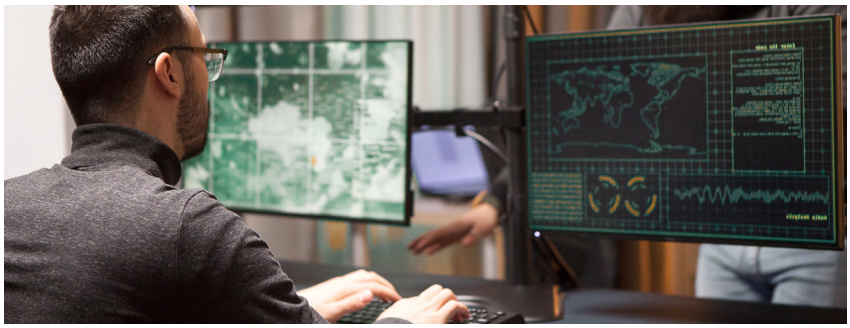


Détecter et éliminer les cyberattaques

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

InsightIDR: les points forts

- Solution SIEM en 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 des activités sur Azure et AWS
- Processus d'automatisation et de remédiation prédéfinis pour une élimination rapide
- SOAR en combinaison avec InsightConnect
- Mise à jour des nouveaux schémas d'attaque grâce à des sources telles que Metasploit, Project Heisenberg ou Sonar.

Depuis sa création en 2000, Rapid7 se consacre à la détection, à la hiérarchisation et à la correction des vulnérabilités et des cyberattaques. Basée à Boston, la société emploie plus de 1400 personnes, dont 200 experts en sécurité. En tant que propriétaire de l'outil de test de pénétration Metasploit, elle peut s'appuyer sur les connaissances d'une communauté mondiale de 200 000 hackers «white hat». Les investissements en matière de cybersécurité sont généralement utilisés pour des mesures préventives telles que les pare-feu ou la sécurité des terminaux. Mais cela ne suffit pas. Les cyberattaques sont de plus en plus sophistiquées, dynamiques et individuelles, de sorte que les mesures de prévention classiques ne permettent souvent plus de les détecter. Les pirates pénètrent alors dans le réseau de l'entreprise avec des mots de passe volés restant non détectés pendant des semaines ou des mois – en moyenne 279 jours selon l'étude IBM Ponemon de 2019. Il en résulte des coûts élevés et une atteinte à la réputation.
Et peu importe la taille et le type d'une organisation. Pour détecter et éliminer les attaques, les entreprises ont besoin non seulement de professionnels de la sécurité informatique et de processus adaptés, mais aussi de solutions techniques. La plateforme complète Insight combine les connaissances et la technologie de Rapid7 pour protéger efficacement les entreprises contre les cyberattaques connues et nouvelles. InsightIDR est un composant clé de la plateforme Insight. Il s'agit d'une solution d'analyse comportementale/SIEM qui détecte les activités suspectes dans le réseau de l'entreprise à un stade précoce, les signale en fonction des risques et les prévient également de manière indépendante.

Réagir plus rapidement pour détecter et se défendre contre les attaques

La solution d'analyse comportementale et SIEM InsightIDR, qui se concentre sur les cybermenaces, détecte les processus suspects dans le réseau de l'entreprise, consolide plusieurs fonctions en une seule solution et s'accompagne de processus prédéfinis d'automatisation et de correction pour un traitement rapide des menaces.

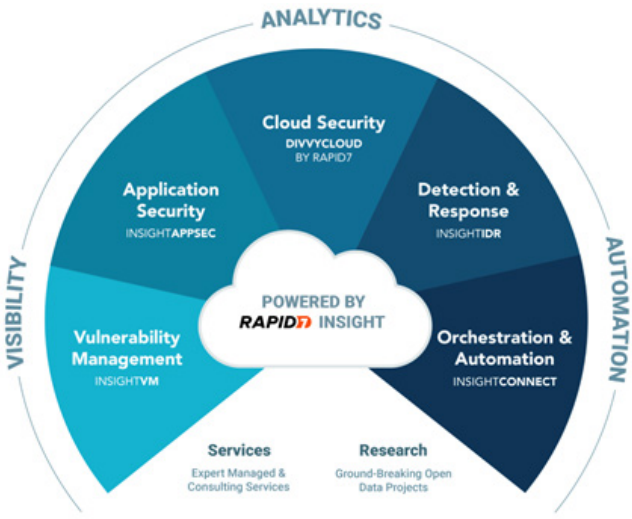
Grâce à des analyses sophistiquées, InsightIDR détecte les intrusions dans le réseau, les processus suspects et les comportements abusifs ou erronés des utilisateurs, et peut déterminer si ces activités représentent une menace réelle. Cela évite les alertes inutiles à l'équipe de sécurité.

Les terminaux sont reliés à InsightIDR au moyen d'un agent local et les fichiers log sont lus à partir 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 pour détecter les 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 pour pouvoir étudier les problèmes. InsightIDR propose également des mesures correctives telles que l'arrêt des processus sur les terminaux concernés ou la déconnexion des terminaux du réseau.
De plus, avec le module complémentaire InsightConnect, les processus multiplateformes peuvent êtes mappés avec des outils de sécurité supplémentaires afin de mettre en œuvre des mesures correctives et des automatisations supplémentaires. Comme Rapid7 fournit de nombreux modèles d'attaque et déclencheurs d'alarme avec InsightIDR et les actualise ou les développe en permanence, la solution déploie toute sa puissance en quelques jours en quelques jours, ce qui constitue un facteur de différenciateur important par rapport aux solutions SIEM existantes.

InsightConnect/SOAR

Les entreprises doivent être capables de pouvoir combler les lacunes identifiées dans leur paysage informatique et parer aux attaques rapidement. Cependant, il y a un manque croissant de professionnels de l'informatique en mesure d'accomplir ces tâches. C'est pourquoi, le SOAR (Security Orchestration, Automation and Remediation) est un sujet actuel. Avec InsightConnect de Rapid7, InsightIDR est capable de déclencher automatiquement des processus dans d'autres outils de sécurité pour éliminer rapidement les menaces détectées.



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

BOLL
IT Security Distribution