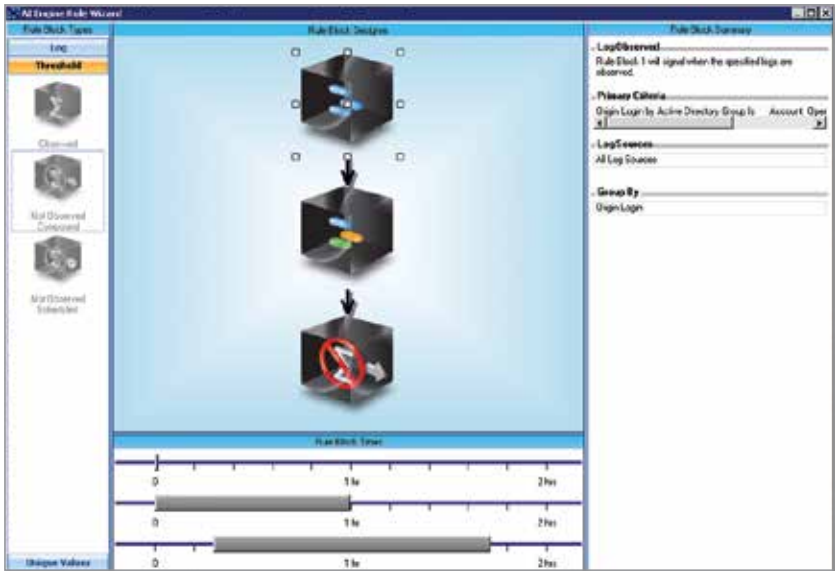
VISÃO GERAL DO PRODUTO

Advanced Intelligence (AI) Engine™

LogRhythm



O AI Engine da LogRhythm é um componente completamente integrado da plataforma da LogRhythm, oferecendo análise e correlação automatizadas e contínuas de toda a atividade observada no ambiente. Com uma abordagem exclusiva, flexível e abrangente, ele oferece visibilidade em tempo real sobre os riscos, ameaças e problemas críticos de operações que, de outra forma, não seriam detectados de forma prática. O AI Engine é a correlação que funciona.

Com mais de 900 conjuntos de regras de correlação pré-configurados e uma interface com funcionalidade de drag and drop para facilitar a criação e personalização de regras complexas, o AI Engine permite que as organizações prevejam, detectem e respondam com agilidade a:

- Intrusões sofisticadas
- Ameaças internas
- Fraude
- Anomalias comportamentais com os usuários, redes e pontos de extremidade
- Violações de conformidade
- Disrupções nos serviços de TI
- E diversos outros eventos úteis críticos

Correlação avançada abrangente

Diferente das soluções legadas de SIEM, o AI Engine utiliza sua integração com as funções de log e gerenciamento de plataforma dentro da plataforma da LogRhythm para correlacionar contra todos os dados — não somente um subconjunto pré-filtrado de eventos de segurança. A integração perfeita também possibilita acesso imediato a todos os dados forenses relacionados diretamente a um evento.

As regras do AI Engine são geradas com mais de 70 campos de metadados diferentes que oferecem dados altamente relevantes para análise e correlação. Esses metadados incluem o valor de Priorização Baseada em Risco (RBP) dinâmica atribuído a todos os dados de máquina, possibilitando que o AI Engine construa tendências e exponha anomalias estatísticas com base no nível de risco associado à atividade específica na rede. Sejam detectados pelas regras inovadoras ou regras criadas/modificadas pelo usuário, o AI Engine identifica e alerta sobre eventos úteis com grande precisão, segurança de suporte, conformidade e casos de uso de operações. O AI Engine também pode ser utilizado para apanhar em grande escala as regras de correlação generalizadas para uma maior visibilidade que acomoda alterações em comportamento de eventos.

Analytics Multidimensional

A LogRhythm combinou correlação avançada em toda a empresa e reconhecimento de padrões com análise comportamental e estatística automatizada para oferecer as primeiras capacidades de Analytics Multidimensional do setor. Combinando análises estatísticas avançadas e heurística com lista de permissões comportamentais, a LogRhythm permite que as organizações automatizem o processo de aprendizado do que constitui um comportamento "normal" em qualquer combinação de atributos vinculados a usuários, hosts, aplicações ou dispositivos. Integrar essas capacidades com correlação avançadas e reconhecimento de padrões elimina três problemas significativos para os usuários de SIEMs de 1ª geração: a incapacidade de definir com precisão o que constitui uma atividade "normal", uma avalanche de falsos positivos que reduzem a compreensão dos eventos significativos e incerteza devido a falsos negativos.

O AI Engine oferece

- Correlação avançada contra todos os dados de log e máquina
- Gerenciamento de ameaças generalizadas e identificadas, e pacotes de automação de conformidade
- Geração automatizada de linha de base comportamental e estatística
- Acesso imediato a dados forenses subjacentes
- Regras extensivas e inovadoras de análise avançada
- Facilidade de uso sem igual

AI Engine em ação

Os diversos conjuntos pré-definidos de regras de correlação avançada do AI Engine são configurados para executar de forma inovadora e agir como modelos para personalização simples. Todas as regras do AI Engine podem ser modificadas rapidamente através de uma GUI altamente intuitiva para atender aos requisitos exclusivos de cada organização.

Proteção

Em geral, um único evento não é o suficiente para indicar uma brecha ou revelar o verdadeiro alcance de um incidente de segurança. O AI Engine gera automaticamente listas de permissões comportamentais da atividade "normal" para identificar padrões de comportamento suspeito e identificar e alertar automaticamente sobre ameaças e brechas em potencial. Por exemplo, malwares podem invadir e se espalhar rapidamente em uma organização, expondo dados e enfraquecendo a segurança antes que os administradores possam reagir. Em muitos casos, a dimensão do dano é desconhecida.

Exemplos:

- Malwares são detectados em um host, seguidos de múltiplos ataques outbound do host infectado.
- A comunicação suspeita de um Endereço IP externo é seguida de dados sendo transferidos para o mesmo Endereço IP.
- Um usuário faz login de um local e, pouco depois, faz login de outra cidade ou país.
- A pontuação de RBP atribuída aos logs do firewall crescem constantemente de 50 a 90 no curso de uma hora.

Conformidade

Quando ocorrem violações de política específicas, o AI Engine aplica uma conformidade contínua gerando eventos. Isso inclui proteger os dados de titulares de cartões ou Informações de Saúde Protegidas (PHI) contra acesso não autorizado e monitorar ativamente o comportamento de usuários com privilégios.

Exemplos:

- Cinco tentativas de autenticação malsucedidas seguidas de um login bem-sucedido a um banco de dados contendo ePHI, seguido de uma grande transferência de dados à máquina de um usuário, tudo em menos de 30 minutos.
- Um arquivo contendo dados de cartões de crédito é acessado, seguido de uma tentativa de transferir as informações do mesmo host a um pen-drive, em menos de 10 minutos.
- Diversas contas são criadas, recebem privilégios escalados e acessam dados críticos em um curto período de tempo.

Otimização

A correlação avançada oferece um valor substancial para insight operacional e garantia dos serviços de TI. Pequenas variações em atividades específicas ou uma sequência particular de eventos típicos de operações comuns podem indicar problemas críticos de operações.

Exemplos:

- Um processo de backup é iniciado, mas nenhum log é gerado indicando que ele foi concluído.
- Um processo crítico para e não é iniciado novamente dentro de um período de tempo específico.
- Um grande grupo de servidores é desligado, seguido por um grupo menor de servidores sendo reiniciado.
- Altas taxas de E/S em um servidor crítico, geralmente só observadas horas depois durante os procedimentos de backup, são observadas durante o horário de funcionamento normal da empresa.

Opções de implementação do AI Engine

Como um componente completamente integrado de qualquer implementação da LogRhythm, o AI Engine pode ser implementado como um equipamento dedicado, de alto desempenho, instalado como software em um equipamento dedicado do cliente, ou implementado em múltiplas plataformas de virtualização, incluindo VMware ESX, Microsoft Hyper-V and Citrix XenServer. Os equipamentos de alto desempenho podem processar dezenas de milhares de logs por segundo e bilhões de logs por dia. O AI Engine possui uma arquitetura horizontal escalável, permitindo uma expansão simplificada e incremental da implementação para atender os requisitos de volume de processamento de qualquer empresa. Todas as instâncias do AI Engine são gerencias de forma central através do console do cliente da LogRhythm.

CITRIX XenServer
vmware
Windows Server 2012

Linha do equipamento	Processamento máximo	CPU	Memória (Expansível)	Armazenamento	Chassi	Energia	Ethernet	Dimensões	Peso
AIE5400 	30.000 MPS*	16 núcleos	128 (256) GB	1 TB	1U	100 a 240 V	Broadcom 5720 (4 x 1 GB)	H4.28CM x W48.24CM x D67.73CM	19,3 kg
AIE7400 	75.000 MPS*	32 núcleos	256 (512) GB	1 TB	1U	100 a 240 V	Broadcom 5720 (4 x 1 GB)	H4.28CM x W48.24CM x D67.73CM	19,3 kg

*Mensagens por segundo