NOTE DE SYNTHÈSE

# ENRICHISSEZ VOTRE SIEM SPLUNK ET SOAR AVEC INFOBLOX

## Optimisez votre investissement Splunk Enterprise SIEM et SOAR grâce à une visibilité DNS approfondie.

### DÉFIS

Les équipes de sécurité s'appuient sur les outils SIEM et SOAR pour enquêter efficacement et répondre aux événements de sécurité. Face à des attaques toujours plus furtives et difficiles à détecter, les entreprises ont été contraintes de renforcer leurs mesures de surveillance, ce qui nécessite d'intégrer un nombre croissant de journaux dans leurs plateformes de sécurité. Ce processus augmente les besoins en stockage, le nombre d'alertes générées et d'enquêtes menées, ce qui entraîne souvent une surcharge de travail et un épuisement des analystes de sécurité.

Il peut être difficile d'accéder à la threat intelligence et aux données pertinentes sur les appareils et les réseaux, et de les corréler afin d'obtenir des informations utiles à l'enquête et de mettre en place une automatisation efficace. Les playbooks sont limités sans ces informations contextuelles essentielles.

### VALORISATION RAPIDE GRÂCE À UNE INTÉGRATION FACILE

Infoblox, leader des infrastructures DNS et de la sécurité, et Splunk, fournisseur majeur de solutions SIEM et SOAR, proposent des intégrations simples qui améliorent les capacités de chaque solution et optimisent l'efficacité globale des opérations de sécurité.

La plateforme Splunk Cloud et Splunk Enterprise Security fournissent des services cloud hybrides avec des processus proactifs et réactifs pour la consommation de données externes. Sur la base de ces données, ces plateformes permettent aux équipes de sécurité de rechercher, d'analyser, de visualiser et d'agir.

Infoblox BloxOne® Threat Defense avec SOC Insights s'intègre aux solutions Splunk pour fournir des informations uniques et hiérarchisées ainsi que des données liées aux événements grâce à des outils tels que Infoblox Threat Intelligence Data Exchange (TIDE) et Infoblox Dossier. Chaque fonctionnalité peut transmettre à Splunk des données priorisées afin de réduire les besoins de stockage et d'optimiser les enquêtes, l'automatisation ainsi que les autres efforts des analystes de sécurité.

### VISUALISEZ LES DONNÉES DE THREAT INTELLIGENCE D'INFOBLOX DANS SPLUNK ENTERPRISE SECURITY ET SUR LA PLATEFORME CLOUD

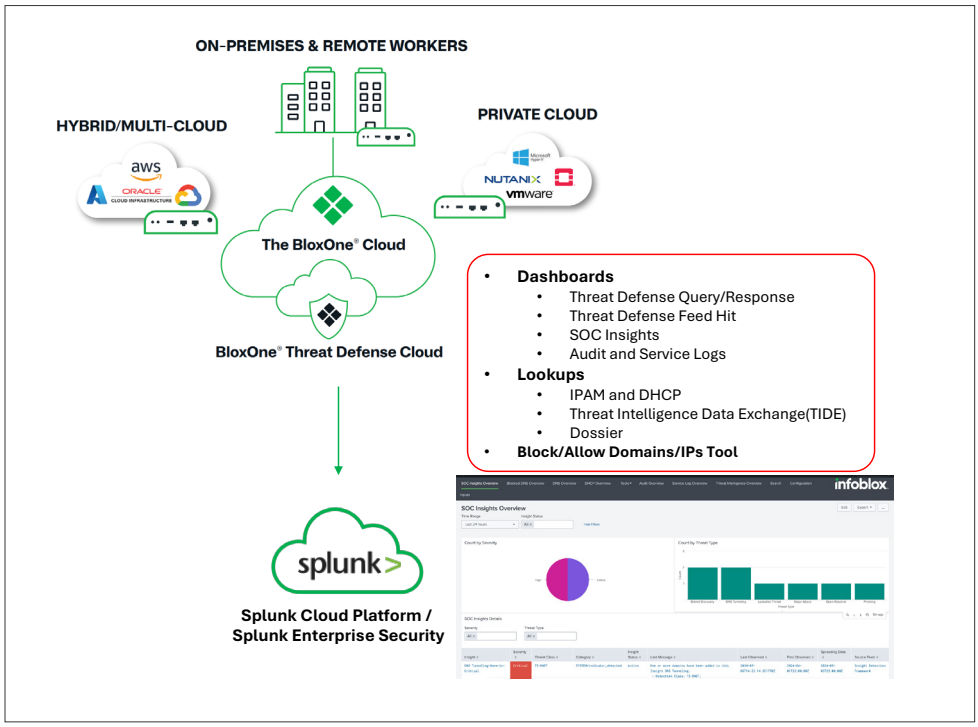
Infoblox TIDE fournit à Splunk des informations de threat intelligence précises et exploitables par des machines afin d'aider les équipes de sécurité à détecter les activités malveillantes et à réduire le temps de latence. Ensemble, la solution intégrée Infoblox et Splunk aide les équipes de sécurité à réduire les temps d'enquête et à accroître la visibilité pour soutenir le réseau hybride moderne.

### FONCTIONNALITÉS CLÉS

L'intégration d'Infoblox avec Splunk Cloud Platform, Splunk Enterprise Security et Splunk SOAR améliore les performances de Splunk et accroît la visibilité des événements et la threat intelligence, ce qui permet d'accélérer les enquêtes et d'apporter des réponses plus efficaces. L'intégration permet aux équipes de sécurité et de réponse aux incidents de mieux exploiter la puissance de SIEM et SOAR sur site ou dans Splunk Cloud Platform en les associant aux événements de sécurité DNS, aux métadonnées IPAM (gestion des adresses IP) et aux informations sur les menaces d'Infoblox.

Les capacités SIEM de Splunk, renforcées par Infoblox TIDE, permettent aux équipes de sécurité de :

- Accéder à des données détaillées sur les appareils et le réseau pour obtenir plus de contexte
- Optimiser les exigences de stockage grâce au filtrage intelligent
- Corréler des données de threat intelligence complètes et hiérarchisées autour des événements




## FONCTIONNALITÉS CLÉS

- Accédez à des données disséminées sur les appareils et le réseau (y compris les domaines, les adresses IP et d'autres données de requête DNS) qui fournissent un contexte inestimable autour des événements pour prendre des décisions éclairées.
- Corrélez les informations de threat intelligence prioritaires et complètes autour des événements afin de fournir aux analystes des informations sur les activités malveillantes et d'accélérer les enquêtes et les réponses.
- Optimisez les exigences de stockage grâce à un filtrage intelligent pour maximiser les performances de Splunk tout en garantissant que les analystes disposent de toutes les données « pertinentes » à la demande.
- Résumez les incidents de sécurité à l'aide d'indicateurs de compromission (IoC) et surveillez l'évolution des menaces au fil du temps en fonction de leur gravité grâce à l'accès aux données Infoblox Dossier.
- Accélérez la réponse en hiérarchisant les événements de sécurité les plus risqués grâce à l'accès à des dizaines de flux de threat intelligence.
- Supervisez l'activité et les tendances des appareils sur l'ensemble de la plateforme grâce à une visibilité consolidée.

## STIMULEZ VOTRE PRODUCTIVITÉ AVEC INFOBLOX DOSSIER

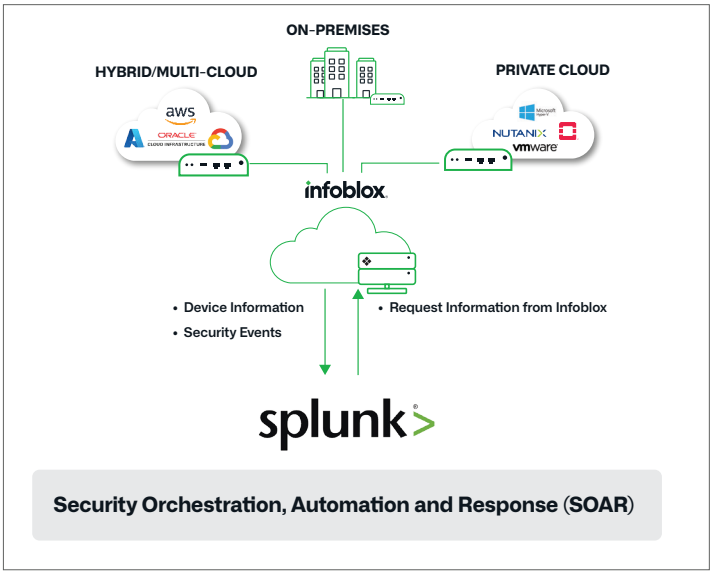
Outre les événements, le contexte et les métadonnées relatives aux appareils et au réseau, Infoblox Dossier donne accès à une threat intelligence très complète. Cela permet aux analystes d'enquêter et d'évaluer les risques, mais aussi de déclencher des réponses automatisées et de renforcer les capacités des playbooks.

Les capacités SOAR de Splunk, renforcées par Infoblox Dossier, permettent aux analystes de sécurité de :

- Accéder directement à Infoblox Threat Intelligence pour détecter les activités malveillantes
- Automatiser une réponse efficace aux menaces avec des métadonnées complètes de l'appareil
- Renforcer les playbooks avec une vision complète des menaces et des informations réseau.

## FONCTIONNALITÉS CLÉS

- Accédez directement aux IoC dans Infoblox Threat Intelligence pour détecter et bloquer les menaces et les activités suspectes
- Automatisez l'isolation efficace des appareils et les réponses aux autres menaces grâce à une visibilité étendue et à des métadonnées des appareils
- Offrez aux administrateurs un accès à des données supplémentaires sur les menaces et les informations réseau pour améliorer vos playbooks SOAR
- Automatisez et accélérez la réponse avec un ensemble complet d'API de threat intelligence
- Accélérez la réponse grâce à une meilleure threat intelligence et en priorisant les événements de sécurité à haut risque




## AVANTAGES GLOBAUX DE L'INTÉGRATION DE SPLUNK ET D'INFOBLOX

- **Efficacité SIEM :** assurez des performances optimales en accédant uniquement aux threat intelligence et aux données réseau pertinentes.
- **Efficacité SOAR** : optimisez vos playbooks grâce à un accès supplémentaire à des données agrégées et sourcées sur la threat intelligence et les dispositifs.
- **Simplicité d'intégration :** profitez facilement des applications Splunk éprouvées pour accélérer le délai de rentabilité.
- **Productivité SecOps :** améliorez la visibilité et offrez des capacités de filtrage avancées, améliorant ainsi l'efficacité des équipes SecOps.
- **Retour sur investissement :** maximisez votre investissement dans SIEM et SOAR en plus des avantages uniques en matière de sécurité de BloxOne Threat Defense.

## CONCLUSION

Les équipes SecOps ont des difficultés à gérer les charges de travail, à maîtriser les coûts de stockage et à se tenir à jour avec tous les outils existants pour enquêter et répondre aux événements de sécurité. L'intégration de Splunk Enterprise SIEM et SOAR avec des threat intelligence et métadonnées sur les appareils et le réseau améliore l'efficacité de ces outils ainsi que celle de vos équipes de sécurité. Infoblox avec Splunk accroît la valeur de l'ensemble de votre pile de sécurité, améliore la productivité et l'efficacité des équipes SecOps, et rend votre programme de sécurité global plus fiable et réactif.

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 : 20240724v4