NOTE DE SOLUTION

SOC INSIGHTS

Appliquer l'analyse pilotée par l'IA pour transformer de vastes quantités de données d'événements, de réseaux, d'écosystèmes et d'intelligence DNS en informations exploitables afin d'optimiser l'efficacité des opérations de sécurité (SecOps)

LES OBSTACLES À L'EFFICACITÉ SECOPS

Comme pour d'autres fonctions des entreprises ou des organisations gouvernementales aujourd'hui, le SOC moderne s'efforce d'en faire plus avec les ressources disponibles. Selon l'enquête SANS 2023 sur les SOC[1], 80 % des 10 principaux obstacles à l'utilisation complète des capacités des SOC se répartissent en trois catégories principales :

- La compréhension et la gestion des alertes
- L'intégration ou l'automatisation limitée entre les outils
- L'exécution des tâches clés avec le personnel et les compétences disponibles

Mais la statistique la plus tragique est peut-être que tous ces obstacles constituent un défi pour le SOC depuis plus d'une décennie. Les améliorations progressives, dues à la simple hiérarchisation automatique des incidents en fonction des classements des malwares et d'autres filtres de base, n'ont pas été en mesure de suivre le rythme de la croissance des alertes et d'autres événements pouvant nécessiter l'attention des analystes SOC. Les choses n'ont donc fait qu'empirer.

LES SOC INSIGHTS PILOTÉS PAR L'IA

Les menaces persistantes modernes reposent sur une infrastructure d'attaquant flexible et des systèmes de commande et contrôle (C2) dynamiques pour héberger et déployer les nombreux outils de pentest, d'exploitation, de chiffrement et autres utilisés même dans une seule attaque. Cela les rend extrêmement dépendants du DNS et met en évidence une faiblesse clé que les défenseurs peuvent exploiter pour détecter et perturber ces menaces.

Le DNS voit les activités légitimes et malwares indépendamment du protocole, de la plateforme, du système d'exploitation, de l'application ou même de l'emplacement. Grâce à cette visibilité unique, un programme pilote mené par le directeur de la direction de la cybersécurité de la NSA a révélé que la sécurisation du DNS pouvait réduire les attaques de malware de 92 %[2] !

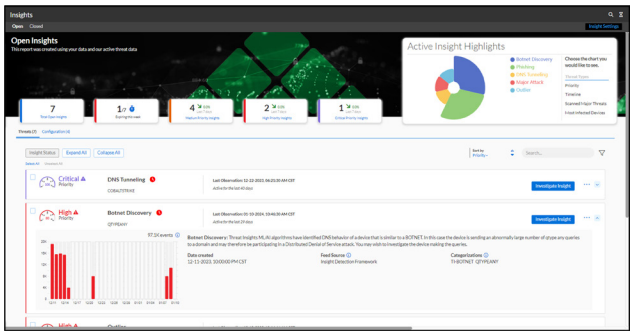

Figure 1 : La page de résumé des Insights SOC offre aux analystes un accès, en un clic, à l'essentiel.

DES FAITS ET DES CHIFFRES

- 60 % des analystes SOC déclarent que leur **charge de travail augmente** et 65 % sont **susceptibles de changer d'emploi** au cours de l'année à venir[4].
- 55 % des personnes interrogées ont déclaré que **des alertes critiques sont souvent manquées** chaque semaine et même chaque jour[5].
- 64 % des analystes déclarent qu'ils **consacrent plus de la moitié de leur temps aux tâches manuelles**[6].
- La mauvaise configuration est l'un des **trois principaux facteurs de violations liées à des erreurs**[3].
- 8 des 10 principaux **obstacles à l'utilisation complète du SOC** sont liés aux alertes, à l'intégration des outils et à la pénurie de compétences[1]
- 77 % des chefs d'entreprise s'inquiètent du **manque de compétences clés**[7].
- **92 % des malwares et des activités C2 peuvent être contrôlés au niveau** de la couche DNS grâce à la bonne intelligence et visibilité DNS[2].

SOC Insights travaille avec la solution DNS Detection and Response (DNSDR) d'Infoblox, BloxOne Threat Defense, pour offrir des analyses uniques basées sur l'IA afin de détecter des activités de menaces inconnues que d'autres outils ratent, d'augmenter l'efficacité du SOC et d'améliorer le retour sur investissement global des investissements actuels en matière de sécurité.

LA RÉSOLUTION DE MULTIPLES PROBLÈMES GRÂCE À UNE GAMME D'INSIGHTS

Les enquêtes menées après un incident ou une violation révèlent souvent que les premiers indicateurs d'activité malveillante n'ont pas été détectés en raison de mauvaises configurations, de problèmes d'intégration des outils de sécurité ou d'une simple surcharge d'alertes. SOC Insights utilise des analyses pilotées par l'IA sur un vaste volume de données pour aider à gérer ces risques.

La sécurité d'Insights

Le module complémentaire de sécurité de SOC Insights est disponible pour BloxOne Threat Defense « Business Cloud » ou « Advanced ». Il utilise l'IA pour transformer une vaste quantité de données sur les événements, les réseaux, les écosystèmes et le DNS en un ensemble d'informations de sécurité exploitables et gérables.

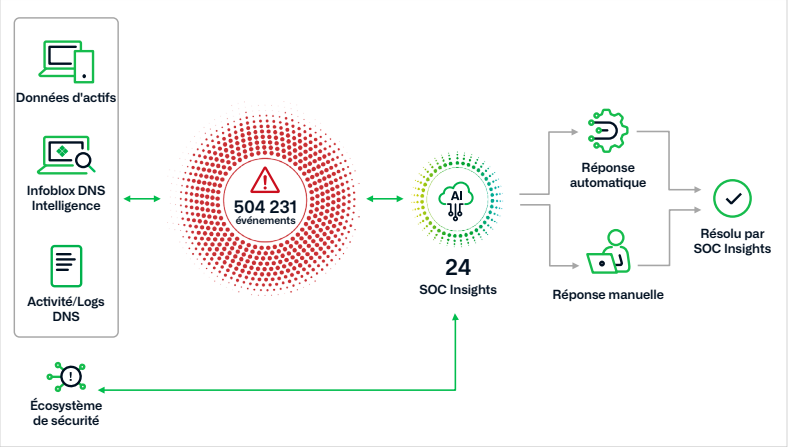

Figure 2 : SOC Insights réduit la surcharge d'alertes en transformant une multitude d'événements en informations significatives et exploitables

- Zero Day DNS™
- Menace persistante
- Propagation active de la menace
- Attaque majeure
- Découverte de botnet
- Communication hors norme
- Phishing
- Malware
- Résolveur DNS ouvert
- DNS Tunneling
- Activité de perte de données
- Attaque ciblée
- Erreurs DNS excessives
- Domaine similaire surveillé

La configuration d'Insights

La fonctionnalité de configuration de SOC Insights est incluse avec BloxOne Threat Defense « Business Cloud » et « Advanced » pour aider les utilisateurs à maximiser l'utilisation des meilleures pratiques actuelles et à éviter les erreurs courantes. Regardez les vidéos et autres guides pour vous aider à corriger les erreurs et les failles, ou désactivez les alertes inutiles pour les exceptions autorisées.

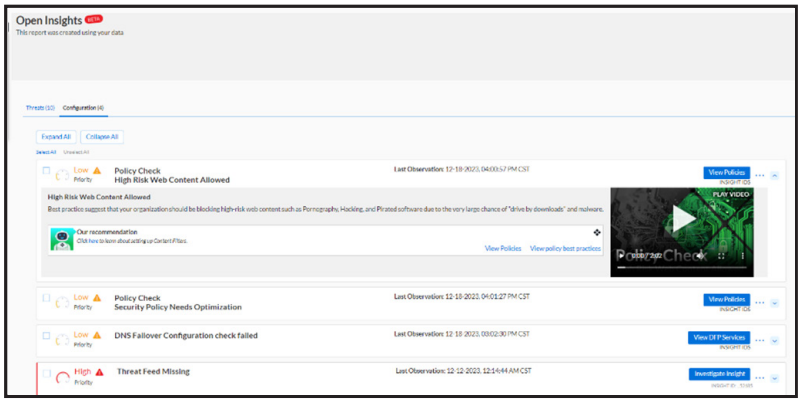

Figure 3 : Identification proactive des erreurs de configuration mineures ou critiques afin de garantir des capacités optimales de défense, d'investigation et de réponse.

- Flux de menaces DNS manquant
- Clé gratuite VirusTotal manquante
- Politique de sécurité à optimiser
- Échec de la vérification de basculement DNS
- Incompatibilité des actions de flux
- DFP masquant les détails des actifs
- Politique de sécurité en mode journalisation
- Filtres de contenu Web désactivés
- Contenu Web à haut risque autorisé

UN IMPACT FINANCIER, OPÉRATIONNEL ET COMMERCIAL POSITIF

Alors que la plupart des outils de sécurité ne promettent que « facilité d'utilisation » et « moins de failles », SOC Insights va bien au-delà : il réduit le stress des analystes, diminue leur taux de rotation et résout de nombreux problèmes de sécurité liés à l'expansion, aux fusions et acquisitions, ainsi qu'à d'autres initiatives commerciales. Par exemple :

- La nature du DNS permet d'unifier facilement un nouveau site ou un nouveau partenaire commercial sur une infrastructure DNS commune en quelques minutes plutôt qu'en plusieurs mois.
- La configuration d'Insights est très proactive pour prévenir les violations ou les pertes de données dues à des « mauvaises configurations », l'un des trois principaux facteurs signalés[3].
- L'autocorrélation des activités telles que le « malware », le « phishing », les « botnets » et d'autres menaces « majeures » ou « propagées » permet aux intervenants de traiter plusieurs menaces simultanément, augmentant ainsi leur efficacité.
- Adopter une posture de sécurité plus proactive en surveillant des catégories telles que les« anomalies », le « Tunneling DNS » et les « Résolveurs ouverts », ainsi que les fonctionnalités uniques de visibilité des applications et des imitations de BloxOne Threat Defense.
- L'intégration des informations à l'écosystème de sécurité améliore le retour sur investissement de l'ensemble de la pile de sécurité en fournissant des « informations » exploitables au lieu de se contenter de journaux et d'événements bruts.
- SOC Insights collecte automatiquement les données pertinentes et permet aux analystes de les consulter et de les modifier pour tirer des conclusions plus rapidement et en toute confiance. Cela contribue à réduire le stress et à mieux fidéliser les professionnels de la sécurité compétents et expérimentés.

DES RÉSULTATS INCROYABLES

Les clients signalent des avantages significatifs en utilisant SOC Insights avec BloxOne® Threat Defense, notamment :

- Une réduction des alertes EDR et FW de 50 %
- Une économie en moyenne de 500 heures d'analyste SOC par mois
- Des économies de productivité de 400 000 $ réalisées par an

ÉLEVER SIEM, SOAR ET AUTRES PARTIES DE L'ÉCOSYSTÈME AVEC DES INFORMATIONS

SecOps connaît la valeur et les limites du partage de données brutes dans l'écosystème de sécurité. Cela a fait de l'expertise SIEM et SOAR l'un des ensembles de compétences les plus difficiles à acquérir pour la plupart des organisations. SOC Insights allège la charge de ces autres outils et peut partager les informations qui en résultent au sein de la pile de sécurité afin de rendre les autres outils plus efficaces et d'améliorer encore l'efficacité globale SecOps.

1 "SANS 2023 SOC Survey", juin 2023, par Chris Crowley, Barbara Filkins, John Pescatore

2 "NSA launches pilot program to secure defense contractors", 18 juin 2020, par Lauren C. Williams, NEXTGOV/FCW

3 "Verizon 2023 DBIR Report"

4 Voice of the SOC Analyst

5 The Orca Security 2022 Cloud Security Alert Fatigue Report

6 Voice of the SOC Analyst

7 https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

infoblox.

Infoblox unifie le réseau et la sécurité pour offrir des performances et une protection sans égales. Reconnu par les entreprises listées au classement Fortune 100 et les innovateurs émergents, nous offrons une visibilité et un contrôle en temps réel sur les personnes et les appareils se connectant au réseau d'une organisation afin d'accélérer son fonctionnement et d'arrêter les menaces plus tôt.

Siège social
2390 Mission College Boulevard, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version : 20240411v2