Infoblox
CONTROL YOUR NETWORK

Infoblox Threat Intelligence Data Exchange (TIDE) for ActiveTrust®

SOLUTION NOTE

Challenges

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

Threats come from internal as well as external sources. Bottom line is, organizations are under tremendous pressure to manage threats. Though information in the form of raw data is available abundantly, it is hard and time-consuming to get meaningful information based on which proactive measures can be set. This naturally pulls more and more users towards threat intelligence as it helps to prioritize threats within the deluge of data, alerts, and attacks and provides actionable information.

According to Ponemon Institute, 2016 Second Annual Study on Exchange Cyber Threat Intelligence: There Has to Be a Better Way,

- 70% of survey respondents felt that Threat Intel was not timely
- 46% of survey respondents were unable to prioritize the threats by category
- 45% of respondents lacked context for threat intel to make it actionable

To surmise, ineffective threat intelligence leads to poor incidence response and slows remediation.

Solution

Infoblox ActiveTrust 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 infrastructure. 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 Infoblox DNS Firewall and its cybersecurity ecosystem updated in real time on new and evolving malicious Internet destinations. Infoblox threat intelligence uses over 300 distinct classifications (categories) to help provide context and insight on threats. TIDE streams 10-15 million newly confirmed threat locations per week across all our sources. We provide data on observed malicious Internet destinations with which devices have attempted to communicate and detailed threat information to enable operators to quickly understand the nature of the threats they are experiencing. The sources of threat intelligence are reviewed, the data correlated, and whitelists applied to significantly minimize false positives.

This comprehensive intelligence of observed malicious Internet destinations known to be used by cybercriminals can be leveraged by DNS Firewall (via automatic updates to its Response Policy Zone (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 on security such as next-generation firewalls, web proxies, SIEMs, and others.

This document explains the threat intelligence offered by Infoblox ActiveTrust, which is offered in three versions: ActiveTrust Standard, ActiveTrust Plus, and ActiveTrust Advanced. ActiveTrust Standard offers a basic threat data set without TIDE. ActiveTrust Plus offers a more expanded data set with TIDE that includes data from an Infoblox threat intelligence OEM partner, SURBL. ActiveTrust Advanced offers the most comprehensive data set, including data sets available through ActiveTrust Standard and ActiveTrust Plus products.

Infoblox Threat Intelligence Data Exchange (TIDE) for ActiveTrust®

SOLUTION NOTE

TIDE Benefits

- Collects and manages real-time curated threat intelligence from internal and external sources in a single, open and flexible platform
- Enable threat prioritization with context by providing over 300 distinct threat classifications leading to faster threat remediation
- Improve security posture and situational awareness of your organization by sharing the curated threat intelligence data with the security infrastructure
- Apply threat intel data at the DNS control plane, preventing malware communications with C&C sites and data exfiltration

Policy Enforcement Using DNS Firewall

ActiveTrust Standard (does not include TIDE)

Five reputation data sets can be applied to the Infoblox DNS Firewall RPZ 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 take action on or 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 paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coerce the user into paying.
4. **Bogon**: Bogons are commonly found as 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. **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 Department of Homeland Security'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 as 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 this AIS_IP and AIS_Hostname feeds includes AIS data subject to the U.S. Department of Homeland Security Automated Indicator Sharing Terms of Use available at https://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.

Please email ncciccustomerservice@hq.dhs.gov for additional information

ActiveTrust Plus

ActiveTrust Plus offers the data sets available with ActiveTrust Standard plus additional data sets that can be applied to the Infoblox DNS Firewall RPZ policy.

Malware IPs: The malware IP set enables protection against known malicious or compromised IP addresses. These are known to host threats that can take action on or control of your system, such as malware command and control, malware download, and active phishing sites.

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 command-and-control 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.

Exploit Kit IPs: This set enables protection against distributable packs that contain malicious programs used to execute "drive-by download" attacks in order 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.

Malware DGA hostnames: Domain generation algorithms (DGA) are algorithms seen in various families of malware that are used to periodically generate a large number of domain names that can be used 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 be used to monitor Tor traffic (after it leaves the onion network). The Tor network is designed so that locating the source of that traffic through the network should be difficult to determine.

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.

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 can be loaded, SURBL Multi Lite is narrowed down to include concise and targeted threat intelligence focusing on only the most current malicious sites. The combined set includes malware, phishing, and botnet activity.

SURBL Fresh domains: The SURBL Fresh feed deals with newly observed domains (NOD), providing critical, accurate information on the time new domains are placed into service. This set of domains can be applied to Infoblox DNS Firewall RPZ secure policy (block, quarantine, walled garden, etc.) to prevent resolution of new domains, based on the user's defined policies. The set is based on data provided by our partner SURBL.

US OFAC Sanctions IPs - Policy based feed that contains IPs of United States sanctioned countries listed by US Treasury Office of Foreign Assets Control (OFAC). The Treasury Department's Office of Foreign Asset Control (OFAC) administers and enforces economic sanctions imposed by the United States against foreign countries. More information can be found by visiting the "Sanctions Programs and Country Information" page found here:

https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

EECN IPs - Policy based feed that contains IPs of countries in Eastern Europe and China. These countries are often found in cyber-attacks seeking intellectual property or other sensitive or classified data and stealing credit card or financial information.

ActiveTrust Advanced

ActiveTrust Advanced offer the data sets available with ActiveTrust Standard plus ActiveTrust Plus and additional data sets that can be applied to the Infoblox DNS Firewall RPZ policy. These additional data sets are:

Extended TTL feeds: An extension of the Base, Antimalware, Ransomware, ExploitKits, and TOR Exit Node feeds that contain recently expired threats with an extended time-to-live (TTL) applied. The extended time-to-live (TTL), provides extended reach of protection for your DNS FW, but may also increase the risk of false positives as indicators may no longer be active.

The Extended TTL feeds are:

- Extended Base & Antimalware – Base and Malware hostname feeds combined into a single feed with the extended TTL's applied
- Extended Malware IP's
- Extended TOR Exit Node IPs
- Extended Ransomware IPs
- Extended ExpoitKit IPs

SpamBot IPs: Enables protection against a computer or bot node as part of a botnet seen sending spam. IP's listed are also frequently found withpoor/negative reputation on that IP address.

Policy Enforcement Using Third-party Infrastructure via Infoblox Threat Intelligence Data Exchange (TIDE) Platform

We recognize that organizations use a number of security systems such as next-generation firewalls, web proxies, SIEMs, network access control, vulnerability management, advanced threat protection, and endpoint security on which they deploy and use threat intelligence data. ActiveTrust Plus and ActiveTrust Advanced bundles enable customers to use Infoblox TIDE. This allows you to access and use all of your threat intelligence data, including ActiveTrust data, native/locally created data, and third-party data on any third- party infrastructure. ActiveTrust Plus enables access to only one of three datatypes: IP addresses, hostnames, and, URLs whereas ActiveTrust Advanced provides access to all three data types. Infoblox makes creating custom API feeds quick and easy by providing the ability to choose the data type you need for your security ecosystem (be it a firewall, SIEM, or other) such as JSON, STIX, CSV, TSV, CEF, XML, RPZ, etc. to quickly remediate threats. TIDE integrates with the following security infrastructure vendors to improve the overall security posture of your organization:

Cisco Threat Intelligence Director: Infoblox TIDE, can distribute curated Infoblox and 3rd party threat intelligence in STIX format for consumption on Cisco security platforms via the Cisco Threat Intelligence Director. This integration enables our customers to monitor or block more threats as well as reduce the amount of events to review.

Check Point ThreatCloud: Curated and prioritized threat intel from Infoblox TIDE, is now available to Check Point customers through ThreatCloud. Whether you're monitoring, or flat out blocking network traffic to malicious sites (especially those known for command and control activities), threat indicators provided by ActiveTrust via TIDE will reliably help you identify and stop malicious activity.

Palo Alto Networks Next Gen 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 the situational awareness and security posture of our customers.

Infoblox
CONTROL YOUR NETWORK

Infoblox Threat Intelligence Data Exchange (TIDE) for ActiveTrust®

SOLUTION NOTE

Third-party Threat Indicator Feed Data Marketplace

ActiveTrust Plus and ActiveTrust Advanced

ActiveTrust Plus and ActiveTrust Advanced offer the option to supplement ActiveTrust threat data with threat data from third-party sources by allowing that data to be managed from within Infoblox TIDE. This helps to eliminate costs of onboarding additional third-party data and to maximize resources by giving back time to the security operations and threat intelligence team. The security partners whose data we currently support include:

- SURBL
- Proofpoint Emerging Threats
- FireEye ISIGHT Threat Intelligence
- OpenPhish
- CrowdStrike
- ThreatTrack Security
- Farsight Security

OpenPhish: Provides real-time insight into live phishing URLs. The data is updated every five minutes with information from the past 24 hours. It utilizes OpenPhish's proprietary phishing campaign tracking technology to provide feeds that can help identify high-risk accounts of users, customers, and employees, and prevent account intrusion and takeover activities.

CrowdStrike: 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.

FireEye iSIGHT Threat Intelligence: It's IP and hostname cyber threat intelligence equips enterprises with strategic, operational and tactical analysis derived by their global team of experts. ThreatScape subscription provide the intelligence necessary to align your security program with business risk management goals and to proactively defend against new and emerging cyber threats.

In addition, both ActiveTrust Plus and ActiveTrust Advanced subscribers can leverage the following third party vendor feeds (requires additional subscription) in RPZ format to increase their threat coverage at the DNS control plane:

ThreatTrack Security BorderPatrol Feed: The BorderPatrol Sites list is a "black list" consisting of domains associated with the distribution of potentially unwanted software and advertising.

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

Proofpoint Emerging Threats (ET) IP and Domain Reputation Feed: Provides actionable IP and domain reputation entries that are scored based upon observed in the wild threat actor behavior and as observed directly 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.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.