierten Ländern. Indikatoren aus den folgenden Ländern sind im Feed enthalten: Belarus, Kambodscha, Zentralafrikanische Republik, China, Kuba, DR Kongo, Iran, Irak, Libyen, Macau, Myanmar, Nordkorea, Russland, Syrien, Venezuela und Jemen.

US OFAC Sanctions IPs (Medium Risk): Dieser Feed enthält alle Indikatoren mit mittlerem Risiko aus sanktionierten Ländern. Indikatoren aus den folgenden Ländern sind im Feed enthalten: Belarus, Kambodscha, Zentralafrikanische Republik, China, Kuba, DR Kongo, Iran, Irak, Libyen, Macao, Myanmar, Nordkorea, Russland, Somalia, Südsudan, Sudan, Syrien, Venezuela, Jemen und Simbabwe.

ZUSÄTZLICHE MÖGLICHKEITEN ZUR OPTIMIERUNG IHRER NUTZUNG VON INFOBLOX THREAT INTEL

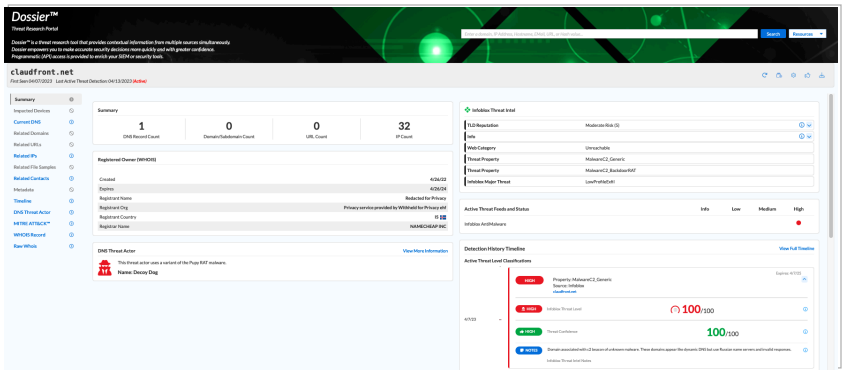
Threat Defense Advanced bietet zwei einzigartige Funktionen, die Bedrohungsuntersuchungen und die Reaktion auf Vorfälle beschleunigen, die Bedrohungssuche erleichtern und zahlreiche weitere SecOps-Aktivitäten verbessern.

TIDE (THREAT INTELLIGENCE DATA EXCHANGE)

TIDE ist eine Plattform, die die Einspeisung, Verwaltung und Verteilung von Infoblox Threat Intel automatisieren kann und dabei die Verwendung zusätzlicher Feeds aus Quellen wie der Regierung/Branche, Open Source, Drittanbietern von Threat Intelligence (TI), allgemeinen Sicherheitsanbietern oder sogar Ihrer eigenen internen Threat Intelligence unterstützt.

DOSSIER

Dossier bietet Analysten eine DNS-zentrierte Ansicht von Threat Intelligence, die die Auswirkungen innerhalb ihres eigenen Netzwerks und einen vollständigen Beurteilungsverlauf eines Indikators umfasst. Zur einfachen Beurteilung anhaltender Bedrohungen werden relevante Indikatoren und Informationen zu Bedrohungsakteuren hervorgehoben. Zu den Anreicherungen gehören Infoblox-Reputationsbewertungen, Registrierungsinformationen, Inhaltskategorisierung, Veröffentlichungslinks und andere aktuelle DNS-Informationen. Eine API bietet programmgesteuerten Zugriff zur Integration mit SIEM-Produkten.



FÜR INFOBLOX THREAT DEFENSE ADVANCED VERFÜGBARE BEDROHUNGS-FEEDS VON DRITTANBIETERN

Threat Defense Advanced bietet Kunden die Möglichkeit, die vielen Threat-Intelligence-Optionen von Infoblox mit zusätzlichen Bedrohungsdaten aus Drittanbieterquellen zu ergänzen. Während die TIDE-Funktionen von Threat Defense die Einspeisung und Weitergabe von Bedrohungsinformationen automatisieren können, bieten einige Partner Unterstützung für eine schnelle und einfache BYOL-Integrationsfunktion (Bring Your Own License). Nach dem Erwerb der entsprechenden Lizenzen von den folgenden Partnern geben Kunden ihre Lizenz einfach auf der BYOL-Seite in Threat Defense Advance ein, um die sofort einsatzbereite Integration zu aktivieren. Danach kann es direkt losgehen. Einige Partner haben auch mit Infoblox zusammengearbeitet, um den Onboarding-Prozess für Kunden zu vereinfachen. Die folgenden Partner unterstützen sofortige Einsatzbereitschaft:

FireEye iSIGHT Threat Intelligence: Die IP- und Hostnamen-Cyber-Threat-Intelligence dieses Partners stattet Unternehmen mit strategischen, operativen und taktischen Analysen aus, die von seinem globalen Expertenteam erstellt werden. Ein ThreatScape-Abonnement liefert die Informationen, die notwendig sind, um ein Sicherheitsprogramm mit den Zielen des Unternehmensrisikomanagements in Einklang zu bringen und sich proaktiv gegen neue und aufkommende Cyber-Bedrohungen zu schützen. Obwohl Kunden den iSight-Feed direkt von FireEye kaufen müssen, kann Infoblox dabei helfen, den Feed in der TIDE-Plattform zu „aktivieren“.

Farsight Security Newly Observed Domains (NOD) Feed: Dieser Feed von DomainTools bietet eine zusätzliche Verteidigungsebene zum Schutz vor Malware-Exfiltration, Markenmissbrauch und Spam-basierten Angriffen, die von neu gestarteten Domänen ausgehen oder dort enden.

VirusTotal ist die global umfassendste und effektivste Crowdsourcing-Plattform für Threat Intelligence. Durch die Bereitstellung eines umfassenden Kontexts unterstützt sie Sicherheitsteams, die beim Versuch, einen Angriff zu verstehen, häufig mit unbekannten Dateien/URLs/Domänen/IP-Adressen konfrontiert werden. Durch die Integration von VirusTotal-Threat-Intelligence in Threat Defense können Sicherheitsanalysten diesen einzigartigen Kontext nutzen, um sich anhand von Geräte-, Ereignis- und Threat-Intelligence-Daten schnell ein Bild von einem Vorfall zu machen.

Hinweis: Dies ist eine Marketingzusammenfassung der Threat-Intelligence-Funktionen der Threat Defense-Angebote. Sie wird regelmäßig aktualisiert. Da es sich jedoch um ein SaaS-Produkt handelt, können die tatsächlichen Produktfunktionen von den Angaben in diesem Dokument abweichen.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1.408.986.4000
www.infoblox.com

Version: 20251902v2