VitalSigns SIEM Agent for z/OS (VSA)

Eventos de Segurança de Mainframe, em tempo real, para o SIEM corporativo

Notícias recorrentes provam que as empresas se mantêm vulneráveis e, infelizmente, sendo invariavelmente invadidas por hackers. Para minimizar o risco de uma violação do sistema é imperativo que se busque, de imediato, a proteção e a prevenção de problemas de segurança, e não horas depois da execução de Jobs que podem ocasionar um evento adverso.

O VitalSigns SIEM Agent ™ para z/OS, ou simplesmente **VSA**, posiciona o Mainframe no centro da infraestrutura de segurança da sua empresa - em tempo real. Os filtros avançados e granulares da solução separam, de modo rápido e fácil, incidentes críticos dos eventos do dia a dia, para que possam ser rastreados em todos os cantos da empresa.

O **VSA** se integra totalmente aos recursos de segurança padrão do z/OS, como RACF, ACF2 e Top Secret, reunindo informações detalhadas sobre eventos de segurança do Mainframe, em todos os sistemas z/OS e LPARes da sua rede.

Melhorias significativas na segurança

O **VSA** captura mensagens em tempo real do console do sistema z/OS e do SMF (recurso de gerenciamento do sistema).
Um extenso dicionário de dados oferece um controle, sem precedentes, para definir dados significativos e criar os filtros adequados.
O agente utiliza esses filtros definidos para determinar quais eventos SMF são críticos.

O agente também reformata os dados como eventos syslog, CEF ou LEEF e os encaminha para um ou dois SIEMs corporativos, dentre eles: Splunk, LogRhythm, QRadar, AlienVault, ArcSight.

O SIEM interpreta os dados e os entrega ao pessoal e também aos sistemas responsáveis pela segurança da empresa.
Sua equipe de segurança terá a disposição uma visão central e completa dos eventos que precisam ser reconhecidos.

O VSA pode alertar sobre ameaças antes que se tornem 'manchetes'.

Conformidade e auditoria simplificadas

O monitoramento de eventos de segurança em toda a empresa é fundamental, não apenas para rastrear atividades maliciosas, mas também para alcançar os exigentes padrões de conformidade atuais. Os administradores podem definir itens específicos para níveis extras de monitoramento ou auditoria: arquivos que contêm informações de crédito, por exemplo, ou detalhes de atendimentos médicos. As equipes de Mainframe podem contar com o **VSA** para filtrar e formatar os dados corretos e, desta forma, atender as políticas rígidas de auditoria.

O **VitalSigns SIEM Agent** ™ para z/OS foi indicado para a lista 2020 da 'Trend-Setting Products', na categoria ***Gerenciamento de Dados e Informações*** da revista 'Database Trends and Applications'.

Veja como o **VSA** pode melhorar a segurança da sua empresa!

O VSA preenche uma lacuna importante na infraestrutura de segurança, fornecendo registros de eventos do z/OS para sua solução SIEM, em tempo real. Com a utilização de filtros SMF, fica fácil a descoberta de eventos críticos e o envio de alertas, **para qualquer produto SIEM distribuído**.

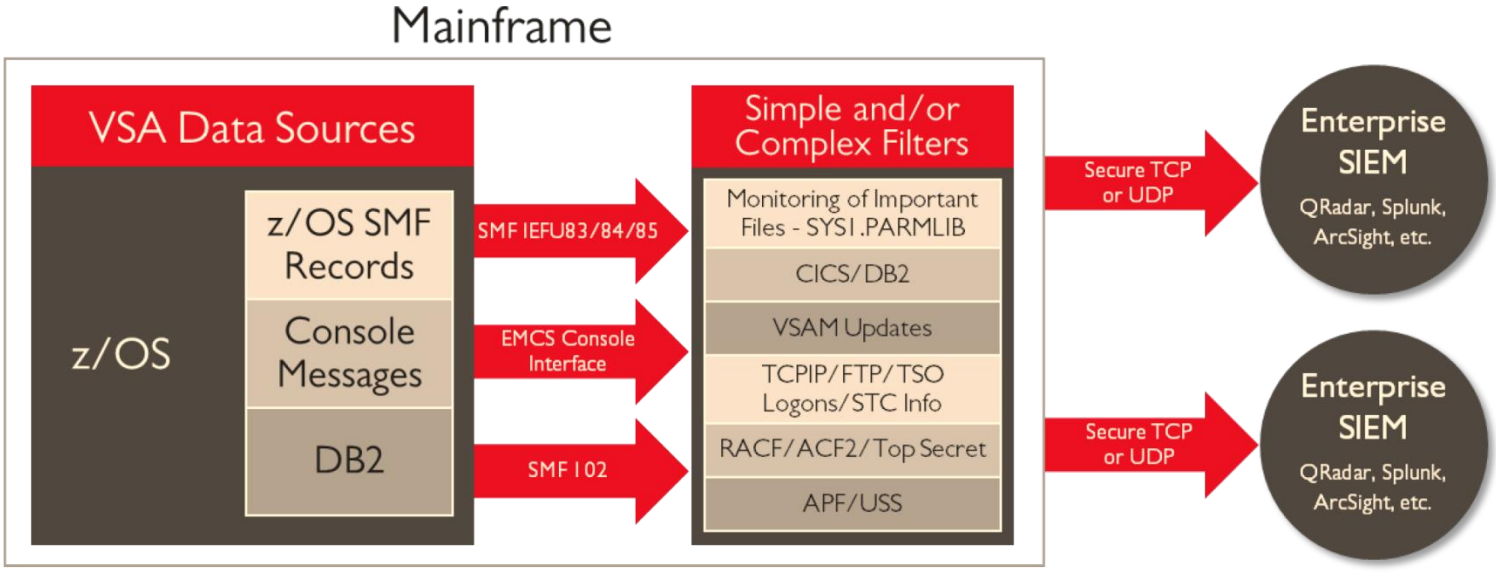
O **VSA** tem como alvo dados significativos e definidos, reduzindo custos e alarmes falsos, minimizando o número de eventos enviados ao SIEM.

Sua equipe de segurança terá a visibilidade para rastrear eventos de segurança de todos os segmentos da empresa.

Com um monitoramento contínuo, alertas em tempo real e processos simplificados de auditoria, o **VSA** ajuda a atender aos regulamentos de segurança de dados, incluindo:

- **GDPR**
- **SOX**
- **FISMA**
- **23 NYCRR 500**
- **PCI DSS HIPAA**
- **GLBA**
- **IRS Pub. 1075**

VitalSigns SIEM Agent for z/OS (VSA)



Segurança significa vigiar todas as portas

Os agentes do software VSA convertem dados de Mainframe em eventos syslog, CEF ou LEEF para entregar às tecnologias SIEM ou qualquer outro software que utilize o protocolo TCP/IP.

Os SIEMs corporativos consolidam as informações do VSA com a inteligência da segurança de outros sistemas, como UNIX, Windows e Cisco. Os SIEMs poderão, então, analisar e visualizar dados em todo o espectro.

Não serão mais necessárias várias equipes de segurança para proteger diversas plataformas. Seu ambiente de segurança irá dispor de total visibilidade do ambiente z/OS, bem como dos sistemas distribuídos e abertos.

Deixe o VSA trabalhar para você:

- Interage com produtos de segurança padrão z/OS: RACF, ACF2, Top Secret, DB2, CICS, FTP, TCP/IP, etc.
- Monitora z/OS, USS (UNIX System Services) e DB2.
- APIs permitem definir e filtrar eventos TSO, CICS e batch.
- Instalação fácil e rápida, com recursos mínimos e sem IPLs no z/OS.
- Regras de monitoramento simples ou complexas são facilmente definidas, através do editor ISPF.
- Utiliza detecção de ataque baseada em assinaturas e anomalias.
- A configuração pode ser compartilhada pelos agentes do VSA, executando em diferentes LPARes.
- Ocupa pouco recurso em cada LPAR e baixo overhead da CPU.
- Certificado CEF e LEEF.

Para obter mais informações sobre o VitalSigns SIEM Agent para z/OS, visite www.workers.com.br/vsa-siem