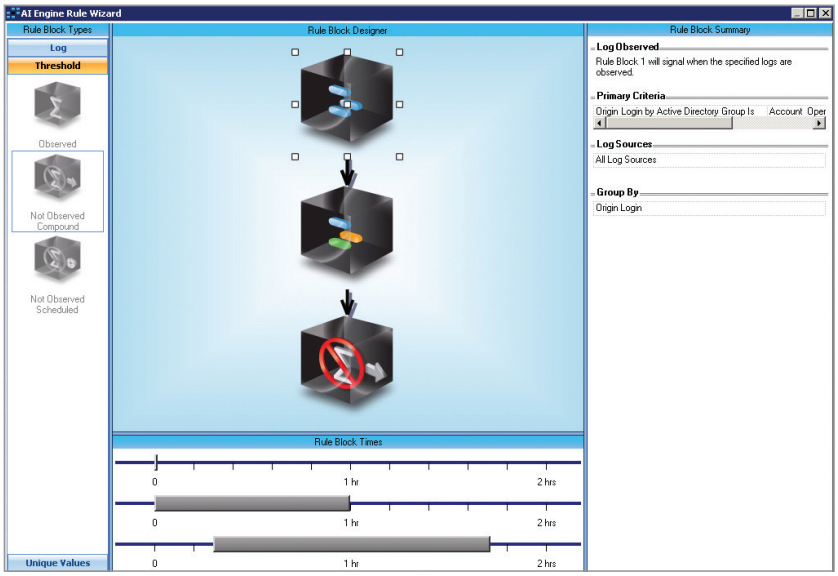
PRODUKTÜBERSICHT

Advanced Intelligence (AI) Engine™

LogRhythm
The Security Intelligence Company

Die AI Engine von LogRhythm ist eine vollständig integrierte Komponente der LogRhythm-Plattform, die automatisierte, fortlaufende Analysen durchführt und alle innerhalb der Umgebung beobachteten Aktivitäten korreliert. Dank der einzigartigen Flexibilität und des umfassenden Ansatzes erlaubt sie Echtzeit-Einblicke in Risiken, Bedrohungen und kritische betriebliche Fehler, die sonst nicht möglich wären.

Die AI Engine umfasst über 900 vorkonfigurierte, einsatzbereite Korrelationsregeln und eine Wizard-basierte Drag-and-Drop-Oberfläche zur Erstellung und spezifischen Anpassung komplexer Regeln. Damit eröffnet sie Unternehmen die Möglichkeit, eine Vielzahl von Problemen zu prognostizieren, aufzudecken und schnell darauf zu reagieren. Dazu zählen:



- Unbefugtes Eindringen
- Insider-Bedrohungen
- Betrug
- Verhaltensanomalien bei Benutzern, Netzwerken und Endpunkten
- Compliance-Verstöße
- Unterbrechung von IT-Services
- Und viele andere kritische Ereignisse

Umfassende, fortschrittliche Korrelationsanalysen

Im Unterschied zu älteren SIEM-Lösungen unterstützt die AI Engine die Integration mit den Funktionen für Protokoll- und Plattformverwaltung innerhalb der LogRhythm-Plattform, damit sämtliche Daten korreliert werden können, anstatt nur eine vorgefilterte Teilmenge von Sicherheitsereignissen. Die nahtlose Integration ermöglicht zudem den sofortigen Zugriff auf die forensischen Daten, die mit einem Ereignis direkt in Verbindung stehen.

Die Regeln der AI Engine werden aus über 70 verschiedenen Metadaten-Feldern bezogen, die hoch relevante Daten für die Analyse und Korrelation bieten. Diese Metadaten beinhalten einen dynamischen Risk Based Prioritization (RBP)-Wert, der allen Maschinendaten zugeordnet wird. So kann die AI Engine Trends herausarbeiten und statistische Anomalien aufdecken, basierend auf dem Risikograd, der mit einer spezifischen Aktivität im Netzwerk verbunden ist. Unabhängig davon, ob die Entdeckung durch vorgefertigte Regeln oder benutzerdefinierte/geänderte Regeln erfolgt, identifiziert die AI Engine mit außerordentlicher Präzision praxisrelevante Ereignisse, um Sicherheits-, Compliance- und betriebliche Ziele zu unterstützen. Die AI Engine kann auch genutzt werden, um mit generalisierten Korrelationsregeln ein weites Netz auszuwerfen und breite Sichtbarkeit zu gewährleisten, damit Änderungen im Ereignisverhalten aufgespürt werden können.

Mehrdimensionale Analyse

LogRhythm hat unternehmensweite, fortschrittliche Korrelation und Mustererkennung mit automatisierter Verhaltens- und statistischer Analyse kombiniert, um die erste mehrdimensionale Analyse der Branche anzubieten. Durch die Kombination moderner statistischer und heuristischer Analysen mit verhaltensbezogenem Whitelisting befähigt LogRhythm Unternehmen, den Lernprozess zu automatisieren, der erkennbar macht, was „normales" Verhalten ist – für eine beliebige Kombination von Merkmalen von Benutzern, Hosts, Anwendungen oder Geräten. Die Integration dieser Fähigkeiten in fortschrittliche Korrelationsanalysen und Mustererkennung beseitigt drei signifikante Probleme, vor denen die Benutzer der ersten SIEM-Generation standen: die Unfähigkeit, genau zu definieren, welche Aktivitäten „normal" sind; eine Flut von falsch positiven Werten, die das Verständnis der wirklich wichtigen Ereignisse erschwert; und Unsicherheit aufgrund falsch negativer Werte.

Die AI Engine bietet:

- Fortschrittliche Korrelation gegen alle Protokoll- und Maschinendaten
- Generalisierte und gezielte Bedrohungsverwaltung und Compliance-Automatisierung
- Automatisches Verhaltens- und statistisches Baselining
- Sofortiger Zugriff auf zugrundeliegende forensische Daten
- Umfassende, einsatzbereite, fortschrittliche Analyseregeln
- Unübertroffene Benutzerfreundlichkeit

Die AI Engine in Aktion

Die zahlreichen vordefinierten Korrelationsregeln der AI Engine sind so konfiguriert, dass sie direkt eingesetzt und als Vorlagen für eine einfache Anpassung verwendet werden können. Alle Regeln der AI Engine können schnell über die hoch intuitive Oberfläche geändert werden, um den individuellen Anforderungen jedes Unternehmens gerecht zu werden.

Sicherheit

Ein einziges Ereignis reicht nicht immer aus, um auf eine Sicherheitsverletzung hinzuweisen oder das wahre Ausmaß eines Vorfalls deutlich zu machen. Die AI Engine erstellt automatisch eine Verhaltens-Whitelist mit„normalen" Aktivitäten, um verdächtige Verhaltensmuster leichter erkennbar zu machen und potenzielle Bedrohungen und Sicherheitsverletzungen automatisch zu identifizieren und zu melden. Malware dringt beispielsweise oft sehr schnell in ein Unternehmen ein, sodass Daten ausgespäht werden und die Sicherheit geschwächt wird, bevor die Administratoren reagieren können. In den meisten Fällen ist das Ausmaß des Schadens unbekannt.

Beispiele:

- Auf einem Host wird Malware entdeckt, gefolgt von zahlreichen Angriffen, die von diesem infizierten Host ausgehen.
- Auf die verdächtige Kommunikation von einer externen IP-Adresse folgt ein Datentransfer zu der gleichen IP-Adresse.
- Ein Benutzer meldet sich von einem Ort aus an und kurz danach aus einer anderen Stadt oder einem anderen Land.
- Der Firewall-Protokollen zugewiesene RBP-Wert erhöht sich innerhalb einer Stunde kontinuierlich von 50 auf 90.

Compliance

Die AI Engine gewährleistet laufend Compliance, indem sie Ereignisse generiert, wenn bestimmte Richtlinien verletzt werden. Dazu zählt etwa die Absicherung von Karteninhaberdaten oder geschützten personenbezogenen Gesundheitsdaten (PHI-Daten) gegen unerlaubte Zugriffe sowie die aktive Überwachung des Verhaltens privilegierter Nutzer.

Beispiele:

- Fünf fehlgeschlagene Authentifizierungsversuche, gefolgt von einer erfolgreichen Anmeldung bei einer Datenbank, die ePHI-Daten enthält; anschließend werden große Datenmengen auf den Computer des Benutzers übertragen, alles innerhalb von 30 Minuten.
- Zugriff auf eine Datei mit Kreditkarteninformationen, gefolgt von dem Versuch, Daten vom gleichen Host auf ein USB-Laufwerk zu übertragen, alles binnen 10 Minuten.
- Mehrere neue Konten werden erstellt und erweiterte Benutzerrechte gewährt, gefolgt von einem Zugriff auf kritische Daten, alles innerhalb kurzer Zeit.

Optimierung

Die erweiterte Korrelation ermöglicht betriebliche Einblicke und trägt zur Sicherstellung der IT-Dienste bei. Geringe Veränderungen bei bestimmten Aktivitäten oder üblichen Betriebsabläufen können auf kritische Betriebsprobleme hinweisen.

Beispiele:

- Ein Sicherungsprozess wird gestartet, jedoch kein Protokoll erstellt, das angibt, dass die Sicherung abgeschlossen ist.
- Ein kritischer Prozess wird gestoppt und erst nach einer gewissen Zeit wieder gestartet.
- Eine große Gruppe Server fährt herunter, anschließend wird eine kleinere Gruppe Server wieder hochgefahren.
- Hohe I/O-Werte auf einem kritischen Server, die normalerweise während eines Sicherungsprozesses auftreten, werden während der normalen Geschäftszeiten beobachtet.

Einsatzmöglichkeiten der AI Engine

Die AI Engine ist eine vollständig integrierte Komponente jeder LogRhythm-Installation. Sie lässt sich als dedizierte, hochperformante Appliance einsetzen, als Software auf spezifischem Kunden-Equipment installieren oder für mehrere Virtualisierungsplattformen bereitstellen, einschließlich VMware ESX, Microsoft Hyper-V und Citrix XenServer. Hochperformante Appliances können Zehntausende von Protokollen pro Sekunde und Milliarden von Protokollen pro Tag erstellen. Die AI Engine verfügt über eine horizontal skalierbare Architektur, die eine vereinfachte, schrittweise Erweiterung der Installation erlaubt, um dem Arbeitsvolumen jedes Unternehmens gerecht zu werden. Alle Instanzen der AI Engine werden zentral über die Client-Konsole von LogRhythm verwaltet.

CITRIX XenServer

vmware

Windows Server 2012

Serie	Max. Verarbeitung	CPU	Speicherplatz (erweiterbar)	Speicherung	Gehäuse	Leistung	Ethernet	Abmessungen	Gewicht
 AIE5400	30.000 MPS*	16 Core	128 (256) GB	1 TB	1U	100-240 V	Broadcom 5720 (4 x 1 GB)	Höhe 4,28 cm x Breite 48,24 cm x Länge 67,73 cm	19,3 kg
 AIE7400	75.000 MPS*	32 Core	256 (512) GB	1 TB	1U	100-240 V	Broadcom 5720 (4 x 1 GB)	Höhe 4,28 cm x Breite 48,24 cm x Länge 67,73 cm	19,3 kg

*Meldungen pro Sekunde