SKYBOX VULNERABILITY CONTROL

GESTION DES VULNÉRABILITÉS CENTRÉE SUR LES MENACES

Fiche technique

Skybox® Vulnerability Control adopte une approche systématique unique en son genre axée sur la gestion des vulnérabilités. Notre solution repose sur une visibilité totale de votre surface d'attaque. Elle utilise son contexte pour évaluer, hiérarchiser et corriger rapidement les vulnérabilités présentant les risques les importants.

- Centraliser et améliorer les processus de gestion des vulnérabilités, de leur découverte à leur hiérarchisation et correction
- Exploiter les données de la sévérité des vulnérabilités et des actifs, ainsi que la topologie de réseau et les contrôles de sécurité
- Utiliser la modélisation des réseaux et la simulation d'attaques pour identifier les vulnérabilités exposées
- Obtenir davantage de données relatives aux vulnérabilités avec des informations sur l'environnement actuel des menaces
- Connaître les meilleures mesures correctives à votre disposition, y compris les correctifs, les signatures IPS et les modifications basées sur le réseau

« Nous pouvons conduire des opérations pour atténuer uniquement les vulnérabilités les plus critiques — celles qui nécessitent une attention immédiate. Il est vital que l'agence puisse percevoir les risques d'un point de vue opérationnel et commercial, et nous devions savoir si des vulnérabilités faibles ou moyennes créaient en réalité plus de risques que ce que l'agence avait bien voulu reconnaître. »

— Responsable de programme, équipe USAID ISSO

De nouvelles vulnérabilités apparaissent quotidiennement sur votre réseau. L'environnement des menaces est en constante évolution. Vous devez vous assurer que vos efforts se concentrent sur la réponse aux vulnérabilités présentant les risques les plus importants avant que les attaquants ne les découvrent.

Vulnerability Control utilise la visibilité du réseau et de la couche d'actifs, ainsi que des informations sur l'environnement actuel des menaces pour repérer les vulnérabilités exposées et celles les plus exploitables dans le monde. Skybox rend les informations disponibles en un clic à l'aide de la collecte, la modélisation, la simulation et l'analyse de données automatisées qui vous permettent d'être proactif et de fournir la meilleure réponse dans un délai bien moindre que celui des approches manuelles.

PROCESSUS TCVM

1. Recueillir des données concernant les actifs, l'infrastructure et la configuration ; les corréler avec le flux d'informations de Skybox pour déceler les vulnérabilités sans attendre les résultats d'une analyse
2. Corréler les informations relatives aux menaces sur les exploits disponibles et actifs avec vos vulnérabilités
3. Utiliser le modèle de réseau et la simulation d'attaques Skybox pour identifier les vulnérabilités exposées
4. Répondre aux menaces imminentes par l'intermédiaire de correctifs ou de modifications basées sur le réseau ; surveiller les vulnérabilités restantes pour les modifications d'exposition et d'exploitation
5. Effectuer un suivi et rendre compte de l'efficacité des mesures correctives

Vulnerability Control et TCVM Skybox

Vulnerability Control est au cœur de la technologie unique de gestion des vulnérabilités centrée sur les menaces (TCVM) Skybox.

Le processus TCVM commence avec des données à jour sur les vulnérabilités. Skybox utilise un large éventail de sources, y compris des systèmes de gestion des actifs et des correctifs, ainsi que des périphériques réseau pour évaluer les vulnérabilités sans analyse. De plus, nous recueillons, centralisons et fusionnons les données provenant de plusieurs analyses afin de vous fournir à la demande les évaluations de vulnérabilité les plus précises — pour des réseaux sur site, multicloud et de technologie opérationnelle (TO).

Nous intégrons un contexte aux données relatives aux vulnérabilités grâce à notre flux d'informations, en mettant à disposition des renseignements sur les détails des vulnérabilités, les menaces et les options de mesures correctives fournis par Skybox® Research Lab. Les données sont corrélées à un modèle de topologie de votre réseau hybride, aux contrôles de sécurité et aux actifs afin de fournir un contexte plus détaillé.

Avec ce modèle et nos capacités de simulation d'attaques, Skybox identifie les actifs vulnérables exposés aux menaces sur votre réseau. Nos conseils en matière de mesures correctives vous amènent à vous concentrer sur ces vulnérabilités exposées, ainsi que sur celles fortement actives dans le monde. Et, grâce à notre connaissance du réseau, les mesures proposées ne se limitent pas seulement aux correctifs. Skybox vous informe des modifications basées sur le réseau qui isolent de manière efficiente et efficace l'actif vulnérable susceptible de subir une attaque.

Évaluations à la demande

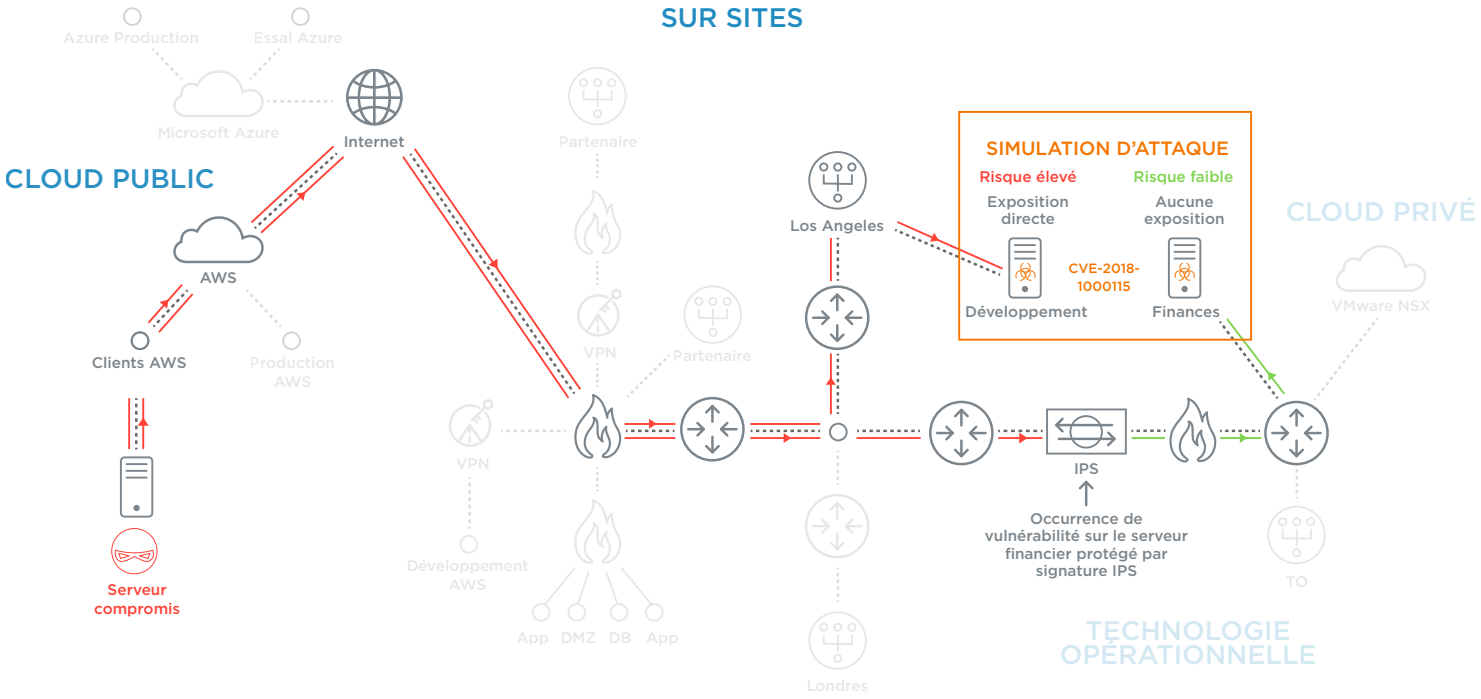
- Elles utilisent les données des systèmes de gestion des correctifs et des actifs ainsi que le flux d'informations de Skybox pour déceler les vulnérabilités sans que les résultats d'une analyse ne soit nécessaires
- Elles collectent, centralisent et fusionnent les données de plusieurs analyses de vulnérabilités
- Elles découvrent les vulnérabilités sur les périphériques réseau et de sécurité et dans les zones traditionnellement non analysables
- Elles combinent les résultats de l'analyse active et passive des environnements sur site, multicloud et TO pour des évaluations de vulnérabilité sur demande les plus complètes

Analyse de l'exposition et informations relatives aux menaces

L'étape la plus critique de l'analyse de vulnérabilité consiste à déterminer le niveau d'exposition sur votre réseau, comme illustré dans la représentation graphique ci-dessous.

Comprendre le niveau d'exposition permet de consacrer les ressources nécessaires soit aux vulnérabilités accessibles aux menaces, soit à l'identification des options d'atténuation destinées à bloquer les chemins d'attaque.

- Elle identifie les vulnérabilités exposées à l'aide du modèle de réseau, des données analytiques des vecteurs d'attaque et des simulations d'attaques à niveaux multiples
- Elle décèle les scénarios d'attaques potentielles et détecte les mesures de sécurité contournées ou compromises
- Elle souligne les vulnérabilités avec les exploits disponibles, les exploits actifs ou ceux impliqués dans les campagnes d'attaque telles que les ransomwares, les kits d'exploits, etc.
- Elle améliore la gestion des modifications du réseau en évaluant les modifications proposées en fonction des nouvelles expositions aux vulnérabilités



Mesures correctives intelligentes et réponse rapide aux menaces

- Elles vous informent des correctifs et des modifications ou mises à niveau disponibles pour les signatures IPS, la configuration et les LCA susceptibles d'éliminer la vulnérabilité ou d'atténuer ses risques
- Elles recommandent les meilleures mesures correctives afin d'éliminer les menaces imminentes non plus en quelques jours, mais en quelques heures
- Elles optimisent la réduction graduelle des risques afin de réduire systématiquement la surface d'attaque et contenir la prolifération des menaces potentielles
- Elles déterminent l'efficacité des mesures correctives à l'aide d'indicateurs de risque personnalisés

« Il est vraiment essentiel d'obtenir des informations exploitables. Les décisions les plus importantes doivent être prises en un minimum de temps sans que cela n'impacte considérablement l'activité. C'est ce que Skybox nous aide à faire : minimiser les risques plus rapidement et réduire notre fenêtre d'exposition aux vulnérabilités. Au lieu de surveiller quatre cents serveurs, je peux me focaliser sur trois.

On peut concentrer nos efforts sur l'essentiel, pour les bonnes raisons et dans les meilleurs délais. »

- RSSI, National federal credit union

Mesures correctives contre les vulnérabilités conçues pour réduire les risques

- Elles identifient les vulnérabilités exposées et celles probablement les plus exploitables et les placent en tête de votre liste de mesures correctives prioritaires
- Elles analysent les vulnérabilités dans le contexte du réseau, des actifs, des contrôles de sécurité et de l'environnement de menaces
- Elles donnent la priorité aux menaces imminentes afin de mettre en œuvre des actions correctives immédiates et identifient les menaces potentielles dans le cadre d'une réduction graduelle

À propos de Skybox Security

Skybox met à disposition la plus grande plate-forme de gestion de la cybersécurité de l'industrie afin de relever les défis de sécurité au sein de réseaux vastes et complexes. Grâce à l'intégration de 120 technologies de réseau et de sécurité, la suite Skybox® Security offre une visibilité complète de la surface d'attaque et fournit le contexte nécessaire à des actions réfléchies et pertinentes. Nos analyses, notre automatisation et les informations dont nous disposons améliorent l'efficacité et la performance des opérations de sécurité dans la gestion des vulnérabilités et des menaces, ainsi que dans la gestion des pare-feu et des politiques de sécurité pour les plus grandes entreprises du monde.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060