# Cyberattacken erkennen und beseitigen

Rapid7 befasst sich mit der Erkennung, Priorisierung und Behebung von Schwachstellen und Cyberattacken. Das im Jahr 2000 gegründete 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. Mehr als 9000 Kunden vertrauen auf die Technologie, die Dienstleistungen sowie die Forschungstätigkeit von Rapid7, um ihre Cybersecurity zu verbessern.

## Rapid7 im Magic Quadrant von Gartner

Rapid7 ist Mitglied der CVE Numbering Authorities und figuriert in der Kategorie «Managed Detection and Response Providers» im «Forrester Wave» für das erste Quartal 2021 als «Strong Performer».

## Rapid7 und BOLL – zwei starke Partner im Gespräch

Weshalb ist Rapid7 in der DACH-Region so erfolgreich? Was sind die besonderen Stärken der Technologie von Rapid7? Diese und weitere Fragen erläutern der aus der Schweiz stammende Andre Cuenin, CRO von Rapid7, und Thomas Boll, CEO von BOLL Engineering, im persönlichen Gespräch. Zudem unterhalten sie sich über Themen wie Erfolgsfaktoren, Technologietrends und die Wandlung der Reseller vom Hardwareanbieter zum MSSP. Hier erfahren Sie mehr.

Link zum Youtube-Video des Gespräches

## Wissen kompakt

Nehmen Sie teil an den kommenden Webinaren von BOLL und erfahren Sie mehr über die wegweisenden Produkte, Lösungen und Technologien von Rapid7. Dabei profitieren Sie vom hochgradigen Fach- und Expertenwissen der Referenten.

Hier finden Sie Informationen über die **kommenden Events.**

## Schwachstellenmanagement der nächsten Generation

Cleveres Schwachstellenmanagement: Mit der modularen und skalierbaren Insight-Plattform erreicht Rapid7 im Bereich Vulnerability Management eine neue Dimension. Sie vereint das Wissen und die Technologien von Rapid7, um Unternehmen vor bekannten wie auch neuen Cyberattacken erfolgreich zu schützen. Das Wissen basiert auf der Schwachstellenforschung von Nexpose, den Exploit-Daten von Metasploit, dem weltweiten Angreiferverhalten, internetweiten Scan-Daten und Bedrohungsanalysen und liefert über anschauliche Dashboards direkt umsetzbare, priorisierte Erkenntnisse zur Sicherheitslage im Unternehmen.

**Wichtige Elemente der Insight-Plattform sind die folgenden Module:**

- InsightIDR: Behavioral-Analytics- und SIEM-Lösung
- InsightVM und InsightAppSec: Vulnerability-Risk-Management-Lösungen

# InsightIDR – cloudbasierte SIEM-Lösung für schnelle, effektive Resultate bei der Abwehr von Bedrohungen

Die auf Cyberbedrohungen fokussierte Behavioral-Analytics- und SIEM-Lösung InsightIDR erkennt verdächtige Vorgänge im Unternehmensnetzwerk. Zahlreiche Security-Funktionen wie UEBA, ABA, NTA, EDR, FIM, Deception oder Log Search sind in InsightIDR zusammengefasst und unter einer Oberfläche verfügbar – eine Art «SOC in the Box». Da Rapid7 viele Angriffsmuster und Alarmtrigger bereits mitliefert, entfaltet die Lösung innerhalb von wenigen Tagen ihre volle Stärke.

## Cyberattacken erkennen und beseitigen

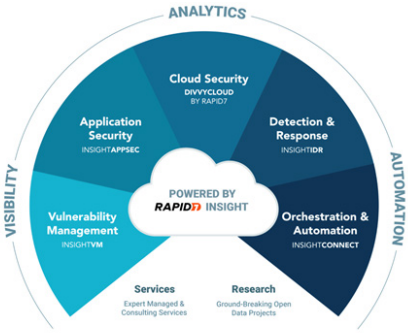
Durch ausgefeilte Analysen erkennt InsightIDR Einbrüche ins Netzwerk, verdächtige Prozesse sowie missbräuchliches oder irrtümliches Anwenderverhalten und kann beurteilen, ob solche Vorgänge eine tatsächliche Bedrohung darstellen. So lassen sich unnötige Warnmeldungen an das Security-Team vermeiden. Die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

## 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 Insight Connect
- Update von neuen Angriffsmustern dank Quellen wie Metasploit, Project Heisenberg oder Sonar

## 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. InsightConnect von Rapid7 kann mit InsightIDR und InsightVM kombiniert werden und ist dann in der Lage, automatisch Prozesse in anderen Security-Tools anzustossen, um die erkannten Gefahren rasch zu beseitigen.




# InsightVM und InsightAppSec – umfassende Transparenz mit Vulnerability Risk Management für Netzwerk und Web-Apps

Mit InsightVM und InsightAppSec bietet Rapid7 Vulnerability-Risk-Management-Lösungen an, um eine umfassende Transparenz im Unternehmensnetzwerk und bei Web-Applikationen zu erhalten. Nur wer die eigenen Schwachstellen kennt, kann gezielt Massnahmen definieren, die schliesslich die Angriffsfläche und somit das Risiko verringern.

## Neue Dimension für das Schwachstellenmanagement

Mit InsightVM ermöglicht Rapid7 in Echtzeit umfassende Sichtbarkeit aller Schwachstellen im gesamten Unternehmensnetzwerk inklusive virtualisierter Infrastrukturen, Container-Repositorien und Cloud-Diensten. Die Lösung priorisiert die Sicherheitsprobleme mit dem sogenannten Real Risk Score in Stufen von 1 bis 1000 – im Gegensatz zum branchenüblichen CVSS Score mit einer Einteilung von 0 bis 10. Darüber hinaus berücksichtigt InsightVM neben dem unveränderlichen Grundrisiko einer Schwachstelle auch deren Alter, das Vorhandensein von Exploit Kits sowie den konkreten Einfluss auf das individuelle Unternehmen und ermöglicht so eine realistische Einschätzung der Tragweite des Problems.

## Rapid7 InsightVM: Die Highlights

- Priorisierung der Scan-Ergebnisse (Real Risk Score)
- Analyse von Containern sowie virtueller und Cloud-Infrastrukturen
- Festlegung von Remediation-Projekten
- Automation-Integration in ServiceNow, Jira und weitere Drittanbieter
- Offene RESTful-API
- Erhältlich als Cloud Service oder als On-Premises-Version

## Umfassende Sicherheit für Web-Applikationen

Web-Applikationen gehören zu den Schlüsselanwendungen für die Interaktion zwischen Unternehmen, Kunden und Mitarbeitenden. Viele Web-Applikationen sind von aussen erreichbar und somit für Cyberattacken exponiert. Mit InsightAppSec können Unternehmen ihre Web-Apps bereits während deren Entwicklung sowie in der produktiven Umgebung laufend auf Sicherheitslücken überprüfen. Ein übersichtliches Reporting zeigt auf, welche Lücken welche Risiken aufweisen und wie diese geschlossen werden können, um so die Prioritäten für deren Beseitigung richtig definieren zu können. Um bestehende wie auch künftige Frameworks und Technologien für Web-Applikationen auf deren Lücken zu prüfen, setzt Rapid7 auf den Universal Translator.

## Rapid7 InsightAppSec: Die Highlights

- Dynamic Application Security Testing (DAST)
- Universal Translator
- Unterstützt einfache und komplexe Authentifizierungsmethoden
- Über 95 Arten von simulierten Attacken
- Aufzeichnung und Abspielen von Angriffen
- Erhältlich als Cloud Service