Détecter et éliminer les cyberattaques

Rapid7 traite la détection, la hiérarchisation et l'élimination des vulnérabilités et des cyberattaques. Fondée en 2000 et basée à Boston, la société emploie plus de 1 400 personnes, dont 200 chercheurs experts en sécurité. En tant que propriétaire de l'outil de test de pénétration Metasploit, elle peut s'appuyer sur les découvertes d'une communauté mondiale de 200 000 hackers «white hat». Plus de 9000 clients font confiance à la technologie, aux services et à la recherche de Rapid7 pour améliorer leur cybersécurité.

Rapid7 dans la «Forrester Wave» pour MDR en tant que «Strong Performer»

Rapid7 est membre de la CVE Numbering Authorities et figure dans la catégorie «Managed Detection and Response Providers» du «Forrester Wave» pour le premier trimestre de 2021 en tant que «Strong Performer».

Rapid7 et BOLL – entretien entre deux grands partenaires

Pourquoi Rapid7 a-t-il un tel succès dans la région DACH? Quels sont les atouts particuliers de la technologie Rapid7? Le Suisse Andre Cuenin, CRO de Rapid7, et Thomas Boll, CEO de BOLL Engineering, élucident ces questions et d'autres dans un entretien personnel. En outre, ils abordent des sujets tels que les facteurs de succès, les tendances technologiques et la transformation des revendeurs de fournisseurs de matériel en MSSP. Cliquez ici pour en savoir plus.

Lien vers la vidéo Youtube de l'entretien.

Connaissances compactes

Participez aux prochains webinaires BOLL et apprenez-en davantage sur les produits, solutions et technologies révolutionnaires de Rapid7. Vous profitez ainsi des connaissances spécialisées des experts.

Vous trouverez ici des informations sur les **prochains évènements.**

Gestion des vulnérabilités de nouvelle génération

Gestion intelligente des vulnérabilités: avec la plateforme Insight modulaire et évolutive, Rapid7 atteint une nouvelle dimension dans le domaine de la gestion des vulnérabilités. Elle combine les connaissances et les technologies de Rapid7 afin de protéger avec succès les entreprises des cyberattaques déjà connues et nouvelles. Les connaissances sont basées sur la recherche de vulnérabilité de Nexpose, les données d'exploitation de Metasploit, le comportement des attaquants à l'échelle mondiale, les données d'analyse sur internet et les analyses des menaces et fournissent des informations directement applicables et hiérarchisées sur la situation de sécurité dans l'entreprise via des dashboards clairs.

Voici les modules importants de la plateforme Insight:

- InsightIDR: Solutions Behavioral Analytics et SIEM
- InsightVM et InsightAppSec: Solutions de Vulnerability-Risk-Management

InsightIDR – solution SIEM basée sur le cloud pour des résultats rapides et efficaces dans la lutte contre les menaces

La solution d'analyse comportementale et SIEM InsightIDR, qui se concentre sur les cybermenaces, détecte les processus suspects dans le réseau de l'entreprise. De nombreuses fonctions de sécurité telles que UEBA, ABA, NTA, EDR, FIM, Deception ou Log Search sont combinées dans InsightIDR et disponibles sous une seule interface – une sorte de «SOC in the box». Vu que Rapid7 dispose déjà de nombreux modèles d'attaque et de déclencheurs d'alarme, la solution déploie toute sa force en quelques jours.

Détecter et éliminer les cyberattaques

Grâce à des analyses sophistiquées, InsightIDR détecte les intrusions dans le réseau, les processus suspects ainsi que les comportements abusifs ou erronés des utilisateurs et peut déterminer si ces processus représentent une menace réelle. Cela évite les messages d'avertissement inutiles à l'équipe de sécurité. Les terminaux sont reliés à InsightIDR au moyen d'un agent local et les fichiers log sont lus par d'autres sources telles que le pare-feu, le trafic réseau, le serveur d'authentification ou le proxy web. La plateforme Insight met en corrélation les données et les analyse à la recherche d'anomalies. Des technologies telles que honeypots ou machine learning sont également utilisées. Si des activités suspectes sont détectées et classées comme dangereuses, InsightIDR avertit les responsables de sécurité et fournit des données forensiques afin de pouvoir étudier les problèmes. InsightIDR propose également des mesures de correction telles que l'arrêt des processus sur les terminaux concernés ou la séparation des terminaux du réseau. De plus, avec le module complémentaire InsightConnect, les processus multiplateformes peuvent être mappés avec des outils de sécurité supplémentaires afin de mettre en œuvre des mesures correctives et d'automatisation supplémentaires. Comme Rapid7 fournit de nombreux modèles d'attaque et déclencheurs d'alarmes avec InsightIDR et les actualise ou les développe en permanence, la solution déploie toute sa puissance en quelques jours – un facteur de différenciateur essentiel par rapport aux solutions SIEM existantes.

InsightIDR: Les points forts

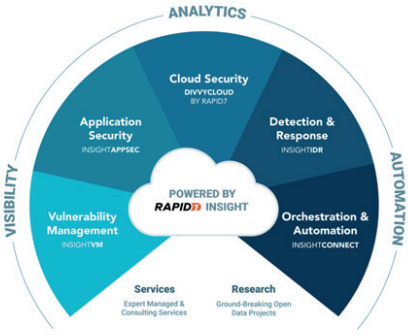
- Solution SIEM basée sur le cloud axée sur les cybermenaces
- SIEM, UEBA, ABA, EDR, Deception Technology, FIM, NetMon, Endpoint Telemetry, Honeypots dans un seul produit
- Résultats rapides – les règles de corrélation sont «prepacked» out of the box
- Gestion centralisée des logs
- Collecte et analyse également les activités sur Azure et AWS
- Processus d'automatisation et de correction prédéfinis pour une élimination rapide
- SOAR en combinaison avec Insight Connect
- Mise à jour de nouveaux schémas d'attaque grâce à des sources telles que Metasploit, Project Heisenberg ou Sonar

RAPID7

Dépliant du fabricant
Rapid7

InsightConnect/SOAR

Les entreprises doivent rapidement combler les lacunes identifiées dans leur paysage informatique et parer aux attaques. Cependant, il y a un manque croissant de professionnels de l'informatique capables d'effectuer de telles tâches. Pour cette raison, SOAR (Security Orchestration, Automation and Remediation) est un sujet sensible. InsightConnect de Rapid7 peut être combiné avec InsightIDR et InsightVM et est ensuite capable de déclencher automatiquement des processus dans d'autres outils de sécurité afin d'éliminer rapidement les dangers identifiés.



InsightVM et InsightAppSec – transparence complète avec gestion des risques de vulnérabilité pour les applications réseau et web

Avec InsightVM et InsightAppSec, Rapid7 propose des solutions de gestion des risques de vulnérabilité afin d'assurer une transparence complète du réseau de l'entreprise et des applications web. Seuls ceux qui connaissent leurs propres points faibles peuvent définir spécifiquement des mesures qui réduisent finalement la zone cible et donc le risque.

Nouvelle dimension de la gestion des vulnérabilités

Avec InsightVM, Rapid7 permet une visibilité complète en temps réel de tous les points faibles de l'ensemble du réseau de l'entreprise, y compris les infrastructures virtualisées, les référentiels de conteneurs et les services cloud. La solution hiérarchise les problèmes de sécurité avec ce qu'on appelle le Real Risk Score qui s'échelonne de 1 à 1000 – contrairement au CVSS Score habituel du secteur avec un échelonnement de 0 à 10. De plus, InsightVM tient compte non seulement du risque de base d'une vulnérabilité, mais aussi de son ancienneté, de la présence de kits d'exploitation et de l'impact concret sur l'entreprise, ce qui permet une évaluation réaliste de l'ampleur du problème.

Rapid7 InsightVM: Les points forts

- Hiérarchisation des résultats du scan (Real Risk Score)
- Analyse des conteneurs ainsi que des infrastructures virtuelles et cloud
- Définition des projets de remédiation
- Intégration d'automatisation dans Service Now, Jira et d'autres fournisseurs tiers
- RESTful API
- Disponible en version Cloud Service ou on-premises

Sécurité complète des applications web

Les applications web font partie des applications clés de l'interaction entre les entreprises, les clients et les employés. De nombreuses applications web sont accessibles de l'extérieur et sont donc exposées à des cyberattaques. Grâce à InsightAppSec, les entreprises peuvent vérifier en permanence leurs applications web pour détecter les failles de sécurité pendant leur développement ainsi que dans leur environnement productif. Un reporting clair montre quelles lacunes présentent quels risques et comment celles-ci peuvent être comblées afin de pouvoir définir correctement les priorités pour leur élimination. Pour vérifier les lacunes des frameworks et des technologies existants et futurs pour les applications web, Rapid7 s'appuie sur Universal Translator.

Rapid7 InsightAppSec: Les points forts

- Dynamic Application Security Testing (DAST)
- Universal Translator
- Prend en charge des méthodes d'authentification simples et complexes
- Plus de 95 types d'attaques simulées
- Enregistrer et repasser les attaques
- Disponible en tant que service cloud

BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / téléphone +41 21 533 01 60 / contact@boll.ch
BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / téléphone +41 56 437 60 60 / info@boll.ch / www.boll.ch

BOLL
IT Security Distribution