SOLUTION NOTE

THREAT INTELLIGENCE (TI)

Uplift the entire security stack by optimizing your custom blend of threat intelligence

OBSTACLES TO OPTIMIZING THREAT INTELLIGENCE USE

Defending a modern enterprise requires a broad collection of security tools, orchestrated to provide maximum coverage of the attack surface. But, regardless of the tool, its effectiveness can be limited by the underlying threat intelligence, particularly for more mature security programs where Indicators of Compromise (IoCs) make up only one aspect of the overall threat intelligence required.

Unfortunately, numerous studies in recent years have underscored the inadequacies of depending on a limited number of threat intelligence sources (aka feeds). This puts the burden on SecOps to identify, collect, normalize, and distribute different kinds of threat intelligence from dozens of available sources to the appropriate tools. From protection and detection to investigation and response, having fast access to the right blend of threat intelligence is key to success.

COMPREHENSIVE, MULTI-SOURCED THREAT INTELLIGENCE FROM INFOBLOX

While most security products come with a single feed from the vendor, Infoblox offers customers a broad range of options to customize the threat intelligence they receive. This includes a variety of feed sources that are managed and curated by the Infoblox threat research team for effectiveness and quality, as well as several specialized feeds from trusted third-parties including government, open source, and other threat feed sources.

The precise blend of threat intelligence available with BloxOne® Threat Defense depends on the package purchased. The Advanced package even includes a tool that can support any threat intelligence feed, and automate TI distribution across the entire security stack. This enables you to empower all your defenses with a custom 'super-feed' of threat intelligence, maximizing the value of all your security investments.

OUT-OF-THE-BOX THREAT INTELLIGENCE AVAILABILITY

BloxOne Threat Defense is available as four packages:

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

FACTS & FIGURES

According to the 2021 SANS Cyber Threat Intelligence (CTI) Survey:

- 77% of respondents use **Open Source or public threat intelligence** feeds
- 71% use data from **CTI-specific vendors**, while 63% use data from **general security vendors**
- Just over 2/3rds of respondents use TI from **community or industry groups (i.e. ISACs, CERTs)**
- **63.4% are trying to use Internal TI** gathered from security tools (i.e. IDS, firewall, endpoint, etc.)

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

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

Bloxone Threat Defense Essentials				
• Base Hostnames • Anti malware	• Ransomware • Bogon	• DHS AIS IP • DHS AIS Hostnames	• DoH Public Hostnames	• DoH Public IPs
Bloxone Threat Defense Business On-Premises and Business Cloud				
• Base Hostnames • AntiMalware • Ransomware • Bogon • DHS AIS IP	• DHS AIS Hostnames • DoH Public Hostnames • DoH Public IPs	• AntiMalware IPs • Malware DGA Hostnames • TOR Exit Node IPs	• NOED • Cryptocurrency Hostnames • EECN IPs	• US OFAC Sanctions IPs • US OFAC Sanctions IPs (High Risk) • US OFAC Sanctions IPs (Medium Risk)
Bloxone Threat Defense Advanced				
• Base Hostnames • AntiMalware • Ransomware • Bogon • DHS AIS IP • DHS AIS Hostnames	• DoH Public Hostnames • DoH Public IPs • AntiMalware IPs • Malware DGA hostnames • TOR Exit Node IPs	• NOED • Cryptocurrency Hostnames • EECN IPs • US OFAC Sanctions IPs	• US OFAC Sanctions IPs (High Risk) • US OFAC Sanctions IPs (Medium Risk) • Extended Base & AntiMalware Hostnames	• Extended Ransomware IPs • Suspicious Domains • Suspicious Lookalikes • Suspicious NOED

BLOXONE THREAT DEFENSE ESSENTIALS

The following threat feeds are included with the purchase of the 'Essentials' package of BloxOne Threat Defense.

- **Base hostnames:** The base feed enabled protection against known hostnames that are dangerous as destinations and are sources of threats such as APTs, bots, compromised host/domains, exploit kits, malicious name servers and sinkholes.
- **AntiMalware:** This feed enables protection against hostnames that contain known malicious threats that can action or take control of your system, such as malware command and control (C&C), malware download and active phishing sites.
- **Ransomware:** The ransomware set enables protection against hostnames that contain malware that restricts access to the computer system that it infects and demands a ransom for removal of the restriction. Some forms of ransomware encrypt files on the system's hard drive. Others some may simply lock the system and display messages intended to coerce the user into paying.

- **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 usually are the result of accidental or malicious misconfiguration.
- **DHS AIS IP and DHS AIS Hostname (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. IP indicators contained in this feed are not validated by DHS because the emphasis is on 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, AIS Hostname feeds include AIS data subject to the U.S. DHS Automated Indicator Sharing Terms of Use available at www.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 nccicccustomerservice@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.

BLOXONE THREAT DEFENSE BUSINESS ON-PREMISES AND BLOXONE THREAT DEFENSE BUSINESS CLOUD

BloxOne Threat Defense Business On-Premises and BloxOne Threat Defense Business Cloud offer the same data sets available with BloxOne Threat Defense Essentials plus additional data sets that can be applied to the security infrastructure, including Infoblox DNS Firewall RPZ policy. The additional data sets included in BloxOne Threat Defense Business On-Premises and BloxOne Threat Defense Business Cloud are:

- **AntiMalware IPs:** The AntiMalware IP set enables protection against known malicious or compromised IP addresses. These are known to host threats that can act on or control a system by way of C&C malware downloads and active phishing sites.
- **Malware DGA Hostnames:** Domain generation algorithms (DGA) appear in various families of malware used to periodically generate many domain names that can act as rendezvous points with their C&C servers. Examples include Ramnit, Conficker and Banjori.
- **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.
- **NOED (Newly Observed Emergent Domains):** These are newly observed domains and those that show a significant uptick in traffic globally, which indicates that this domain is active and relatively new.

BLOXONE THREAT DEFENSE ADVANCED

BloxOne Threat Defense (B1TD) Advanced includes all the data feeds described above plus additional data feeds and the TIDE platform. The additional data sets in BloxOne Threat Defense Advanced include:

Extended TTL feeds: These feeds expand the base, antimalware, ransomware and other feeds that contain recently expired threats with an extended time-to-live (TTL) applied. The extended TTL feeds increase the reach of protection for a DNS Firewall. However, they may also increase the risk of false positives because indicators may no longer be active.

The Extended TTL feeds are:

- **Extended Base & AntiMalware:** Base and AntiMalware hostname feeds combined into a single feed with the extended TTL feeds applied.
- **Extended Ransomeware IPs**

LEVERAGING "SUSPICIOUS" THREAT INTELLIGENCE FOR A PROACTIVE DEFENSE

While the production of 'known' threat lists, and even published, detailed analysis of emerging threats through public and private sector reporting is critical to understanding the threat landscape, such threat intelligence is retrospective in nature and the release of indicators often come long after the first attacks take place. Consumers and corporations are best protected by a proactive, low regret model that enables threats to be blocked before they are validated. Infoblox's suspicious threat intelligence feeds help identify many of the domains used in in threat campaigns such as those used in phishing campaigns.

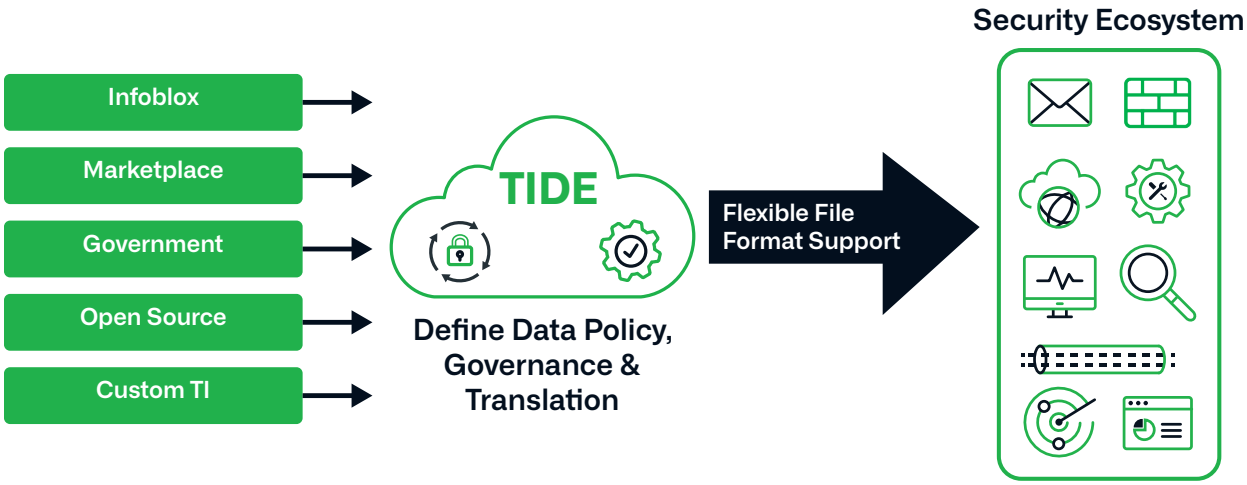
- **Suspicious Domains:** These are domains that share common indicators with other known malicious sites, although not to the level that would also make them malicious. This feed contains high confidence IoCs, and we recommend blocking them for most users.
- **Suspicious Lookalikes:** These are suspicious domains with the additional factor of appearing to impersonate a trusted domain, which is a common technique used in 'phishing' threat activity.
- **Suspicious NOED (Newly Observed Emergent Domains):** These are suspicious domains that have demonstrated a significant uptick in traffic globally among our customers, which may indicate that this domain is now part of an active campaign.

ADDITIONAL OPPORTUNITIES TO OPTIMIZE YOUR USE OF THREAT INTELLIGENCE

BloxOne Threat Defense Advanced offers two unique features to create the ideal blend of threat intelligence for your needs, and apply it in ways that will speed threat investigations, accelerate incident response, facilitate threat hunting, and enhance numerous other SecOps activities.

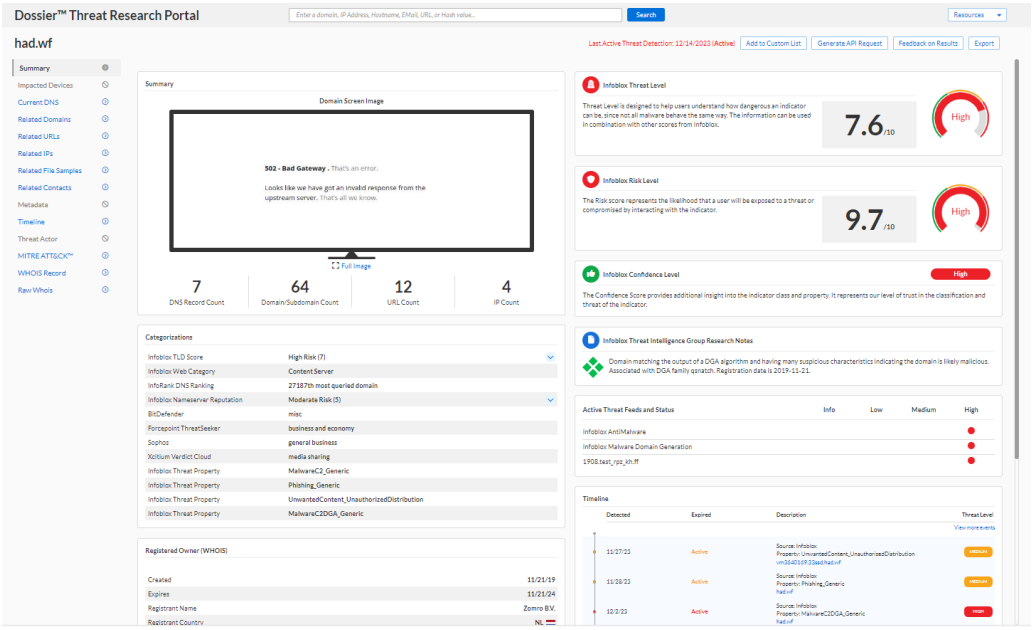
TIDE (THREAT INTELLIGENCE DATA EXCHANGE)

TIDE is a platform that can automate the ingestion, management, and distribution of threat intelligence, 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 puts analysts in the middle of available threat intelligence, with on-demand access to threat severity, WHOIS data, MITRE ATT&CK guidance, related IPs/URLs/Domains, file samples, timelines, threat actor background, and more. It empowers analysts to easily pivot to where they need to go and reach confident conclusions faster.



THIRD-PARTY THREAT FEEDS AVAILABLE FOR BLOXONE THREAT DEFENSE ADVANCED

BloxOne 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 BloxOne 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 in the BYOL page in BloxOne 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 by 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 BloxOne 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 BoxOne Threat Defense offerings. It is updated periodically but, as a SaaS product, actual product capabilities may vary from what is noted in this document.

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

+1.408.986.4000
www.infoblox.com

Version:20231122v2