VitalSigns SIEM Agent™ for z/OS • VSA

Real-Time Mainframe Security Events Delivered to Any Enterprise SIEM

When data security is on the line, it's imperative to quickly find issues and threats to mitigate the risks. VitalSigns SIEM Agent for z/OS (VSA) brings the mainframe into the center of your enterprise security infrastructure to filter out the noise and uncover critical events in real time.

VSA integrates with standard z/OS security facilities – RACF, ACF2, and Top Secret – to gather detailed information about mainframe security events from all z/OS systems and LPARs in your network.

Advanced, granular filters quickly and easily separate critical incidents from everyday issues, and sends them in the right format to your enterprise SIEM.

Event processing is made fully zIIP-eligible without additional configuration. In benchmark tests, the VSA agent achieved more than 99% zIIP eligibility overall when processing SMF records alone, and up to 60% zIIP eligibility when processing console messages alone.

Meaningful Security Improvements

VSA acquires messages in real time from the z/OS system console, system management facility (SMF), and information management system (IMS). An extensive data dictionary gives you unprecedented control to define meaningful data and create filters.

The agent uses the defined filters to detect significant events, then reformats the data as syslog, CEF, or LEEF events and forwards them to one or two enterprise SIEMs. The SIEM interprets the data, then delivers it to the people and systems responsible for enterprise security. The security team has a central view of all the events they need to recognize.

Simplified Compliance and Auditing

Enterprise-wide monitoring of security events is essential, not only for tracking malicious activity, but also to attain today's demanding compliance standards. Administrators can define specific items for extra levels of monitoring or auditing: files that contain credit information, for example, or health care details. Mainframe teams can rely on VSA to filter and format the right data to comply with strict audit policies.

With continuous monitoring, real-time alerts, and simplified audit processes, VSA helps meet data security regulations including GDPR, SOX, FISMA, 23 NYCRR 500, PCI DSS, HIPAA, GLBA, and IRS Pub. 1075.

VSA fills a major gap in your security infrastructure by delivering z/OS event records to your SIEM solution in real time.

Using powerful, granular filters for SMF and IMS records, VSA finds critical events, then sends real-time alerts to any distributed SIEM such as:

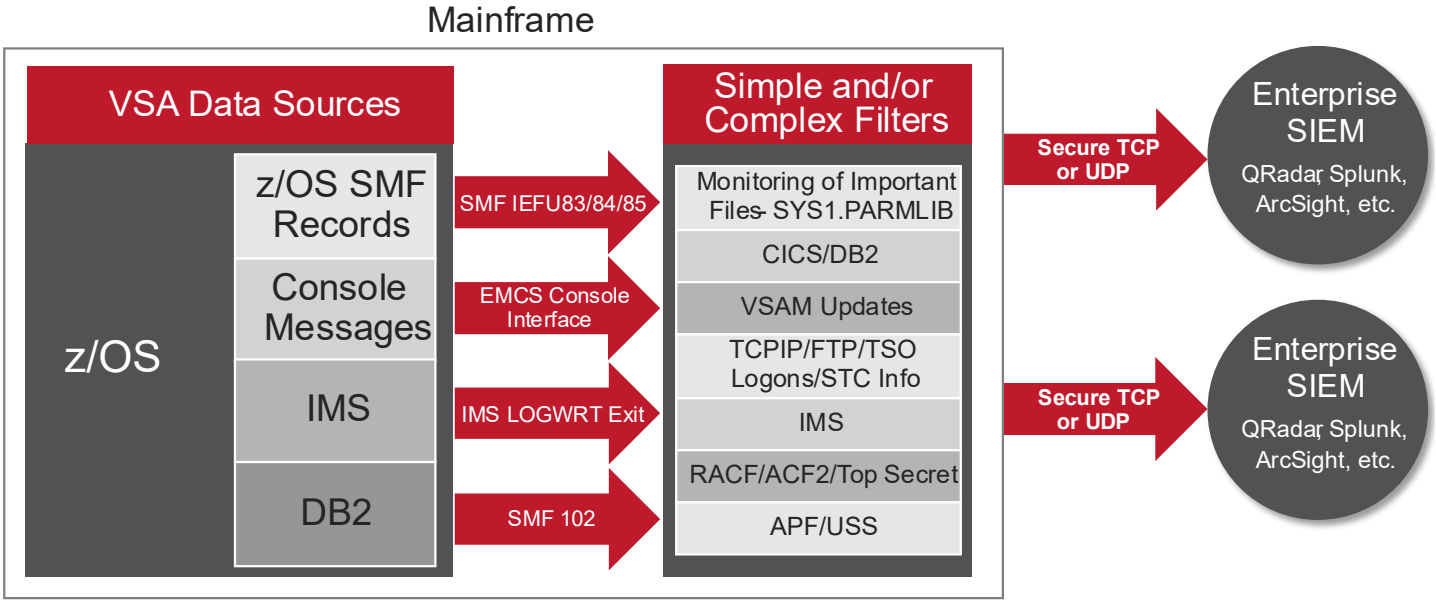
- Splunk
- LogRhythm
- QRadar
- AlienVault
- ArcSight
- and many others

Sample dashboards can be imported into Splunk to see security events, LPAR activity, and access failures from the VSA agent on z/OS.

With VSA, you gain the visibility to find and track targeted, defined security events on the mainframe.

VitalSigns SIEM Agent™ for z/OS was named a **trend-setting product** for data and information management by Database Trends and Applications magazine.

See how VSA can improve your enterprise security.



Security Means Watch All the Doors

VSA software agents convert mainframe data to syslog, CEF, or LEEF events for delivery to SIEM technologies or to any other software that uses TCP/IP protocol.

The enterprise SIEMs consolidate VSA information with security intelligence from other systems such as UNIX, Windows, and Cisco. The SIEMs can then analyze and visualize data across the spectrum.

You no longer need multiple security teams to guard multiple platforms. You get total visibility into the z/OS environment, as well as distributed and open systems environments.

For more information about VitalSigns SIEM Agent for z/OS, please visit www.sdsusa.com/siem/

Let VSA Work for You

- Interfaces with standard z/OS security products: RACF, ACF2, Top Secret.
- Monitors z/OS, UNIX System Services (USS), and DB2.
- Collects and monitors SMF records, IMS log records, and CICS performance data records.
- APIs allow for defining and filtering TSO, CICS, and batch events.
- Formats mainframe data as syslog, CEF, or LEEF.
- Installs easily and quickly with minimal resources and no z/OS IPLs.
- Simple or complex monitoring rules are easily defined using ISPF Edit.
- Uses both signature-based and anomaly-based attack detection.
- Configuration can be shared by VSA agents running on different LPARs.
- Small footprint in each LPAR and little CPU overhead.

Quality Mainframe Software Since 1982

Software Diversified Services delivers comprehensive, affordable mainframe and distributed software with a focus on cybersecurity and compliance. Hundreds of organizations worldwide, including many Fortune 500 companies, rely on SDS software. Our expert development and award-winning technical support teams are based in Minneapolis, MN. To learn more, please visit our website.