SDS

Webinar

Fill your Mainframe Security Monitoring Gap via SIEM

+

Custom, Granular Filtering

SDS

About Us

sdsusa.com

Quality Mainframe Software since 1982

- Expert development & technical support teams based in Minneapolis, MN.
- 25+ products for z/OS, z/VM, z/VSE, and distributed platforms.
- Hundreds of organizations worldwide rely on SDS solutions.
- Focus on mainframe security and compliance.
- Cost savings and legacy tool replacements: DO MORE WITH LESS!
- Long-standing global partnerships complement SDS software.
- Recognized as cybersecurity trend-setter.

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

IBM Registered Business Partner

database TRENDS AND APPLICATIONS TREND-SETTING PRODUCTS for 2019

SDS

Future Events

sdsusa.com

October 16	Nov-Dec
▶ Secure FTP for z/OS – Exploring the Technology • A joint webinar with the SSH experts at SSH Communications Technology! • Register on www.sdsusa.com: 1:00PM CT and Available On Demand after the 16th!	▶ Happy Holidays everyone! • We will pick up with webinars in January of 2020!

Presenters

Jed Lampi

Operations and Marketing Lead

SDS

2018 Mainframe SIEM Survey Results *(from Enterprise Systems Media)*

Colin van der Ross

Sr. Systems Engineer

SDS

Importance of Incorporating z/OS Security Events into SIEM and Custom, Granular Filtering

Presenter

Jed Lampi
Operations & Marketing Lead
SDS

2018 Mainframe SIEM Survey Results *(from Enterprise Systems Media)*

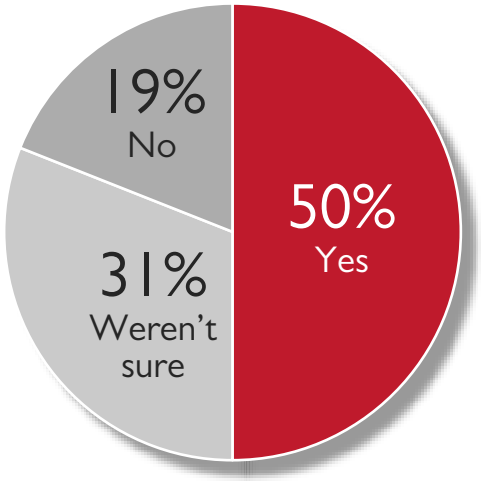
Agenda

- Results from 2018 ESM Survey focused on the state of SIEM in the enterprise
- Polls contain 2019 SIEM Questions – Answer to be included in this year's results

2018 SIEM Survey Results

Question 1:

Does your company have an enterprise Security Information and Event Management (SIEM) solution in place?

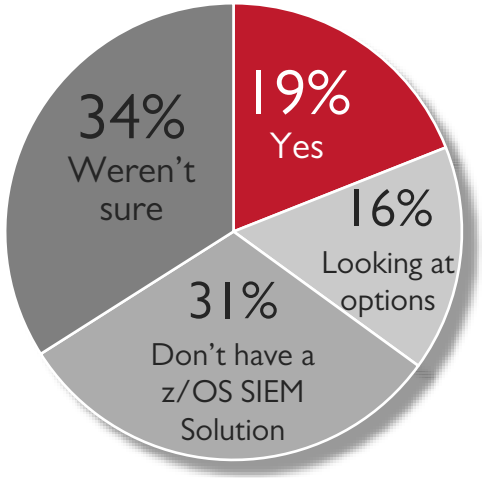


Organizations with an enterprise SIEM in place

2018 SIEM Survey Results

Question 2:

Does your company have a SIEM solution in place for your IBM z/OS system?

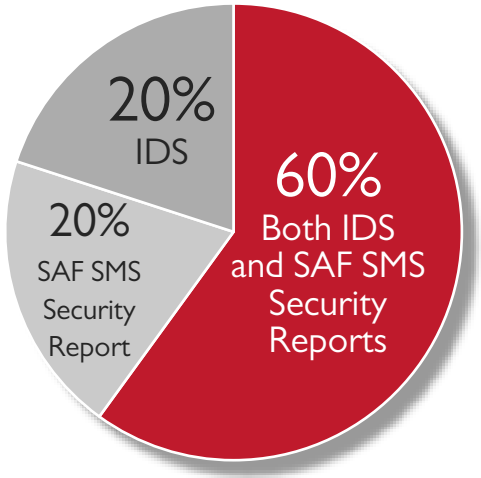


Organizations with a z/OS SIEM Agent in place

2018 SIEM Survey Results

Question 3:

How do you currently monitor your z/OS security events?

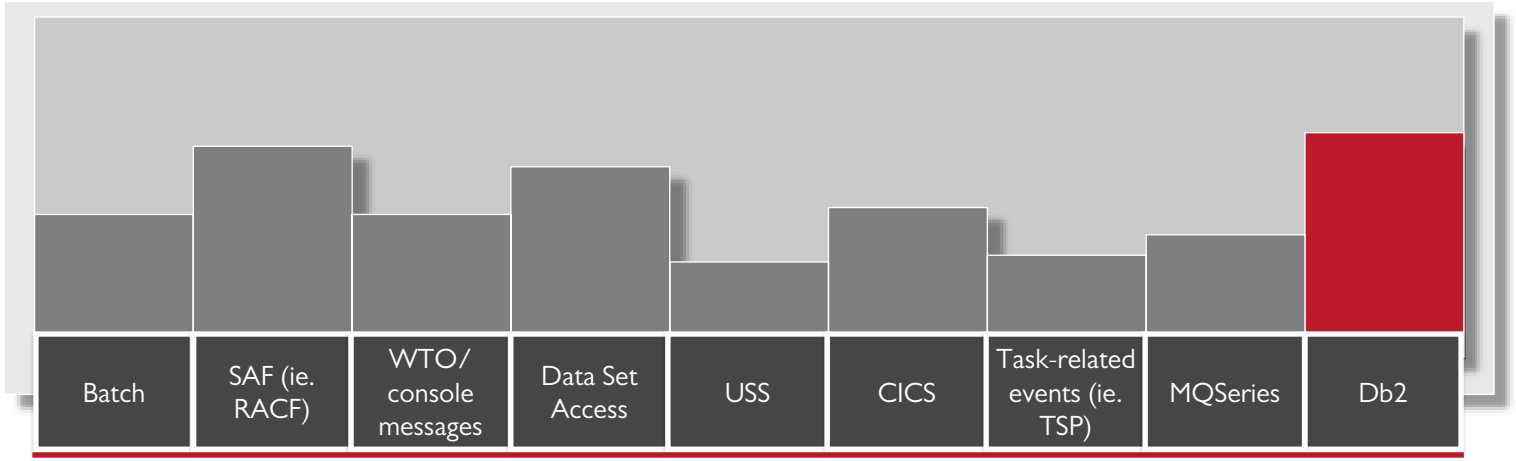


Current methods used to monitor z/OS security events

2018 SIEM Survey Results

Question 4:

Which SIEM areas are you most interested in, concerned about, or focused on? Select all the apply.

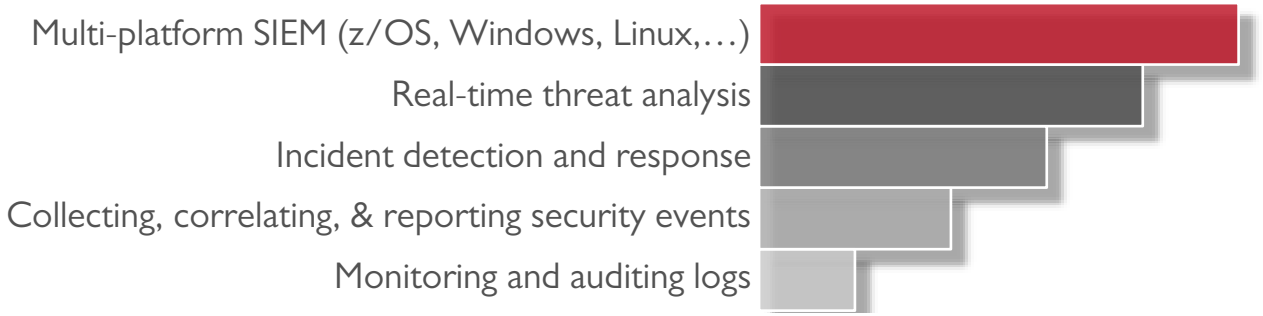


Mainframe SIEM Areas of Interest

2018 SIEM Survey Results

Question 5:

Please rank the following SIEM solution requirements from most important to least important based on your job.

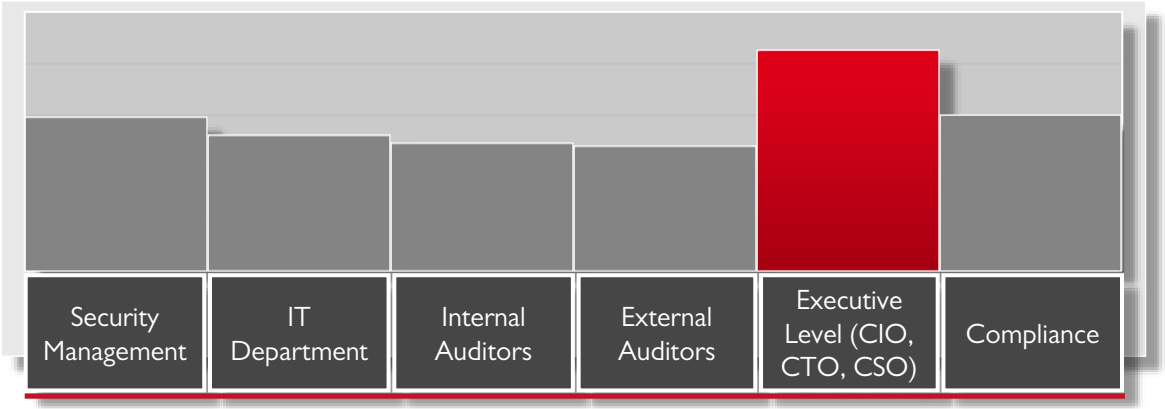


SIEM Solution Requirements
(ranked from most to least important)

2018 SIEM Survey Results

Question 6:

Which group(s) in your company is pushing for Security Information Event Management (SIEM) to be implemented?



Departments Pushing SIEM

Presenter

Colin van der Ross
Sr. Systems Engineer
SDS

Importance of Integrating z/OS Security Events into SIEM & Granular Filtering

Agenda

- What is a SIEM and why incorporate z/OS data into your SIEM ?
- What's new in VSA 4.1?
- VSA 4.1 Data Dictionary
- Demo of VSA 4.1 Filters

SIEM: What is it?

- Security Management provides a holistic view of an organization's information technology security
- SIEM combines SIM (Security Information Management) and SEM (Security Event Management) functions into ONE Security Management System

Importance of SIEM

SIEM – Security Information & Event Management

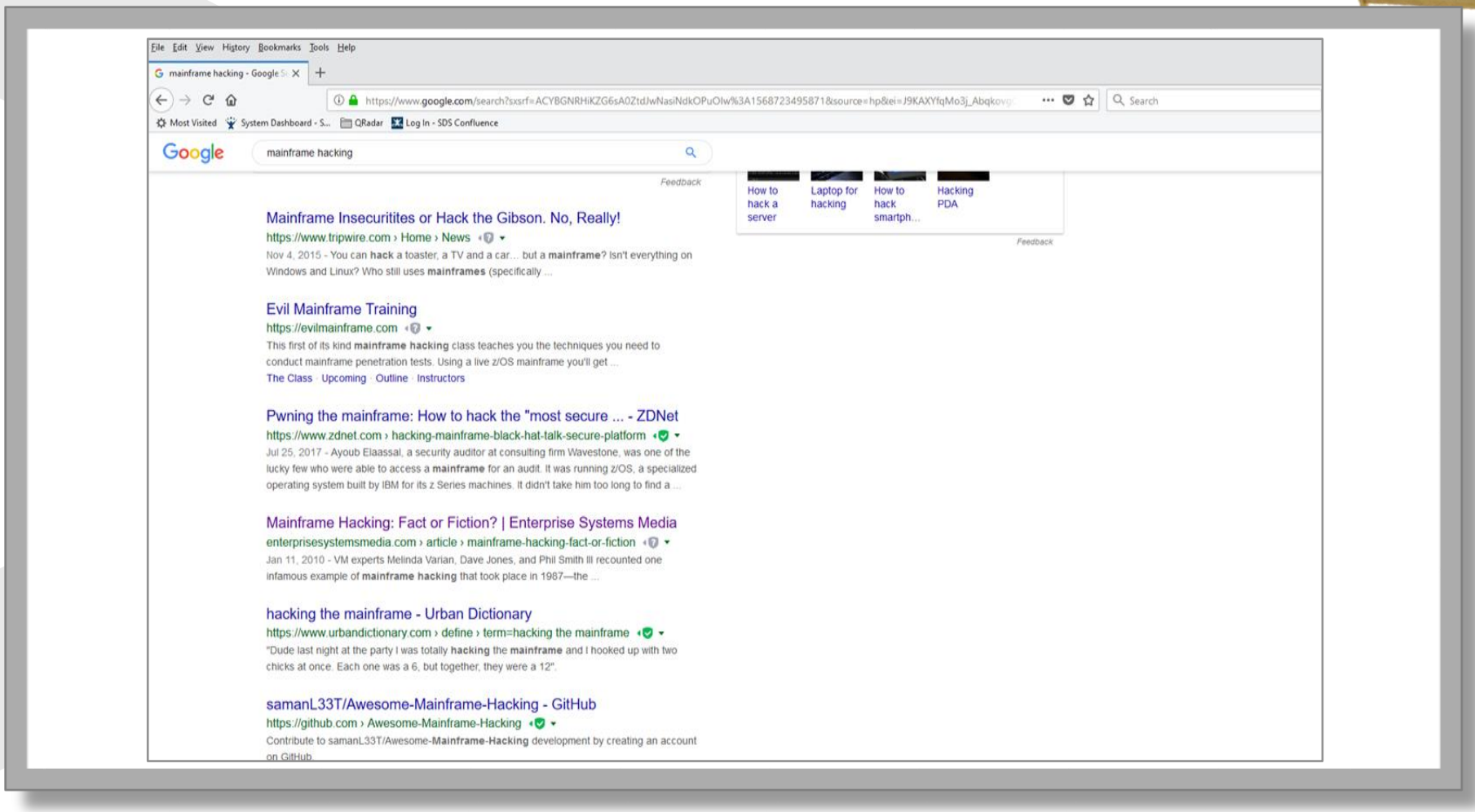
Security Information & Event Management System	
Security Event Management (SEM)	Security Information Management (SIM)
Provides -	Provides -
▶ Event Management	▶ Centralized log collections
▶ Real Time Threat Analysis	▶ Long term log collection
▶ Incident Detection & Response	▶ Log search and reporting
▶ Basic ticketing capabilities	
▶ Security operations	

Importance of SIEM

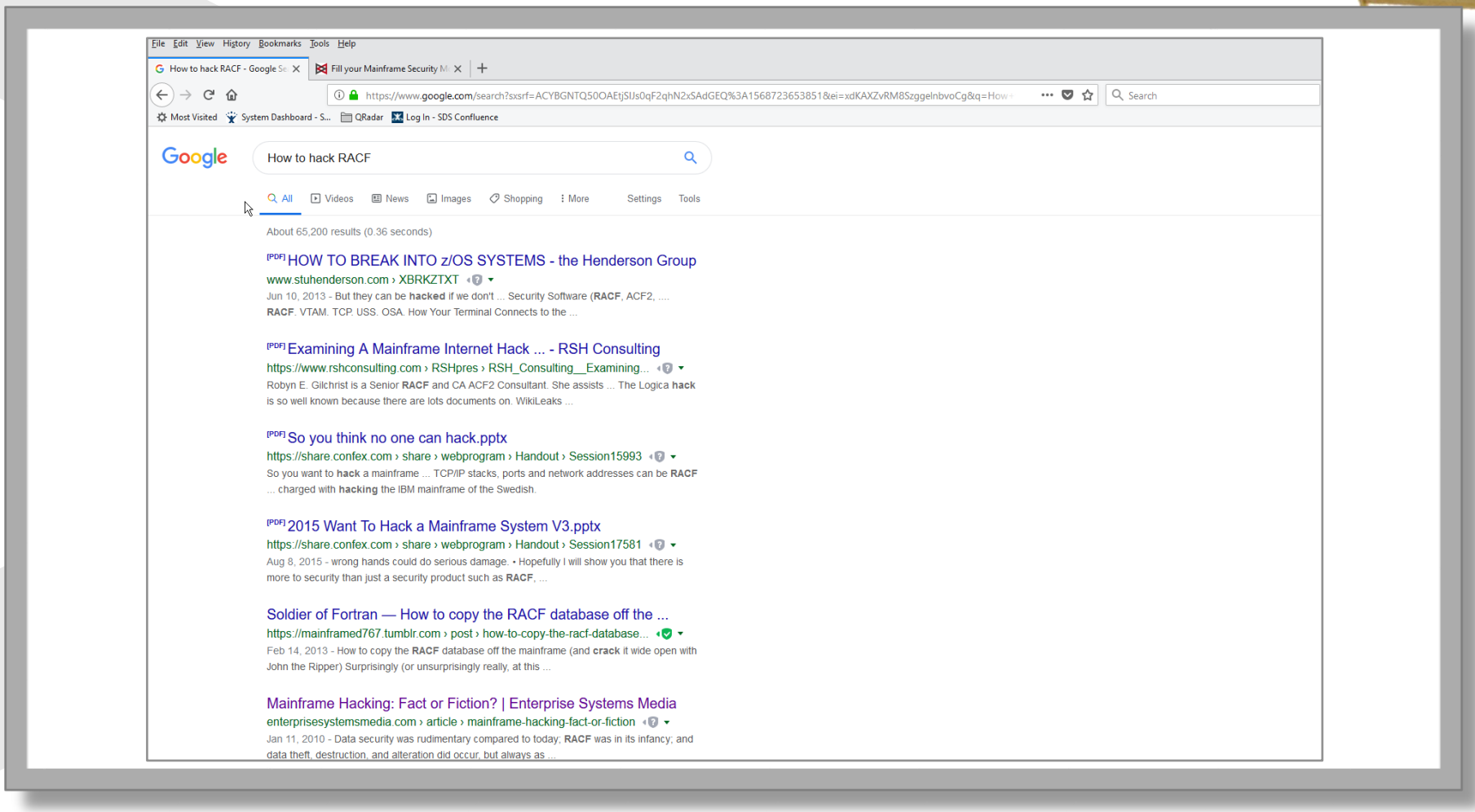
Security Requirements

- SIEM is the core of a defense in-depth strategy
- Attackers leave behind a trace – Logs
- Security Events provide insight into
  - When the event occurred
  - Why it happened
  - What happened

Why Incorporate z/OS Events into SIEM?



Why Incorporate z/OS Events into SIEM?



Why Incorporate z/OS Events into SIEM?

More Reasons for z/OS SIEM

- Mainframe contains sensitive data
  - Large corporations have 70% of data on mainframes
- z/OS is NOT invulnerable
- If you have a SIEM, why not include your mainframe data
- Compliance requirement
  - PCI, SOX, HIPAA,GLBA, etc.

SDS VitalSigns SIEM Agent for z/OS

What's New in VSA 4.1?

- Dynamic Configuration Updates
- Simplified Installation
- Greater Consistency in Function and Appearance
- Improved Reliability and Service Ability
- Simplified and modernized code base in preparation for future enhancements

What's New in VSA 4.1?

- New Infrastructure
- Improved Licensing Process
- New and Simplified Configuration model
- New Messages
- New Set of Commands for operator interaction

What's New in VSA 4.1?

- Multiple TCP Server Destinations using TCP
- Dynamic MCS Consoles
  - The Subsystem Interface (SSI) is replaced with a MCS Console
- Dynamic SMF Exits
  - 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.

What's New in VSA 4.1?

- Complex SMF Filters
  - Complex SMF Filters allow you to escalate or suppress SMF records at field level
  - A Data Dictionary containing over 900 individual fields and Boolean values has been defined, together with filtering semantics that give you unprecedented control over the decision to escalate an SMF record into a SIEM event or drop it from consideration.
  - The Data Dictionary describes all the field values that may be used in complex filters, their lengths, and their default formats

SDS VitalSigns SIEM Agent for z/OS

SMF TYPE 17

Name	FORMAT	Len	Description
SMF17TME	SMFTIME	4	Time since midnight, in hundredths of a second, when the record was moved into the SMF buffer.
SMF17DTE	SMFDATE	4	Date when the record was moved into the SMF buffer, in the form 0cyydddF.
SMF17SID	DSTRING	4	System identification (from the SID parameter).
SMF17JBN	EBCDIC	8	Job name. The job name, time, and date that the reader recognized the JOB card (for this job) constitute the job log identification, or transaction name (for APPC output).
SMF17RST	SMFTIME	4	Time since midnight, in hundredths of a second, that the reader recognized the JOB card (for this job).
SMF17RSD	SMFDATE	4	Date when the reader recognized the JOB card (for this job), in the form 0cyydddF.
SMF17UID	EBCDIC	8	User-defined identification field (taken from common exit parameter area, not from USER=parameter on job statement).
SMF17DSN	EBCDIC	44	Data set name.
SMF17FVL	EBCDIC	6	List of volume serial numbers. Filter Engine will scan the list for a match to the comparand.

SDS VitalSigns SIEM Agent for z/OS

SMF TYPE 80

Name	FORMAT	Len	Description
SMF80TME	SMFTIME	4	Time since midnight, in hundredths of a second, that the record was moved into the SMF buffer.
SMF80DTE	SMFDATE	4	Date when the record was moved into the SMF buffer, in the form 0cyydddF.
SMF80SID	DSTRING	4	System identification (from the SID parameter).
T80DES_VIOLATION	BOOLEAN	-	The event is a violation. (Bit 0 of field SMF80DES+0.)
T80DES_USER_NDEF	BOOLEAN	-	User Not Defined to RACF. (Bit 1 of field SMF80DES+0 .)
T80DES_WARNING	BOOLEAN	-	The event is a warning. (Bit 3 of field SMF80DES+0.)
SMF80EVT	UINT	1	Event code. For information about RACF event codes, see the IBM manual *z/OS Security Server RACF Macros and Interfaces*.
SMF80EVQ	UINT	1	Event code qualifier. For information about RACF event codes, see the IBM manual *z/OS Security Server RACF Macros and Interfaces*.
SMF80USR	EBCDIC	8	Identifier of the user associated with this event (jobname is used if the user is not defined to RACF).
SMF80GRP	EBCDIC	8	Group to which the user was connected (stepname is used if the user is not defined to RACF).
Authorities used for processing commands or accessing resources			
SMF80ATH	BIT8MASK	1	Authorities used for processing commands or accessing resources. These flags indicate the

SDS VitalSigns SIEM Agent for z/OS

SMF TYPE 119

Name	FORMAT	Len	Description
SMF119HDTime	SMFTIME	4	Time since midnight, in hundredths of a second, that the record was moved into the SMF buffer.
SMF119HDDate	SMFDATE	4	Date when the record was moved into the SMF buffer, in the form 0cyydddF.
SMF119HDSID	DSTRING	4	System identification (from the SMFPRMxx SID parameter).
SMF119HDSubType	UINT	2	Record sub-type. Two (2) byte field.
Common TCP/IP identification section			
SMF119TI_SYSName	EBCDIC	8	System name from SYSNAME in IEASYSxx
SMF119TI_SysplexName	EBCDIC	8	Sysplex name from SYSPLEX in COUPLExx
SMF119TI_Stack	EBCDIC	8	TCP/IP stack name
SMF119TI_Comp	EBCDIC	8	TCP/IP subcomponent (right padded with blanks): FTPC FTP Client FTPS FTP server IP IP layer STACK Entire TCP/IP stack TCP TCP layer TN3270C TN3270 Client TN3270S TN3270 server UDP UDP layer
SMF119TI_ASName	EBCDIC	8	Started task qualifier or address space name of address space that writes this SMF record
SMF119TI_UserID	EBCDIC	8	User ID of security context under which this SMF record is written
SMF119TI_Reason	UINT	1	Reason for writing this SMF record: X'08' Event record X'C0' Interval statistics record, more records follow

SDS

Demonstration

Time for a Demo!

VSA 4.1 Filters

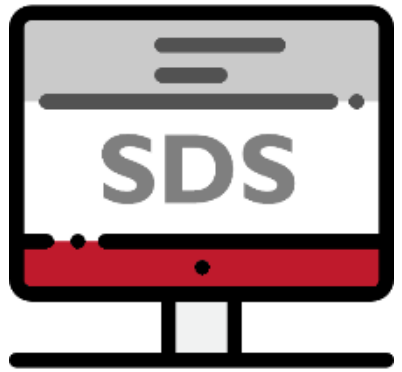
SDS

Have a Question?

Would you like additional information?

info@sdsusa.com

(800) 443-6183
(763) 571-9000



www.sdsusa.com