CloudAI für UEBA

LogRhythm
The Security Intelligence Company

Benutzerseitige Bedrohungen erkennen und entschärfen – mit künstlicher Intelligenz

Ihr Unternehmen ist mit einer wachsenden Zahl schnell veränderlicher Bedrohungen konfrontiert, die immer komplexer werden – und die gefährlichsten sind diejenigen, die am schwersten zu finden sind. Darüber hinaus haben Sie vielleicht mit Personalmangel und ineffizienten manuellen Workflows zu kämpfen. Um all diese Herausforderungen zu bewältigen, müssen Ihre Sicherheitsanalytiker zeitaufwändige Routineaufgaben abgeben können, um sich auf die wichtigen Probleme zu konzentrieren, die menschliche Entscheidungen erfordern. Zudem braucht Ihr Team aussagekräftigere Analysen, um verborgene Bedrohungen aufzudecken.

LogRhythm CloudAI, ein Add-on zur LogRhythm Threat Lifecycle Management (TLM) Plattform, hilft Ihrem Team mit künstlicher Intelligenz (KI) und maschinellem Lernen, komplexe Bedrohungen zu finden. Für die Cloud konzipiert, wendet CloudAI selbstlernende künstliche Intelligenz auf Daten zu Ihrer IT-Umgebung an. Dies ermöglicht es, bislang unentdeckte Bedrohungen zu finden und schnell einzuordnen und zu untersuchen. Zugleich beschleunigt dieser Ansatz die Wertschöpfung.

CloudAI erkennt interne Bedrohungen, kompromittierte Konten, Missbrauch und falsche Nutzung von Administratorenrechten und andere benutzerseitige Bedrohungen. Insbesondere eignet sich die Lösung zur maschinengestützten Überwachung hochriskanter Benutzer, etwa in den IT-, Finanz- und Führungsteams. Die hochentwickelten Analysen von CloudAI liefern Ihren Analytikern evidenzbasierte Ausgangspunkte für die Bedrohungssuche und aussagekräftige Datenvisualisierungen zur maschinengestützten Einordnung und Untersuchung von Bedrohungen.

CloudAI für UEBA auf einen Blick

- Mit künstlicher Intelligenz und maschinellem Lernen komplexe Bedrohungen erkennen
- Bislang unbekannte Angriffe und Angriffsmethoden aufdecken
- Interne Bedrohungen, kompromittierte Konten, Missbrauch von Admin-Rechten und andere benutzerseitige Bedrohungen erkennen
- Aussagekräftige Datenvisualisierungen helfen, Bedrohungen einzuordnen und zu untersuchen
- Effiziente Workflows und die enge Integration mit der LogRhythm-Plattform erleichtern den Analytikern die Arbeit
- Schnelle Amortisierung dank Cloud-Bereitstellung, automatisierter Datenverarbeitung und sich selbst weiterentwickelnder Analysen

Das CloudAI-Dashboard für Benutzeraktivitäten ermöglicht es, potenziell riskante Benutzer und Rechnerkonten zu überwachen und anormales Verhalten schnell im Detail einzusehen.

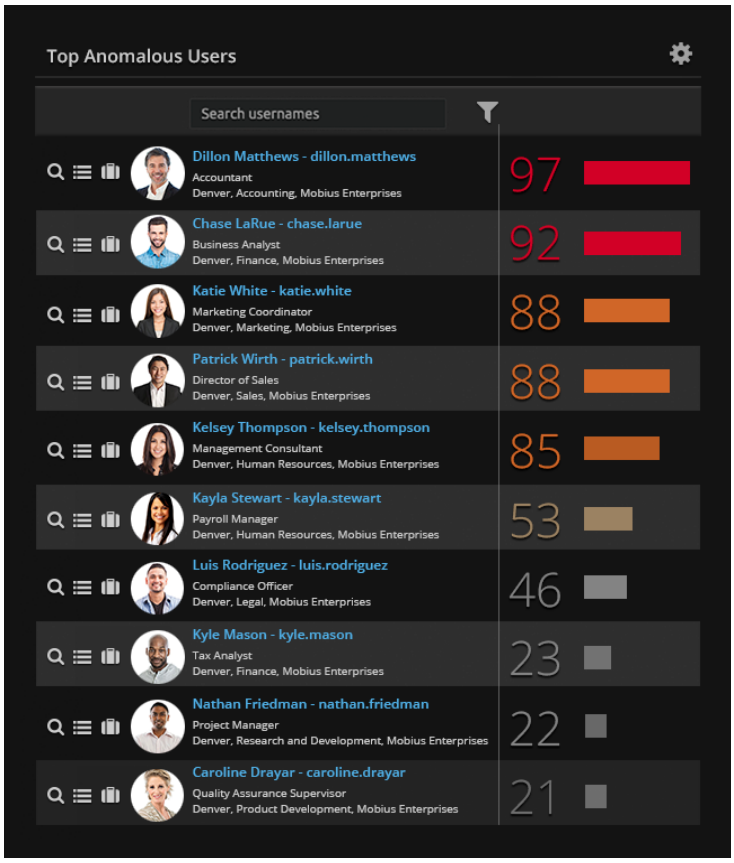
Vielfältige Analysetechniken für ein breites Spektrum von Angriffen

Das Add-on CloudAI identifiziert verborgene Bedrohungen, indem es wichtige Veränderungen im Benutzerverhalten erkennt, die auf Risiken für das Unternehmen hindeuten. Es ergänzt dabei die praxisbewährten Bedrohungsmodelle, die die LogRhythm AI Engine anwendet. Hand in Hand eingesetzt, liefern die beiden Lösungen fundierte Analysen. Dazu setzen sie eine Vielzahl einander ergänzender Analyseverfahren ein, um bekannte wie auch unbekannte Bedrohungen zu entdecken. Zudem lassen sich dank dieser einzigartigen Methoden Verdachtsmomente besser erhärten und Bedrohungen somit präziser priorisieren. Gemeinsam liefern CloudAI und AI Engine automatisierte Echtzeitanalysen zu sämtlichen Aktivitäten in der IT-Umgebung und vermitteln einen tiefgehenden Einblick in benutzerseitige Bedrohungen, die andernfalls nicht erkannt würden.

Bedrohungen schneller erkennen

CloudAI verbindet ein breites Spektrum von Verhaltensmodellen mit maschinellem Lernen und künstlicher Intelligenz, um Veränderungen in der Interaktion der Benutzer mit der IT-Umgebung zu erkennen und zu charakterisieren. Davon ausgehend, können Ihre Analytiker benutzerseitigen Bedrohungen nachgehen, einschließlich signaturloser und verborgener Bedrohungen.

Mittels LogRhythm TrueIdentity bildet CloudAI verschiedene Benutzerkonten (z.B. VPN, geschäftliche E-Mail, persönlicher Cloudspeicher) sowie die entsprechenden Kennungen (z.B. Benutzername, E-Mail-Adresse) auf die tatsächliche Identität des Benutzers ab, um umfassende verhaltensbezogene Baselines zu erstellen. Da die Aktivitäten eines Benutzers einer Identität zugeordnet werden, unabhängig davon, wie seine Konten dargestellt werden, können Sie sicher sein, dass bei Analysen alle relevanten Benutzeraktivitäten einbezogen werden. CloudAI baut die Benutzerprofile auf Verhaltensmodelle auf, die die Aktivität des Benutzers mittels zahlreicher relevanter Datenmerkmale detailliert widerspiegeln.



Die CloudAI-Listen der „Top Anomalous Users" und „Top Anomalous Machine Accounts" bieten sich als Ausgangspunkt für die Suche nach Bedrohungen an.

Überlassen Sie die Datenaufbereitung LogRhythm

Dank langjähriger Erfahrung im Bereich Sicherheitsanalysen besitzt LogRhythm unerlässliches Know-how für die Aufbereitung und Analyse von Maschinendaten zu Sicherheitszwecken. CloudAI gibt Ihnen Zugriff auf die branchenweit saubersten und sicherheitsrelevantesten Daten, aufbereitet durch das LogRhythm Machine Data Intelligence (MDI) Fabric. Daher können die meisten Unternehmen darauf verzichten, externe Beratungsdienstleistungen in Anspruch zu nehmen, wie es bei anderen UEBA-Anbietern notwendig ist. Durch die Anwendung hochentwickelter künstlicher Intelligenz und maschineller Lernverfahren auf hochwertige Daten kann CloudAI potenzielle Bedrohungen besser ans Licht bringen.

Datenanreicherung durch das LogRhythm MDI Fabric

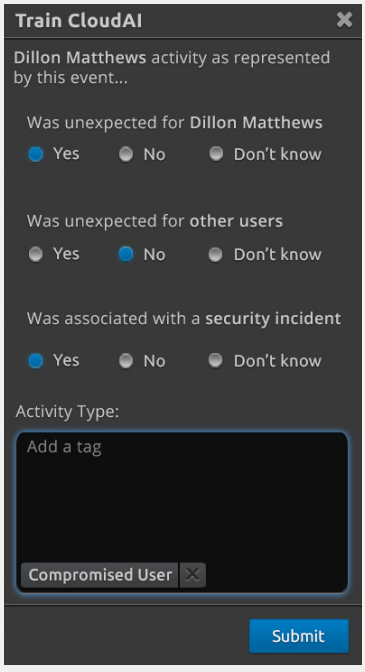
- Daten-Parsing
- Klassifizierung von Ereignissen
- Geolokalisierung
- Risikobasierte Priorisierung
- Zeitnormalisierung
- Und mehr ...

Schnelleres Lernen

CloudAI ist in der Lage, von Ihrer IT-Umgebung zu lernen. So kann Ihr Team die Umgebung sowohl vor aktuellen als auch künftigen Bedrohungen schützen. Die Lösung entwickelt sich selbst weiter, was sich schon binnen Tagen bezahlt macht und eine laufende Feinabstimmung ohne manuelle Eingriffe ermöglicht. Zudem wird CloudAI im üblichen Verlauf einer Untersuchung von den Sicherheitsanalytikern trainiert. Dieser hybride Ansatz erschließt sämtliche Vorteile unüberwachten Lernens (zügige Übernahme und Nutzung) und überwachten Lernens (präzisere Erkennung von Bedrohungen), sodass die Intelligenz der Lösung noch schneller zunimmt.

Die Benutzeroberfläche von CloudAI unterstützt Feedback durch die Analytiker, indem sie im natürlichen Workflow der Sicherheitsmaßnahmen relevante Informationen sammelt. Wenn Ihr Mitarbeiter beispielsweise ein Ereignis auf der Nutzer-Timeline einsieht, wird er gebeten anzugeben, ob es sich dabei um eine potenzielle Bedrohung handelt. Mithilfe dieses Feedbacks kann CloudAI im Lauf der Zeit immer zuverlässiger entscheiden, ob die beobachteten Unregelmäßigkeiten echte Bedrohungen sind.

Neben dem Lernen aus der Gesamtheit der Aktivitäten in Ihrem eigenen Unternehmen ist die Lösung auch darauf ausgelegt, Trainingsdaten zu Bedrohungen bei der breiteren CloudAI-Kundenbasis zu sammeln. Die Sammlung von Feedback bei allen SOC-Analytikern und Incident Respondern hilft CloudAI, schneller Verhaltensmodelle zu entwickeln, und nützt somit allen Kunden.



CloudAI holt Feedback der Analytiker ein und lernt so laufend dazu.

Maximiert die Effizienz Ihrer Analytiker

CloudAI verbessert die Effizienz und Leistungsfähigkeit Ihres Sicherheitsteams erheblich. Die laufenden automatisierten Analysen machen das manuelle Bedrohungs-Monitoring überflüssig, sodass sich Ihre Mitarbeiter auf die gravierendsten Gefahren konzentrieren können.

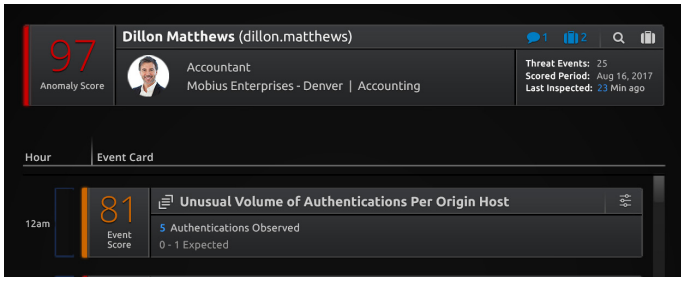
Künftige Weiterentwicklungen werden CloudAI schließlich in die Lage versetzen, die autonome Automatisierung einer breiten Palette von SOC-Aufgaben zu unterstützen.

Mit seinen aussagekräftigen Visualisierungen ermöglicht CloudAI maschinengestützte Untersuchungen und Threat Hunting. Die enge Integration des Add-ons in die gesamte LogRhythm TLM-Plattform verhindert Ineffizienzen und Lücken, die durch fragmentierte Prozesse entstehen. Die Lösung bietet native Unterstützung für LogRhythms eingebettete Sicherheitsautomatisierung und -orchestrierung mit Workflows für das Fall- und Ereignismanagement sowie automatisierten SmartResponse™-Reaktionen.

Das CloudAI Dashboard für Benutzeraktivitäten vermittelt umfassenden Überblick und unterstützt die Überwachung hochriskanter Benutzer (z.B. Führungskräfte, IT-Personal und ausscheidende Mitarbeiter). Diese Gruppen können im Einklang mit den Erfordernissen Ihres Unternehmens angepasst werden. Verwandte Visualisierungen erlauben die Überwachung von Servicekonten.

Mit CloudAI kann Ihr Team das Verhalten eines Benutzers in mehreren Dimensionen analysieren. Eine Zeitleiste des Benutzerverhaltens zeigt die Bedrohungsereignisse auf, die in die Bedrohungseinstufung eines Benutzers eingeflossen sind, damit Ihre Mitarbeiter beurteilen können, ob sein Verhalten bösartig ist. Zudem illustrieren Peergroup-Vergleiche das Verhalten eines Benutzers im Verhältnis zu dynamischen Listen mit echten Peers, die durch Ähnlichkeiten in ihrem tatsächlichen Verhalten definiert werden.

Während des gesamten Verlaufs einer Untersuchung präsentiert CloudAI automatisch Identitätsinformationen aus dem Windows Active Directory. Die Lösung ermöglicht sofortigen Zugriff auf die zugrunde liegenden Log- und Ereignisdaten, die mit einem Klick für einen zugehörigen Fall gespeichert werden können. Diese integrierten Funktionalitäten unterstützen den TLM-Workflow, erhöhen die Produktivität der Analytiker und beschleunigen die Reaktion auf Sicherheitsvorfälle.



Die Benutzer-Timeline von CloudAI ermöglicht schnelle Untersuchungen des Benutzerverhaltens und liefert effiziente Workflows für weitere Maßnahmen.

Schnelle Amortisierung

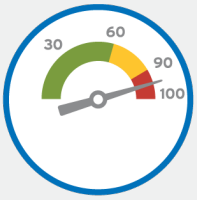
CloudAI ist ein Add-on zur Plattform von LogRhythm, das auf Abonnementbasis über die Cloud bereitgestellt wird. Da Sie keine On-Premises-Hardware benötigen und keine Regeln implementieren und optimieren müssen, fallen nur geringe Einführungskosten an. Dank flexibler Lizenzierungsoptionen haben Sie die Möglichkeit, zunächst Ihre wichtigsten Benutzer zu überwachen und die Lösung später auszuweiten, wenn es die Ressourcen erlauben. Zudem vereinfacht die schlüsselfertige Bereitstellung die Administration und Pflege, sodass sich Ihr Sicherheitsteam auf seine Kernaufgaben konzentrieren kann.

Die Architektur von CloudAI minimiert die betrieblichen Auswirkungen für Ihr Unternehmen und räumt der Datensicherheit Vorrang ein. Bei der Implementierung wird LogRhythm so konfiguriert, dass Metadaten aus hochwertigen Datenquellen (z.B. Authentifizierungsvorgänge, Zugriffe auf Anwendungen und Hosts, Standort) an die auf AWS gehostete Cloud-Infrastruktur von CloudAI übertragen werden. Da CloudAI mit Metadaten statt Logs arbeitet, sind die Anforderungen an die Bandbreite minimal. Die Daten werden mittels TLS 1.2 übertragen und mit symmetrischer Zwei-Wege-Zertifizierung geschützt. CloudAI speichert Daten auf sichere Weise, und veraltete Daten werden programmgesteuert vernichtet. Der Datenzugriff steht im Einklang mit dem SOC 2 Standard.

Steigern Sie mit CloudAI die Leistungsfähigkeit Ihres SOCs

Ihr Sicherheitsteam muss den Schutz Ihres Unternehmens gewährleisten und dabei gegen eine ständig wachsende Angriffsfläche und Ressourcenknappheit ankämpfen. CloudAI erweitert die Plattform von LogRhythm, um mithilfe künstlicher Intelligenz benutzerseitige Bedrohungen zu erkennen, verborgene Gefahren aufzuspüren und Ihre Analytiker zu unterstützen. Da die Lösung als Service bereitgestellt wird, sind die leistungsfähigen Analysen schnell und leicht verfügbar. Auf einer Cloud-Architektur aufsetzend, wird die Lösung durch maschinelles Lernen im Lauf der Zeit immer intelligenter. Diese Fähigkeiten verbessern die Produktivität Ihrer Sicherheitsanalytiker und beschleunigen die Erkennung und Reaktion.

Verborgene Bedrohungen erkennen



Effizienz der Analytiker maximieren

Schnelle Rentabilität erzielen

Erfahren Sie mehr. Kontaktieren Sie unser Vertriebsteam noch heute.
sales@logrhythm.com