Infoblox

SOLUTION NOTE

Threat Intelligence Data Exchange (TIDE)

Drive SecOps efficiency with threat intelligence management and automation

FACTS & FIGURES

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

- 2/3rds of respondents struggle to distribute CTI information via email or in documents
- Over half of respondents cite lack of staff, skills, or funding as inhibitors to CTI effectiveness
- SANS survey authors conclude that automation is needed to support CTI efficiency and scale

Security Effectiveness Depends on Diverse, Accurate Threat Intelligence (TI)

For decades, most of the largest and most secure enterprises in the world followed a 'multi-vendor' security approach with the belief that no single vendor could provide sufficient threat intelligence to protect them against a constantly evolving threat landscape. So they would orchestrate their defenses to force attacks through multiple solutions, from multiple vendors, in hopes that at least one of those vendors would have the necessary threat intelligence to detect some part of an attack across the kill-chain.

In recent years, studies have validated and highlighted the value of this approach by revealing how little overlap there is among threat feeds from vendors, open source, community and other sources. In one study, a comparison of the threat intelligence data provided by two security vendors found only an 11% overlap, meaning that 89% of the data from each vendor was unique.

This has resulted in a drive for the optimum blend of threat intelligence to help organizations get the most out of their overall security investment. Unfortunately, this effort has further burdened SecOps to identify, collect, normalize, and distribute different kinds of threat intelligence from dozens of available sources and deliver the right mix of TI to each security tool. This leaves most struggling with a mix of commercial and homegrown tools, connected with APIs, scripts, and macros, in an attempt to achieve some sense of success.

Infoblox TIDE Streamlines Efforts to Optimize TI

Infoblox BloxOne Threat Defense Advanced offers a feature to streamline threat intelligence collection and management called TIDE (Threat Intelligence Data Exchange.) In addition to up to 30 threat feeds included with BloxOne Threat Defense, TIDE provides the capability to ingest threat intelligence from other sources and control how that threat intelligence is distributed across the security stack to make very tool as effective as possible.

Key TIDE benefits include:

- Collect and manage real-time, curated threat intelligence from multiple sources in a single, open and flexible platform
- Support faster threat investigation and response with the context of over 300 distinct threat classification areas
- Improve SecOps efficiency and the effectiveness of the entire security stack with easily shared threat intelligence
- See and control highly evasive threat activity at the DNS-layer as this same threat intelligence is applied by BloxOne Threat Defense to reveal risks such as backdoor's, C2 communications, data tunneling or exfiltration over DNS

Infoblox's TIDE is designed to keep security systems such as Infoblox BloxOne Threat Defense and the rest of the cybersecurity ecosystem updated in real time against new and evolving threats. Combine up to 30 different threat intelligence sources provided by Infoblox with any others available commercially, from government or industry sources, open source, or your own internal TI data sets. Automation capabilities and support for a wide variety of file formats enables TIDE to help customers collect and distribute the appropriate blend of threat intelligence to different tools in their ecosystem including firewalls, SIEM, SWG, SOAR, Vulnerability Scanners, and more.

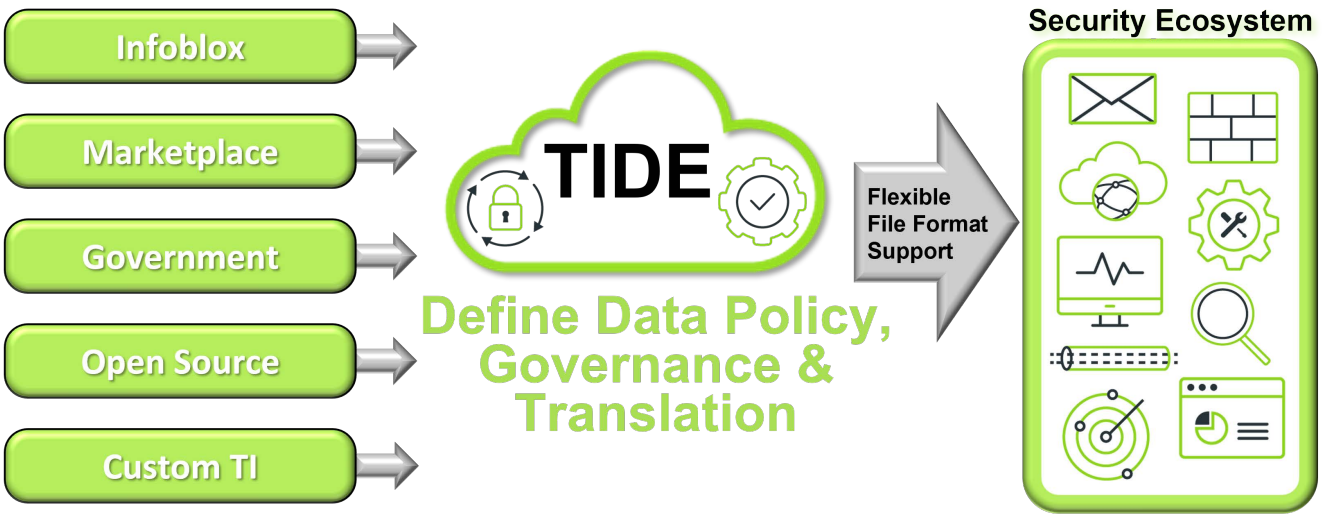

Figure 1: TIDE facilitates the exchange of threat intelligence across the security ecosystem, uplifting defenses and improving reporting.

Just One of the Many Valuable Features of BloxOne Threat Defense

TIDE is one of several features that make up BloxOne Threat Defense, a cloud-native security solution to protect against modern malware, ransomware, C&C communications, data exfiltration and other advanced threats using DNS as the first line of defense. It includes features to uplift the entire security stack and make SecOps more efficient such as enabling them to speed threat investigations and respond to threats faster and with greater confidence. It is the industry's first security solution for our modern hybrid reality to provide pervasive protection everywhere for all of the devices on the network including BYOD and IOT/OT.

Optimize Threat Hunting, Investigation and Response

BloxOne Threat Defense Advanced offers another feature that enables analysts to access and pivot around the full breadth of threat intelligence within a single view called Dossier. Dossier provides on-demand access to threat severity, WHOIS data, MITRE ATT&CK guidance, file samples, related IPs/URLs/Domains, threat actor background, activity timelines, and more. It empowers analysts to pivot where they need to go, following the data and their experience, so they can reach confident conclusions faster.

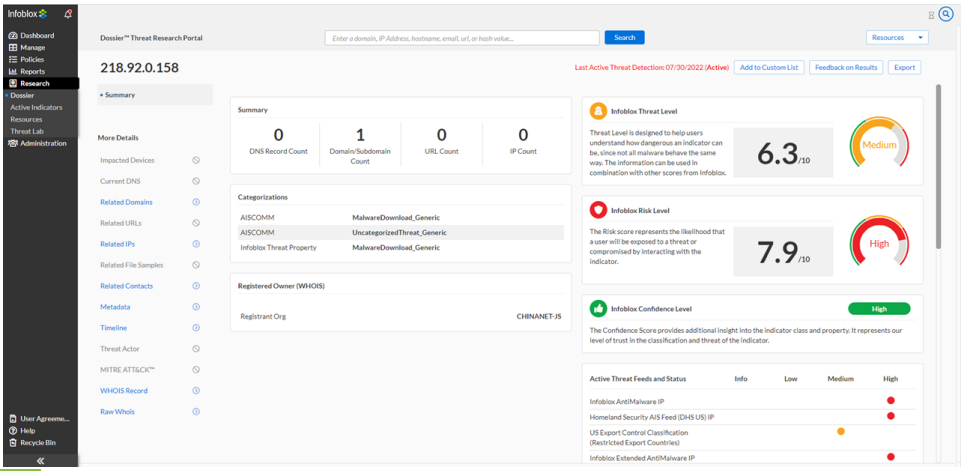

Figure 2: The Dossier dashboard with the power to dive and pivot on-demand.

Out-of-the-Box Integrations: Third-party Threat Feeds

While the TIDE feature of BloxOne Threat Defense can simplify and automate the process of integration almost any threat intelligence feed, and distribute to almost any security tool, some partners have worked with Infoblox to simplify a customer's on-boarding process.

The following partners offer out-of-the-box support for the TIDE feature:

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 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 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 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.

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

+1.408.986.4000 | info@infoblox.com | www.infoblox.com