Infoblox
NEXT LEVEL NETWORKING

Infoblox Threat Intelligence Data Exchange (TIDE) for ActiveTrust® Suite

SOLUTION NOTE

Challenges

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging threat or hazard. It can be used to inform decisions regarding the subject's response to that threat or hazard. Threats can come from internal as well as external sources, and can come in the form of malicious IP addresses, hostnames, domain names and URLs.

As such organizations are under tremendous pressure to manage threats. Though information in the form of raw data is available freely, 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 flood of data, alerts, and attacks and provides actionable information.

According to the Ponemon Institute's 2016 Second Annual Study on Exchange Cyber Threat Intelligence:

- 66% of survey respondents felt that Threat Intel was not timely
- 41% of survey respondents were unable to prioritize the threats by category
- 37% of respondents lacked context for threat intel to make it actionable

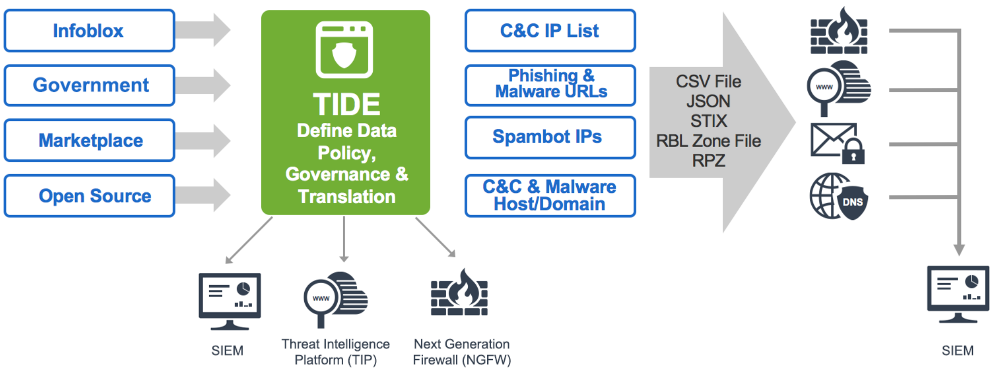
To summarize, ineffective threat intelligence leads to poor incidence response and slows remediation.

Solution – Infoblox Threat Intelligence Data Exchange (TIDE)

TIDE is available as part of the ActiveTrust Suite. Infoblox ActiveTrust Suite 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.

Leveraging Threat Intel Across Entire Security Infrastructure



RESULT: Single-source of TI management | Threat Prioritization | Improve Security Posture

Infoblox Threat Intelligence Data Exchange (TIDE) for ActiveTrust® Suite

SOLUTION NOTE

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

TIDE provides data based on observed malicious Internet destinations with which devices have attempted to communicate, and detailed threat information around those endpoints to enable security teams 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 work is handled by the Infoblox Cyber Threat Intelligence (CTI) team. TIDE was originally formed in 1997 by the CTI after receiving requests from leading financial institutions for this kind of service.

The CTI also have a team looking at very large DNS query and response data sets to find new behavioral and heuristic patterns. Because of our deep experience with the DNS protocol we've also applied that experience to how we approach our threat hunting, large scale spam-traps, reverse- engineering and passive DNS analysis. The TIDE platform is also used to build out a multi-sourced RPZ marketplace for robust DNS security. More sources represent a broader view. More focus brings a more timely, accurate, clean stream of data. We are advancing on both fronts.

This comprehensive intelligence of indicators can also be leveraged at the DNS control plane (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 via an API in various formats (CEF, CSV, XML, STIX and JSON) on security infrastructure such as next-generation firewalls, email gateways, web proxies, SIEMs and others.

ActiveTrust Suite includes on-premises ActiveTrust and SaaS based ActiveTrust Cloud

Infoblox ActiveTrust is offered in three tiers:

- ActiveTrust Standard offers a basic **8 RPZ data feeds** without TIDE.
- ActiveTrust Plus offers a more expanded **19 data feeds** with TIDE that includes data from ActiveTrust Standard and threat intelligence OEM partner, SURBL.
- ActiveTrust Advanced offers the most comprehensive **26 data feeds** with TIDE, including data sets from ActiveTrust Standard and ActiveTrust Plus.

Infoblox ActiveTrust Cloud is offered in two tiers:

- ActiveTrust Standard offers a basic **6 RPZ data feeds** without TIDE.
- ActiveTrust Cloud Plus offers a more expanded **13 data feeds** with TIDE that includes data from ActiveTrust Standard and threat intelligence OEM partner, SURBL.

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 over 20 plus properties leading to faster threat remediation
- Improves security posture and situational awareness of your 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

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

Organizations often use several 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, ActiveTrust Cloud Plus and ActiveTrust Advanced bundles enable customers to use Infoblox TIDE for these systems. This allows you to access and use all your threat intelligence data, including ActiveTrust data, native/locally created data, and third-party data on any third-party infrastructure.

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 number 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 situational awareness and security posture.

ActiveTrust Tiers

ActiveTrust Standard and ActiveTrust Cloud Standard (does not include Infoblox TIDE)

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

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.

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.

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 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.

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.

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.

DHS AIS NCCIC Watch list Hostnames and Domains and DHS AIS NCCIC Watch list IP's – Indicators contained in this feed appear on the watch list from the National Cybersecurity & Communications Integration Center (NCCIC) and are not verified or validated by DHS or Infoblox. DHS's National Cybersecurity and Communications Integration Center (NCCIC) acts as a hub of information sharing activities among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations.

Data included in this AIS_IP, AIS_Hostname, DHS AIS NCCIC Watch list Hostnames and Domains and DHS AIS NCCIC Watch list IP's feeds include 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 available at: https://www.us-cert.gov/ais. Please email ncciccustomerservice@hq.dhs.gov for additional information

ActiveTrust Plus and ActiveTrust Cloud Plus (includes Infoblox TIDE)

ActiveTrust Plus and ActiveTrust Cloud Plus offer data sets available with ActiveTrust Standard plus additional data sets that can be applied to the security infrastructure including Infoblox DNS Firewall RPZ policy. It provides a total of 17 feeds. The additional data sets included in ActiveTrust Plus are:

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 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 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 many 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.

Cryptocurrency Hostnames and Domains: This feed features threats that allow malicious actors to perform illegal and/or fraudulent activities, coinhives that allows site owners to embed cryptocurrency mining software into their webpages as a replacement to normal advertising, Cryptojacking that allows site owners to mine for cryptocurrency without the owner's consent, and cryptocurrency mining pools working together to mine cryptocurrency.

ActiveTrust Advanced (includes Infoblox TIDE)

ActiveTrust Advanced offers the data sets available with ActiveTrust Standard plus ActiveTrust Plus and additional data sets that can be applied to the security infrastructure including Infoblox DNS Firewall RPZ policy. It provides a total of 23 feeds. These additional data sets to ActiveTrust Standard and Plus are:

Extended TTL feeds: An extension of the Base, Antimalware, Ransomware, Exploit Kits, 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.

Spambot IP's DNSBL: In DNSBL format, this feed contains IPs of known spam servers. Enables protection against a computer or bot node as part of a botnet seen sending spam. Can be used to help block incoming Spam or potentially malicious emails from known spam sources by feeding into your email platform or appliance.

Infoblox
NEXT LEVEL NETWORKING

Infoblox Threat Intelligence Data Exchange (TIDE) for ActiveTrust®

SOLUTION NOTE

Third-party Threat Indicator Feeds Available Only For ActiveTrust Plus, ActiveTrust Cloud Plus and ActiveTrust Advanced subscribers

ActiveTrust Plus, ActiveTrust Cloud Plus and ActiveTrust Advanced

These offer the option to supplement ActiveTrust threat data with threat data from third-party sources at an additional subscription 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:

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, ActiveTrust Plus, ActiveTrust Cloud Plus and ActiveTrust 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:

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 is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.