SDS

z/OS Security Webinar

Importance of Delivering Critical z/OS Security Events to your SIEM in Real Time

Presenters

Lori Kettles

Sales Manager

SDS introduction and interactive host

Colin van der Ross

Sr. Systems Engineer

Technical information and product demo

Gain Real-Time Visibility into Z

Agenda

- Cost of a Data Breach 2021
- Why deliver z/OS event records to your SIEM?
- What's new in VSA 4.2
- Demonstration of VSA and Splunk in action

About Us

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 for providing highest quality technical support.

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

Silver Business Partner IBM

database TREND-SETTING PRODUCTS 2020

Gain Real-Time Visibility into Z

Hacking the Mainframe: 5 Security Facts CISOs Need to Know

1. It is easier to hack the mainframe than you think.
2. There are more vulnerabilities on the mainframe than you realize.
3. Compliance regulations now require scanning every system. That includes the mainframe.
4. It's not enough to rely on your vendors.
5. Your competitors are likely already ahead of the curve.

*https://www.dbta.com/Editorial/News-Flashes/Hacking-the-Mainframe-5-Security-Facts-CISOs-Need-to-Know-142377.aspx

Gain Real-Time Visibility into Z

Cost of a Data Breach Report 2021

- 17th year of the "Cost of a Data Breach Report"
- Research conducted by Ponemon Institute
- IBM Security sponsored, analyzed, and published the 2021 report
- 537 real breaches were studied
  - 17 countries
  - 17 industries
  - over 3,500 interviews

"2021 Cost of Data Breach Study: Global Overview" – Ponemon Institute, IBM Security, July 2021

Gain Real-Time Visibility into Z

Cost of a Data Breach Report 2021

- 10% increase in average cost of a breach from 2020-21
- $1.07 million – additional cost where remote work was factor in causing breach
- 11 straight years healthcare had highest industry cost
- Lost business cost – 38% of total breach costs
- Average Breach Costs & Response Time
  - Average cost of an enterprise data breach is $4.24 million
  - Time it takes to identify and contain a data breach is 287 days

"2021 Cost of Data Breach Study: Global Overview" – Ponemon Institute, IBM Security, July 2021

Gain Real-Time Visibility into Z

Cost of a Data Breach Report 2021

- Breach Avoidance/Minimization
  - Recent history has shown that no organization is immune to a breach
  - Silver lining: how you react and security infrastructure in place will matter
  - Cost difference for breaches - mature zero trust vs. no zero trust: $1.76 million
  - Cost difference for breaches - high vs. low compliance failures: $2.3 million
  - Fully deploy AI security and automation – breaches cost 80% less than those not deploying these security tactics

"2021 Cost of Data Breach Study: Global Overview" – Ponemon Institute, IBM Security, July 2021

Gain Real-Time Visibility into Z

Why Deliver z/OS Event Records to your SIEM?

- SIEM systems are the standard for enterprise network security
  - Log collection and correlation for real-time security event notifications
  - Stored audit trails for compliance
- SIEM systems are an excellent hub for enterprise security, BUT they don't include mainframe data
- A tool, such as VitalSigns SIEM Agent for z/OS, is needed to fill the mainframe security gap

VSA 4.2: What's New?

IMS Support

- Collects and monitors IMS log records
- An IMS log writer (LOGWRT) exit is provided to gather IMS log records in real time
- Or in Batch when logs are archived
  - VSA Supports:
    - Log record x'10' Security Violations
    - Log record x'16' Sign on/sign off
    - Log record x'22' Type 2 commands
- Using LOGWRT exit, the VSA batch utility can read and forward an IMS log dataset to the VSA Agent

VSA 4.2: What's New?

IMS Filters

- ImsLogrecTypes
  - Use this parameter to specify which IMS log record types are to be presented to the VSA Agent
  - VSA Supports:
    - Log record x'10' Security Violations
    - Log record x'16' Sign on/sign off
    - Log record x'22' Type 2 commands

VSA 4.2: What's New?

IMS Filters

- ImsSmfRec
  - IMS Logs are presented to the VSA Agent as SMF records
  - Use this parameter to specify the SMF record type to use
- ImsSsids
  - Use this parameter to specify which IMS subsystems should be monitored by VSA
  - Example ImsSsids=(IVP1,IMS2)

VSA 4.2: What's New?

ISPF Dashboard

- New ISPF dashboard to allow users to easily monitor event activity and agent statistics in real time

VSA 4.2: What's New?

CICS Support

- Collects and monitors CICS performance data records (SMF110, subtype1, class3)

VSA 4.2: What's New?

APF Dataset Monitoring

- Support for monitoring changes to APF-authorized datasets
- Maintains a copy of the system's current APF list in storage
- When event that VSA monitors reports an update to an APF library, the event is escalated

VSA 4.2: What's New?

Performance Improvements

- New buffering technique improves the buffering of SMF records between the SMF exits and the Agent. This also reduces the likelihood of dropped records.

VSA 4.2: What's New?

TCP/IP Buffers Moved Above the Bar

- Buffers used to hold event messages in their final form for transmission via TCP or UDP have been moved into high virtual storage above the 1GB bar

VSA 4.2: What's New?

Support for System Symbols

- System symbols can be used within the VSA configuration member according to the system symbols defined for the installation

Gain Real-Time Visibility into Z

Sample Splunk Dashboards

SDS | Product Downloads

VitalSigns SIEM Agent for z/OS VSA 4.1

Sample Splunk Dashboards

Follow the steps provided below to import sample Splunk dashboards for VSA.

For assistance, contact SDS technical support.

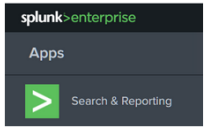
Instructions

This article shows how to import the sample Splunk dashboards provided for VSA. There are four sample dashboards:

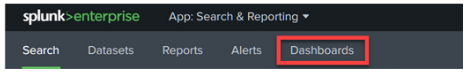
- All Activity, by LPAR
- FTP Activity
- APF Events
- Access Failures from RACF

Any of the dashboards can be imported independent of the others. To import any of the dashboards, follow the instructions below:

1. From the Splunk Enterprise main page, click the Search & Reporting app:



2. Click Dashboards:



3. Click the Create New Dashboard button:

- Select a Different Product
- Create Issue/Ticket
- SDS staff can get more details here.

- Sample Splunk Dashboards
- VSA Download Page

Support Resources:

- Get Help Now!
- Current Product Versions
- Product Keys
- Product Downloads
- Legacy Documentation

Gain Real-Time Visibility into Z

How VSA and SIEM can Assist Customers?

- SIEM is the core of a defense in-depth strategy
- Attackers leave behind a trace
- Security events provide insight into:
  - When the event happened?
  - Why and what happened?
- Compliance requirements
- Mainframes contain most sensitive data and are not invulnerable

Gain Real-Time Visibility into Z

How VSA and SIEM can Assist Customers?

- Separation of duties
- Choose what events you want to send to your SIEM
- Set realistic thresholds
- Some events require immediate escalation
- Ensure events are delivered to your SIEM on time
  - TCP not UDP
- SIEM redundancy?
  - Send events to multiple SIEMs

SDS

Questions?

Would you like additional information?

info@sdsusa.com

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

www.sdsusa.com