SOLUTION NOTE

Threat Intelligence

FACTS & FIGURES

According to the Ponemon Institute's 2018 report on Exchanging Cyber Threat Intelligence:

- More than **60%** of survey respondents were not satisfied with the quality of threat intelligence
- Nearly **25%** of survey respondents were unable to prioritize the threats by category
- Nearly **40%** of respondents lacked context to make threat intelligence actionable

Challenges

Security organizations are under tremendous pressure to protect their infrastructure and data from existing and emerging cyberthreats and hazards. 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 or hazard. Threats can have internal as well as external sources and can come in the form of malicious IP addresses, hostnames, domain names and URLs.

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.

BloxOne™ Threat Defense

With BloxOne Threat Defense organizations can protect their traditional networks and digital transformations like SD-WAN, IoT and the cloud. It automatically blocks modern malware, ransomware, C&C communications, data exfiltration and other advanced threats using DNS as the first line of defense. It also empowers security teams to respond to threats faster by enabling them to share threat data with the rest of the security ecosystem, including security orchestration, automation and response (SOAR) tools. It is the industry's first hybrid security solution that provides pervasive protection on-premises and in the cloud and leverages DNS for foundational security.

BloxOne Threat Defense is available in

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

Each package contains a set of threat intelligence data. The Advanced package contains the additional Threat Intelligence Data Exchange platform, or TIDE.

Threat feeds for each BloxOne Threat Defense package include:

BLOXONE THREAT DEFENSE ESSENTIALS (9)				
• Base Hostnames • Anti-malware • Ransomware	• Bogon • DHS_AIS_IP • DHS_AIS_ Hostname	• DHS AIS NCCIC Watch list Hostnames and Domains	• DHS AIS NCCIC Watch list IPs	• DoH Public IPs and Hostnames
BLOXONE THREAT DEFENSE BUSINESS ON-PREMISES AND BUSINESS CLOUD (20)				
• Base Hostnames • Anti-malware • Ransomware • Bogon • DHS_AIS_IP	• DHS_AIS_ Hostname • DHS AIS NCCIC Watch list Hostnames and Domains • DHS AIS NCCIC Watch list IPs	• DoH Public IPs and Hostnames • Malware IPs • Bot IPs • Exploit Kit IPs	• Malware DGA hostnames • TOR Exit Node IPs • SURBL Multi domains • SURBL Multi Lite domains	• SURBL Fresh domains • US OFAC Sanctions IPs • EECN IPs • Cryptocurrency hostnames and domains
BLOXONE THREAT DEFENSE ADVANCED (27)				
• Base Hostnames • Anti-malware • Ransomware • Bogon • DHS_AIS_IP • DHS_AIS_ Hostname • DHS AIS NCCIC Watch list Hostnames and Domains	• DHS AIS NCCIC Watch list IPs • DoH Public IPs and Hostnames • Malware IPs • Bot IPs • Exploit Kit IPs • Malware DGA hostnames	• TOR Exit Node IPs • SURBL Multi domains • SURBL Multi Lite domains • SURBL Fresh domains • US OFAC Sanctions IPs • EECN IPs	• Cryptocurrency hostnames and domains • Extended Base & anti-malware Hostnames • Extended malware IPs • Extended TOR Exit Node IPs	• Extended Ransomware IPs • Extended Exploit Kits IPs • SpamBot IPs • Spambot IPs DNSBL

BloxOne Threat Defense Essentials

Eight reputation data sets can be applied to the Infoblox DNS Firewall RPZ security policy.

1. **Base hostnames:** The base hostnames set 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 set enables protection against hostnames that contain known malicious threats that can act on 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 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.

4. **Bogon:** Bogons 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.

5/6. **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. 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.

7/8. **DHS AIS NCCIC Watch list Hostnames and Domains and DHS AIS NCCIC Watch list IPs (2 feeds):** Indicators contained in these feeds appear on the watch list from the National Cybersecurity and Communications Integration Center (NCCIC) and are not verified or validated by DHS or Infoblox. NCCIC acts as a hub for information-sharing a ctivities among public and private sector partners to build awareness of vulnerabilities, incidents and mitigations.

Data included in these AIS_IP, AIS_Hostname, DHS AIS NCCIC Watch list Hostnames and Domains and DHS AIS NCCIC Watch list IPs feeds includes AIS data subject to the U.S. DHS Automated Indicator Sharing Terms of Use available: 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 nccicustomerservice@hq.dhs.gov for additional information.

9. **DoH Public IPs and Hostnames:** This policy-based feed contains Domain names and IPs of 3rd 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 through the use of 3rd-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 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. It provides a total of 19 feeds. The additional data sets included in BloxOne Threat Defense Business On-Premises and BloxOne Threat Defense Business Cloud are:

10. **Malware IPs:** The 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 and active phishing sites.

11. **Bot IPs:** This set enables protection against self-propagating malware designed to infect a host and connect back to a central server or servers that act as a C&C center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, remote-control flood-type attacks against targets. Bots can also log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam and open back doors on the infected host.

12. **Exploit kit IPs:** This set enables protection against distributable packs that contain malicious programs used to execute "drive-by down-load" attacks to infect users with malware. These exploit kits target vulnerabilities in the user's machine (usually due to unpatched versions of Java, Adobe Reader, Adobe Flash, Internet Explorer and other applications) to load malware onto the victim's computer.

13. **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.

14. **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's source.

15. **SURBL Multi domains:** This set of malicious domains includes up-to-date intelligence on active malware, phishing, botnet and spam domains, based on data provided by our partner SURBL.

16. **SURBL Multi Lite domains:** A subset of SURBL Multi threat feed, Multi Lite is designed to fit on appliances with limitations on the number of threat intelligence entries that they can accommodate. SURBL Multi Lite offers more concise and targeted threat intelligence focusing on only the most current malicious sites. The combined set includes malware, phishing and botnet activity.

17. **SURBL Fresh domains:** The SURBL Fresh feed deals with newly observed domains (NOD), providing critical, accurate information about when new domains are placed into service. This set of domains can be applied to Infoblox DNS Firewall RPZ security policies (e.g., block, quarantine, walled garden and others) to prevent resolution of new domains, based on the user's defined policies. The set is based on data from our partner SURBL.

18. **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.

19. **EECN IPs:** This policy-based feed contains IPs of 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.

20. **Cryptocurrency hostnames and domains:** 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.

BloxOne Threat Defense Advanced

BloxOne Threat Defense (B1TD) Advanced includes all the data feeds described above plus additional data feeds and the TIDE platform. It provides a total of 27 feeds. The additional data sets in BloxOne Threat Defense Advanced include:

Extended TTL feeds: These feeds expand the base, anti-malware, ransomware, exploit kits and TOR Exit Node 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:

21. **Extended base & anti-malware:** Base and anti-malware hostname feeds combined into a single feed with the extended TTL feeds applied

22. **Extended malware IPs**

23. **Extended TOR Exit Node IPs**

24. **Extended ransomware IPs**

25. **Extended exploit kit IPs**

26. **Spambot IPs:** This feed protects against a computer or bot node as part of a botnet seen sending spam. IPs listed are also frequently found with a poor or negative reputation for those addresses.

27. **Spambot IPs DNSBL:** In DNSBL format, this feed contains IPs of known spam servers. It guards against a computer or bot node as part of a botnet seen sending spam. It can help block incoming spam or potentially malicious emails from known spam sources by feeding into your email platform or appliance.

Leveraging Threat Intel Across Entire Security Infrastructure

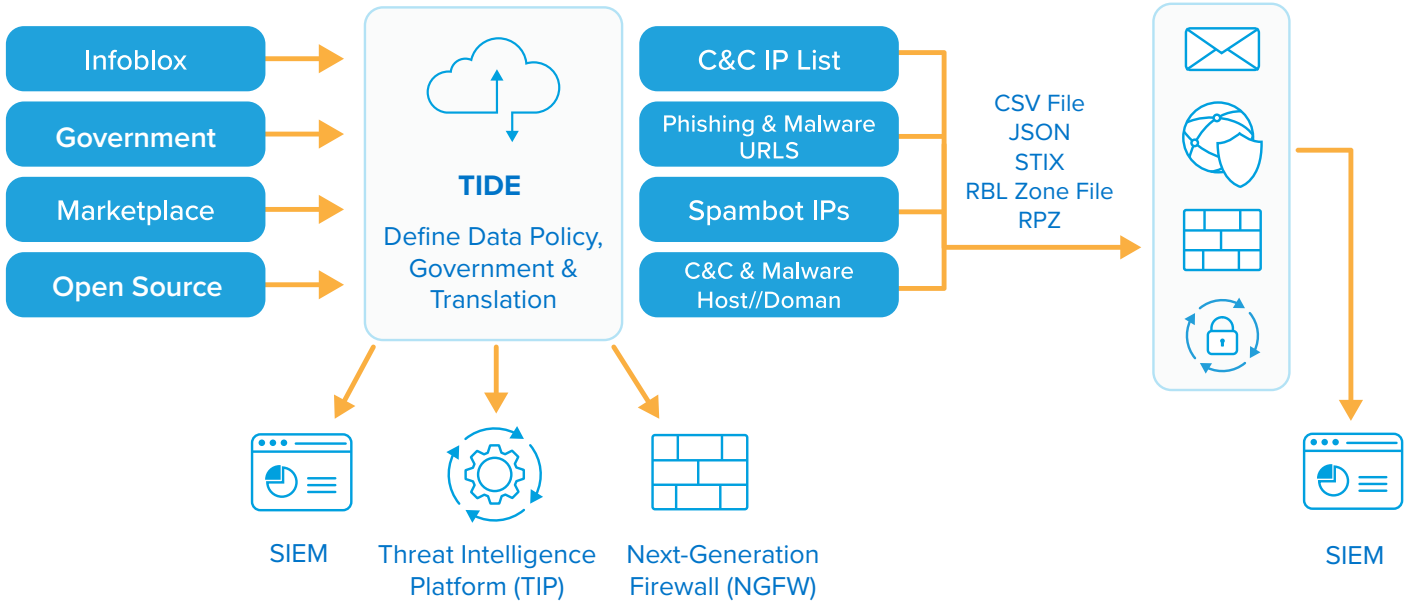

Figure 1: TIDE facilitates threat intelligence exchange across the security ecosystem

TIDE BENEFITS

- Collects and manages real-time curated threat intelligence from internal and external sources in a single, open and flexible platform
- Enables threat prioritization with context by providing over 300 distinct threat classifications and more than 20 properties, leading to faster threat remediation
- Improves security posture and situational awareness of an organization by sharing the curated threat intelligence data with the security infrastructure
- Prevents malware communications with C&C sites and data exfiltration by providing real-time threat feeds at the DNS control plane

Third-party Threat Indicator Feeds Available for BloxOne Threat Defense Advanced

BloxOne Threat Defense Advanced offers the option to supplement Infoblox threat intelligence with threat data from third-party sources. Many partners have aligned with Infoblox to simplify a customer's onboarding process, offering for purchase additional threat feeds to help improve security while freeing operations and threat intelligence teams to focus on more urgent tasks. The BloxOne Threat Defense Advanced TIDE capability is supported by the following threat feed partners:

CROWDSTRIKE

CrowdStrike: This is a leading provider of next-generation endpoint protection, threat intelligence and services. CrowdStrike Falcon hostname and IP intelligence enables customers to prevent damage from targeted attacks, detect and attribute advanced malware and adversary activity in real time and effortlessly search all endpoints, reducing overall incident response time. Customers must purchase the CrowdStrike feed directly from CrowdStrike, but Infoblox can help to "turn on" the feed in the TIDE platform.

FIREEYE

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 to purchase the iSight feed directly from FireEye, Infoblox can help to "turn on" the feed in the TIDE platform.

In addition, BloxOne Threat Defense Advanced subscribers can leverage the following third-party vendor feeds (requires additional subscription) in RPZ format (at no additional cost) to increase their threat coverage at the DNS control plane:

FARSIGHT SECURITY

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

proofpoint.

Proofpoint Emerging Threats (ET) IP and Domain Reputation Feed: This feed provides actionable IP and domain reputation entries that are scored based on observations of in-the-wild threat actor behavior and direct observations by Proofpoint's ET Labs. Built upon a proprietary process that leverages one of the world's largest active malware exchanges, victim emulation at massive scale, original detection technology and a global sensor network, Proofpoint ET Intelligence is updated in real time to provide organizations with the actionable intelligence to combat today's emerging threats.

Infoblox Threat Intelligence Data Exchange (TIDE)

Protecting your infrastructure must start with the core. Infoblox uses highly accurate machine-readable threat intelligence data via a flexible and open Threat Intelligence Data Exchange (TIDE) platform to aggregate, curate and enable distribution of data across a broad range of infrastructures.

TIDE enables organizations to ease consumption of threat intelligence from various internal and external sources and to effectively defend against and quickly respond to threats.

Infoblox's TIDE is designed to keep security systems such as BloxOne Threat Defense and its cybersecurity ecosystem updated in real time on new and evolving malicious Internet destinations. TIDE uses over 300 distinct classifications and more than 20 properties to help prioritize security responses by providing context and insight on threats.

TIDE provides data based on observed malicious Internet destinations with which devices have attempted to communicate, plus detailed threat information about those endpoints to enable security teams to quickly understand the nature of the threats they are experiencing. The Infoblox Cyber Threat Intelligence (CTI) team reviews the sources of threat intelligence, correlates the data and applies whitelists to significantly minimize false positives. The CTI team originally formed in TIDE 1997 after receiving requests from leading financial institutions for this kind of service.

The CTI team also examines large DNS query and response data sets to uncover new behavioral and heuristic patterns. The team applies Infoblox's deep experience with the DNS protocol in its approach to threat hunting, large-scale spam traps, reverse engineering and passive DNS analysis. The TIDE platform is also a key contributor to the response policy zone (RPZ) marketplace, a community-sourced authoritative database designed to enable more robust DNS security. Reliance on multiple sources in the RPZ provides a broader view of threats and enables more timely, accurate and cleaner data sets.

This comprehensive intelligence of indicators can also be leveraged at the DNS control plane (via automatic updates to its RPZ policy) to enforce policies set by the user to block unwanted IP communications. The threat intelligence is also easily deployable via the Infoblox TIDE platform via an API in various formats (CEF, CSV, XML, STIX and JSON) on security infrastructures, such as next-generation firewalls, email gateways, web proxies, SIEMs and others.

Consolidating Policy Enforcement Using Third-party Infrastructure and Infoblox TIDE

Organizations often use multiple security systems to handle threat intelligence data. Examples include next-generation firewalls, web proxies, SIEMs, Network Access Control, vulnerability management, advanced threat protection and endpoint security. With the BloxOne Threat Defense Advanced bundle, organizations can use TIDE to access all threat intelligence data, regardless of source or system, in one consolidated platform. TIDE incorporates threat data created natively or locally, from third-party sources or generated by third-party infrastructure.

Security teams can readily create custom API feeds by choosing the data type necessary for their security ecosystem (be it a firewall, SIEM or other) such as JSON, STIX, CSV, TSV, CEF, XML or RPZ to quickly remediate threats. TIDE integrates with the following security infrastructure vendors:

Cisco Threat Intelligence Director: Infoblox TIDE can distribute curated Infoblox and third-party threat intelligence in STIX format for consumption on Cisco security platforms via the Cisco Threat Intelligence Director. This integration enables security organizations to monitor or block more threats as well as r educe the number of events to review.

Check Point ThreatCloud: Curated and prioritized threat intel from Infoblox TIDE is available to Check Point customers through ThreatCloud. Whether teams are monitoring or flat out blocking network traffic to malicious sites (especially those known for C&C activities), threat indicators provided by BloxOne Threat Defense Advanced via TIDE will reliably help organizations identify and stop malicious activity.

Palo Alto Networks Next-Generation Firewall (NGFW): Palo Alto Networks next generation firewall customers can download curated threat intel in text format from Infoblox TIDE to increase threat coverage and improve their situational awareness and security posture.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com