infoblox

DIE 7 WICHTIGSTEN GRÜNDE, WARUM DNS MTTRs FÜR SICHERHEITSPROFIS

DNS ist nicht mehr nur für Netzwerke.
DNS wird als erste Verteidigungslinie immer wichtiger, um Ihre wachsende Netzwerkinfrastruktur zu schützen und Ihre Mean Time To Respond (MTTR) zu reduzieren.

SIE STEHEN VOR KRITISCHEN SICHERHEITSHERAUSFORDERUNGEN:

Expanding attack surface
Da die Anforderungen an WFA und Multi-Clouds steigen, gibt es immer mehr Möglichkeiten für Malware, C2, Lookalikes und andere Bedrohungen, die aktuellen Schutzmaßnahmen zu umgehen.

Blinde Flecken bei Benutzern und Geräten
Sicherheit bietet keine einheitliche Echtzeitansicht aller Netzwerkbenutzer und -geräte, einschließlich Multi-Cloud und IoT/OT.

Mangelnde wichtige Ressourcen
Der Mangel an Sicherheitskompetenzen und die daraus resultierende Belastung für SecOps führen dazu, dass kritische Warnungen täglich übersehen werden oder auf wöchentlicher Basis.

Langsame Untersuchung und Remediation
Ein verzögerter Zugriff auf Benutzer- und Geräteforensik führt zu Engpässen bei Untersuchungen und verlängert die Verweildauer von Bedrohungen, wodurch Ihr Unternehmen größerem Schaden ausgesetzt ist.

4 MIO. $
Durchschnittliche Kosten einer Datenschutzverletzung

ÜBER 270
Stunden im Durchschnitt, um Bedrohungen zu identifizieren und einzudämmen

92%
der Malware nutzt DNS für Befehl und Kontrolle

WIE DNS-ERKENNUNG UND REAKTION VON INFOBLOX IHNEN HILFT, DIESE UND WEITERE HERAUSFORDERUNGEN ZU LÖSEN:

1. **Erkennen Sie Bedrohungen früher**
Zuordnen von DNS-Abfragen zu Benutzer und Gerät Aktivität in Echtzeit mit IPAM DNS-basierte Anwendungserkennung.

2. **Stoppen Sie Angriffe schneller**
Nutzen Sie erweiterte Bedrohungsinformationen, um Phishing, Ransomware, Malware, C2, DGA, Data Exfil und andere früher zu blockieren.

3. **Schützen Sie Systeme überall**
Schützen Sie Ihre expandierende Angriffs- Oberfläche durch Verteidigung über Clouds hinweg und am Edge, einschließlich IoT/OT.

4. **Blockieren Sie aufkommende Bedrohungen**
Nutzen Sie die globale Bedrohungssuche, um neue verdächtige Domains zu erkennen und sie bis zu 3 Monate früher zu blockieren.

5. **Lookalikes abschalten**
Verwenden Sie KI/ML-Analysen für DNS-Abfragen um DGAs, Datenexporte und anspruchsvolle Lookalike-Domains schneller zu erkennen.

6. **Automatisieren Sie den Sicherheits-ROI**
Automatisieren Sie Ökosystemintegrationen, um DNS-Daten mit SOC-Tools zu teilen und SecOps zu ermöglichen, Warnmeldungen besser zu priorisieren und den Aufwand zu minimieren.

7. **Verwenden Sie weniger Ressourcen**
Vereinen Sie Netzwerk- und Sicherheitsinformationen, um Bedrohungen früher zu erkennen und zu stoppen, und es SecOps zu ermöglichen, mit weniger Aufwand mehr zu erreichen.

DNS MTTRs

Erfahren Sie mehr darüber, wie DNS-Erkennung und -Reaktion
zu enormen wirtschaftlichen Vorteilen führt, durch die Verbesserung Ihrer proaktiven Sicherheit und der Beschleunigung der Mean Time To Response in Ihrem gesamten Unternehmen.

Lesen Sie heute den Forrester Total Economic Impact™ Bericht