RSA NetWitness® UEBA – Anwendungsfälle

Leistungsstarke Erkennung von nutzerbasierten Bedrohungen

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 RSA NetWitness UEBA eine umfassende verhaltensbasierte Erkennung unbekannter Bedrohungen und kann so auf eine Vielzahl von Anwendungsfällen angewendet werden. RSA NetWitness UEBA erweitert Ihr vorhandenes Sicherheitsteam, um schnelle Erkennung und umsetzbare Einblicke in jedem Schritt des Angriffslebenszyklus zu ermöglichen.

Achten Sie bei der Bewertung von UEBA (User and Entity Behavior Analytics)-Lösungen auf folgende wichtige Features und Funktionen:

- Vollautomatische und kontinuierliche Bedrohungserkennung und -überwachung
- Sichtbarkeit über den gesamten Angriffslebenszyklus durch Datenerhebung, Erkennung, Ermittlung und Reaktion
- Natürliche Sprachindikatoren, abgestimmt auf das MITRE ATT&CK™-Framework
- Unüberwachtes maschinelles Lernen anhand eines gebrauchsfertigen Data-Science-Modells mit Zero Touch und ohne Tuning
- Zentraler Endpunkt-Agent der Plattform für kombinierte Protokollerfassung mit Endpunkterkennung und -reaktion

Hauptfunktionen von UEBA der Enterprise-Klasse

Native Datenerhebung

Eine große Herausforderung vieler SOC-Teams besteht darin, die Erfassung, Speicherung und Analyse aller Protokolle zu managen, die von den umfangreichen Portfolios der lokalen und Cloud-basierten Systeme des Unternehmens in unterschiedlichen Formaten produziert werden. RSA NetWitness UEBA löst dieses Problem, indem Protokollrohdaten von diesen Systemen erfasst, Aktivitäten, die von Personen und Prozessen aus zahlreichen Quellen erzeugt werden, dynamisch analysiert und relevante Sicherheitsinformationen aus diesen Datenquellen interpretiert werden.

Einheitliche Metadatentaxonomie

Damit eine UEBA-Lösung optimal ausgeführt werden kann, sollten die erfassten Daten von Protokollen, Netzwerkverkehr und Endpunkten analysiert, normalisiert und zum Erfassungszeitpunkt in eine einheitliche, konsistente Metadatentaxonomie umgewandelt werden. Da RSA NetWitness UEBA eine zentrale Komponente von fortschrittlichem SIEM der RSA NetWitness Platform ist, geschieht dies automatisch.

Erkennung im Tempo des maschinellen Lernens

In vielen Fällen lassen sich Bedrohungsindikatoren von Punktsicherheitslösungen nicht zuverlässig oder konsistent für die Angriffsidentifizierung verwenden, da diese Aktivitäten selbst meist kein Angriffsziel sind. Warnmeldungen dieser Aktivitäten würden also dazu führen, dass Analysten von sinnlosen Warnmeldungen überflutet werden. Mit RSA NetWitness UEBA werden viel fokussiertere und umsetzbare Warnmeldungen ausgegeben als von Punktsicherheitslösungen, denn das Tool untersucht die Aktivitäts- und Verhaltensmuster im Laufe der Zeit, setzt maschinelles Lernen ein, um Abweichungen im Baseline-Verhalten zu identifizieren, und lernt aus vorherigen Warnmeldungen, die als falsch positive Ergebnisse erkannt wurden.

Warum ist UEBA zu einer zentralen Sicherheitsanforderung geworden?

- 28 % der gemeldeten Sicherheitsverstöße stammen von internen Akteuren. Mit UEBA ist es einfacher, solche Bedrohungen zu erkennen.
- Diese gemeldeten internen Sicherheitsverstöße werden hauptsächlich von Systemadministratoren und Endnutzern verursacht.
- 68 % der Verstöße werden erst nach zwei Monaten oder noch später erkannt. Mit UEBA können Sicherheitsteams diese Bedrohungen schneller erkennen.
- In erster Linie geht es bei den gemeldeten Verstößen um gestohlene Zugangsdaten und den Missbrauch von Zugriffsrechten. UEBA ist darauf ausgelegt, bei solchen Aktivitäten Warnmeldungen auszugeben.

Verizon Data Breach Investigations Report 2018, Verizon.

Weitere Informationen

Besuchen Sie RSA.com/de-de/DoMore oder planen Sie eine Demo.

RSA

6 Anwendungsfälle, für deren Erkennung RSA NetWitness UEBA entwickelt wurde

Ungewöhnliche Aktionen/ Änderungen

Falls ein Angreifer Zugriffsrechte auf eine Active-Directory (AD)-Domäne oder einen Domain Controller erhält, kann er über diesen Zugriff die gesamte AD-Struktur steuern oder sogar zerstören. Wenn er nur einen einzigen Domain Controller kompromittiert, können alle Änderungen an diesem Controller auch auf jedes andere System repliziert werden. RSA NetWitness UEBA hilft Analysten bei der Erkennung solcher Szenarien, da Spitzen bei der Anzahl von Nutzeraktionen in einer AD-Domäne identifiziert werden, die darauf hindeuten, dass ein Konto kompromittiert und/oder verwendet wird, um wichtige Verzeichnisdaten zu beschädigen oder zu zerstören.

Ungewöhnliche Zugriffsrechte

Mit RSA NetWitness UEBA können Sie feststellen, ob über die Zugriffsrechte eine mögliche Insiderbedrohung vorliegt. Falls beispielsweise ein Helpdesk-Techniker beginnen sollte, von seinen „normalen“ Routinen und festgelegten Sicherheitsrichtlinien abzuweichen und die Kennwörter von neuen Nutzern so zu konfigurieren, dass diese nie ablaufen, würde RSA NetWitness UEBA das bemerken.

Snooping

Snooping bezeichnet den unbefugten Zugriff auf die Daten einer anderen Person oder eines Unternehmens. Dazu zählt zum Beispiel, wenn ein interner Nutzer oder externer Angreifer versucht, Server und Ordner zu durchsuchen, auf die er keinen Zugriff hat. Das geschieht in der Regel mit der Absicht, wichtige Unternehmensinformationen aufzuspüren. Bei ausgeklügeltem Snooping werden bestimmte Programme eingesetzt, um Aktivitäten auf einem Computer remote zu überwachen oder eine automatische Dateierkennung durchzuführen.

RSA NetWitness UEBA kann Snooping auf verschiedene Weise erkennen: Die Lösung erfasst sowohl fehlgeschlagene als auch erfolgreiche Versuche der Nutzer, auf Daten zuzugreifen, für die sie keine Zugriffsberechtigung haben. Wenn die Lösung eine ungewöhnlich hohe Anzahl fehlgeschlagener und erfolgreicher Zugriffsversuche auf Dateien an einem neuen Speicherort in kurzer Zeit erkennt, wird eine Warnmeldung ausgelöst.

Brute-Force-Authentifizierung

Ausgefeilte UEBA-Lösungen können zwischen einem tatsächlichen Brute-Force-Angriff und einer „normalen“ fehlgeschlagenen Authentifizierung unterscheiden, da sie letztere im Kontext weiterer ungewöhnlicher Nutzeraktivitäten betrachten. RSA NetWitness UEBA löst nur Warnmeldungen aus, wenn zusätzlich zu wiederholten fehlgeschlagenen Authentifizierungen auch andere verdächtige Verhaltensmuster erkannt werden. Auf diese Weise werden falsch positive Ergebnisse aufgrund von fehlerhaften Netzwerkkonfigurationen oder falsch eingegebenen Kennwörtern der Nutzer vermieden.

Maschinengesteuerte Aktivitäten

RSA NetWitness UEBA kann erkennen, wenn ein bösartiges Programm versucht, mit kompromittierten Zugangsdaten auf Unternehmensressourcen mit eingeschränktem Zugriff zuzugreifen. Über Nutzerprofile lassen sich Anzeichen eines Brute-Force-Angriffs erkennen, wohingegen Entity-Profile einen erheblichen Anstieg bei verdächtigem Entity-Verhalten erfassen. Beispielsweise, wenn bei Hunderten Konten sehr viele Aktivitäten erkannt werden, die über ein einziges Gerät oder eine einzelne IP-Adresse erfolgen, oder wenn auf mehreren Computern extrem viele Dateien umbenannt werden, und zwar von einem einzigen Computer aus, auf dem das bösartige Programm installiert ist.

Erweiterte Berechtigungen

Angreifer versuchen häufig, die regulären Nutzer des Unternehmens zu verwenden. Das ist meist einfacher, als sich selbst erweiterte Berechtigungen für spätere Netzwerkangriffe zu verschaffen. Das sorgfältige Monitoring von Aktivitäten im Zusammenhang mit Zugriffsrechten, gewährtem Zugriff, sensiblen Gruppen usw. ist entscheidend, um kompromittierte Zugangsdaten zu bekämpfen. Da die Nutzer mit ihren Zugriffsrechten nicht immer einem „normalen“ Verhaltensmuster folgen, sind falsch positive Ergebnisse unvermeidlich. Daher sind die Identifizierung, Erfassung und Analyse von angehäuften Indikatoren von entscheidender Bedeutung, um die bösartigen herauszufiltern.

Falls sich also ein Akteur mit erweiterten Berechtigungen nach mehreren fehlgeschlagenen Authentifizierungsversuchen an einem ungewöhnlichen Ort anmeldet und anschließend neue Nutzerkonten mit erweiterten Berechtigungen erstellt werden, führt dies zu einem hohen Risiko in der Liste der Top-Warnmeldungen.

Bevor Sie Ihrem Sicherheitspaket eine weitere Punktlösung (in diesem Fall UEBA) hinzufügen, sollten Sie sich die Frage stellen, ob das wirklich einen Mehrwert bringt oder eher für mehr Störungen sorgt. Der Vorteil von RSA NetWitness UEBA ist, dass es neben herkömmlichen Bedrohungen auch kritische nutzerbasierte Anomalien erkennt – und das alles mit einer vereinheitlichten Plattform.

09/20 Anwendungsfall, H17457-1 W386667