NOTE DE SYNTHÈSE

OPTIMISEZ LA PRODUCTIVITÉ DU SOC AVEC DES ALERTES DE SÉCURITÉ EN TEMPS RÉEL SUR SLACK

Envoyez automatiquement des messages Slack contenant des données de sécurité basées sur le DNS, corrélées et priorisées

Le paysage de la cybersécurité actuel est complexe et en constante évolution. Les cybercriminels ciblent de plus en plus l'infrastructure DNS pour mener des attaques sophistiquées, telles que des campagnes de phishing, la diffusion de malwares ou l'exfiltration de données. Les analystes en sécurité subissent une pression considérable pour identifier et répondre à ces menaces en temps voulu, et ils ne disposent pas des ressources nécessaires pour surveiller et rechercher de manière proactive les multiples applications dont ils sont responsables. Cette pratique, souvent qualifiée de « jeu des chaises musicales », est très inefficace et souligne la nécessité de communiquer et de collaborer à l'aide d'un outil unique et familier, ce qui accélère à la fois le temps moyen de détection (MTTD) et le temps moyen de réponse (MTTR). Pour les entreprises qui ont adopté la puissance de Slack, Infoblox a développé une intégration certifiée conçue pour fournir des notifications de sécurité immédiates et priorisées directement sur Slack, permettant une prise de décision et une action rapides du SOC.

DÉFIS

Les équipes de sécurité sont confrontées à de nombreux défis dans le paysage complexe des menaces actuelles :

- **Surcharge d'alertes :** les analystes de sécurité sont submergés d'alertes incessantes provenant de divers outils de sécurité, ce qui rend difficile l'identification et la hiérarchisation des menaces les plus critiques.
- **Visibilité limitée :** les solutions de sécurité classiques manquent souvent de la capacité d'analyser facilement le contexte et la portée des menaces et de déterminer les étapes suivantes.
- **Des flux de travail inefficaces :** pour enquêter sur les menaces, il est souvent nécessaire de passer d'un outil de sécurité à l'autre, ce qui entraîne une perte de temps et d'efficacité précieux.

TEMPS DE RENTABILITÉ RAPIDE GRÂCE À UNE INTÉGRATION FACILE : INFOBLOX + SLACK

La solution de détection et de réponse DNS (DNSDR) d'Infoblox, BloxOne Threat Defense, enrichie par SOC Insights, exploite automatiquement de grandes quantités de données de Threat Intel DNS et de données d'actifs afin de corréler et de hiérarchiser des réponses exploitables aux menaces. La solution transforme 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 données de sécurité détaillées générées par BloxOne Threat Defense avec SOC Insights comblent les zones d'ombre et améliorent la capacité à comprendre pleinement les attaques basées sur le DNS.

AVANTAGES CLÉS

- **Communication et collaboration centralisées :** recevez automatiquement des notifications d'alertes de sécurité prioritaires directement dans Slack et réduisez la nécessité de surveiller manuellement plusieurs outils.
- **Réponse accélérée :** accélérez la réponse aux incidents grâce à un accès direct au contexte et aux informations sur la menace pour déterminer rapidement les prochaines étapes.
- **Réduction de la fatigue liée aux alertes :** soyez informé uniquement des menaces critiques, réduisant ainsi le bruit et la charge de travail des analystes de sécurité.
- **Retour sur investissement maximisé :** amplifiez la valeur de votre investissement dans Slack en optimisant les flux de travail de sécurité et en réduisant les transitions entre les applications.

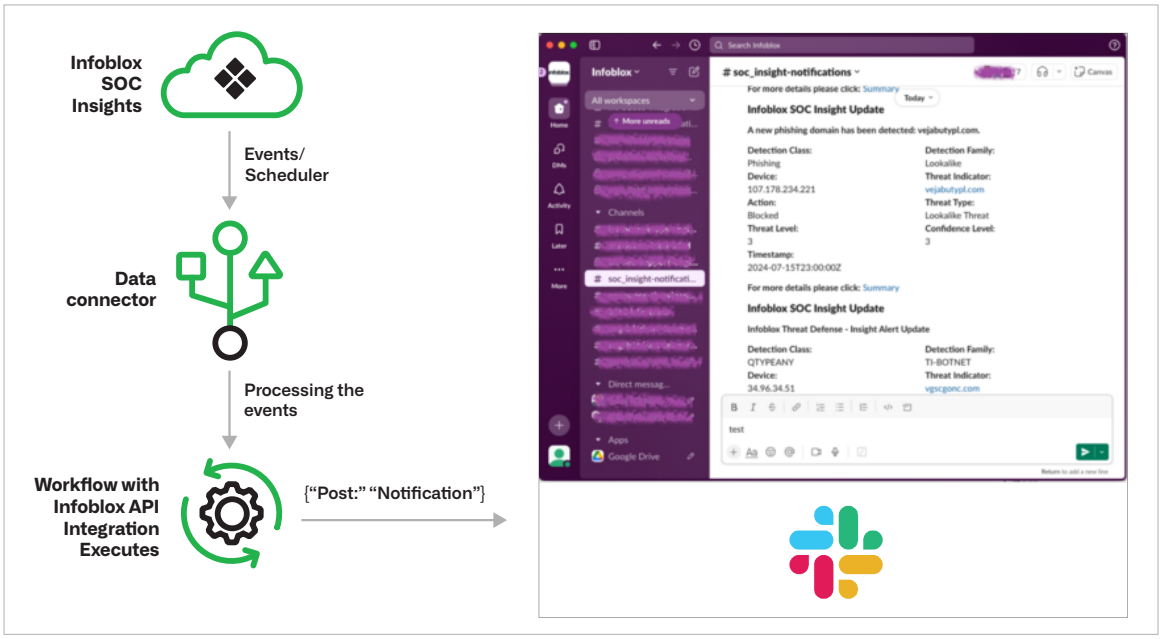
Afin d'améliorer encore l'efficacité globale du SOC, Infoblox propose une intégration low-code à Slack, qui permet de maximiser les avantages de chaque solution et de réduire ainsi le coût total de possession. Cette puissante combinaison optimise la détection et la réponse aux menaces, en fournissant aux équipes de sécurité des notifications immédiates contenant les informations essentielles pour protéger l'entreprise.

Infoblox + Slack permettent aux équipes de sécurité de :

- **Unifier les alertes liées aux menaces :** Infoblox déclenche des messages en temps réel sur Slack pour informer les analystes de sécurité des menaces prioritaires, éliminant ainsi immédiatement le besoin de surveiller manuellement plusieurs outils. Les alertes sont envoyées sur un canal Slack personnalisé, offrant aux analystes une gestion centralisée des alertes, avec un historique complet pour la documentation et le suivi.
- **Simplifier les enquêtes :** les messages Slack générés par Infoblox offrent une visibilité sur les informations essentielles et leur contexte, nécessaires pour prioriser les alertes et collaborer sur les prochaines étapes. Il suffit de cliquer sur le lien intégré au message pour accéder directement au portail Infoblox et approfondir l'analyse.
- **Prendre des mesures décisives :** grâce aux informations et au contexte fournis par Infoblox, les analystes de sécurité peuvent répondre efficacement et rapidement aux menaces les plus critiques et mettre à jour le statut dans le fil de discussion Slack pour tenir l'équipe informée.

En déployant Infoblox pour Slack, les équipes de sécurité peuvent transformer leur stratégie de sécurité en obtenant une vue centralisée des alertes critiques, en rationalisant les investigations et en accélérant leur réponse aux menaces.

COMMENT ÇA FONCTIONNE



MEILLEURES PERFORMANCES SOC GRÂCE À L'INTÉGRATION D'INFOBLOX ET DE SLACK

L'intégration d'Infoblox avec Slack offre une solution de sécurité collaborative qui renforce votre infrastructure existante. Cette synergie garantit :

- **Efficience SOC :** assurez des performances optimales en envoyant immédiatement les alertes de menaces prioritaires vers un canal Slack centralisé. Cela améliore la communication tout en permettant un suivi historique.
- **Efficacité SOC :** donnez aux analystes de sécurité le contenu et le contexte des menaces directement dans l'alerte Slack pour qu'ils puissent prendre rapidement des mesures appropriées.

- **Productivité opérationnelle et ROI :** rationalisez les flux de travail et limitez les changements d'applications peut améliorer l'efficience de votre équipe SecOps, entraînant des économies de temps et de coûts.
- **Simplicité d'intégration :** intégrez facilement grâce à une solution low-code testée et certifiée, accélérant ainsi votre délai de rentabilisation.

CONCLUSION

L'automatisation des workloads de sécurité, la réduction des délais de détection et de réponse, ainsi que le maintien d'une communication et d'une collaboration efficaces en matière de réponse aux menaces constituent des défis majeurs pour les équipes SecOps. L'intégration d'Infoblox avec la messagerie Slack renforce la valeur de l'ensemble de votre pile de sécurité en offrant une plateforme unifiée pour des communications riches en threat intelligence. Cette combinaison augmente la productivité de SecOps, améliore l'efficacité et assure un programme de sécurité plus fiable et réactif. En intégrant Infoblox à Slack, vous renforcez les capacités de sécurité de votre entreprise et maximisez le retour sur vos investissements en sécurité.

infoblox.

Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et les innovateurs émergents, nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

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

+1.408.986.4000
www.infoblox.com

Version : 20240724v1