Identification précoce des dangers et des risques

Les dangers et les risques du réseau de l'entreprise doivent être identifiés précocement, catégorisés et corrigés. La plateforme Insight de Rapid7 renforce considérablement la gestion de la sécurité informatique – Aujourd'hui comme dans le futur.

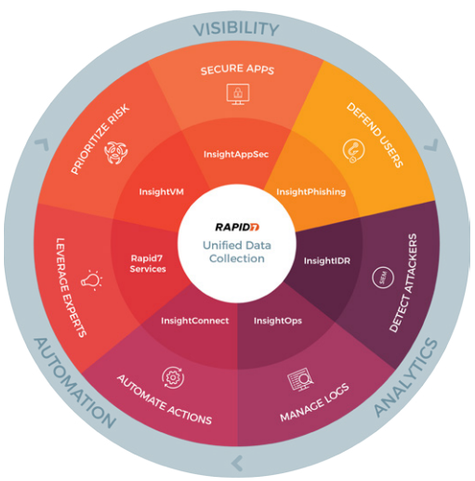
Les réseaux d'entreprise modernes sont exposés à d'énormes risques. Le nombre de cyberattaques est en constante augmentation et les méthodes d'attaque sont de plus en plus sophistiquées. De plus, le réseau ne se limite plus aux serveurs et aux postes de travail. Au contraire, les infrastructures virtuelles, les technologies de conteneurs et les services Cloud caractérisent le paysage informatique.

Les grandes entreprises utilisent en moyenne 75 produits de sécurité pour contrer les nombreux dangers. Ceux-ci génèrent un nombre infini de logs, d'alarmes et de rapports propriétaires – un flot de données difficile à gérer. C'est là qu'interviennent les solutions de gestion de vulnérabilité. Elles donnent un aperçu des vulnérabilités et des risques existants. Mais certains outils de cette catégorie n'offrent guère plus que de longues listes et des tableaux statiques.

Gestion des vulnérabilités NextGen

Rapid7, fondé en 2000, fait un pas en avant significatif avec InsightVM. La solution offre une visibilité complète sur toutes les vulnérabilités – des PC individuels aux services Cloud utilisés. Pour ce faire, elle collecte toutes les données relatives à la sécurité à l'aide d'un agent léger qui est installé sur les endpoints.

Contrairement aux solutions comparables, InsightVM analyse et hiérarchise les vulnérabilités très finement sur une échelle de 1 à 1000. Ce que Rapid7 appelle le «Real Risk Score» prend en compte non seulement le score CVSS mais aussi différents autres facteurs d'une vulnérabilité, son âge, l'existence actuelle d'exploit-kits et de malwares ainsi que l'impact concret sur la société. Par exemple, une vulnérabilité plus ancienne peut avoir un score plus élevé parce qu'un logiciel malveillant existe déjà pour l'exploiter. InsightVM présente les résultats sur des tableaux de bord interactifs en temps réel, offrant ainsi une base solide et unifiée pour toutes les personnes impliquées afin de traiter les vulnérabilités à la demande et de minimiser le risque global. InsightVM fonctionne avec des solutions de ticketing telles que Jira et ServiceNow.



Détection précoce des attaques

Un composant important de la plateforme Insight de Rapid7 réside dans la solution de détection et de réponse aux incidents, InsightIDR. Elle permet une analyse basée sur le comportement soutenue par du Machine Learning qui identifie de manière fiable les attaques inconnues. InsightIDR recherche les abus d'informations d'identification, détecte les attaques qui se déplacent sur plusieurs systèmes et met en place des pièges tels que des Honeypots ou des informations d'identification factices. Comme InsightVM, InsightIDR fournit des tableaux de bord avec des aperçus hiérarchisés et des informations détaillées. Il est par exemple possible d'afficher des processus suspects qui ne fonctionnent que sur un seul système.

Rapid7 est bien positionné pour une gestion des nouvelles vulnérabilités: l'équipe de recherche de plus de 200 spécialistes est membre de la CVE Numbering Authority depuis 2016. En tant que propriétaire de l'outil de test d'intrusion Metasploit, Rapid7 peut également s'appuyer sur les connaissances d'une communauté mondiale de 200 000 «White Hats». De plus, l'entreprise effectue ses propres tests d'intrusion, maintient 300 Honeypots avec les plus grands fournisseurs Cloud et fait partie de la Cyber Threat Alliance. Fort de cette expérience, Rapid7 est en mesure de comprendre les attaquants et leurs méthodes de manière très détaillée. Rien d'étonnant à ce que Rapid7 soit qualifié de leader dans le «Forrester Vulnerability and Risk Management Wave» de 2020.

InsightVM: Les points forts

- Visibilité complète de toutes les vulnérabilités
- Priorisation des résultats de l'analyse (Real Risk Score)
- Support Container & Cloud
- Remediation Projects
- Automation Integration in ServiceNow, Jira et autres
- API open

InsightIDR: Les points forts

- Solution SIEM basée sur le cloud, priorité sur les attaques via les terminaux
- Des résultats rapides – les règles de corrélation sont «préemballées» dès le départ
- Gestion centralisée des logs
- Collecte et analyse également les activités sur Azure et AWS
- Mise à jour des nouveaux modèles d'attaque grâce à Metasploit, Project Heisenberg ou Sonar
- SIEM, UEBA, ABA, EDR, DECEPTION, FIM, NETMON dans un seul produit

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne

Tél: 021 533 01 60
vente@boll.ch
www.boll.ch