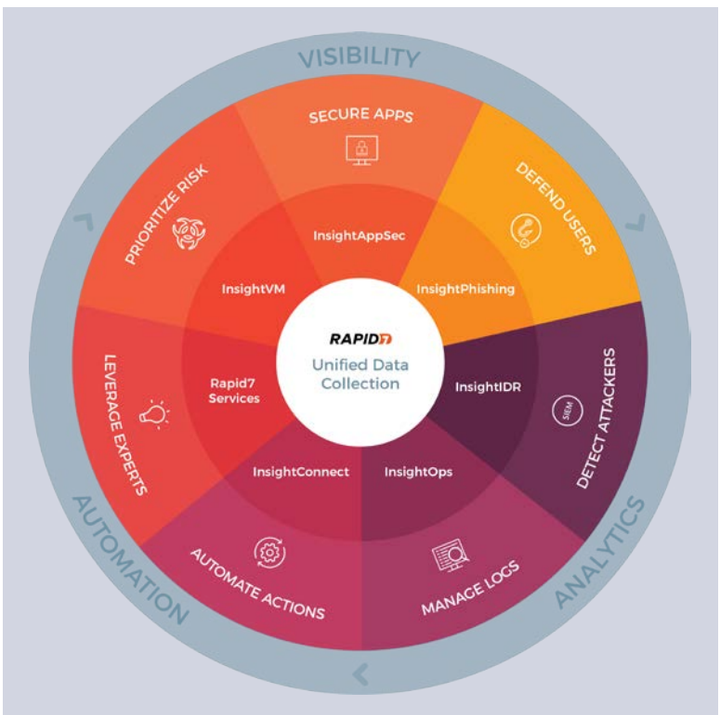
Risiken frühzeitig erkennen

Gefahren im Unternehmensnetzwerk müssen frühzeitig erkannt, kategorisiert und behoben werden. Die umfassende Insight-Plattform von Rapid7 stärkt die IT-Security markant – heute und in Zukunft.



Moderne Unternehmensnetzwerke sind enormen Gefahren und Risiken ausgesetzt. Die Anzahl der Cyberattacken nimmt stetig zu und die Angriffsmethoden werden raffinierter. Zudem beschränkt sich das Netzwerk nicht mehr auf Server und Workstations. Vielmehr prägen virtuelle Infrastrukturen, Containertechnologien und Cloud-Services die IT-Landschaft.

Um den vielfältigen Gefahren zu begegnen, setzen grössere Unternehmen durchschnittlich 75 Sicherheitsprodukte ein. Diese generieren unendlich viele proprietäre Statusmeldungen, Alarme und Berichte – eine Datenflut, die kaum noch handelbar ist. Hier setzen Vulnerability-Risk-Management-Lösungen ein. Sie gewähren Übersicht über die vorhandenen Schwachstellen und Risiken. Doch manche Tools dieser Kategorie bieten kaum mehr als ellenlange Listen und statische Dashboards.

Vulnerability Management der nächsten Generation

Rapid7, gegründet im Jahr 2000, geht mit InsightVM einen bedeutenden Schritt weiter. Die Lösung bietet eine umfassende Sichtbarkeit sämtlicher Schwachstellen – vom einzelnen PC bis zu den genutzten Cloud-Services. Dazu sammelt sie sämtliche sicherheitsrelevanten Daten mithilfe eines schlanken Agenten, der auf den Endpunkten installiert wird.

Anders als vergleichbare Lösungen analysiert und priorisiert InsightVM die Schwachstellen fein granuliert in Stufen von 1 bis 1000. Rapid7 nennt dies «Real Risk Score» und berücksichtigt dabei nicht nur wie der CVSS-Score das unveränderliche Basisrisiko einer Schwachstelle, sondern auch deren Alter, die aktuelle Existenz von Exploit-Kits und Malware sowie den konkreten Einfluss auf das Unternehmen. So kann eine ältere Schwachstelle einen höheren Score aufweisen, weil bereits Malware zu deren Ausnutzung existiert. InsightVM präsentiert die Resultate auf interaktiven Echtzeit-Dashboards und schafft so eine solide, einheitliche Grundlage für alle involvierten Personen, um die Schwachstellen bedarfsgerecht zu beheben und das Gesamtrisiko zu minimieren. Die Lösung arbeitet dazu mit Ticketing-Lösungen wie Jira und ServiceNow zusammen.

Attacken frühzeitig erkennen

Eine wichtige Komponente der Insight-Plattform von Rapid7 ist ferner die Incident-Detection-and-Response-Lösung InsightIDR. Sie ermöglicht eine verhaltensbasierte, durch Machine Learning unterstützte Analyse, die unbekannte Attacken zuverlässig identifiziert. InsightIDR sucht nach Missbrauch von Anmeldedaten, erkennt Angriffe, die sich über verschiedene Systeme hinwegbewegen und stellt Fallen wie Honeypots oder Honey Credentials. Wie InsightVM bietet auch InsightIDR Dashboards mit priorisierten Erkenntnissen und detaillierten Informationen. So lassen sich zum Beispiel verdächtige Prozesse anzeigen, die nur auf einem einzigen System laufen.

Rapid7 ist auch für neuartige Cyberattacken gut aufgestellt. Das Research-Team mit mehr als 200 Spezialisten ist seit 2016 Mitglied der CVE Numbering Authority. Als Eigner des Penetration-Testing-Tools Metasploit kann Rapid7 zudem auf die Erkenntnisse einer weltweiten Community von 200 000 «White Hats» zurückgreifen. Darüber hinaus führt das Unternehmen eigene Penetration-Tests durch, unterhält 300 Honeypots bei den grössten Cloud-Anbietern und ist Mitglied der anbieterübergreifenden Cyber Threat Alliance. Mit diesem soliden Hintergrund ist Rapid7 in der Lage, Angreifer und ihre Methoden bis ins Detail zu verstehen. Kein Wunder, dass Gartner Rapid7 im Magic Quadrant 2020 für SIEM als Leader einstuft.

InsightVM: die Highlights

- Umfassende Sichtbarkeit aller Schwachstellen
- Priorisierung der Scan-Ergebnisse (Real Risk Score)
- Container- und Cloud-Unterstützung
- Remediation-Projekte
- Automation Integration in ServiceNow, Jira und weitere Drittanbieter
- Offene Rest-API

InsightIDR: die Highlights

- Cloudbasierte SIEM-Lösung mit Fokus auf Hackerangriffe über Endpoints
- Schnelle Resultate – Korrelations-Regeln sind «pre-packed» out of the box
- Zentralisiertes Log Management
- Sammelt und analysiert auch Aktivitäten auf Azure und AWS
- Update von neuen Angriffsmustern dank Quellen wie Metasploit, Project Heisenberg oder Sonar
- SIEM, UEBA, ABA, EDR, DECEPTION, FIM, NETMON in einem Produkt

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60
info@boll.ch
www.boll.ch