infoblox.

7 RAISONS MAJEURES POURQUOI LES DNS MTTR SONT CLÉS POUR LES EXPERTS EN SÉCURITÉ

Le DNS ne se limite plus au réseau.
Le DNS est de plus en plus indispensable comme première ligne de défense pour sécuriser votre infrastructure réseau en expansion et pour réduire votre temps moyen de réponse (MTTR).

FAIRE FACE À DE GRAVES PROBLÈMES DE SÉCURITÉ :

Élargir la surface d'attaque
Avec l'augmentation des demandes en télétravail et en multi-cloud, les possibilités pour les malwares, les commandes et contrôles (C2) et autres menaces de contourner les systèmes de sécurité actuels deviennent de plus en plus nombreuses.

Les zones d'ombre des utilisateurs et des appareils
La sécurité manque d'une vue unifiée et en temps réel de tous les utilisateurs et appareils du réseau, y compris le multicloud et l'IoT/OT.

Un manque de ressources essentielles
Le manque de compétences en matière de sécurité et le fardeau qui en résulte pour les SecOps se traduisent par des alertes critiques manquées chaque jour ou chaque semaine.

Des enquêtes et résolutions lentes
L'accès tardif à l'historique des utilisateurs et des appareils entrave les investigations et prolonge la portée des menaces, exposant ainsi votre entreprise à des risques accrus.

4 MILLIONS DE DOLLARS
est le coût moyen d'une violation de données

+ DE 270
heures en moyenne à identifier et contenir les menaces

92 %
des malwares exploitent le DNS pour commander et contrôler

COMMENT LA DÉTECTION ET LA RÉPONSE DNS AIDE À RELEVER CES DÉFIS ET PLUS ENCORE :

1. **Identifier les menaces plus rapidement**
Associez les requêtes DNS à l'activité de l'utilisateur et de l'appareil en temps réel grâce à la découverte d'applications basée sur le DNS IPAM.

2. **Arrêter les attaques plus rapidement**
Utilisez la threat intelligence pour bloquer les phishing, les ransomwares, les malwares, les C2, les DGA, l'exfiltration de données et d'autres menaces plus tôt.

3. **Protéger vos systèmes où que vous soyez**
Protégez votre surface d'attaque en pleine expansion en vous défendant sur tous les clouds et à la périphérie, y compris dans l'IoT/OT.

4. **Contrer les menaces émergentes**
Utilisez la détection mondiale des menaces pour détecter et neutraliser les domaines suspects émergents jusqu'à 3 mois plus tôt.

5. **Bloquer les domaines similaires**
Utilisez les analyses IA/ML sur les requêtes DNS pour détecter plus rapidement les DGA, les exfiltrations de données et les domaines similaires sophistiqués.

6. **Automatiser le ROI lié à la sécurité**
Automatisez les intégrations de l'écosystème pour partager les données DNS avec les outils SOC et permettre aux SecOps de mieux prioriser les alertes et minimiser les efforts.

7. **Utiliser moins de ressources**
Unifiez les informations relatives au réseau et à la sécurité afin de détecter et de contrer les menaces plus rapidement, et de permettre aux SecOps d'en faire plus avec moins.

LES DNS MTTR

En savoir plus sur Infoblox : La détection et la réponse DNS
génèrent d'énormes avantages économiques en améliorant votre sécurité proactive et en accélérant le temps moyen de réponse dans toute votre entreprise.

Lire aujourd'hui l'étude Forrester Total