NOTE DE SYNTHÈSE

ENRICHISSEZ VOTRE SIEM QRADAR AVEC INFOBLOX DDI ET BLOXONE THREAT DEFENSE

Découvrez davantage avec votre solution IBM Security QRadar grâce à une visibilité DNS inégalée d'Infoblox

Le secteur de la sécurité 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 malware et l'exfiltration de données. Les analystes en sécurité subissent une pression considérable pour identifier et répondre à ces menaces dans les meilleurs délais. Cependant, les solutions classiques de gestion des informations et des événements de sécurité (SIEM) manquent souvent du niveau d'intégration nécessaire avec les données de sécurité DNS pour mener des enquêtes et apporter des réponses efficaces.

DÉFIS

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

- **Une surcharge d'alertes :** les analystes de sécurité sont submergés par un flux constant d'alertes provenant de divers outils de sécurité, ce qui complique l'identification et la priorisation des menaces les plus critiques.
- **Une visibilité limitée :** les solutions SIEM classiques manquent souvent de moyens pour capturer et analyser les données de sécurité riches générées par l'infrastructure Infoblox DDI et BloxOne Threat Defense. Cela crée des zones d'ombre et empêche de cerner pleinement les attaques basées sur le DNS.
- **Des flux de travail inefficaces :** l'investigation des menaces nécessite souvent de passer d'un outil de sécurité à un autre, entraînant ainsi une perte de temps et d'efforts précieux.

RAPIDITÉ DE LA MISE EN VALEUR GRÂCE À UNE INTÉGRATION FACILE

Infoblox, leader dans le domaine de la gestion DNS, DHCP et des adresses IP (DDI) ainsi que de la sécurité DNS, s'associe à IBM Security QRadar, fournisseur de premier plan de solutions SIEM et SOAR, pour offrir une intégration facile qui améliore les capacités de chaque solution et optimise l'efficacité globale des SecOps. Cette combinaison puissante renforce les capacités de détection et de réponse aux menaces, fournissant à votre équipe de sécurité les informations essentielles nécessaires pour protéger votre entreprise plus efficacement.

Cette combinaison puissante permet aux équipes de sécurité de :

- **Simplifier les enquêtes :** optimisez vos workflows de sécurité grâce aux tableaux de bord prédéfinis et des actions utilisateur au sein de QRadar. Ces fonctionnalités offrent un accès rapide aux informations essentielles sur l'activité DNS, la threat intelligence et les données réseau contextuelles, réduisant ainsi le temps nécessaire pour enquêter sur les incidents et y répondre.

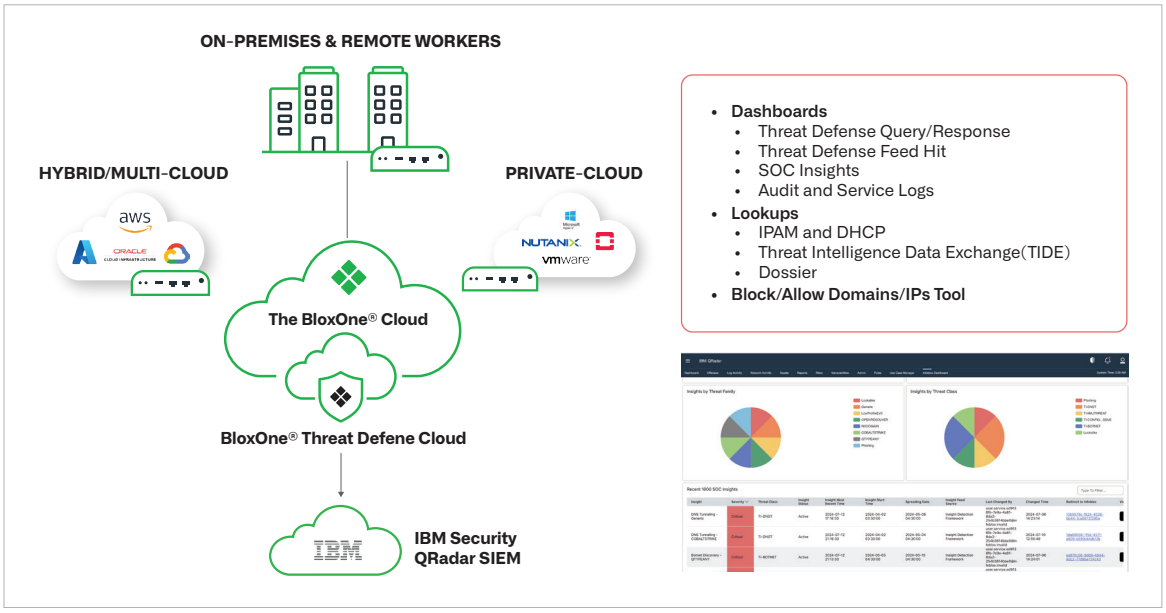
AVANTAGES CLÉS

- **Visibilité renforcée :** Obtenez une visibilité approfondie sur les activités DNS, DHCP et IPAM de votre réseau, pour un contrôle complet.
- **Réponse rapide :** Accélérez la réponse aux incidents grâce à un accès direct à la threat intelligence d'Infoblox et aux données contextuelles depuis QRadar.
- **Réduction de la fatigue liée aux alertes :** Concentrez-vous sur les menaces critiques en filtrant les alertes non essentielles, allégeant ainsi la charge de travail de vos analystes de sécurité.
- **ROI optimisé :** Maximisez la valeur de votre investissement QRadar en exploitant la threat intelligence avancée d'Infoblox.

- **Unifier la Threat Intelligence :** bénéficiez d'une vue complète de l'activité de votre réseau en corrélant les données Infoblox, telles que les événements DNS, les concessions DHCP, les journaux d'audit et les flux de threat intelligence, avec d'autres événements de sécurité collectés par QRadar. Cette vue globale permet aux analystes d'identifier et de comprendre l'étendue des menaces potentielles.
- **Prendre des mesures décisives :** donnez à vos analystes en sécurité la possibilité d'agir immédiatement contre les menaces directement depuis QRadar. L'application Infoblox permet de bloquer les domaines et les adresses IP malveillants en un seul clic, minimisant ainsi les dommages potentiels causés par une attaque.

En déployant l'application Infoblox pour QRadar, les équipes de sécurité peuvent optimiser leur stratégie en obtenant une vue centralisée des activités réseau, en simplifiant les investigations et en accélérant leur réponse aux menaces.

FONCTIONNALITÉS CLÉS



Configuration de l'application

- **Configuration fluide :** une configuration simple dans QRadar pour se connecter aux services de sécurité avancés d'Infoblox.

Tableaux de bord

- **Aperçu des événements DNS :** fournit une visualisation claire des activités DNS, facilitant l'identification rapide des menaces potentielles.
- **Aperçu des concessions DHCP :** surveille les attributions DHCP afin de détecter les comportements inhabituels et les problèmes de sécurité potentiels.
- **Aperçu des journaux d'audit :** suit les modifications de configuration du réseau, garantissant ainsi la conformité et la sécurité.
- **Aperçu des requêtes DNS bloquées :** analyse les requêtes bloquées pour prévenir et répondre aux menaces.
- **Aperçu des SOC Insights :** résume les informations et alertes de sécurité critiques.

Actions utilisateur

- **Recherche Dossier :** enquêtez rapidement sur les domaines, les adresses IP et d'autres indicateurs de compromission avec Infoblox Dossier.
- **Recherche TIDE :** accédez à des threat intelligence détaillées pour prendre des décisions de sécurité éclairées.

- **Recherche IPAM :** récupérez les données d'adresse IP pour corréler les activités réseau avec les menaces potentielles.
- **Recherche des concessions DHCP :** suivez les activités des appareils grâce aux enregistrements des concessions DHCP.
- **Blocage de domaines/IP :** bloquez ou autorisez directement des domaines et des IP dans QRadarpour optimiser l'atténuation des menaces.

L'application Infoblox pour QRadar renforce vos opérations de sécurité avec une visibilité avancée, des temps de réponse améliorés et une efficacité accrue, garantissant ainsi une meilleure protection de votre entreprises contre les menaces émergentes.

INTÉGRATION GLOBALE DE QRADAR ET INFOBLOX

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

- **L'efficacité du SIEM :** assurez des performances optimales en accédant uniquement aux threat intelligence et aux données réseau pertinentes.
- **L'efficacité de SOAR :** renforcez l'orchestration et l'automatisation de votre sécurité avec des données enrichies et des capacités de filtrage avancées.
- **La simplicité d'intégration :** une intégration rapide et facile à l'aide de méthodes éprouvées accélère le délai de rentabilisation.
- **La productivité opérationnelle :** améliorez l'efficacité de vos opérations de sécurité en fournissant des capacités avancées de visibilité et de filtrage.
- **Le retour sur investissement :** optimisez le rendement de vos investissements SIEM et SOAR grâce aux avantages supplémentaires de BloxOne Threat Defense en matière de sécurité.

CONCLUSION

La gestion des charges de travail de sécurité, le contrôle des coûts de stockage et le maintien d'une réponse efficace aux menaces représentent des défis majeurs pour les équipes SecOps. L'intégration d'Infoblox avec QRadar augmente la valeur de votre pile de sécurité en fournissant une threat intelligence enrichie et des données réseau complètes. Cette combinaison accroît la productivité de SecOps, améliore l'efficacité et assure un programme de sécurité plus fiable et réactif. En tirant parti de l'application Infoblox pour QRadar, vous améliorez les capacités de sécurité de votre entreprise et optimisez le retour sur vos investissements en matière de sécurité.

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

+1.408.986.4000
www.infoblox.com

Version : 20240703v1