RSA NetWitness® Platform – fortschrittliches SIEM

Übersicht

Informationssicherheit ist für Unternehmen seit Beginn des digitalen Zeitalters eine große Herausforderung. Heutzutage sind jedoch mehrere Faktoren zusammengekommen, die die Sicherheit noch weiter erschweren:

- Der rasante Wechsel zu einer virtualisierten und Cloud-basierten Infrastruktur hat den herkömmlichen perimeterbasierten Sicherheitsansatz effektiv durchbrochen.
- Cyberbedrohungen wurden für die Massennutzung kommerzialisiert und viele Angriffe haben ihren Ursprung in staatlichen Geheimdienstorganisationen.
- Das Cyberrisikomanagement hat sich von einem IT-Problem zu einer zentralen Unternehmensverantwortung entwickelt.

RSA erkennt und versteht diese Herausforderungen: Mit Tools und Services für fortschrittliches SIEM und Threat Defense können Unternehmen Bedrohungen in dieser sich ständig weiter entwickelnden Umgebung schneller erkennen und darauf reagieren.

Fortschrittliches SIEM beschleunigt die Bedrohungserkennung und -reaktion, bietet zusätzliche Sichtbarkeit und umfasst sowohl Threat Intelligence als auch Unternehmenskontext, um Bedrohungen und Sicherheits-Incidents zu priorisieren. Die Vorteile:

- Beispiellose Erkennung von Bedrohungen überall
- Fähigkeit, das gesamte Ausmaß eines Angriffs sofort zu erkennen
- Unternehmenskontext, sodass Analysten schnell auf die wichtigsten Bedrohungen reagieren können

Cyberkriminelle senden Phishing- oder Schadsoftwareangriffe per E-Mail an Unternehmen, Staaten wollen sich Zugang zu geistigem Eigentum verschaffen oder Insider verwenden sensible Daten missbräuchlich: Wir leben in einer Welt, in der es unmöglich erscheint, sich vor Sicherheitsverletzungen zu schützen. Angesichts der Geschwindigkeit, mit der Cyberkriminelle neue Sicherheitsbedrohungen weltweit erstellen und ausführen, müssen Unternehmen ihren Sicherheitsansatz ändern.

Warum ist fortschrittliches SIEM erforderlich?

Die Komplexität von Bedrohungsakteuren und die ständig wachsende Angriffsfläche einer modernen IT-Infrastruktur haben die Fähigkeiten von Legacy SIEMs und zugehörigen Tools bereits überschritten. Sicherheitsteams benötigen Fähigkeiten, um Risiken schnell zu erkennen und ihren vollen Umfang zu verstehen, damit sie reagieren können, bevor sich diese Bedrohungen auf das Unternehmen auswirken.

Angreifer erhalten schneller als je zuvor Zugriff auf die Infrastruktur eines Unternehmens – in der Regel innerhalb von Minuten – und fast alle extrahieren sensible Daten innerhalb weniger Stunden. Es kann jedoch Wochen oder sogar Monate dauern, um diese Sicherheitsverletzungen zu erkennen. Meist erfolgt dies nicht durch interne Systeme und Kontrollen, sondern durch externe Quellen wie Kunden oder Behörden.

Unternehmen haben aus folgenden Gründen Schwierigkeiten mit schneller Erkennung und Reaktion:

- Unverhältnismäßiges Vertrauen auf präventive Kontrollen
- Blinde Flecken im Netzwerk, am Endpunkt sowie in der virtuellen und Cloud-Infrastruktur
- Datenflut aus Silos an Datenquellen, mit eingeschränkter oder fehlender Korrelation oder Analyse zwischen diesen
- Fehlende dynamische Threat Intelligence und ergänzende Unternehmenskontexte für die Sicherheitsdaten
- Unerfahrene und zu wenige Analysten

Die Bedrohungslandschaft ist ausgefeilter:

- Wenn Unternehmen Anwendungen, Daten und alltägliche Datenverarbeitungsaufgaben in die Cloud migrieren, erhalten sie eine skalierbare Infrastruktur, sind jedoch anfälliger und haben nur eingeschränkte Sichtbarkeit in Ereignisse, die außerhalb herkömmlicher Netzwerkumgebungen stattfinden.
- Die Angreifer sind gut ausgestattet, gehen zielgerichtet vor und kennen die „blinden Flecken“ der Unternehmen.
- Angreifer müssen nur einmal erfolgreich sein, Sicherheitsteams hingegen müssen jedes Mal richtig liegen.

Die Sicherheitsteams haben Schwierigkeiten, effizient und effektiv zu erkennen und zu reagieren:

- Technische Experten haben Schwierigkeiten, der Flut von Warnmeldungen mit geringer Priorität Herr zu werden.
- Sicherheitsanalysten verlassen sich auf manuelle Korrelation, Erkennung und Ermittlungen.
- Es dauert zu lange, um nachzuvollziehen, wie sich Sicherheits-Incidents auf das gesamte Unternehmen auswirken.

Das fortschrittliche SIEM der RSA NetWitness Platform ist die Lösung für Bedrohungserkennung und -reaktion, mit der Sicherheitsteams die Bedrohungen erst vollständig verstehen und dann ausmerzen können, bevor sie sich auf das Unternehmen auswirken.

- Systemübergreifende Sichtbarkeit zur schnellen Erkennung von Bedrohungen
- Unternehmenskontext und Sicherheitsrisiken abgleichen, Lücken von reinen Technologielösungen schließen
- Darauf vertrauen, dass Sie den vollen Umfang der Bedrohung erkannt haben
- Effizienz durch Automatisierung der Workflows von Analysten und Unterstützung von Compliance-Zielen erzielen
- Unbekannte Bedrohungen umfassend auf Basis des Verhaltens erkennen. Bedrohungssensitive Authentifizierung für die Definition von Authentifizierungsrichtlinien einsetzen, die auf verdächtige Aktivitäten reagieren und Vertrauen erhöhen

197

Tage

Durchschnittliche Zeit von Unternehmen, um eine Sicherheitsverletzung zu erkennen.

Quelle: *Ponemon Institute 2018 Cost of a Data Breach Study*

RSA NetWitness Platform – fortschrittliches SIEM

Mit dem fortschrittlichen SIEM der RSA NetWitness Platform können Sicherheitsteams den vollen Umfang einer Bedrohung erkennen und verstehen, da Daten und Verhaltensweisen von allen Protokollen, Paketen und Endpunkten im Unternehmen sowie das Verhalten der Mitarbeiter und Prozesse im Netzwerk analysiert werden. Die Lösung verwandelt diese Daten durch ergänzenden Unternehmenskontext in Echtzeit und Threat Intelligence aus zahlreichen Quellen in umsetzbare Bedrohungseinblicke. Das fortschrittliche SIEM erstellt für diese gesamten Daten eine einheitliche Taxonomie und beschleunigt so die Erkennung von sowohl bekannten als auch unbekannten Bedrohungen.

Das fortschrittliche SIEM der RSA NetWitness Platform verfügt über leistungsstarke Funktionen, die auf maschinellem Lernen, User and Entity Behavior Analytics (UEBA), Korrelationsregeln und Advanced Threat Intelligence basieren. Das fortschrittliche SIEM der RSA NetWitness Platform bietet rollenbasierte Orchestrierung und Workflows für die Bedrohungserkennung und -reaktion sowie flexible Bereitstellungsmodelle (Cloud, virtualisiert oder Appliance) zur Unterstützung moderner IT-Infrastrukturen.

Dank dieser umfassenden und flexiblen Plattform kann das fortschrittliche SIEM der RSA NetWitness Platform die Prozesse für Bedrohungserkennung und -reaktion ganz erheblich optimieren. In einer Umgebung, in der Sicherheitsexpertise knapp und teuer ist, sorgt das fortschrittliche SIEM der RSA NetWitness Platform dafür, dass Sicherheitsanalysten die Unternehmen weitaus effektiver vor ausgefeilten Cyberbedrohungen schützen können.

Das fortschrittliche SIEM der RSA NetWitness Platform hat folgende Hauptfunktionen:

- **Eine einheitliche Plattform für all Ihre Daten.** Es ist die einzige Lösung, die eine Analyse der Bedrohungserkennung, Protokoll- und Ereignismonitoring sowie Endpunkt- und Netzwerksichtbarkeit mit Ermittlungs- und Threat-Intelligence-Funktionen datenübergreifend kombiniert. Durch die „dynamische Analyse“ liefert das fortschrittliche SIEM der RSA NetWitness Platform sofortigen Nutzen für neue und unbekannte Quellen, ohne dass benutzerdefinierte Analysen oder Coding erforderlich sind.
- **Integrierter Bedrohungs- und Unternehmenskontext.** Dank des hinzugefügten Unternehmenskontexts zur Bedrohungsanalyse können Unternehmen Bedrohungen basierend auf den potenziellen Auswirkungen für das Unternehmen priorisieren. Darüber hinaus werden die aus Branchenforschung und von unserer Kundenbasis gewonnenen Daten sowie eigene Informationen des Unternehmens vollständig aggregiert und bei der Erfassung operationalisiert, um Bedrohungen schneller erkennen zu können.
- **Integrierte Verhaltensanalyse.** RSA NetWitness® UEBA ist eine speziell entwickelte Big-Data-basierte Lösung für die Analyse des Nutzer- und Entitätsverhaltens (User and Entity Behavior Analytics, UEBA), die als zentraler Teil in die RSA NetWitness Platform integriert ist. Durch den Einsatz von unüberwachter statistischer Anomalieerkennung und maschinellem Lernen bietet die RSA NetWitness Platform eine umfassende verhaltensbasierte Erkennung unbekannter Bedrohungen und kann so auf eine Vielzahl von Anwendungsfällen angewendet werden. Die RSA NetWitness Platform erweitert Ihr vorhandenes Sicherheitsteam, um schnelle Erkennung und umsetzbare Einblicke in jedem Schritt des Angriffslebenszyklus zu ermöglichen.

- **Schnelle Ermittlungen.** Das fortschrittliche SIEM der RSA NetWitness Platform bietet eine erweiterte Workbench für Analysten, mit der Warnmeldungen und Incidents selektiert werden, einschließlich einer Schnittstelle, die speziell für Sicherheitsermittlungen entwickelt wurde. Durch die gewonnenen umfassenden Einblicke in Daten aus der gesamten Infrastruktur können Analysten einen Netzwerkangriff oder eine Datenexfiltration in Gänze nativ und visuell rekonstruieren. Das fortschrittliche SIEM versetzt Analysten in die Lage, im Verlauf der Zeit aufgetretene Incidents zu verbinden, um den vollen Umfang eines Angriffs aufzudecken und besser zu verstehen.
- **Automatisierung und Orchestrierung.** Bei RSA NetWitness® Orchestrator handelt es sich um eine umfassende Sicherheits- und Automatisierungstechnologie, die vollständiges Fallmanagement, intelligente Automatisierung und Orchestrierung sowie kooperative Ermittlungsfunktionen kombiniert. Mit RSA NetWitness Orchestrator können SOC-Analysten konsistente, transparente und dokumentierte Funktionen für Bedrohungsermittlung und Threat Hunting nutzen, indem sie Playbook-basierte automatisierte Reaktionen, automatische Erkennung und maschinelles Lernen verwenden, um mit optimierten Einblicken eine schnellere Problembehebung und bessere SOC-Effizienz zu erzielen.
- **Flexible, skalierbare Architektur.** Dank des breiten Spektrums an flexiblen Bereitstellungsoptionen lässt sich das fortschrittliche SIEM der RSA NetWitness Platform schrittweise skalieren und erfüllt so die Anforderungen und Sicherheitsprioritäten der Unternehmen. Ob es als einzelne Appliance oder im Dutzend, nur teilweise oder vollständig virtualisiert oder vor Ort oder in der Cloud bereitgestellt wird: Das fortschrittliche SIEM der RSA NetWitness Platform unterstützt die kundenspezifischen Architekturen.
- **End-to-End Security Operations.** Das fortschrittliche SIEM der RSA NetWitness Platform ist die einzige Plattform, die Analysen, Protokoll- und Ereignismonitoring sowie Endpunkt- und Netzwerksichtbarkeit mit Advanced Threat Intelligence und automatisiertem Incident-Management für optimierte Security Operations vereint.

Digitale Risiken betreffen alle
Wir helfen Ihnen, sie zu beherrschen

RSA bietet unternehmensgesteuerte Sicherheitslösungen, mit denen Unternehmen einen einheitlichen Ansatz für das Management digitaler Risiken nutzen können, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Aktionen basiert. RSA-Lösungen sollen Unternehmen die effektive Erkennung und Abwehr komplexer Angriffe, das Management der Nutzerzugriffskontrolle sowie die Verringerung von Geschäftsrisiken, Betrug und Cyberkriminalität ermöglichen. RSA schützt Millionen Nutzer auf der ganzen Welt und trägt dazu bei, dass mehr als 90 % der Fortune 500-Unternehmen Erfolg haben und sich kontinuierlich an Transformationsänderungen anpassen.

Finden Sie heraus, wie Sie in einer dynamischen, hochriskanten digitalen Welt erfolgreich sein können. Besuchen Sie rsa.com/de-de

RSA