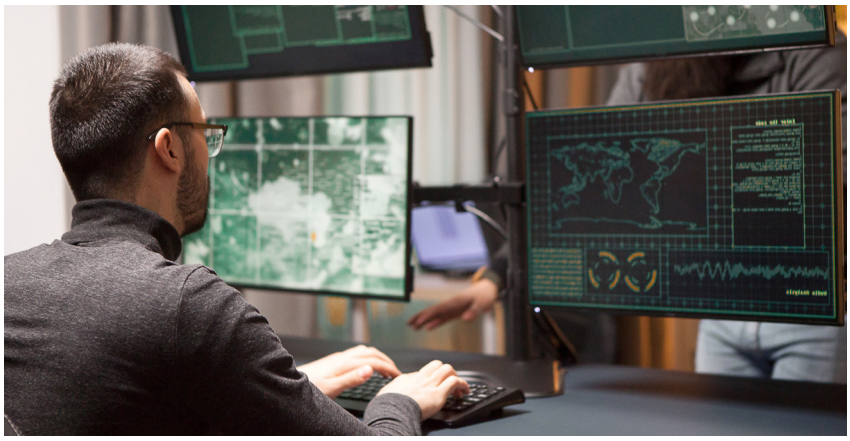


Cyberattacken erkennen und beseitigen

Cloudbasierte SIEM-Lösung für schnelle, effektive Resultate bei der Abwehr von Bedrohungen

InsightIDR: die Highlights

- Cloudbasierte SIEM-Lösung mit Fokus auf Cyberbedrohungen
- SIEM, UEBA, ABA, EDR, Deception Technology, FIM, NetMon, Endpoint Telemetry, Honeypots in einem Produkt
- Schnelle Resultate – Korrelationsregeln sind «prepacked» out of the box
- Zentralisiertes Log-Management
- Sammelt und analysiert auch Aktivitäten auf Azure und AWS
- Vordefinierte Automation- und Remediation-Prozesse für rasche Beseitigung
- SOAR in Kombination mit InsightConnect
- Update von neuen Angriffsmustern dank Quellen wie Metasploit, Project Heisenberg oder Sonar

Rapid7 befasst sich seit der Gründung im Jahr 2000 mit der Erkennung, Priorisierung und Behebung von Schwachstellen und Cyberattacken. Das Unternehmen mit Hauptsitz in Boston beschäftigt über 1400 Mitarbeitende, darunter 200 Sicherheitsforschende, und kann als Eigner des Penetration-Test-Tools Metasploit auf die Erkenntnisse einer weltweiten Community von 200 000 «White Hat»-Hackern zurückgreifen. Cybersecurity-Investitionen werden oft für Präventionsmassnahmen wie Firewalls oder Endpoint Security eingesetzt. Dies reicht jedoch nicht aus. Cyberangriffe werden raffinierter, dynamischer und individueller, sodass klassische Präventionsmassnahmen diese öfters nicht mehr erkennen. Oft dringen Hacker mit gestohlenen Passwörtern ins Firmennetzwerk ein und bleiben über Wochen oder Monate unerkannt – laut der IBM-Ponemon-Studie 2019 durchschnittlich 279 Tage. Die Folge sind hohe Kosten und ein Reputationsschaden. Die Grösse und Art einer Organisation spielen dabei keine Rolle. Um Angriffe zu erkennen und zu beseitigen, brauchen Unternehmen nicht nur IT-Security-Professionals und passende Prozesse, sondern auch technische Lösungen. Die umfassende Insight-Plattform vereint das Wissen und die Technologie von Rapid7, um Unternehmen vor bekannten wie auch neuen Cyberattacken erfolgreich zu schützen. InsightIDR ist eine wichtige Komponente der Insight-Plattform. Sie ist eine Behaviour-Analytics/SIEM-Lösung, die verdächtige Aktivitäten im Firmennetzwerk frühzeitig erkennt, risikobasiert meldet und auch selbstständig unterbindet.

Bei der Erkennung und Abwehr von Angriffen schneller reagieren

Die auf Cyberbedrohungen fokussierte Behaviour-Analytics- und SIEM-Lösung InsightIDR erkennt verdächtige Vorgänge im Unternehmensnetzwerk, fasst zahlreiche Funktionen in einer Lösung zusammen und ist mit vordefinierten Automatisierungs- und Behebungsprozessen zur raschen Beseitigung von Bedrohungen ausgestattet.

Durch ausgefeilte Analysen erkennt InsightIDR Einbrüche ins Netzwerk, verdächtige Prozesse sowie missbräuchliches oder irrtümliches Anwenderverhalten und kann beurteilen, ob solche Vorgänge eine tatsächliche Bedrohung darstellen. So lassen sich unnötige Warnmeldungen an das Security-Team vermeiden.

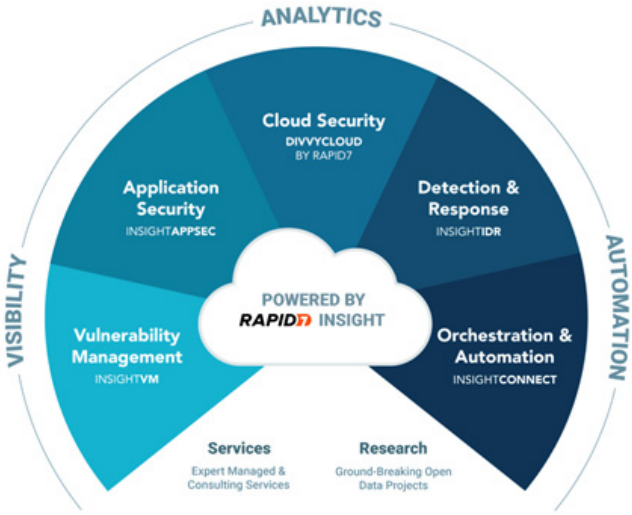
Die Endgeräte werden mittels eines lokalen Agenten an InsightIDR angebunden und Log-Files von anderen Quellen wie Firewall, Netzwerk-Traffic, Authentification Server oder Web Proxy eingelesen. Die Insight-Plattform korreliert die Daten und analysiert diese auf Auffälligkeiten. Dabei werden auch Technologien wie Honeypots oder Machine Learning eingesetzt.

Werden auffällige Aktivitäten erkannt und als gefährlich eingestuft, warnt InsightIDR die Security-Verantwortlichen und stellt forensische Daten zur Verfügung, um den Problemen nachgehen zu können. Auch bietet InsightIDR Remediation-Massnahmen wie den Abbruch von Prozessen auf den betroffenen Endgeräten oder die Trennung der Endgeräte vom Netzwerk. Zusätzlich können mit dem Add-on InsightConnect plattformübergreifende Prozesse mit weiteren Security-Tools abgebildet werden, um zusätzliche Remediation-Massnahmen und Automatisierungen umzusetzen.

Da Rapid7 viele Angriffsmuster und Alarmtrigger bei InsightIDR mitliefert und diese stets aktualisiert oder erweitert, entfaltet die Lösung innerhalb weniger Tage die volle Stärke – ein starkes Unterscheidungsmerkmal zu bestehenden SIEM-Lösungen.

InsightConnect/SOAR

Unternehmen müssen erkannte Lücken in ihrer IT-Landschaft rasch beseitigen und Angriffe abwehren. Zunehmend fehlen jedoch IT-Professionals, die solche Aufgaben wahrnehmen können. Aus diesem Grund ist SOAR (Security Orchestration, Automation and Remediation) ein aktuelles Thema. Mit InsightConnect von Rapid7 kann InsightIDR automatisch Prozesse in anderen Security-Tools anstossen, um die erkannten Gefahren rasch zu beseitigen.



BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com

BOLL IT Security Distribution