SOLUTION NOTE

THREAT INTELLIGENCE (TI) FOR SERVICE PROVIDERS

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

CHALLENGES

Service providers are under tremendous pressure to protect their infrastructure, subscribers and data from existing and emerging cyberthreats. Through threat intelligence, security teams can make informed decisions on how best to respond to these threats. Threat intelligence is evidence-based knowledge that includes context, mechanisms, indicators, implications and actionable advice about an existing or emerging threat. Threat indicators can come in the form of malicious IP addresses, hostnames, domain names and URLs. From protection and detection to investigation and response, having fast access to the right blend of threat intelligence is key to success.

Although threat information in the form of raw data is freely available, it can be enormously difficult and time-consuming to make sense of it in a timely fashion. Many organizations lack the visibility and contextual insight required to prioritize threats, much less to respond to them proactively. Additionally, overburdened security personnel must contend with a multitude of siloed tools and hundreds to thousands of alerts every day. A lack of effective threat intelligence leads to poor incident response and slows remediation.

COMPREHENSIVE THREAT INTELLIGENCE FROM INFOBLOX

Infoblox provides service providers with diverse choices to tailor their threat intelligence through the BloxOne® Threat Defense product. BloxOne Threat Defense encompasses Infoblox's in-house DNS infrastructure-focused threat intelligence, complemented by additional feeds from reputable third-party sources based on add-on licenses. The evaluation, curation, and management of these feeds are conducted by the skilled Infoblox threat research team to ensure optimal efficacy and minimal false positives.

BloxOne Threat Defense for Service Providers is available in three packages through our Service Provider License Agreement program (SPLA):

1. SPLA BloxOne Threat Defense Essentials for Service Providers
2. SPLA BloxOne Threat Defense Premium Security for Service Providers
3. SPLA BloxOne Threat Defense Advanced Security for Service Providers

The Advanced package includes Infoblox's original DNS-centric threat intel with the "Suspicious Domains" category of feeds that helps identify attacker infrastructure and block access to those domains even before they are weaponized. This early detection helps protect end users against emergent domains that are setup for malicious attacks in the future.

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.)

The threat feeds available for each BloxOne Threat Defense package are as follows:

SPLA BLOXONE THREAT DEFENSE ESSENTIALS FOR SERVICE PROVIDERS				
• Base Hostnames • Anti-Malware	• Ransomware • Bogon	• DHS AIS IP • DHS AIS Domains	• DoH Public Hostnames	• DoH Public IPs
SPLA BLOXONE THREAT DEFENSE PREMIUM FOR SERVICE PROVIDERS				
• **Essential Feeds Above +** • Anti-Malware IPs • Cryptocurrency Hostnames • EECN IPs	• Extended Base and Anti-Malware Hostnames • Extended Ransomware • Malware DGA Hostnames • NOED	• TOR Exit Node IPs • US OFAC • Sanctions IP Embargoed IPs • US OFAC Sanctions IPs (High Risk)	• US OFAC Sanctions IPs (Medium Risk) • Extreme Block • Extreme log • High Block • High Log	• Low Block • Low Log • Med Block • Med Log
SPLA BLOXONE THREAT DEFENSE ADVANCED FOR SERVICE PROVIDERS				
• **Premium Feeds Above +**	• Suspicious Domains	• Suspicious Lookalikes	• Suspicious NOED	

Note: The above feeds are generated based on analyzing customer and SP-generated Passive DNS data.

SPLA BLOXONE THREAT DEFENSE ESSENTIALS FOR SERVICE PROVIDERS

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

1. **Base Hostnames:** The base feed enables 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.
2. **Anti-Malware:** This feed enables protection against hostnames that contain known malicious threats that can take action or take control of your system, such as malware command and control (C&C), malware download and active phishing sites.
3. **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 the removal of the restriction. Some forms of ransomware encrypt files on the system's hard drive. Others may simply lock the system and display messages intended to coerce the subscriber into paying.
4. **Bogon:** Bogon 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.

5. **and 6. 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. 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, 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, which are available at www.us-cert.gov/ais. Please email nccicustomerservice@hq.dhs.gov for additional information.

7. **and 8. 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.

SPLA BLOXONE THREAT DEFENSE PREMIUM FOR SERVICE PROVIDERS

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

BloxOne Threat Defense Premium offers the same data sets available with BloxOne Threat Defense Essentials plus additional data sets below:

9. **Anti-Malware IPs:** The Anti-malware 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.
10. **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.
11. **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.
12. **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, crypto-jacking that lets site owners mine for cryptocurrency without the owner's consent and cryptocurrency mining pools.
13. **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.
14. **Extended Base & Anti-malware:** Base and Anti-malware hostname feeds combined into a single feed with the extended TTL feeds applied. These feeds 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.
15. **Extended Ransomware:** Ransomware feed with extended TTL applied when they expire from base Ransomware feed. These feeds 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.

16. **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 by the United States against foreign countries. More information is available on the "Sanctions Programs and Country Information" page found here: www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.
17. **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.
18. **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.
19. **NOED (Newly Observed Emergent Domains):** These are newly observed domains that show a significant uptick in traffic globally, which indicates that this domain is active and relatively new.
20. **Extreme Block:** This feed is a pre-configured recommended set of feeds to block the most malicious behaviors. This feed is not appropriate for most users and is not recommended unless your specific environment has a unique need. Use at your own risk. It is a companion to the Extreme Log feed.
21. **Extreme Log:** This feed is a pre-configured recommended feeds designed to log potentially malicious indicators that are too low confidence to include in the Extreme Block list. This feed is not appropriate for most uses and is not recommended unless your specific environment has a unique need. Use at your own risk. It is a companion to the Extreme Block feed.
22. **High Block:** This feed is a pre-configured set of feeds that can be used as a best practice feed to block possibly risky sites and is for environments where it is more important to block potential malicious behavior than it is to avoid blocking the occasional non-malicious site. This is primarily used in environments where behavior is predictable, like server farms, point-of-sales terminals, etc. It is a companion to the High Log feed.
23. **High Log:** This is a best practice feed to log potentially malicious behavior. While these feeds are the most sensitive to blocking malicious behavior, these indicators still have a confidence level that runs the risk of occasionally blocking benign sites. It is a companion to the High Block feed.
24. **Med Block:** This feed is a pre-configured set of feeds that can be used as a best practice feed to block risky sites and is applicable for most environments. For the most part it aligns with feeds recommended in the default global policy. It is a companion to the Med Log feed. This applies to a wide variety of accounts & situations.
25. **Med Log:** This is a best practice feed to log potentially malicious behavior, and that is too sensitive to block. It is a companion to the Medium Block feed.
26. **Low Block:** This is a pre-configured set of feeds that can be used as a best practice feed to block malicious sites for organizations that are more concerned about accidental blocks than allowing the occasional threat. Examples: Service Providers, Universities, Public WiFi Access Points.
27. **Low Log:** This is a best practice feed to log potentially malicious sites for organizations that are more concerned about accidental blocks than allowing the occasional threat. This is a companion to the Low Block feed.

In addition to the above threat intel feeds, the following are also available with the premium package:

- Dossier, a threat investigation and research tool. Infoblox will support 64K queries in Dossier. See the Dossier section below for more information.
- Threat Insight, a unique technology that detects and automatically blocks DNS tunnels and data exfiltration via DNS without the need for endpoint agents or additional network infrastructure. See the Threat Insight section below for more information.

SPLA BLOXONE THREAT DEFENSE ADVANCED FOR SERVICE PROVIDERS

BloxOne Threat Defense Advanced includes all the data feeds described above plus suspicious domains (see the section Leveraging Threat Intelligence on Suspicious Indicators section below).

The Advanced package also includes the Dossier threat investigation tool and Threat Insight. Infoblox will support 64K queries in Dossier. See the Dossier and Threat Insight sections below for more information.

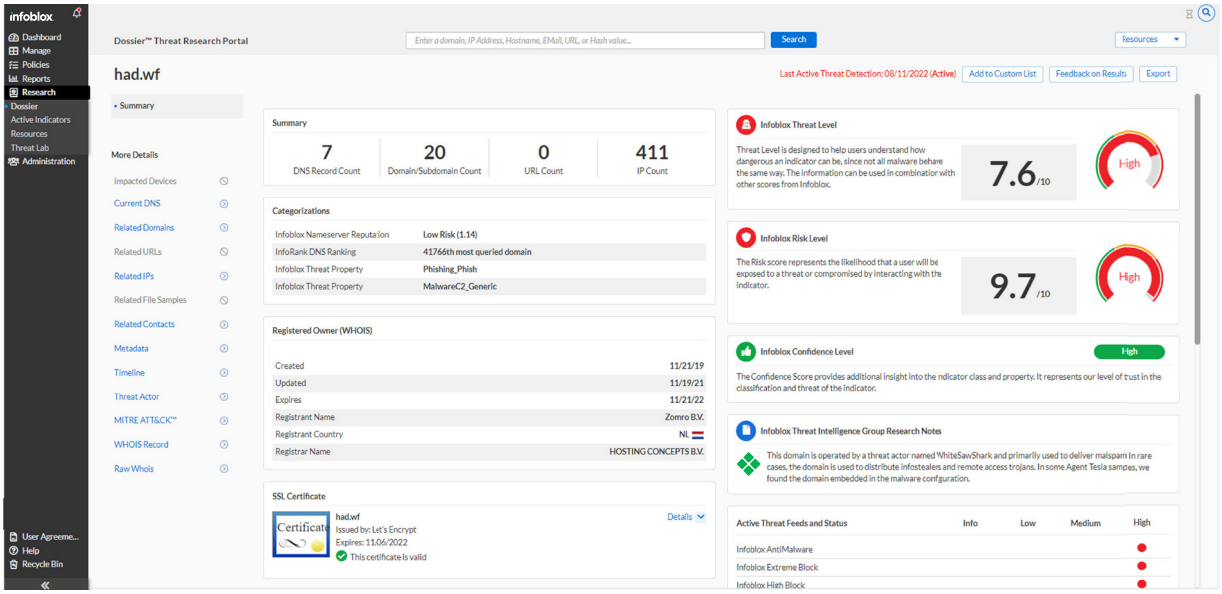
LEVERAGING THREAT INTELLIGENCE ON SUSPICIOUS INDICATORS FOR A PROACTIVE DEFENSE

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 comes 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 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.

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.



THREAT INSIGHT

Threat Insight is a unique technology that detects and automatically blocks DNS tunnels and data exfiltration via DNS without the need for endpoint agents or additional network infrastructure. It uses real-time streaming analytics of live DNS queries and machine learning to accurately detect the presence of data in queries. Threat Insight provides protection against both DNS tunneling and sophisticated data exfiltration techniques. It examines host.subdomain and TXT records in DNS queries and uses entropy, lexical analysis, time series, and other factors to determine the presence of data in queries.

- Looks at TXT records, A, and AAAA records
- Detects presence of data using lexical and temporal analysis
- Certain attributes add to a threat score; others subtract from it
- The final score classifies a request as exfiltration (or not)
- If exfiltration is found, it automatically adds destinations to special internal RPZ feed and scales protection to other parts of the network

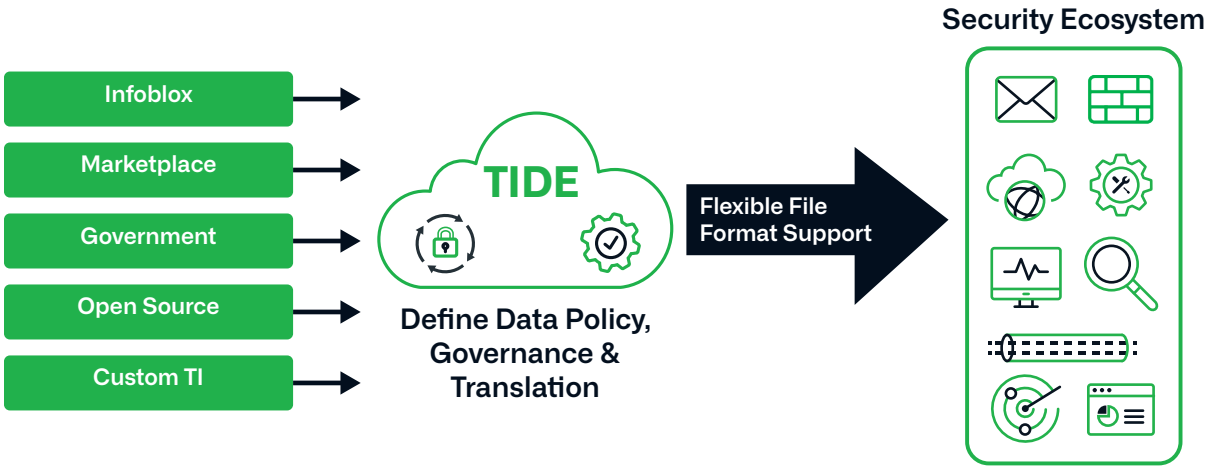
Infoblox is the only vendor to offer DNS infrastructure with built-in analytics for the protection of your data.

ADDITIONAL ADD-ONS TO OPTIMIZE YOUR USE OF THREAT INTELLIGENCE AND PROTECT YOUR BRAND

The following are available as additional add-ons that can be leveraged by service providers to provide a superior, secure experience for end users.

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.



THIRD-PARTY THREAT FEEDS

Infoblox offers service providers 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, end customers simply enter their license on the BYOL page in BloxOne Threat Defense 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:

DomainTools

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.

To learn more, visit www.infoblox.com/sp or contact your local Infoblox representative today.

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

+1.408.986.4000
www.infoblox.com

Version: 20240315v3