LÖSUNGSHINWEIS

THREAT INTELLIGENCE DATA EXCHANGE (TIDE)

Steigerung der SecOps-Effizienz mit Threat Intelligence Management und Automatisierung

DIE WIRKSAMKEIT DER SICHERHEIT HÄNGT VON VIELFÄLTIGER UND PRÄZISER THREAT INTELLIGENCE (TI) AB

Jahrzehntelang verfolgten die meisten der größten und sichersten Unternehmen der Welt einen „Multi-Vendor"-Sicherheitsansatz in der Überzeugung, dass kein einzelner Anbieter genügend Bedrohungsdaten bereitstellen kann, um sie vor einer sich ständig weiterentwickelnden Bedrohungslandschaft zu schützen. Also haben sie ihre Verteidigung so ausgerichtet, dass Angriffe durch mehrere Lösungen von mehreren Anbietern erzwungen werden. Dabei hofften sie, dass zumindest einer dieser Anbieter über die notwendigen Bedrohungsdaten verfügt, um einen Teil eines Angriffs in der gesamten Kill-Chain zu erkennen.

In den letzten Jahren haben Studien den Wert dieses Ansatzes bestätigt und hervorgehoben, indem sie aufzeigten, wie wenig Überschneidungen es zwischen den Bedrohungsdaten von Anbietern, Open Source, Community und anderen Quellen gibt. In einer Studie wurden bei einem Vergleich der Threat-Intelligence-Daten von zwei Sicherheitsanbietern nur 11 % Überschneidungen festgestellt, was bedeutet, dass 89 % der Daten von jedem Anbieter einzigartig waren.

Dies führte zu einem Streben nach einer optimalen Mischung von Threat Intelligence, damit Unternehmen das Beste aus ihrer gesamten Sicherheitsinvestition herausholen können. Leider hat dieses Bestreben dazu geführt, dass die SecOps-Abteilung die verschiedenen Arten von Threat Intelligence aus Dutzenden von verfügbaren Quellen identifizieren, sammeln, standardisieren und verteilen und die richtige Mischung für jedes Sicherheitstool bereitstellen muss. Das führt dazu, dass die meisten Unternehmen mit einer Mischung aus kommerziellen und selbstentwickelten Tools zurechtkommen müssen, die mit APIs, Skripten und Makros verbunden sind, um überhaupt einen gewissen Erfolg zu erzielen.

INFOBLOX TIDE VEREINFACHT DIE BEMÜHUNGEN ZUR OPTIMIERUNG VON TI

Mit TIDE (Threat Intelligence Data Exchange) bietet Infoblox BloxOne Threat Defense Advanced eine Funktion zur Rationalisierung der Sammlung und Verwaltung von Threat-Intelligence-Daten. Zusätzlich zu den bis zu 30 in BloxOne Threat Defense enthaltenen Threat-Feeds bietet TIDE die Möglichkeit, Threat-Intelligence-Daten aus anderen Quellen aufzunehmen und zu steuern, wie diese Threat-Intelligence-Daten über den gesamten Sicherheits-Stack verteilt werden, um das Tool so effektiv wie möglich zu machen.

ZAHLEN UND FAKTEN

Ergebnisse aus der SANS Cyber Security Intelligence (CTI) Umfrage 2021:

- **Zwei Drittel der Befragten haben Schwierigkeiten**, CTI-Informationen per E-Mail oder in Dokumenten zu verteilen
- Mehr als die Hälfte der Befragten nennen **Personalmangel, fehlende Kompetenzen oder fehlende Finanzierung** als Hemmnisse für die Wirksamkeit von CTI
- Die Autoren der SANS-Studie kommen zu dem Schluss, dass eine **Automatisierung zur Unterstützung der Effizienz und Skalierung von CTI erforderlich ist**

Zu den wichtigsten Vorteilen von TIDE zählen:

- Erfassung und Verwaltung kuratierter Echtzeit-Threat-Intelligence aus verschiedenen Quellen auf einer einzigen, offenen und flexiblen Plattform
- Unterstützen Sie eine schnellere Bedrohungsuntersuchung und -reaktion im Kontext von über 300 verschiedenen Bedrohungsklassifizierungsbereichen
- Verbesserung der SecOps-Effizienz und der Effektivität des gesamten Sicherheits-Stacks durch einfach zu teilende Threat Intelligence
- Erkennung und Kontrolle von hochgradig diffusen Bedrohungsaktivitäten auf der DNS-Ebene, da BloxOne dieselbe Threat Intelligence einsetzt
- Bedrohungsabwehr zur Aufdeckung von Risiken wie Backdoors, C2-Kommunikation, Datentunneling oder Datenexfiltration über DNS

TIDE von Infoblox wurde entwickelt, um Sicherheitssysteme wie Infoblox BloxOne Threat Defense und den Rest des Cybersecurity-Ökosystems in Echtzeit gegen neue und sich entwickelnde Bedrohungen auf dem Laufenden zu halten. Kombinieren Sie bis zu 30 verschiedene Quellen für Bedrohungsdaten, die von Infoblox bereitgestellt werden, mit anderen, die im Handel, von Regierungs- oder Industriequellen, Open Source oder Ihren eigenen internen TI-Datensätzen verfügbar sind. Dank der Automatisierungsfunktionen und der Unterstützung einer Vielzahl von Dateiformaten kann TIDE Kunden bei der Erfassung und Verteilung der richtigen Mischung von Threat Intelligence an verschiedene Tools in ihrem Ökosystem helfen, darunter Firewalls, SIEM, SWG, SOAR, Schwachstellen-Scanner und mehr.

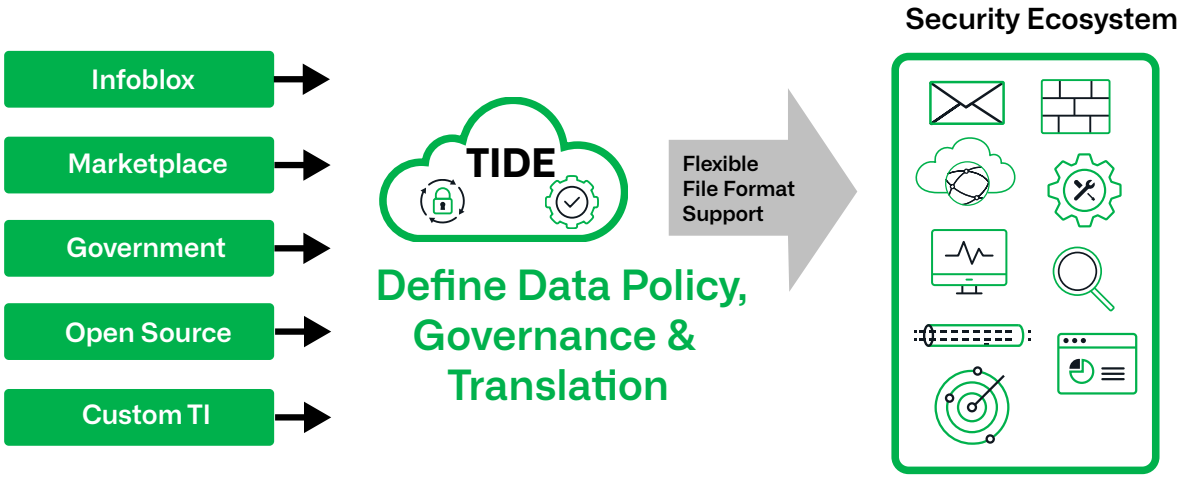

Abbildung 1: TIDE erleichtert den Austausch von Threat Intelligence im gesamten Sicherheitsökosystem, stärkt die Abwehr und verbessert die Berichterstattung.

NUR EINE DER VIELEN WERTVOLLEN FUNKTIONEN VON BLOXONE THREAT DEFENSE

TIDE ist eine von mehreren Funktionen, die BloxOne Threat Defense ausmachen, eine cloudnative Sicherheitslösung zum Schutz vor moderner Malware, Ransomware, C&C-Kommunikation, Datenexfiltration und anderen komplexen Bedrohungen, die DNS als erste Verteidigungslinie einbeziehen. Die Lösung enthält Funktionen, die den gesamten Sicherheits-Stack aufwerten und den SecOps-Bereich effizienter machen, z. B. indem sie die Untersuchung von Bedrohungen beschleunigen und schneller und zuverlässiger auf Bedrohungen reagieren können. Es ist die branchenweit erste Sicherheitslösung für unsere moderne hybride Realität, die überall einen durchgängigen Schutz für alle Geräte im Netzwerk bietet, einschließlich BYOD und IOT/OT.

OPTIMIEREN SIE DIE BEDROHUNGSSUCHE, -UNTERSUCHUNG UND -REAKTION

BloxOne Threat Defense Advanced bietet eine weitere Funktion, mit der Analysten auf die gesamte Bandbreite der Threat Intelligence in einer einzigen Ansicht namens Dossier zugreifen und darin navigieren können. Dossier bietet bei Bedarf Zugriff auf den Schweregrad der Bedrohung, WHOIS-Daten, MITRE ATT&CK-Anleitungen, Dateimuster, zugehörige IPs/URLs/Domains, den Hintergrund der Bedrohungsakteure, Zeitpläne für die Aktivitäten und mehr. Dadurch sind Analysten in der Lage, sich anhand der Daten und ihrer Erfahrung dorthin zu bewegen, wo sie gebraucht werden, um schneller zu verlässlichen Schlussfolgerungen zu gelangen.

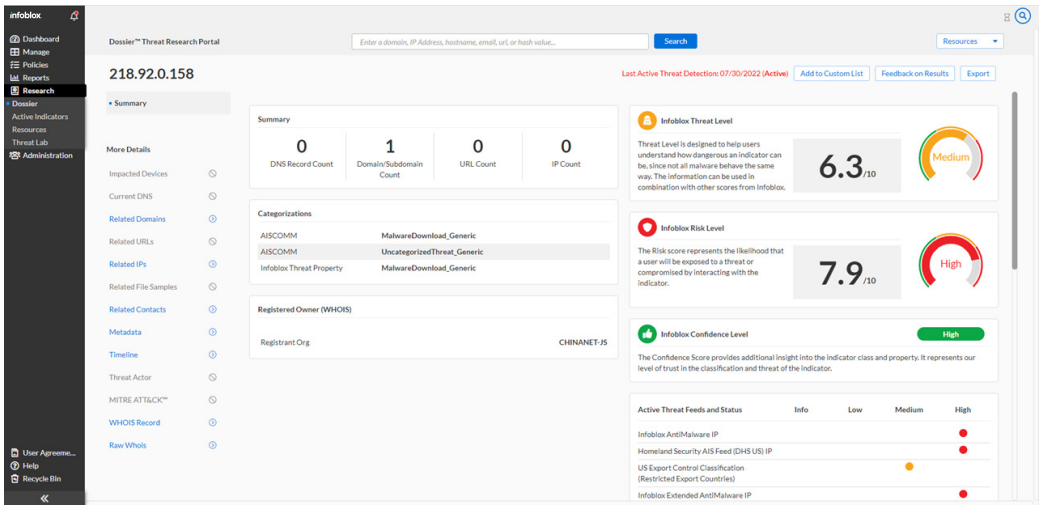

Abbildung 2: Das Dossier-Dashboard mit der Möglichkeit, bei Bedarf genauer zu analysieren und gezielt zu reagieren.

SOFORT EINSATZBEREITE INTEGRATIONEN: THREAT-FEEDS VON DRITTANBIETERN

Während die TIDE-Funktion von BloxOne Threat Defense den Prozess der Integration fast aller Bedrohungsdaten vereinfachen und automatisieren und an fast jedes Sicherheitstool weiterleiten kann, haben einige Partner mit Infoblox zusammengearbeitet, um den Onboarding-Prozess eines Kunden zu vereinfachen.

Die folgenden Partner bieten sofortige Unterstützung für die TIDE-Funktion:

CrowdStrike: Dies ist ein führender Anbieter von Endpunktschutz, Bedrohungsdaten und Dienstleistungen der nächsten Generation. CrowdStrike Falcon Hostname und IP Intelligence ermöglicht es Kunden, Schäden durch gezielte Angriffe zu verhindern, fortschrittliche Malware und gegnerische Aktivitäten in Echtzeit zu erkennen und zuzuordnen und mühelos alle Endpunkte zu durchsuchen, was die Reaktionszeit auf Vorfälle insgesamt verkürzt. Kunden müssen den CrowdStrike-Feed direkt von CrowdStrike erwerben, wobei Infoblox ihnen bei der Aktivierung des Feeds auf der TIDE-Plattform helfen kann.

FireEye iSIGHT Threat Intelligence: Die IP- und Hostnamen-Cyber-Threat-Intelligence dieses Partners stattet Unternehmen mit strategischen, operativen und taktischen Analysen aus, die von seinem globalen Expertenteam erstellt werden. Ein ThreatScape-Abonnement liefert die Informationen, die notwendig sind, um ein Sicherheitsprogramm mit den Zielen des Unternehmensrisikomanagements in Einklang zu bringen und sich proaktiv gegen neue und aufkommende Cyber-Bedrohungen zu schützen.Obwohl Kunden den iSight-Feed direkt von FireEye kaufen müssen, kann Infoblox dabei helfen, den Feed in der TIDE-Plattform zu „aktivieren“.

Darüber hinaus können Abonnenten von BloxOne Threat Defense Advanced die folgenden Feeds von Drittanbietern (erfordert ein zusätzliches Abonnement) im RPZ-Format (ohne zusätzliche Kosten) nutzen, um ihre Bedrohungsabdeckung auf der DNS-Steuerungsebene zu erhöhen:

Farsight Security Newly Observed Domains (NOD) Feed: Dieser Feed bietet eine zusätzliche Verteidigungsebene zum Schutz vor Malware-Exfiltration, Markenmissbrauch und Spam-basierten Angriffen, die von neu gestarteten Domänen ausgehen oder dort enden.

Proofpoint Emerging Threats (ET) IP und Domain Reputation Feed: Dieser Feed liefert verwertbare IP- und Domain-Reputationseinträge, die auf der Grundlage von Beobachtungen des Verhaltens von Bedrohungsakteuren in der Praxis und direkten Beobachtungen der ET-Labore von Proofpoint bewertet werden. Proofpoint ET Intelligence basiert auf einem proprietären Prozess, der eine der weltweit größten aktiven Malware-Börsen, Opferemulation in großem Maßstab, originelle Erkennungstechnologien und ein globales Sensornetzwerk nutzt und wird in Echtzeit aktualisiert, um Unternehmen mit verwertbaren Informationen zu versorgen, mit denen sie die heutigen aufkommenden Bedrohungen bekämpfen können.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1.408.986.4000
www.infoblox.com

Version: 20231030v1