VitalSigns SIEM Agent™ for z/OS

Datasheet

Get Real-Time Mainframe Security Events in Your Distributed SIEM

Recent headline-grabbing system breaches prove that you not only need to find security issues – you need to find them fast.

Yet mainframe security and auditing is isolated inside the mainframe(s), available via batch jobs running hours after the events they report. Isolated silos of data simply won't stand up to today's security threats and auditing requirements.

With VitalSigns SIEM Agent™ for z/OS (VSA), you can alert IT security personnel of threats before they happen.

VSA brings your mainframes into the center of your enterprise security infrastructure.

VSA integrates with standard z/OS facilities such as RACF, ACF2, Top Secret, and others. VSA agents acquire messages **in real time** from the z/OS system console and SMF (system management facility), and pass critical security information to your central enterprise SIEM systems such as ArcSight, QRadar, Splunk, LogRhythm, and others.

VSA software agents convert mainframe logs to

Security means watch ALL the doors

VitalSigns SIEM agents allow the SIEM to gather intelligence from all z/OS systems and LPARs in your network.
Mainframe data is then consolidated with security intelligence from other systems in your enterprise, such as UNIX, Windows, and Cisco, for total visibility into the
z/OS environment, as well as distributed and open-systems environments.

Data can then be indexed, searched, analyzed, and visualized across the spectrum. You no longer need multiple security teams to guard your enterprise's multiple platforms.

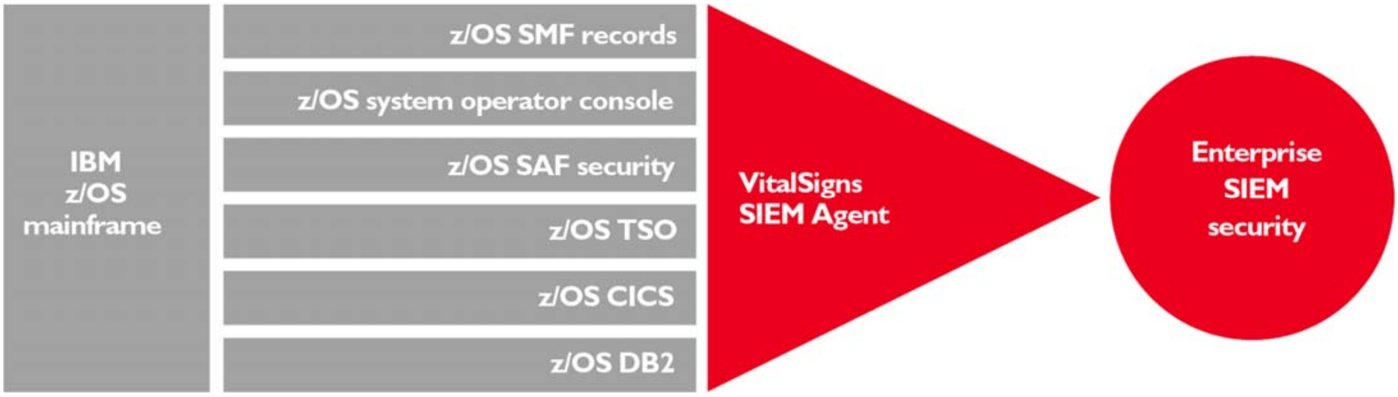
Enterprise-wide monitoring of security events is critical, not only for tracking malicious activity, but also to meet stringent compliance requirements.

Administrators can define specific items of interest for extra levels of monitoring: files that contain credit information, for example, or health care details.

With VSA, your security team has a central, end-to-end view of all the events they need to capture and all the security threats they need to recognize.

VSA Helps Meet Today's COMPLIANCE Requirements

- PCI DSS
- HIPAA
- GLBA
- SOX FISMA
- NERC
- IRS Pub. 1075



VSA delivers mainframe data to all widely-used SIEM products. VSA has certified integrations with HP ArcSight and IBM QRadar, and field integration with RSA Security Analytics, McAfee ESM, Miro Focus NetIQ, Splunk, and enVision.

VSA Features

- Monitors z/OS, DB2, and UNIX System Services (USS).
- Gathers intelligence from the SMF and the system operator interface.
- Interfaces with standard z/OS security products **in real time**: RACF, CA-ACF2, CA-Top Secret, DB2, CICS, FTP, TCP/IP, and others.
- Provides real-time alerts which can be managed, filtered, routed, and searched via the SIEM's GUI interface.
- Uses both signature- and anomaly-based attack detection.
- CEF and LEEF certified.
- Installs easily and quickly with minimal resources and no z/OS IPLs.
- Batch jobs can process SMF archives.
- Small footprint in each LPAR, with little CPU overhead.
- Simple monitoring rules easily defined through a TSO interface.
- APIs allow for defining and filtering TSO, CICS, and batch events.

VitalSigns SIEM Agent for z/OS

gathers detailed information about security events on the mainframe. The SIEM interprets the data, normalizes it in standard, TCP/IP syslog format, then delivers it **in real time** to the people and systems responsible for the enterprise security.

SysperTec Group
196 Bureaux de la colline – 92210 Saint-Cloud - France
www.syspertec.com ▸ info@syspertec.com ▸ +33 146 026 042