Software Diversified Services

1322 - 81st Ave NE
Minneapolis, MN 55432

t 763 571 9000
e info@sdsusa.com
w www.sdsusa.com

FOR RELEASE AT SHARE PITTSBURGH, AUGUST 4, 2019
Software Diversified Services
SHARE Booth #217
Lori Kettles, 763-571-9000 x123, info@sdsusa.com

SDS VitalSigns SIEM Agent™ for z/OS:

VSA 4.1 Adds Powerful SMF Filters to Detect Security Events

MINNEAPOLIS, MN – August 4, 2019 – Software Diversified Services (SDS), a global leader in mainframe software, is pleased to announce Version 4.1 of SDS VitalSigns SIEM Agent™ for z/OS (VSA). This latest release includes new features, commands, and messages, as well as simplified configuration and an improved interface that is more consistent with other SDS VitalSigns products.

VSA integrates with standard z/OS security facilities (RACF, ACF2, Top Secret) to gather mainframe security events from all z/OS systems and LPARs in the network. VSA agents acquire messages in real time from the z/OS system console and SMF (system management facility). Powerful new Complex SMF Filters allow unprecedented, field-level control to determine which SMF records are critical.

The agent reformats the data as syslog, CEF, or LEEF events and forwards them to one or two enterprise SIEMs such as Splunk, LogRhythm, QRadar, AlienVault, ArcSight, and many others.

The SIEM interprets the data and delivers it to the people and systems responsible for enterprise security. VSA 4.1 allows you to specify two SIEM servers to receive notifications via TCP and/or UDP.

Other significant upgrades make VSA more powerful and easier to use:

- New operator MODIFY commands can enable diagnostic features, show activity, and list status reports.
- Configuration is made simpler by using a set of partitioned dataset members which can be shared by VSA agents running on different LPARS, updated using ISPF edit, and refreshed dynamically with a new operator command while the agent is running.
- A new MCS console replaces the former Subsystem Interface (SSI). The console is dynamically activated during VSA agent initialization or can be activated with an operator command while the agent is running.
- The SMF exits are dynamically loaded and installed using the system CSVDYNEX facility. It is no longer necessary to add the load library to the LNKLIST or LPA, or to update the PROGxx PARMLIB member to add the exits.
- VSA monitors user accesses to determine activity related to any system or profile changes, including logon and logoff events.
- All system messages have been revised and fully documented, including new descriptions and suggested actions.

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

Contact:
Jim Lampi
jplampi@sdsusa.com
+1.763.571.9000

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 www.sdsusa.com.

--30--