RSA NetWitness® UEBA

Hauptmerkmale

- *Patentiertes rekursives, unüberwachtes maschinelles Lernen von Verhalten*
- *Native Datenerhebung*
- *Innovatives Feature-Gewichtungsschema*
- *Vereinfachte Engine für Risikobewertung*
- *Breites Spektrum an Anwendungsfällen*
- *Visualisierung von Identitätskontext*
- *Automatische falsch positive Reduktionsalgorithmen*

Hauptvorteile

- *Reduzierte MTTD und MTTI*
- *Schnellere Incident Response*
- *Weniger falsch positive Ergebnisse*
- *Ergänzender identitätsbasierter Kontext*
- *Schnelle Identifizierung riskanter Nutzer*

Besserer Kampf gegen die sich verändernden destruktiven Bedrohungen, und zwar unabhängig davon, auf welchem Gebiet die Angreifer tätig werden.

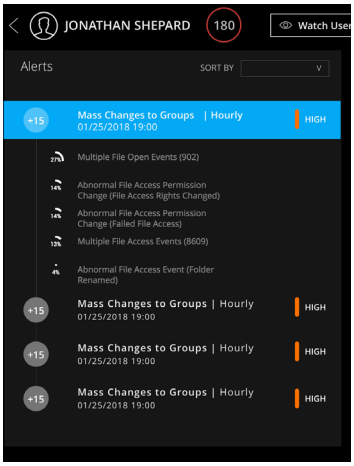
Bedrohungen schneller erkennen. Verkürzte Verweildauer. Automatisierte Reaktion.

In einer Ära ständig wachsender Angriffsflächen ist der Schutz vor Bedrohungsakteuren – von Commodity-Malware über Insiderbedrohungen und Crimeware bis hin zu staatlich tolerierten Angriffen, Hacktivisten und Terroristen – zu einer immer komplexeren Aktivität geworden. Nicht alle Bedrohungen werden auf die gleiche Weise erstellt. Dennoch sind die getrennten Silos der Präventions-, Monitoring- und Ermittlungstechnologien nach wie vor nicht in der Lage, die SOCs (Security Operations Centers) so zu unterstützen, dass falsch positive Ergebnisse schnell erkannt und zielgerichtete Indikatoren bereitgestellt werden (im Gegensatz zu offenen Silo-Warnmeldungen). Eine umfassende und kooperative Lösung ist erforderlich, mit der Sicherheitsanalysten die für ihr Unternehmen wichtigsten Bedrohungen erkennen und darauf reagieren können.

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. Mithilfe von unüberwachten Algorithmen für maschinelles Lernen bietet RSA NetWitness UEBA für eine Vielzahl von Anwendungsfällen eine verhaltensbasierte, umfassende Erkennung unbekannter Bedrohungen, ohne dass ein Analyse-Tuning erforderlich ist. RSA NetWitness UEBA erweitert Ihr vorhandenes Sicherheitsteam, um schnelle Erkennung und umsetzbare Einblicke in jedem Schritt des Angriffslebenszyklus zu ermöglichen. RSA NetWitness UEBA ist ein zentraler Teil der RSA NetWitness Platform und hilft bei den Ermittlungen des vollständigen Angriffslebenszyklus sowie bei der Behebung der Sicherheitsverletzung.

Bedrohungen in allen Umgebungen erkennen

RSA NetWitness UEBA erhöht die gebrauchsfertigen automatisierten Funktionen für Bedrohungserkennung der RSA NetWitness Platform. Mithilfe von nativen und zentralen Funktionen der RSA NetWitness Platform – Netzwerkerfassung, Protokollerfassung, Endpunktsichtbarkeit sowie ergänzende einheitliche Metadaten (im Tempo des maschinellen Lernens) – können Sicherheitsanalysten sowohl interne als auch externe Angreifer durch klare, fokussierte Warnmeldungen aussperren. RSA NetWitness UEBA nutzt künstliche Intelligenz und einen überlegenen mathematischen maschinellen Lernansatz für das Baselining von Nutzern und Benutzergruppen, Entitäten und unternehmensweitem Verhalten, um normale, gute Aktivitäten von bösartigen Abweichungen zu unterscheiden und so eine richtige und umsetzbare Incident Response zu ermöglichen.



Antworten. Keine offenen Fragen

RSA NetWitness UEBA unterstützt Sicherheitsanalysten bei der Identifizierung von Kompromittierungsquellen und verdächtigen Vorkommnissen. Dies geschieht mithilfe der identitätsbasierten chronologischen Visualisierung, die verdächtige Indikatoren in Übereinstimmung mit dem MITRE ATT&CK™-Framework hervorheben und so eine effizientere und vollständigere Incident Response.

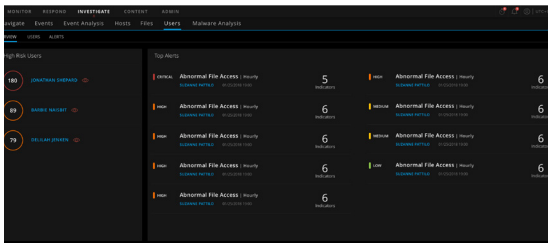
RSA

UEBA-Anwendungsfälle:

- *Insiderbedrohung*
- *Brute-Force*
- *Kontenübernahme*
- *Kompromittiertes Konto*
- *Missbrauch von Kontoberechtigungen*
- *Erweiterte Berechtigungen*
- *Snooping-Nutzer*
- *Datenexfiltration*
- *Ungewöhnlicher Systemzugriff*
- *Laterale Bewegung*
- *Malware-Aktivität*
- *Verdächtiges Verhalten*

RSA NetWitness UEBA wird mit jedem Einschalten intelligenter und zeigt ungewöhnliches Verhalten schnell und präzise an, ohne dass ein ständiges Nachjustieren Ihrerseits erforderlich ist.

Leistungsstarke automatische Erkennung



Das automatisierte und kontinuierliche Monitoring beschleunigt die Erkennung von böswilligen Insidern und Cyberkriminellen, die kompromittierte Konten verwenden – ohne Regeln, Signaturen oder manuelle Analysen. RSA NetWitness UEBA verfügt über leistungsstarke Data-Science-Modelle, die Unternehmen die Möglichkeit bieten, neue Tools, Techniken und Prozesse (TTPs) zu erkennen, und bietet End-to-End-Ermittlungen, die es Analysten ermöglichen, sich von reinen Analyseergebnissen auf die Gesamtrisiken des Unternehmens zu konzentrieren.

Durch die Nutzung einer Big-Data-fähigen und skalierbaren Technologiearchitektur liefert RSA NetWitness UEBA eine leistungsstarke Engine für die Bedrohungserkennung, die unzusammenhängende Ereignisse verknüpft und so ungewöhnliche Aktivitäten sowie bisher unbekannte Nutzerbedrohungen ans Licht bringt – und das alles in einer einzigen Nutzerschnittstelle.

UEBA. Zentraler Teil der Plattform

Fokussierte, umsetzbare und kontextsensitive Warnmeldungen zielen auf Nutzerverhalten ab, das potenziell Anzeichen für verdächtige Aktivitäten enthält. Auf diese Weise erhalten die Sicherheitsanalysten mehr Schlagkraft. Die RSA NetWitness Platform führt adaptive UEBA (User and Entity Behavior Analytics) ein, die mit der Flexibilität und Geschwindigkeit der sich verändernden Bedrohungen Schritt halten können. Die RSA NetWitness Platform ist in der Lage, unbeaufsichtigte Protokolldaten zu erfassen, sodass Sicherheitsanalysten Angreifer entlarven können. Dafür werden dynamische, nicht deterministische Erkennungsalgorithmen, Baselining, Verhaltensmodellierung und Peer-Gruppenanalysen eingesetzt.

RSA NetWitness UEBA und UEBA Essentials bringen Ereignisse mit höherer Priorität ans Licht, die in Echtzeit über Protokollereignisse, Netzwerkdatenverkehr und Endpunktsichtbarkeit hinweg korreliert werden. Damit bietet sich für SOC-Teams die Möglichkeit, die durchschnittliche Erkennungszeit (Mean Time To Detect, MTTD) und die durchschnittliche Ermittlungszeit (Mean Time To Investigate, MTTI) zu senken, Alert-Fatigue (Alarmmüdigkeit) und falsch positive Ergebnisse zu reduzieren sowie präzisere Bedrohungsprognosen und vorausschauende Analysen zu liefern.

Die RSA NetWitness Platform

Mit mehr als 30 Jahren Erfahrung im Sicherheitsbereich ist RSA mit innovativen Lösungen für die größten Herausforderungen bei Security Operations weltweit der Branchenführer. Das neue Produkt RSA NetWitness UEBA erweitert die RSA NetWitness Platform und die Angebote für fortschrittliches SIEM und Threat Defense und bietet so umfassende Sichtbarkeit über Protokolle, Netzwerke und Endpunkte hinweg.

Auf unserer Website RSA.com/de-de/DoMore finden Sie alle aktuellen Integrationen, Fallstudien und Best Practices.