DATENBLATT

User and Entity Behavior Analytics (UEBA)

LogRhythm
The Security Intelligence Company

Benutzerkonten werden von Hackern oft als Angriffsvektor missbraucht, um wertvolle Daten zu stehlen oder verheerende Schäden anzurichten. Insider-Bedrohungen und kompromittierte Anmeldedaten stellen für Ihr Unternehmen ein erhebliches Risiko dar, und entschärfen können Sie sie nur, wenn Sie sie entdecken. Eine Reihe von Faktoren vergrößert diese Herausforderung noch zusätzlich:

- Die Vermischung privater und beruflicher Benutzerkonten
- Die Ausdehnung der IT-Landschaft auf Kunden, Hersteller und Technologiepartner
- Der ständige Druck, Zugriffe zu erteilen, um die geschäftliche Produktivität zu fördern

User and Entity Behavior Analytics (UEBA) von LogRhythm erkennt und neutralisiert sowohl bekannte als auch unbekannte benutzerbezogene Bedrohungen. Die Lösung analysiert die vielfältigen Daten, die LogRhythm erfasst, um Insider-Bedrohungen, kompromittierte Konten sowie die falsche oder missbräuchliche Verwendung von Berechtigungen zu entdecken – alles in Echtzeit.

LogRhythm UEBA ist in die LogRhythm-Plattform integriert und erspart Ihnen dadurch die kostspielige Duplikation von Daten, die Verwaltung von zwei Plattformen sowie komplizierte Analysen mit unterschiedlichen Systemen. Folgende Fähigkeiten ermöglichen die durchgehende Verwaltung des gesamten Lebenszyklus von Bedrohungen:

- Die patentierte LogRhythm AI Engine™ entdeckt Bedrohungen mittels maschinellem Lernen, Verhaltensprofilen, Peergruppen-Analysen und weiteren Methoden
- Unstrukturierte und kontextbezogene Suchen ermöglichen schnelle forensische Untersuchungen
- Die Identity Inference-Funktion nutzt Authentifizierungs-, Zugriffs-, DHCP- und andere Daten, um automatisch zu ermitteln, wer hinter ansonsten anonymen Daten steckt
- Die eingebettete Sicherheitsorchestrierung und -automatisierung standardisiert und automatisiert koordinierte Reaktionen
- Smart**Response**™ Plug-ins automatisieren manuelle Aufgaben und ermöglichen die zentralisierte Ausführung vordefinierter Gegenmaßnahmen

Anwendungsfälle für UEBA

Insider-Bedrohungen: Benutzer mit legitimem Zugriff auf interne Netzwerke stellen oft die größte Gefahr für die Unternehmenssicherheit dar. Insider-Bedrohungen beginnen meist damit, dass sich ein Benutzer auf verdächtige Art umherbewegt und dann in ungewöhnlicher Weise auf Systeme, Anwendungen und Dateien zugreift. Die Überwachung auf Insider-Bedrohungen hilft, Datendiebstahl, Betrug, Sabotage, Richtlinienverletzungen und andere gefährliche Aktivitäten zu entdecken.

Kontoübernahme: Angreifer, die in Ihr Netzwerk eingedrungen sind, werden schnell versuchen, ein Benutzerkonto zu übernehmen. Sie werden ihre Präsenz nach Möglichkeit so lange ausweiten, bis sie am Ziel sind oder aber entdeckt werden. LogRhythm UEBA entlarvt Betrüger durch Festlegung und Analysen des „normalen" Verhaltens individueller Benutzer und der zugehörigen Peergruppen. Externe Bedrohungen werden schnell ermittelt, sodass weitere Kompromittierungen und Schäden verhindert werden.

Missbrauch und falscher Gebrauch von Rechten: Privilegierte Anwender werfen für Unternehmen ein besonderes Risiko auf, da sie erweiterten Zugriff auf Systeme und Daten haben. Mit LogRhythm UEBA können Sie dafür sorgen, dass Zugriffsrechte korrekt verwendet werden. Die Algorithmen der Lösung überwachen automatisch die Erstellung, Nutzung und Löschung privilegierter Konten, die Erhöhung von Berechtigungen sowie die verdächtige Nutzung privilegierter Konten.

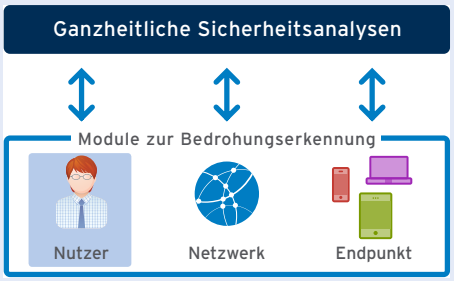
Anwendungsfälle für UEBA

- ✓ Insider-Bedrohungen
- ✓ Kompromittierte Konten
- ✓ Missbrauch und falscher Gebrauch privilegierter Konten

„Wir nutzen LogRhythm, um Innentäter und kompromittierte Konten zu finden und den für die Problembehebung zuständigen Mitarbeitern einen umfassenden Einblick in unsere Umgebung zu verschaffen."

–– Sicherheitsmanager bei einem Hersteller von Computer-Hardware für Unternehmen

TVID: 77A-CD4-677



Die Bedrohungsanalysen von LogRhythm umfassen die gesamte Angriffsfläche, von Ihren Benutzern und Entitäten bis hin zu den Netzwerken und Endpunkten.

LogRhythm bietet eine einheitliche Konsole zur Verwaltung des gesamten Lebenszyklus von Sicherheitsbedrohungen, einschließlich eigener Dashboards für UEBA.

So wird LogRhythm UEBA bereitgestellt

Sie können LogRhythm UEBA über unser User Threat Detection Module (UTDM) aktivieren. Dieses Modul macht die problematischsten Vorgänge in Ihrer IT-Umgebung anhand szenariobasierter Algorithmen erkennbar, die maschinelles Lernen, Verhaltensprofile, Peergruppen-Analysen, statistische Analysen, erweiterte Korrelationen und andere Analysemethoden anwenden. Das Modul wertet zur Erkennung von Bedrohungen primär die Anwenderaktivitäten aus, jedoch auch Netzwerk- und Endpunktaktivitäten. Dank zahlreicher verschiedener Analysetechniken, die auf ein breites Spektrum von Daten angewandt werden, kann das UTDM echte Bedrohungen exakter priorisieren und Fehlalarme reduzieren.

Unsere Sicherheitsanalyse-Module werden von LogRhythm Labs weiterentwickelt und aktiv gepflegt, damit Sie den neuesten benutzerbezogenen Bedrohungen stets einen Schritt voraus bleiben. Diese wertvollen Inhalte werden ohne zusätzliche Kosten über die Cloud bereitgestellt.

Sie erhalten zum UTDM einen leicht verständlichen Bereitstellungsleitfaden, der nach Anwendungsfällen strukturiert ist und detaillierte Implementierungsanweisungen sowie Best Practices für die Feinabstimmung enthält. Viele Kunden implementieren das UTDM eigenständig. Für Expertenhilfe können Sie unseren Dienst Co-Pilot Analytics nutzen: Damit steht Ihren Mitarbeitern eine spezifische LogRhythm-Ressource zur Verfügung, die Sie durch den Setup führt und Sie bei der laufenden Verwendung und Optimierung des UTDM unterstützt.

Fähigkeiten von LogRhythm UEBA

Wichtige Fähigkeiten laut Forrester*	LogRhythm-Funktionalitäten
1) Sammlung verschiedenster Daten – und zwar in großen Mengen.	LogRhythm sammelt Maschinendaten aus Ihrer gesamten Umgebung und füllt durch Überwachung von Endpunkten und Netzwerken die Lücken in Ihrer Forensik. Unser patentiertes Machine Data Intelligence Fabric gewährleistet, dass die Daten für Sicherheitsanalysen optimiert werden.
2) Korrelation von Logdaten, um Identitäten herauszufiltern.	Die Identity Inference-Funktion weist anonymen Log-Meldungen Identitäten zu und zeigt Ihnen damit, wer hinter den Aktionen steckt, die Auswirkung auf Ihre Umgebung haben. Dies erleichtert forensische Untersuchungen.
3) Durchführung von Verhaltensanalysen, um eine heuristische Baseline der Benutzeraktivitäten erstellen zu können.	Die AI Engine™ ermöglicht durch multidimensionales Baselining die Modellierung eines breiten Spektrums von Verhaltensweisen von Benutzern. Die Baselines werden verwendet, um mittels maschinellem Lernen und anderen statistischen Analyseverfahren ungewöhnliches Verhalten zu erkennen.
4) Nutzung der heuristischen Baseline, um ungewöhnliches Verhalten in Echtzeit zu erkennen.	LogRhythm gleicht die aktuellen Aktivitäten kontinuierlich mit den Baselines ab, die die AI Engine™ für jede Identität und jede Peergruppe erstellt hat. Verhaltensweisen, die von den Baselines für die Nutzer und Peergruppen abweichen, werden erkannt.
5) Erkennung von Bedrohungen durch Datenexfiltration, missbräuchliche und falsche Verwendung privilegierter Identitäten und Betrug.	LogRhythms szenariobasierte Analysen umfassen Verhaltensanomalien, um bekannt verdächtige Muster zu erkennen, einschließlich Datenexfiltration, Missbrauch von Rechten und Betrug.
6) Fallmanagement, Untersuchung von Sicherheitsereignissen und umfassende Berichterstattung.	LogRhythm beschleunigt die Untersuchung und Reaktion durch integrierte Funktionalitäten zur Steuerung und Automatisierung von Sicherheitsmaßnahmen. Dank vordefinierter Smart**Response**-Aktionen können Sie schnell reagieren, um forensische Daten zu sammeln und eine gezielte Problembehebung einzuleiten. Zudem können Sie Berichte zu den Ergebnissen Ihrer Sicherheitsmaßnahmen erstellen, einschließlich der Erkennungs- und Reaktionszeiten.

*Forrester, Market Overview: Security User Behavior Analytics, 2016

Vorteile von LogRhythm UEBA

- Minimiert Ihre Gesamtbetriebskosten (TCO) durch eine einheitliche Plattform für Security Intelligence und Sicherheitsanalysen
- Erkennt dank mehrdimensionaler Verhaltensanalysen bekannte und unbekannte Bedrohungen
- Erhärtet und meldet wichtige Ereignisse, die sonst womöglich unentdeckt bleiben würden
- Ermöglicht Ihnen, Fehlalarme aus Ihrer Prioritätsliste zu entfernen, die durch unseren risikobasierten Prioritätsalgorithmus nicht erhärtet werden
- Unterstützt Ihre Sicherheitsanalytiker effizient durch eine einheitliche Konsole, die die umfassende Erkennung, Abwehr und Neutralisierung von Bedrohungen ermöglicht