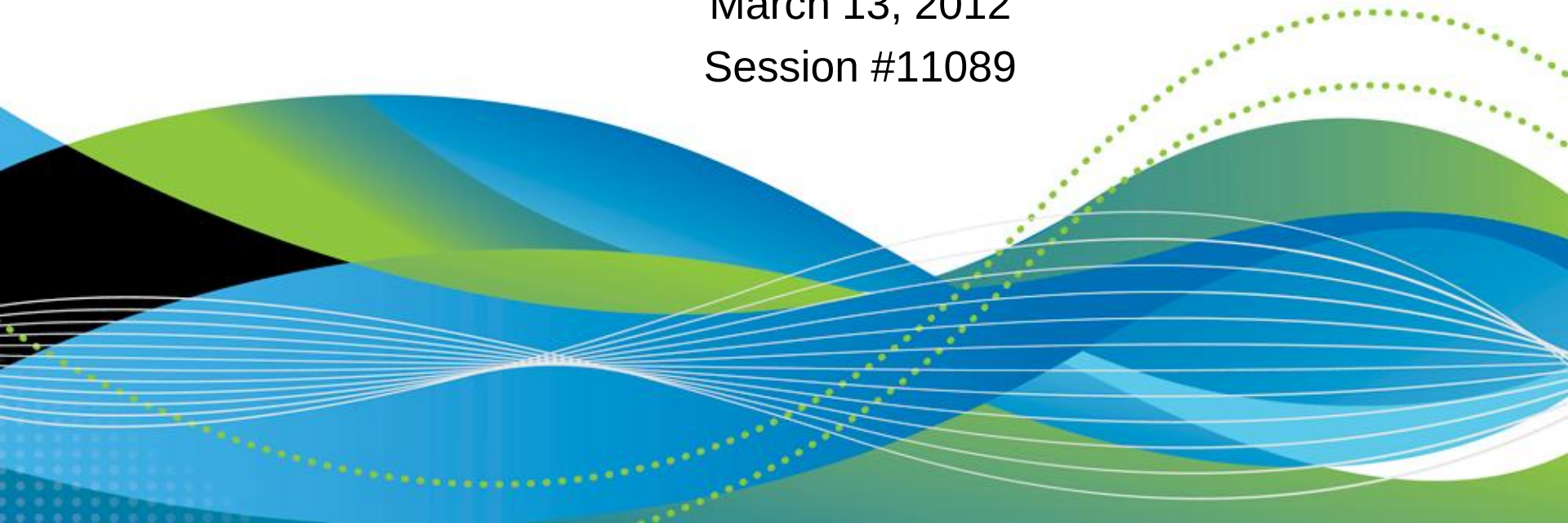
#SHAREorg

SHARE
Technology · Connections · Results

PCI DSS, z/OS and Keeping You from Becoming a News Headline

Charles Mills
CorreLog, Inc.

March 13, 2012
Session #11089



Copyright and Trademarks

- © Copyright 2012 CorreLog, Inc.
- Trademarks
  - CorreLog® is a registered trademark of CorreLog, Inc.
  - The following terms are trademarks of the IBM Corporation in the United States or other countries or both: DB2®, IBM®, MVS, RACF, System z, Tivoli®, z/OS®, zSeries®
  - ACF2® and Top Secret® are registered trademarks of CA Inc.
  - UNIX® is a registered trademark of The Open Group.
  - Windows® is a registered trademark of Microsoft Corporation.
  - PCI Security Standards Council is a trademark of The PCI Security Standards Council LLC.
  - Other company, product, or service names may be trademarks or service marks of others. No association with CorreLog, Inc. is implied.
- We acknowledge the *PCI DSS Requirements and Security Assessment Procedures, Version 2.0*, Copyright 2010 PCI Security Standards Council LLC.

Purpose of this Presentation

- At the end of this presentation, you should
  - Have an overview of PCI DSS requirements, and how they apply in a z/OS installation
  - Understand how SIEM is a part of PCI DSS compliance
    - More on what SIEM is later
  - Learn how to integrate z/OS into an organizational PCI DSS strategy

About the Presenter

- Charles has been developing mainframe software products since 1973
- Founded Firesign Computer Company – the Outbound software product – in 1975 and sold it to ASG in 1998
- Developing mainframe software for SHARE Atlanta exhibitor CorreLog, a SIEM solutions provider
- In keeping with SHARE's Canons of Conduct, this presentation will focus on the educational
  - …to keep you from becoming a security breach news headline

Agenda

- What is PCI DSS? Why PCI DSS?
- What are the requirements?
- What is SIEM and how does it relate to PCI DSS?
- How does it relate to you and your mainframe?
- Practical example

What is PCI DSS?
Why PCI DSS?

What is PCI DSS?

- Payment Card Industry Data Security Standard

  PCI Security Standards Council
  - Founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa

  DSS applies globally to *all* entities that store, process or transmit cardholder data
  - Merchants, payment card issuing banks, processors, developers and other vendors

Why PCI DSS?

- More than 543 million sensitive records breached since January 2005, according to PrivacyRights.org.
- You don't want to turn on *60 Minutes* and see your company
- Credit card companies such as Visa require DSS compliance
- 46 states have security breach disclosure laws
- "Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation." – US Department of Defense

What are the PCI DSS Requirements?

Some Key PCI DSS Concepts

- PAN
  - Primary Account Number, sometimes called just “account number.” The unique card number that identifies the issuer and the cardholder account. There are PCI DSS restrictions on displaying the PAN. PCI DSS applies only if PANs are stored, processed and/or transmitted.
- CAV2/CVC2/CVV2/CID
  - Different card providers have different names for the additional three or four digits on the front or the back of the card that uniquely identifies a particular piece of plastic. Generally you are prohibited from storing the card verification data.

Compensating Controls

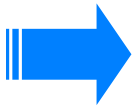
- Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated due to legitimate technical or documented business constraints
- Compensating controls must satisfy the following criteria:
  - Meet the intent and rigor of the original PCI DSS requirement.
  - Provide a similar level of defense as the original PCI DSS requirement
  - Be above and beyond other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)
- Must be documented annually

Compliance Assessment and Reporting

- Exact requirements set by credit card brand
- Third-party assessment firms
- For each requirement there is a specific “Testing Procedure” in the PCI DSS V2 document (reference on last slide)

PCI DSS Requirements

- Build and Maintain a Secure Network



1. Install and maintain a firewall configuration to protect cardholder data

Network Segmentation

- Isolating (segmenting) the cardholder data environment from the remainder of an entity's network
- Not a PCI DSS requirement
- But it reduces
  - The scope of PCI DSS compliance
  - The cost of PCI DSS compliance
  - The risks

1. Install and maintain a firewall configuration

- Establish firewall and router configuration standards …
- Build firewall and router configurations that restrict all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.
- Prohibit direct public access between the Internet and any system component in the cardholder data environment.
- Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization’s network.

PCI DSS Requirements

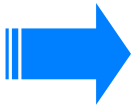
- Build and Maintain a Secure Network
  1. Install and maintain a firewall configuration to protect cardholder data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  3. Protect stored cardholder data

3. Protect stored cardholder data

- Limit cardholder data storage and retention time to that required for business, legal, and/or regulatory purposes
- Do not store sensitive authentication data after authorization.
  - Issuers may store authentication data if a business justification
- Mask PAN when displayed; the first six and last four digits are the maximum you may display.
  - Not applicable for authorized people with legitimate business need
- Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks
- Protect encryption keys from disclosure and misuse.
- Document and implement all appropriate key management processes and procedures for cryptographic keys

PCI DSS Requirements

- Build and Maintain a Secure Network
  1. Install and maintain a firewall configuration to protect cardholder data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  3. Protect stored cardholder data
  4. Encrypt transmission of cardholder data across open, public networks

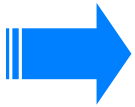


PCI DSS Requirements

- Maintain a Vulnerability Management Program
  5. Use and regularly update anti-virus software or programs
  6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  7. Restrict access to cardholder data by business need to know
  8. Assign a unique ID to each person with computer access
  9. Restrict physical access to cardholder data

PCI DSS Requirements

- Regularly Monitor and Test Networks



10. Track and monitor all access to network resources and cardholder data

What is SIEM and how does it relate to PCI DSS?

What is SIEM?

- SIEM: Security Information and Event Management
- Gartner:
  - Security information management (SIM) provides log management – the collection, reporting and analysis of log data – to support regulatory compliance reporting, internal threat management and resource access monitoring.
  - Security event management (SEM) processes event data from security devices, network devices, systems and applications in real time to provide security monitoring, event correlation and incident response. The technology can be used to discover activity associated with a targeted attack or a security breach, and is also used to satisfy a wide variety of regulatory requirements.
- IDC: “Worldwide revenue for SIEM was $663.3 million in 2009 and is expected to grow to $1.4 billion in 2013”

What Drives SIEM Adoption?

Figure 1 Compliance And Reporting Are Main Drivers Behind SIM Adoption

Base: 1,335 North American and European enterprise and SMB security decision-makers who expressed interest in adopting SIM
(percentages do not total 100 because of rounding)

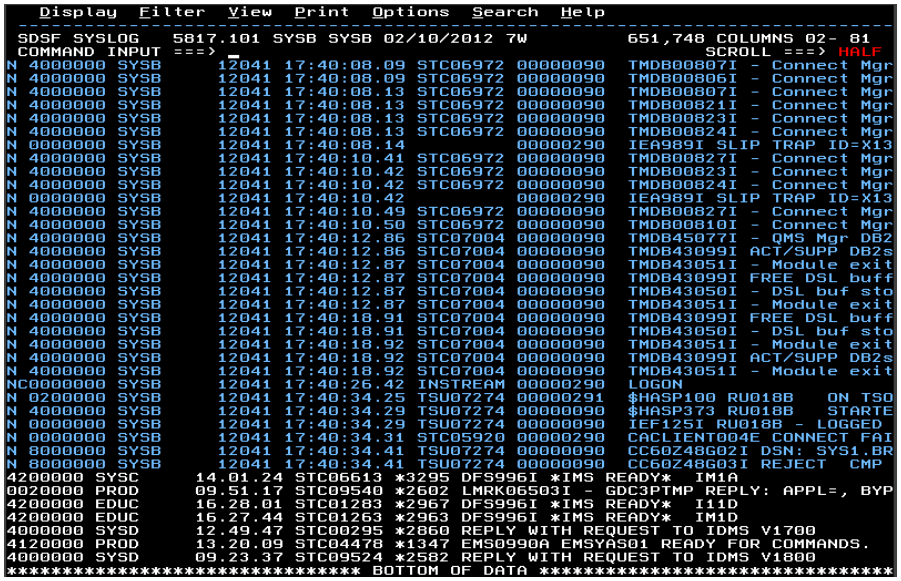
Source: Enterprise And SMB Security Survey, North America And Europe,

53864

Source: Forrester Research, Inc.

“Syslog” – Two Different Meanings

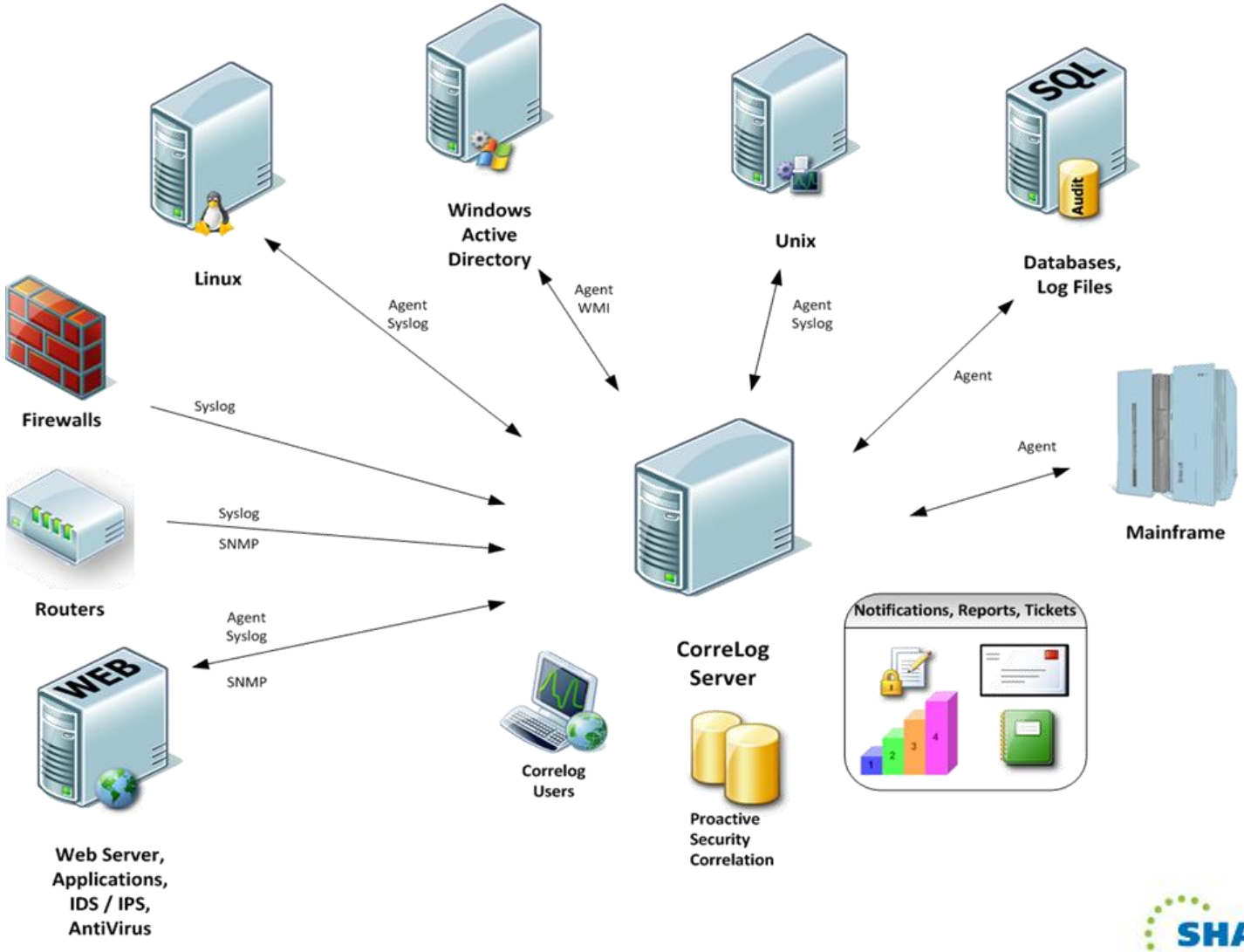
- z/OS: “a data set residing in the primary job entry subsystem's spool space … used by application and system programmers to record communications about problem programs and system functions.”
  – *MVS Planning: Operations*



“Syslog” – The SIEM Meaning

- SIEM and open systems: IETF RFC 3164 “The BSD syslog Protocol” (August, 2001)
  - *Almost* free-format text (ASCII) messages
  - **`<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8`**
  - UDP
  - Generated by most routers, firewalls, UNIX systems, etc.
    - No native Syslog capability: Windows and z/OS

Syslog Collector and Devices



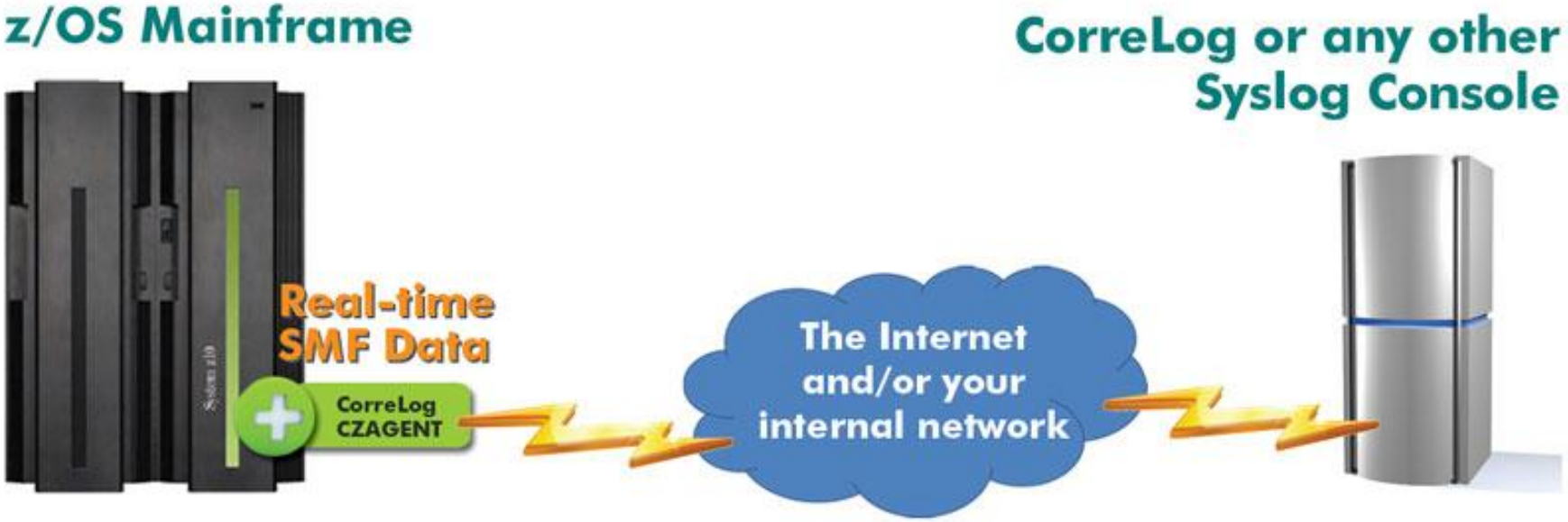
What do SIEM Products Do?

- Gartner: “Critical Capabilities for SIEM Technology”
  - Collect Syslog messages
  - Filtering
  - Correlation: establish relationships among messages and events – important for detecting or analyzing the progress of an attack
  - Event normalization and taxonomy: logon, log on, signon, sign on, session start, session initiation, …
  - Log management: cost-effective storage, indexing, analysis and reporting
  - User monitoring
  - Application monitoring
  - Compliance reporting

SIEM – Three ways to go

- Outsourced Service – Managed Security Service Provider (MSSP)
  - Example: IBM Security Services
- Pure Software
  - Examples: CorreLog, Tivoli Security Operations Manager
- Appliance
- Some products available as appliance or software

z/OS Needs an Agent



Agent and Syslog Collector plug together via the RFC 3164 standard

Agent converts SMF data to Syslog (RFC 3164)

- SMF is good source of events
  - Type 30 records have TSO logons, job and STC failures, etc.
  - Type 80 records have everything RACF: failures as well as successes, including dataset accesses
  - Type 101 records audit DB2 access
  - Type 110 records monitor CICS transactions
  - Type 119 records have everything TCP/IP: TN3270 logons, logoffs, FTP server, FTP client
  - Type 230 records have everything ACF2
- Agent reads via IEFU83/84/85 exits, selects, reformats and transmits
- Real time
  - Historically, SMF reporting has been historical – not great for security incidents

10. Track and monitor all access to network resources and cardholder data

- 10.1 Establish a process for linking all access to system components to each individual user – especially access done with administrative privileges.
- 10.3 Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.
- All access/each user: implies solution that spans heterogeneous platforms

10. Track and monitor all access to network resources and cardholder data

- z/OS agent reformats SMF as RFC 3164 Syslog and sends to SIEM
- RACF SMF Type 80 Event 2.x
  - **mvssysb RACF: Event: 2.3 - RESOURCE ACCESS: Warning Message Issued - Timestamp: 12034 17:44:52.27 - UserID: xxxxxx - Group: RESTRICT - Auth: Normal check - Reas: AUDIT option - Term: TCPB2922 - Job: xxxxxx - Res: SYS1.USER.PROCLIB - Req: UPDATE - Allow: READ - Vol: CATPAK - Type: DATASET - Prof: SYS1.USER.** - Owner: TSOHOLD - Name: CHARLES MILLS - POE: TCPB2922**

10. Track and monitor all access to network resources and cardholder data

- DB2 SMF Type 101
  - **MVSSYSC DB2: Subsys: DACH - CorrID: TMDB760EXPLN - Plan: TDBV50 - UserID: xxxxxx - LU: NA01DACH - Conn: RRSAF - SQL: {Create Synonym: 2 - Create Store Group: 2 - Drop Index: 2}**
- FTP Server Type 119
  - **mvssysb TCP/IP: Subtype: FTP server complete - Stack: TCPIP - UserID: xxxxxx - SubCmd: STOR - FileType: SEQ - RemtCtlIP: ::ffff:10.31.0.179 - DStype: Seq - Bytes: 51.41M - FName: xxxxxx.xxxxxx.LOGC.PSLZOS - Security: {Mech: None - CtlProt: None - DataProt: None - Login: Undefined} - RemtUserID: ZOSUSER**

10. Track and monitor all access to network resources and cardholder data

- 10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; Initialization of the audit logs; creation and deletion of system-level objects.

10.2 Audit trails for … invalid logical access attempts

- Invalid logons
  - **mvssysb RACF: Event: 1.9 - INIT/LOGON: Undefined User ID - UserID: #$@1238 - Group: #$@1238 - Auth: 00 - Reas: VERIFY failure**
- Invalid data access
  - **mvssysb RACF: Event: 2.1 - RESOURCE ACCESS: Insufficient Auth - UserID: xxxxxx - Group: RESTRICT - Auth: Normal check - Reas: AUDIT option - Job: xxxxxxxx - Res: SYS1.PROD.PROCLIBT - Req: READ - Allow: NONE - Vol: SYS001 - Type: DATASET - Prof: SYS1.PROD.PROCLIBT - Owner: DATASET - Name: CHARLES MILLS - POE: INTRDR**

10.2 Audit trails for … invalid logical access attempts

- **mvssysb TCP/IP: Subtype: Connect init - Stack: TCPIP - ResName: TN3270 - RemtIP: ::ffff:10.2.1.152**
- **mvssysb TCP/IP: Subtype: Telnet SNA init - Stack: TCPIP - Term: TCPB2926 RemtIP: ::ffff:10.2.1.152**
- **mvssysb RACF: Event: 1.1 - INIT/LOGON: Invalid Password - UserID: xxxxxx - Group: TSOHOLD - Reas: VERIFY failure - Term: TCPB2926 - Name: xxxx xxxxx**

10. Track and monitor all access to network resources and cardholder data

- 10.4 Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time
- 10.5 Secure audit trails so they cannot be altered
- 10.6 Review logs for all system components related to security functions at least daily
- 10.7 Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis

10.5 Secure audit trails so they cannot be altered

- Key function of a SIEM system
- Logs stored in secure location with checksum to detect modification
- 10.5.1 requires that log access be limited to authorized users
- 10.5.2 requires that logs be protected from modification
- 10.5.3 requires backups of logs

10. Track and monitor all access to network resources and cardholder data

- 10.6 Review logs for all security functions daily
  - SIEM consoles include correlation, ticketing and alerting functions
  - Simplifies review workflow
- 10.7 Retain audit trail history for at least one year with at least three months immediately available for analysis
  - SIEM consoles include configurable retention periods of up to twelve or more years

PCI DSS Requirements

- Regularly Monitor and Test Networks
  10. Track and monitor all access to network resources and cardholder data
  11. Regularly test security systems and processes
  12. Maintain a policy that addresses information security for all personnel

11. Regularly Monitor and Test Security

- 11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.
- 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.
- 11.3 Perform external and internal penetration testing
- 11.4 Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment

11.5 Deploy file integrity monitoring tools

- Through SMF Types 15 and 64
  - **mvssysb FIM: JobNm: xxxxxxx - DDN: OUTDD - DSN: xxxxxx.PREPROD.V660.OBJLIB - Member: INEXIV12**
- Through SMF Type 80 Event 2.0
  - **mvssysb RACF: Event: 2.0 - RESOURCE ACCESS: Successful Access - UserID: xxxxxx - Group: QAL - Auth: Normal check - Reas: AUDIT option - Term: TCPQ2912 - Job: xxxxxxx - Res: SYS1.DEVL.PARMLIB - Req: UPDATE - Allow: UPDATE - Vol: ESACAT - Type: DATASET - Prof: SYS1.DEVL.** - Owner: SYS1 - Name: xxxx xxxxxxxx - POE: TCPQ2912**

12: Maintain a policy that addresses information security for all personnel

- 12.1 Establish, publish, maintain, and disseminate a security policy that addresses all PCI DSS requirements, includes an annual process for identifying vulnerabilities and formally assessing risks, …
- 12.2 Develop daily operational security procedures that are consistent with requirements in PCI DSS.
- 12.3 Develop usage policies for critical technologies to define their proper use by all personnel.
- 12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
- 12.5 Assign to an individual or team information security responsibilities defined by 12.5 subsections.
- 12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
- 12.7 Screen potential personnel prior to hire ...

Practical Example

- Requirement
  - Major North American retailer
  - Committed to SecureWorks – Managed Security Service Provider
    - Receiving events from Windows and UNIX
  - Required PCI DSS compliance for DB2-based credit card data
- Implementation
  - CorreLog z/OS agent installed on multiple LPARs
  - Formatting and forwarding RACF, logon, and DB2 events
    - Over 200,000 messages per hour from busiest LPAR
- Results
  - Enterprise-wide PCI DSS compliance
  - Achieved ambitious 8-week implementation schedule

In conclusion …

- We have discussed
  - An overview of PCI DSS requirements, and how they apply in a z/OS installation
  - What is SIEM
  - How SIEM is a part of PCI DSS compliance
  - How to integrate z/OS into an organizational PCI DSS strategy
- Thank you
- Come see us at SHARE Atlanta booth #510

References

- PCI Security Standards Council: https://www.pcisecuritystandards.org
- PCI DSS Assessment: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
- RFC 3164: http://www.ietf.org/rfc/rfc3164.txt
- CorreLog: http://www.correlog.com/
- CorreLog z/OS Agent: http://www.correlog.com/solutions-and-services/sas-correlog-mainframe.html
- Speaker: Charles.Mills@CorreLog.com