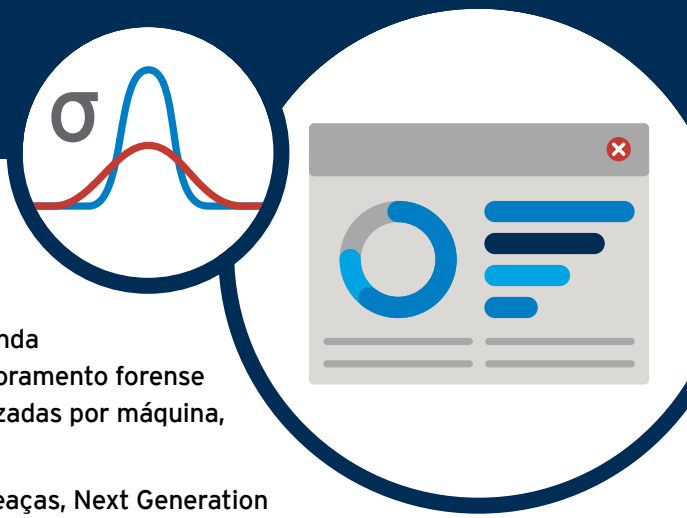
PLATAFORMA DE INTELIGÊNCIA DA SEGURANÇA DA LOGRHYTHM

LogRhythm®



Para proteger contra o panorama atual de ameaças em rápida evolução, é preciso uma visibilidade ampla e profunda de todo o ambiente de TI. As ameaças surgem de diversos ângulos e a evidência de sua existência pode ser encontrada nos dados de log e máquina existentes. Obtém-se ainda mais visibilidade através de pontos de extremidade identificados e monitoramento forense da rede. Quando isso é aplicado a técnicas de análise múltiplas, automatizadas por máquina, as ameaças e riscos ficam expostos como nunca antes.

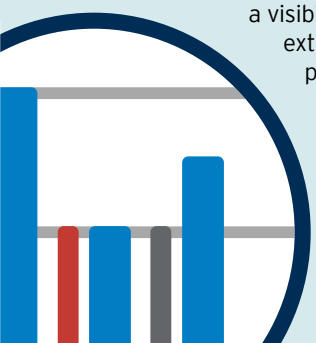
A LogRhythm oferece soluções de gerenciamento do ciclo de vida de ameaças, Next Generation SIEM gerenciamento de log, monitoramento e investigação forense do ponto de extremidade/rede e analytics de segurança em uma Plataforma de Inteligência da Segurança unificada. A plataforma da LogRhythm oferece visibilidade profunda sobre ameaças e riscos que, de outra forma, a organização seria incapaz de identificar. Projetada para prevenir brechas antes que aconteçam, a LogRhythm detecta com precisão uma ampla gama de indicadores prévios de comprometimento, possibilitando resposta e mitigação rápidas. A visibilidade e compreensão profundas oferecidas pela Plataforma de Inteligência de Segurança da LogRhythm capacita as empresas a proteger suas redes e estar em conformidade com os requisitos regulatórios.

Um padrão mais elevado em SIEM e Inteligência da Segurança

A LogRhythm oferece um conjunto unificado de capacidades para detectar, priorizar e neutralizar cyberameaças e os riscos associados. A Plataforma de Inteligência da Segurança da LogRhythm oferece:

- SIEM e gerenciamento de log de última geração
- Investigação forense de ponto de extremidade independente e monitoramento de integridade de arquivos
- Investigação forense de rede com ID de aplicação e captura de pacote completo
- Analytics de máquina de última geração
  - Correlação avançada, reconhecimento de padrão e aprendizado de máquina
  - Detecção multidimensional de anomalias comportamentais do usuário/rede/ponto de extremidade
- Pesquisa rápida contextual e não estruturada
- Análise de conjunto de dados através de analytics visual, pivô e pesquisas detalhadas
- Resposta automática com fluxo de trabalho através do Smart**Response**™
- Caso integrado e gerenciamento de incidentes de segurança

É possível obter verdadeira visibilidade analisando todos os dados de log e máquina disponíveis e combinando-os com a visibilidade forense nos níveis do ponto de extremidade e rede. Esse insight é utilizado pelo AI Engine, nossa tecnologia patenteada de analytics de máquina, para realizar análise contínua, em tempo real, de toda a atividade observada dentro do ambiente. O AI Engine capacita as organizações a identificar ameaças e riscos anteriormente não detectados.



A arquitetura integrada garante que quando as ameaças são detectadas, os clientes podem rapidamente acessar uma visualização unificada da atividade, possibilitando uma visibilidade profunda e resposta rápida. A LogRhythm oferece a inteligência útil e as capacidades de resposta a incidentes necessárias para combater as cyberameaças atuais mais sofisticadas.

Rendimento rápido

Ao proteger uma pequena rede ou executar um centro de operações de segurança (SOC) global, o rendimento e o custo total de propriedade são importantes. A arquitetura integrada da LogRhythm e os fluxos de trabalho de análise unificados ajudam os clientes a resolver com eficiência seus problemas de segurança mais desafiadores.

A LogRhythm Labs™ oferece uma funcionalidade crítica e inovadora, que acelera a detecção e resposta a ameaças. Oferecida automaticamente e atualizada constantemente com novas pesquisas em ameaças e conformidade, a experiência extensiva incorporada na LogRhythm equipa os clientes contra ameaças emergentes e os mantém atualizados com os requisitos de conformidade e auditoria atuais. A LogRhythm Labs oferece:

- Parsing de log e regras de normalização para mais de 700 sistemas operacionais, aplicações, bancos de dados, dispositivos, etc., exclusivos.
- Módulos de automação de conformidade para mais de 14 frameworks regulatórios (PCI, SOX, HIPAA, FISMA, GLBA, ISO 27001, DODI 8500.1, NERC-CIP, entre outros)
- Módulos de gerenciamento de ameaças
  - Detecção de ameaça do usuário/rede/ponto de extremidade
  - Ameaças Persistente Avançada (APT)
  - Honeypot Analytics
  - Cybercrime no varejo
  - E muito mais...

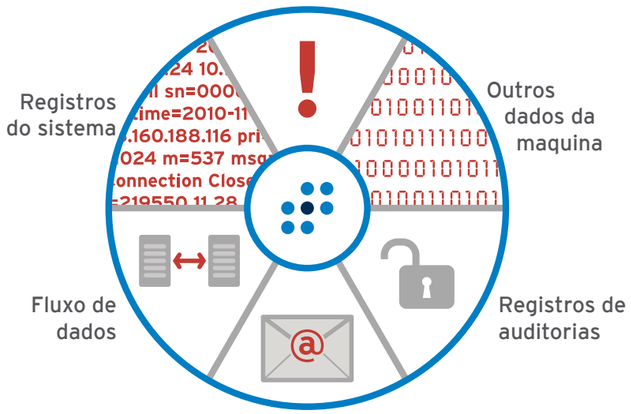
PLATAFORMA DE INTELIGÊNCIA DA SEGURANÇA DA LOGRHYTHM

LogRhythm

ENTRADA

COLETA DE DADOS FORENSES EM TEMPO REAL

Eventos de segurança



GERAÇÃO DE DADOS FORENSES EM TEMPO REAL

ANÁLISE

PROCESSAMENTO

Normalização de tempo

Classificação uniforme de dados

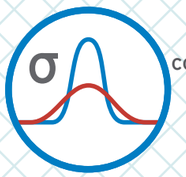
Extração e marcação de metadados

Contextualização de ameaças e riscos

ANÁLISE DA MÁQUINA

Aprendizagem da máquina

Perfil de comportamento



Análise estatística

Lista branca

Lista negra

Correlação avançada

ANÁLISE FORENSE

Pesquisa contextual

Pesquisa não estruturada

Visualização

Análise Pivot/detalhada

ESTRUTURA DE INTELIGÊNCIA DE DADOS DA MÁQUINA (MDI)

LogRhythm Labs Research & Intelligence

SAÍDA

INTELIGÊNCIA ACIONÁVEL

Alarmes priorizados segundo o risco

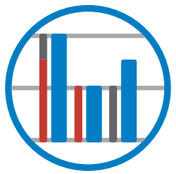
Painéis de informações atualizados em tempo real

Relatórios

RESPOSTA A INCIDENTES

Colaboração para os casos

Baú de evidências



Monitamento e métricas de incidentes

Resposta automatizada

Opções de implementação flexíveis

Equipamentos de alto desempenho

	MULTIFUNCIONAL (XM) (INCLUI PM, DPX, AIE)		GERENTE DE PLATAFORMAS DEDICADO (PM) (INCLUI LICENÇA DO AI ENGINE)		PROCESSADOR DE DADOS DEDICADO (DP)		INDEXADOR DE DADOS DEDICADO (DX)			AI ENGINE (AIE) DEDICADO		COLETOR DE DADOS (DC)	MONITOR DE REDE (NM)		EQUIPAMENTO PARA WEB
Linhas do equipamento	4301	6400	5400	7400	5300	7400	3300	5300	7400	5400	7400	3300	3300	5400	3300
Taxas máximas de arquivamento	10.000 MPS	25.000 MPS	N/A	N/A	10.000 MPS	50.000 MPS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Processamento máximo Taxas	1.000 MPS	5.000 MPS	N/A	N/A	5.000 MPS	15.000 MPS	N/A	N/A	N/A	30.000 MPS	75.000 MPS	N/A	1 Gbps	2,5 Gbps	N/A

> **A SANS COMMUNITY elegeu a LogRhythm como Melhor SIEM de 2014.**
>
> SANS INSTITUTE

> **LogRhythm recebe EXCELENTES AVALIAÇÕES DOS LEITORES em todos os setores.**
>
> INFOWORLD

Software e Virtualização

O Software de Soluções da LogRhythm pode ser implementado facilmente em hardware fornecido pelo cliente e na maioria das plataformas de virtualização, incluindo:

vmware® Windows Server 2012 CITRIX® XenServer

LogRhythm Services

A LogRhythm é o maior fornecedor dedicado do setor de SIEM e Inteligência da Segurança. Seu suporte de classe mundial e equipes de serviços profissionais dedicam-se a maximizar o sucesso do cliente, fornecendo soluções responsivas e práticas.

LogRhythm Labs

LogRhythm® Labs

A LogRhythm Labs é uma equipe de pesquisa de segurança e conformidade dedicada a capacitar os clientes através de experiência incorporada e ferramentas pré-configuradas para gerenciamento de ameaças avançadas e automação da conformidade. A equipe inclui especialistas reconhecidos em detecção de intrusão, malwares avançados, resposta a incidentes, conformidade de TI e diversas outras áreas essenciais. Os pesquisadores da LogRhythm Labs possuem diversas certificações do setor (CISSP, CISA, CEH, etc.) e usam pesquisas e estudos para se manter atualizados com os últimos desenvolvimentos em ameaças, métodos, conformidade e melhores práticas de segurança.

LogRhythm em ação

Detectar malware personalizado com detecção de anomalia comportamental em ponto de extremidade

Desafio: Malwares personalizados vinculados a ataques de dia zero são criados para evitar as soluções de segurança tradicionais, que são construídas para detectar assinaturas específicas e comportamento malicioso conhecido.

1. A LogRhythm determina a linha de base do comportamento "normal" do ponto de extremidade e cria uma lista de permissões de atividades de processos aceitáveis.
2. O Monitoramento de Atividades no Ponto de Extremidade detecta independentemente o início de um novo processo.
3. A LogRhythm reconhece automaticamente que o processo não consta da lista de permissões.
4. O analytics de máquina da LogRhythm confirma o evento contra atividades relacionadas, como tráfego de rede anormal, classificando com precisão a atividade como sendo de risco elevado.
5. Um alarme é enviado para o Administrador do Sistema, que acessa com facilidade os detalhes forenses para investigar.

Expor credenciais comprometidas com detecção de anomalias comportamentais do usuário

Desafio: Com uma força de trabalho móvel crescente e a adoção acelerada de BYOD, as empresas têm dificuldades para distinguir entre comportamentos "normais" e atividades que indicam que as credenciais de um usuário foram comprometidas.

1. A LogRhythm estabelece automaticamente um perfil para usuários específicos, incluindo listas de permissões para atividades aceitáveis e linhas de base comportamentais das atividades observadas do usuário.
2. O AI Engine detecta quando um usuário se envolve em atividades anormais, como fazer login de um local suspeito ou se desviar de uma norma comportamental, como acessar significativamente mais dados, ou dados diferentes, e carregar dados a um aplicativo de compartilhamento em nuvem não constante da lista de permissões.
3. O Smart**Response**™ desativa automaticamente a conta ou coloca a resposta na fila de validação com uma investigação forense pendente mais detalhada sobre a atividade do usuário.

Identificar exfiltração de dados com detecção de anomalias comportamentais na rede

Desafio: Com o fluxo constante de dados de entrada e saída da empresa, é mais difícil detectar quando dados sensíveis saem da rede corporativa.

1. O Network Monitor oferece visibilidade crítica sobre os pontos de entrada/saída da rede, com os dados SmartFlow™ oferecendo visibilidade profunda de pacote sobre cada sessão de rede observada e os aplicativos em uso.
2. O analytics de máquina da LogRhythm estabelece linhas de base comportamentais nas atividades de rede observadas, usando os metadados extensivos de pacote oferecidos pelo SmartFlow™.
3. As anomalias baseadas em rede são identificadas e comparadas contra outros dados de log e máquina para oferecer uma visibilidade precisa sobre a atividade de alto risco.
4. O SmartCapture™ captura automaticamente todos os pacotes associados com sessões suspeitas para investigação forense completa de pacote.