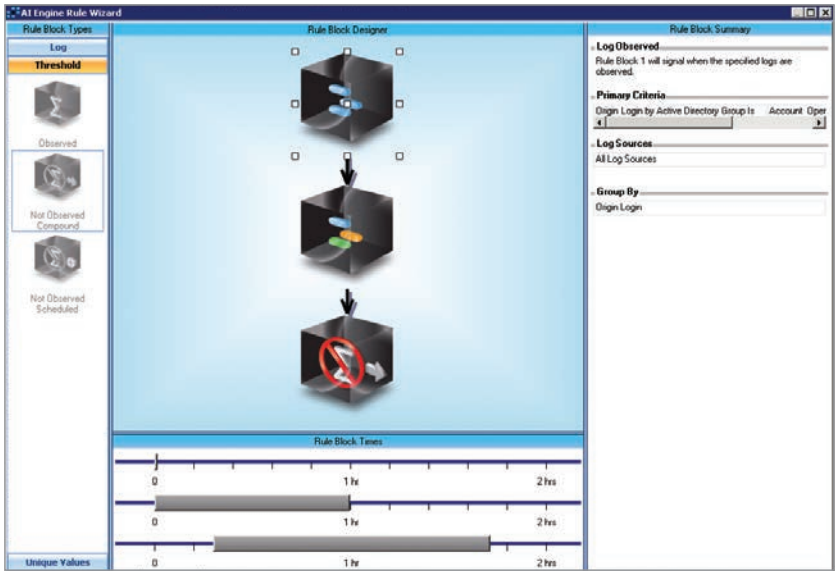
PRÉSENTATION DU PRODUIT

Advanced Intelligence (AI) Engine™

LogRhythm™

Advanced Intelligence (AI) Engine de LogRhythm est un élément totalement intégré de tout déploiement de LogRhythm. Il offre une analyse et une corrélation automatiques et continues de l'ensemble de l'activité observée dans l'environnement informatique d'une manière intuitive et unique. Grâce à une judicieuse combinaison de souplesse, de convivialité et d'analyse complète des données, AI Engine offre une visibilité en temps réel des risques, des menaces et des problèmes opérationnels critiques qui ne sauraient être détectés par aucune autre solution pratique. AI Engine, la corrélation qui marche !



Comptant plus de 525 règles de corrélation prédéfinies prêtes à être utilisées et possédant une interface utilisateur graphique (IUG) de type glisser-déposer à assistants pour la création et la personnalisation de règles encore plus complexes, AI Engine permet aux organisations de prévoir, de détecter et de combattre rapidement les menaces suivantes :

- Intrusions sophistiquées
- Menaces internes
- Fraudes
- Anomalies du comportement réseau
- Non-conformités
- Perturbations des services informatiques
- Et de nombreux autres événements actionnables critiques...

Corrélation avancée complète

À la différence des solutions SIEM classiques, AI Engine tire parti de son intégration avec les fonctions de gestion des journaux et des événements de la plate-forme LogRhythm pour effectuer la corrélation avec toutes les données, et pas seulement avec un sous-ensemble préfiltré d'événements de sécurité. Son intégration parfaite permet également un accès immédiat à toutes les données d'investigation directement liées à un événement.

Les règles d'AI Engine proviennent de plus de 70 champs de métadonnées différents qui fournissent des données très pertinentes pour l'analyse et la corrélation. Quel que soit le type de détection, par des règles prêtes à être utilisées ou par des règles créées/modifiées par l'utilisateur, AI Engine identifie les événements actionnables et génère des alertes avec une précision extrême afin de garantir la sécurité, la conformité et les processus. AI Engine peut également être utilisé pour ratisser large à l'aide de règles de corrélation généralisées pour une plus grande visibilité s'adaptant aux changements du comportement des événements.

Analyse multidimensionnelle

LogRhythm a combiné la corrélation avancée à l'échelle de l'entreprise et la reconnaissance de formes avec l'analyse comportementale et statistique automatique pour offrir les premières capacités d'analyse multidimensionnelle du secteur. En associant l'analyse statistique et heuristique avancée à l'établissement d'une liste blanche, LogRhythm permet aux organisations d'automatiser le processus d'apprentissage de ce qui constitue un comportement « normal » à partir de toute combinaison d'attributs liée aux utilisateurs, aux hôtes, aux applications ou aux dispositifs. L'intégration de ces capacités avec la corrélation avancée et la reconnaissance de formes permet aux utilisateurs des solutions SIEM de première génération d'éluder trois problèmes importants : l'incapacité de définir avec exactitude ce qui constitue une activité « normale », une multitude de faux positifs qui limitent la capacité à identifier et à comprendre les événements significatifs, et l'incertitude causée par les faux négatifs.

Avantages d'AI Engine

- Corrélation avancée avec toutes les données du journal et de la machine
- Établissement d'une base de référence comportementale et statistique automatique
- Accès immédiat aux données d'investigation sous-jacentes
- Règles généralisées et ciblées
- Nombreuses règles de corrélation prêtes à être utilisées
- Facilité d'utilisation sans égale

AI Engine en action

Les nombreuses règles de corrélation avancées prédéfinies d'AI Engine sont configurées pour être prêtes à être utilisées et servent de modèles pour simplifier la personnalisation. Toutes les règles d'AI Engine peuvent être rapidement modifiées grâce à une IUG très intuitive qui répond aux besoins uniques de chaque organisation.

Sécurité

Un seul événement n'est pas toujours suffisant pour indiquer une violation ou pour montrer la véritable portée d'un incident de sécurité. AI Engine crée automatiquement des listes blanches de comportement d'activité « normal » pour aider à identifier les formes de comportement suspectes afin de détecter automatiquement les éventuelles menaces et violations et de générer des alertes. Par exemple, les logiciels malveillants peuvent envahir une organisation et s'y propager rapidement, exposant les données et compromettant la sécurité à une vitesse supérieure à la capacité de réaction des administrateurs. Dans de nombreux cas, l'étendue des dommages est inconnue.

Exemples :

- Un malware est détecté sur un hôte, puis des attaques sont menées depuis cet hôte infecté.
- Une communication suspecte provenant d'une adresse IP externe est suivie d'un transfert de données vers cette même adresse IP.
- Un utilisateur ouvre une session depuis un endroit donné, ne la ferme pas, mais en ouvre une autre depuis une autre ville ou un autre pays dans un court laps de temps.

Conformité

AI Engine garantit une conformité continue en générant des événements lorsque des violations de politique spécifiques se produisent. Il protège notamment les données de titulaires de carte bancaire ou les informations de santé protégées (ISP) contre un accès non autorisé et surveille activement le comportement des utilisateurs privilégiés.

Exemples :

- Échec de cinq tentatives d'authentification suivies d'une ouverture de session avec succès dans une base de données contenant des e-ISP, puis d'un important transfert de données vers la machine de l'utilisateur dans un laps de temps de 30 minutes.
- Accès à un fichier contenant des données de carte bancaire, suivi d'une tentative de transfert d'informations depuis le même hôte vers une clé USB dans un laps de temps de 10 minutes.
- De nombreux comptes sont créés, font l'objet d'une escalade de droits, puis accèdent à des données critiques dans un court laps de temps.

Optimisation

La corrélation avancée est un atout considérable pour garantir une vision opérationnelle et le bon fonctionnement des services informatiques. De légères variations dans des activités spécifiques ou une séquence particulière d'opérations courantes peuvent indiquer des problèmes opérationnels critiques.

Exemples :

- Un processus de sauvegarde est lancé, mais la réalisation de la sauvegarde n'est pas consignée dans le journal.
- Un processus critique s'arrête et ne redémarre pas dans un laps de temps donné.
- Un grand groupe de serveurs s'arrête, puis un plus petit groupe de serveurs redémarre.
- Des taux d'E/S élevés sur un serveur critique, qui ne sont généralement observés qu'après les heures de travail, lors des procédures de sauvegarde, sont détectés pendant les heures normales d'activité.

Options de déploiement d'AI Engine

En tant qu'élément totalement intégré de tout déploiement de LogRhythm, AI Engine peut être déployé comme un appareil hautes performances spécialisé, être installé comme un logiciel sur un équipement client spécialisé ou être déployé sur plusieurs plates-formes de virtualisation, notamment VMware ESX, Microsoft Hyper-V et Citrix XenServer. Les appareils hautes performances peuvent traiter des dizaines de milliers de données de journal par seconde et des milliards de données de journal par jour. AI Engine possède une architecture évolutive à l'horizontale, qui permet une extension progressive et simplifiée du déploiement afin de satisfaire aux exigences liées au volume de traitement de chaque entreprise. Toutes les instances d'AI Engine sont gérées de façon centralisée grâce à la console client de LogRhythm.

Série d'appareils	Traitement max.	Unité centrale	Mémoire (extensible)	Stockage	Châssis	Puissance	Ethernet	Dimensions	Poids
AIE5310 	15 000 MPS*	6 cœurs	64 (128) Go	550 Go	1 U	100-240 V	Broadcom 5720 (4 x 1 Go)	H 4,28 cm x L 48,24 cm x P 67,73 cm	19,3 kg
AIE7310 	30 000 MPS*	16 cœurs	128 (256) Go	1 To	1 U	100-240 V	Broadcom 5720 (4 x 1 Go)	H 4,28 cm x L 48,24 cm x P 67,73 cm	19,3 kg
AIE9310 	75 000 MPS*	32 cœurs	256 (512) Go	1 To	2 U	100-240 V	Broadcom 5720 (4 x 1 Go)	H 8,73 cm x L 48,24 cm x P 75,5 cm	29,5 kg

*Messages par seconde