infoblox.

Threat Intel

SOLUTION NOTE

Infoblox Threat Intel

Hunts, Tracks, Stops Threats Where They Begin - DNS

CHALLENGES OF USING MALWARE-CENTRIC THREAT INTELLIGENCE

Most security solutions take a malware-centric approach to threat intelligence, relying on a compromise to happen before they flag a domain as malicious. This post-incident approach means they are playing whack-a-mole, trying to track down malicious websites as they pop up and adding them to threat intel feeds for blocking.

Therefore, despite best efforts of the security industry, MFA attacks, lookalike domain attacks and targeted phishing attacks continue to impact organizations resulting in data breaches and damage to brand reputation. There is a need to take a different approach to security, one that can proactively protect enterprises from criminal actors as they build their infrastructure to launch attacks.

DISRUPTING CYBERCRIME AT ITS CORE WITH INFOBLOX THREAT INTEL

Infoblox Threat Intel combines market-leading DNS expertise with cutting-edge data science to identify threat actor infrastructure before the actors use it and disrupt communications to those high-risk domains. Infoblox Threat Intel is the first and only solution that focuses on tracking DNS threat actors and their activities on the Internet, proactively protecting customers from emerging attacks, including smishing, lookalike domains, high-risk domains, ransomware, malware C&C and more. Infoblox Threat Defense uses Infoblox Threat Intel to see and stop critical threats months before other security systems. Infoblox Threat Intel specializes in DNS, so you don't have to, allowing you to protect your network without risking performance.

KEY STATS:

In the first quarter of 2024,

- 60% of threats were detected before the first DNS query
- 82% of threats were detected after just one DNS query
- 89% of threats were detected within the first 48 hours

FACTS & FIGURES

- MFA attacks are the single most visible and threatening attack of 2023 that brings together the vulnerability of employees (including WFH/remote) with the use of lookalike domains
- 75% of organizations faced smishing attacks (Proofpoint 2024 State of Phish report)
- In many of the attacks, threat actors age their domains for a very long time, sometimes even months after the domains are registered

OUT-OF-THE-BOX INFOBLOX THREAT INTEL AVAILABILITY

Threat Defense, Infoblox's DNS Detection and Response product, is available in four packages:

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

Each package offers access to a range of Infoblox Threat Intel data via 'RPZ feeds'. The Advanced package also includes a tool for custom threat feed ingestion and distribution called TIDE (Threat Intelligence Data Exchange), a threat research portal called Dossier that leverages this data, and more.

Here are the threat feeds available for each Threat Defense package:

Feeds	Essential	Business OnPrem	Business Cloud	Advanced
Infoblox Base	X	X	X	X
Infoblox Base IP		X	X	X
Infoblox High Risk				X
Infoblox Medium Risk				X
Infoblox Low Risk				X
Infoblox Informational		X	X	X
DoH Public Hostnames	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
Cryptocurrency hostnames and domains		X	X	X
TOR Exit Node IPs		X	X	X

SUMMARY DESCRIPTION OF FEEDS

Infoblox Base: Infoblox Base feed enables protection against known malicious or compromised domains. This includes known Malware, Ransomware, APTs, exploit kits, malicious Name Servers, sinkholes etc. We recommend blocking them for all users.

Infoblox Base IP: Infoblox Base IP feed enables protection against known malicious or compromised IP addresses. These IPs are known infrastructure to host threats that can act on or control a system by way of C&C malware downloads and active phishing sites. We recommend blocking them for all users.

Infoblox High Risk: Infoblox High Risk feed includes domains that are not confirmed yet but are highly suspicious. It's very likely to be used in a malicious act at some point. These domains, though unconfirmed, carry high threat and high confidence, so we recommend blocking them for most users. It includes Suspicious domains, Suspicious Lookalikes and Suspicious NOED (Newly Observed Emergent Domains) with high combined score of threat and confidence levels.

Infoblox Medium Risk: Infoblox Medium Risk feed includes domains that are not confirmed yet but still pose medium risk. They are suspicious domains with lower combined score of Threat and Confidence level than High Risk feed but higher than Low Risk feed. It still could likely be used in a malicious act, so we recommend blocking them for most users. It includes Suspicious domains, Suspicious Lookalikes and Suspicious NOED (Newly Observed Emergent Domains) with medium combined score of threat and confidence levels.

Infoblox Low Risk: Infoblox Low Risk feed includes domains that are not confirmed yet but are still suspicious. It's possible it can be used in a malicious act. These domains carry a lower combined score of threat and confidence levels. It's recommended that most users monitor with the Allow-WithLog option and have it in block mode for sensitive environments. It includes Suspicious domains, Suspicious Lookalikes and Suspicious NOED (Newly Observed Emergent Domains) with lower combined score of threat and low levels.

Infoblox Informational: Infoblox Informational feed includes domains with low threat and confidence levels. These are for informational use per policy and sensitivity of the environment. This feed carries Newly Observed Emergent Domains (NOED). It's recommended to monitor with the Allow-WithLog option for most users and have it in block mode for sensitive environments (as new domains are not mission critical for the most part, and it is best to enable them when they are established for a longer time).

Bogon: Bogons IPs are often the source addresses of DDoS attacks. "Bogon" is an informal name for an IP packet on the public Internet that claims to be from an area of the IP address space reserved but not yet allocated or delegated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The areas of unallocated address space are called "bogon space." Many ISPs and end-user firewalls filter and block bogons because they have no legitimate use and are usually the result of accidental or malicious misconfiguration.

DHS AIS IP and DHS AIS Domain (2 feeds): The Department of Homeland Security (DHS) Automated Indicator Sharing (AIS) program enables the exchange of cyber threat indicators between the federal government and the private sector. AIS is a part of the DHS's effort to create an ecosystem in which, as soon as a company or federal agency observes an attempted compromise, the indicator is shared with AIS program partners, including Infoblox. The IP indicators contained in this feed are not validated by DHS because they emphasize velocity and volume. Infoblox does not modify or verify the indicators. However, indicators from the AIS program are classified and normalized by Infoblox to ease consumption.

Data included in these AIS IP and AIS Hostname feeds include AIS data subject to the U.S. DHS Automated Indicator Sharing Terms of Use available at w w w.us-cert.gov/ais and must be handled in accordance with the Terms of Use. Prior to further distributing the AIS data, you may be required to sign and submit the Terms of Use available at www.us-cert.gov/ais. Please email ncciccustomerser vice@hq.dhs.gov for additional information.

DoH Public Hostnames and DoH Public IPs (2 feeds) This policy-based feed contains domain names and IPs of third-party DoH (DNS over HTTPS) services. Organizations wishing to provide security policy enforcement through DNS may wish to prevent the bypass of DNS security policies by using third-party DoH servers.

Tor Exit Node IPs: Tor Exit Nodes are the gateways where encrypted Tor traffic hits the Internet. This means an exit node can monitor Tor traffic (after it leaves the onion network). The Tor network is designed to make it difficult to determine its traffic source.

Cryptocurrency Hostnames: This feed features threats that allow malicious actors to perform illegal and/or fraudulent activities, coinhives that allow site owners to embed cryptocurrency mining software into their webpages to replace normal advertising, cryptojacking that lets site owners mine for cryptocurrency without the owner's consent and cryptocurrency mining pools.

EECN IPs: This policy-based feed contains IPs of non-EU countries in Eastern Europe and China that are often sources of cyberattacks seeking intellectual property or other sensitive or classified data, as well as theft of credit card or financial information.

US OFAC Sanctions IPs: This policy-based feed contains IPs of U.S.-sanctioned countries listed by the U.S.Treasury Office of Foreign Assets Control (OFAC), which administers and enforces economic sanctions imposed bythe United States against foreign countries. More information is available on the "Sanctions Programs and CountryInformation" page found here: www.treasury.gov/resource-center/ sanctions/Programs/Pages/Programs.aspx.

US OFAC Sanctions IPs (High Risk): This feed includes all high-risk indicators from sanctioned countries. Indicators from the following countries are included in the feed: Belarus, Cambodia, Central African Republic, China, Cuba, DR Congo, Iran, Iraq, Libya, Macao, Myanmar, North Korea, Russia, Syria, Venezuela, and Yemen.

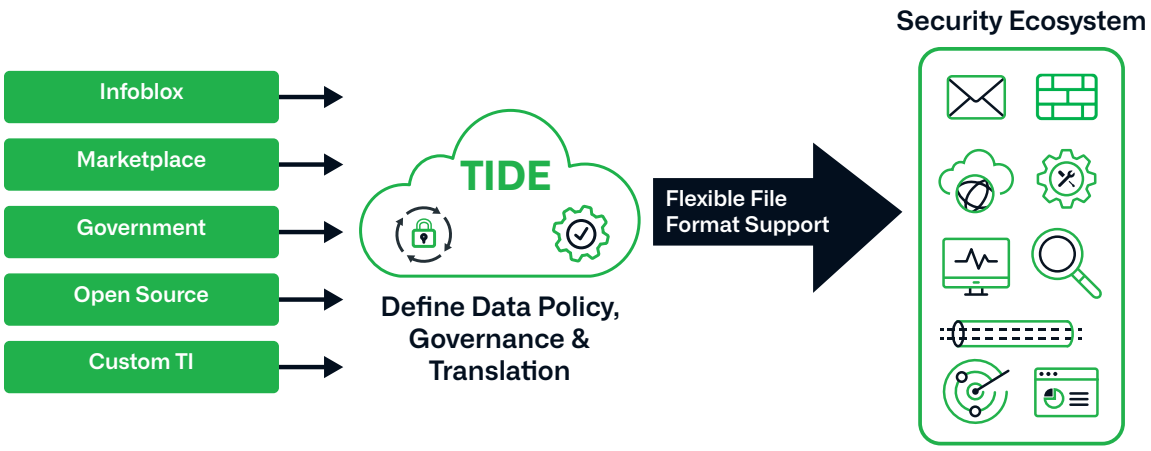
US OFAC Sanctions IPs (Medium Risk): This feed includes all medium risk indicators from sanctioned countries. Indicators from the following countries are included in the feed: Belarus, Cambodia, Central African Republic, China, Cuba, DR Congo, Iran, Iraq, Libya, Macao, Myanmar, North Korea, Russia, Somalia, South Sudan, Sudan, Syria, Venezuela, Yemen, and Zimbabwe.

ADDITIONAL OPPORTUNITIES TO OPTIMIZE YOUR USE OF INFOBLOX THREAT INTEL

Threat Defense Advanced offers two unique features that will speed threat investigations, accelerate incident response, facilitate threat hunting, and enhance numerous other SecOps activities.

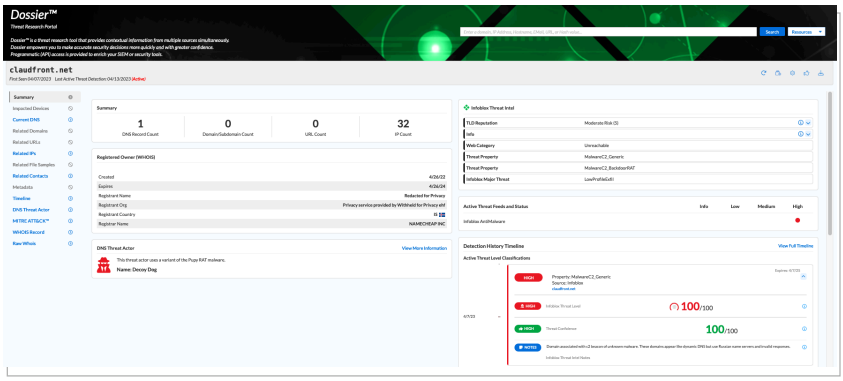
TIDE (THREAT INTELLIGENCE DATA EXCHANGE)

TIDE is a platform that can automate the ingestion, management, and distribution of Infoblox Threat Intel, supporting the use of additional feeds from government/industry, open source, third-party Threat Intelligence (TI) vendors, general security vendors, or even your own internal threat intelligence.



DOSSIER

Dossier provides analysts with a DNS-centric view of threat intelligence which includes the impact within their own network and a full verdict history of an indicator. Related indicators and threat actor information is highlighted for easy assessments of persistent threats. Enrichments include Infoblox reputation scores, registration information, content categorization, publication links, and other current DNS information. An API provides programmatic access to integrate with SIEM products.



THIRD-PARTY THREAT FEEDS AVAILABLE FOR INFOBLOX THREAT DEFENSE ADVANCED

Threat Defense Advanced offers customers the option to supplement the many Infoblox threat intelligence options with additional threat data from third-party sources. While the TIDE features of Threat Defense can automate threat intel ingestion and sharing, some partners provide support for a quick and easy BYOL (Bring Your Own License) integration feature. After purchasing the appropriate licenses from the following partners, customers simply enter their license on the BYOL page in Threat Defense Advance to activate out-of-the-box integration, and they are ready to go; some partners have worked with Infoblox to simplify a customer's onboarding process. The following partners offer out-of-the-box support:

FireEye iSIGHT Threat Intelligence: Its IP and hostname cyber threat intelligence equips enterprises with strategic, operational and tactical analysis derived from its global team of experts. A ThreatScape subscription provides the intelligence necessary to align a security program with business risk management goals and to proactively defend against new and emerging cyber threats. Although customers have to purchase the iSight feed directly from FireEye, Infoblox can help to "turn on" the feed in the TIDE platform.

Farsight Security Newly Observed Domains (NOD) Feed: This feed from DomainTools supplies an incremental layer of defense to combat malware exfiltration, brand abuse and spam-based attacks that originate or terminate at newly launched domains.

VirusTotal is the richest and most actionable crowdsourced threat intelligence platform on the planet. Providing comprehensive context, it helps security teams as they frequently confront unknown files/URLs/domains/IP addresses as they try to make sense of an attack. Integrating VirusTotal threat intelligence into Threat Defense empowers security analysts to easily leverage this unique context as they pivot around device, event, and threat intelligence data to quickly build a picture of an incident.

Notice: This is a marketing summary of the threat intelligence capabilities of the Threat Defense offerings. It is updated periodically but, as a SaaS product, actual product capabilities may vary from what is noted in this document.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20251902v2