



17369: Bridge the Gap: How to Use an Enterprise Product You Already Own to Enhance z/OS Security

Charles Mills
Director of Advanced Projects
CorreLog, Inc.
Charles.Mills@CorreLog.com

© 2015 CorreLog, Inc.

About the Speaker

- Charles is the Director of Advanced Projects for CorreLog, Inc. He is responsible for the CorreLog Agent for z/OS.
- He was the founder and CTO of a company that developed a mainframe/PC file transfer program. As such, he was responsible for both mainframe and non-mainframe technology and developers.



Agenda

- Preface: Two Worlds of IT security
- Real-time Alerts: Make your mainframe more secure by taking advantage of the security tools you probably already have
 - Why, What, How
- Brief Introduction to SIEM Systems

© 2015 CorreLog, Inc.

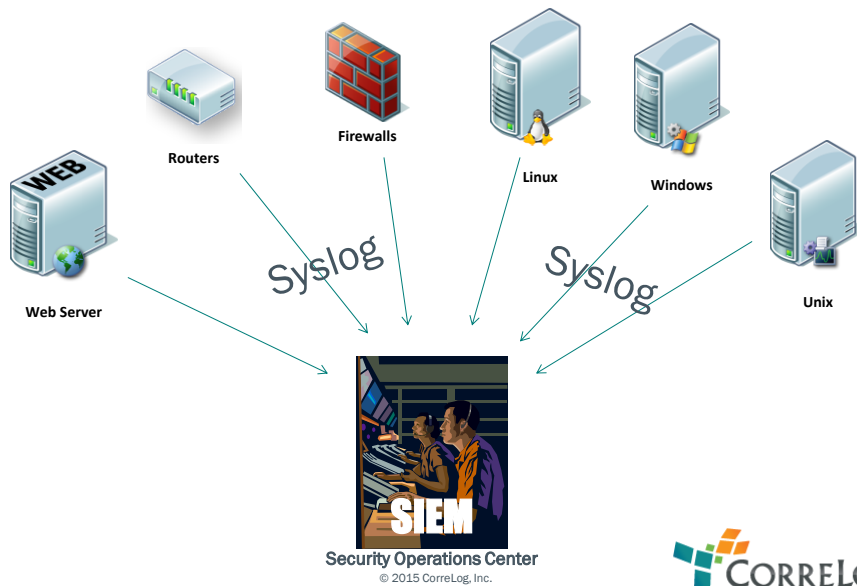


Preface: Two Worlds of IT Security

Security in the Mainframe World



Security in the Network World



What's a SIEM?

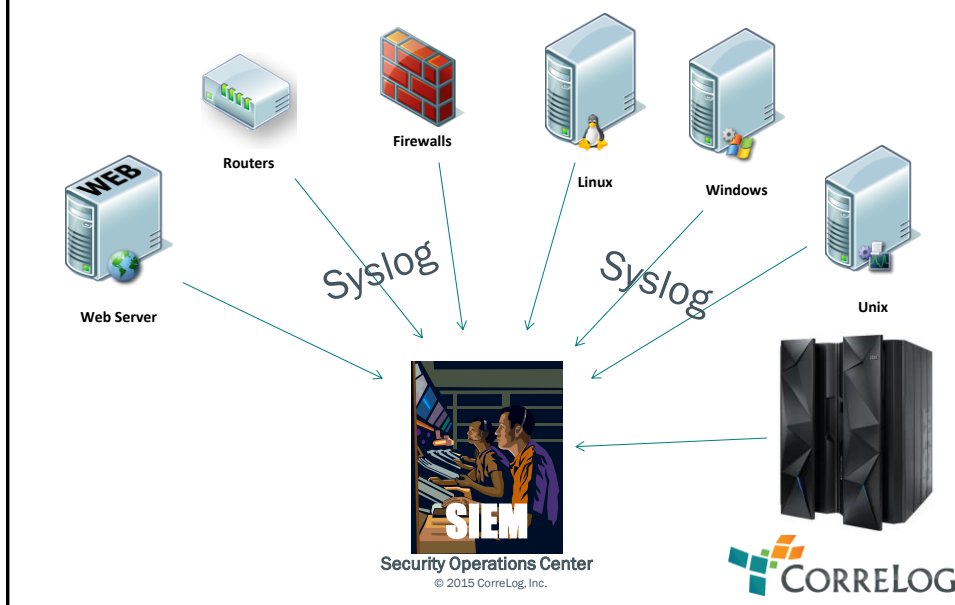
- Security Information and Event Management
- Collects Syslog messages
- Filtering
- Correlation: pattern recognition; establishing relationships among messages and events
- IP Geo-location
- Real-time Alerts
- Log management: cost-effective forensic (tamper-proof or tamper-evident) storage, indexing, analysis, search and reporting
- User and Application Monitoring
- Compliance reporting
- You probably spent or are spending \$\$\$,\$\$\$ on a SIEM

© 2015 CorreLog, Inc.



Real-Time Alerts: Let your mainframe take advantage of network security tools

Mainframe in the Network Security World



Why Integrate z/OS into your SIEM?

- Compliance: PCI DSS, HIPAA, GLBA, SOX, IRS Pub. 1075
 - You need to include the box with 70% of the data
 - CISOs and Auditors are discovering the mainframe
- z/OS is not invulnerable
 - You already paid for a SIEM – why not use it to help protect z/OS?
 - Add z/OS to the correlation mix

Aren't Mainframes Inherently Secure?

- “The mainframe is the most securable platform” – Mark Wilson, RSM Partners, SHARE 2014
- “Insider threats are the leading cause of data breaches in the last 12 months” – *Understand The State Of Data Security And Privacy: 2013 To 2014*, Forrester Research



Source: Wikimedia



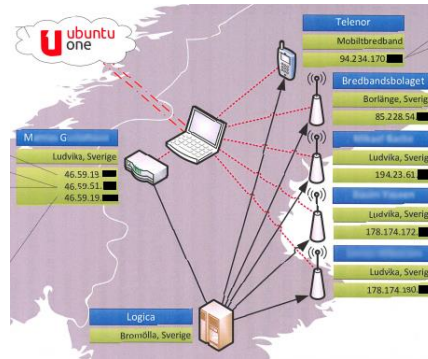
Yes, z/OS Can be Breached!

- Per Gottfrid Svartholm Warg, alias **anakata**, co-founder of The Pirate Bay, a digital content piracy sharing site
- Convicted of violating Swedish copyright law in 2009 – flees to Cambodia
- Pursues vendetta against MPAA lawyer Monique Wadsted
- In 2010, hacks into her account on Infotorg, a browser-accessed database hosted on z/OS at Logica, a Swedish service bureau
- Hacks continue in 2011 and 2012
- Leverages CGI shell command injection into full scale hack against Logica during first quarter of 2012



The Breach Becomes a Crisis

- Data including government agency files, credit cards, and 10,000 social security numbers
- Downloaded RACF databases, used password cracking tool* to decrypt thousands of passwords
- Installed backdoor to allow easy ongoing access
- Attempted to transfer 5.7 million Swedish kronor (~US\$600,000) from Nordea Bank to accomplices
- Logica unable to contain breach and invokes Swedish “national event”
- Svartholm and an accomplice extradited from Cambodia and convicted June 2013



*John The Ripper – you can Google it – includes explicit support for RACF password decryption



“Hackers against Society”

- Breach of CSC Denmark mainframe, April to August, 2012
- Downloaded and also may have modified information in the driver's license registry and the Schengen database of wanted persons
- Same mainframe also served Danish Tax Authority, the citizen ID number registry and other public agencies
- October 31, 2014 Svartholm convicted and sentenced to three-and-one-half years in prison in Denmark. He is appealing



Your Mainframe is not a Silo

- You may have separate mainframe and network security teams, but hackers do not
- Breaches are systemic, not platform-specific
- Svartholm and his accomplices moved freely among PC, Web, z/OS, UNIX – and Hercules
- Protect your mainframe by correlating the indicators

© 2015 CorreLog, Inc.



Correlation is Power

- More failed TSO logons than normal may not be significant ...
- But what if correlated with more intrusion detection system hits than normal, more firewall hits than normal, more Web logon failures than normal?
- That is what SIEM systems do – think how powerful to add your mainframe into the mix

© 2015 CorreLog, Inc.



“Call the Doctor, not the Undertaker”

- Traditional mainframe approach is nightly reports
- But you want to find out about a breach now, not tomorrow morning
- The Network Security World has real-time tools – why not utilize them?
 - When was the last time a batch report sent you a text?
- Leverage the SIEM software you probably already own for real-time alerts
- Separation of duties: move the mainframe log files off of the mainframe
- PCI DSS, IRS Pub. 1075, SOX all require secure, archived log of accesses – why use gigabytes of mainframe DASD?

© 2015 CorreLog, Inc.



z/OS Events Available Real-time

- Everything RACF, ACF2 and Top Secret
 - Failures only, or audit successes too
- File integrity: who modified SYS1.PARMLIB?
 - PDS, QSAM, VSAM and UNIX files written
 - Renames and Scratches
- Start and end of TSO sessions
 - Optionally started tasks, batch jobs, ABENDs, etc.
- TCP/IP, TN3270 and FTP sessions and failures
- New! IND\$FILE events
- Everything needed from DB2 for PCI DSS
- Audited CICS Transactions
- Partner events: NewEra, Vanguard, ...
- Console messages, IMS, ...
- All real-time – no periodic FTP

© 2015 CorreLog, Inc.



What IP Address Edited SYS1.PARMLIB?

<69>Mar 26 05:18:00 mvssysb TCP/IP: Subtype: Telnet
SNA init - TermNm: TCPB2931 - RemtIP: 58.14.0.140

<29>Mar 26 05:18:22 mvssysb SMF: Start - Work: TSO -
JobID: TSU00863 - Group: RESTRICT - UserID: SYS013B
- TermNm: TCPB2931

<118>Mar 26 05:22:09 mvssysb DFSMS: Action:
Add/Replace - JobNm: RU018A - Step: \$TSUSER - Proc:
\$TSUSER - DSN: SYS1.PARMLIB - Vol: LS0501 - Flag:
Replace - Mem: IEAAPF00 - UserID: SYS013B - POE:
TCPB2931 - Group: RESTRICT

© 2015 CorreLog, Inc.



RACF Events

<35>Nov 27 19:44:00 SYSB RACF: RESOURCE ACCESS:
Insufficient Auth - UserID: RU018B - Group:
RESTRICT - Reas: AUDIT option - Job: RU018BTR -
Res: SYS1.PROD.PROCLIBT - Req: READ - Allow: NONE
- Vol: SYS001 - Type: DATASET - Prof:
SYS1.PROD.PROCLIBT - Owner: DATASET - Name: ROBERT
SMITH - POE: INTRDR

<35>May 14 11:11:46 SYSB RACF: INIT/LOGON: Invalid
Password - UserID: QAMLB2 - Group: TSOHOLD - Auth:
00 - Reas: VERIFY failure - Term: TCPA2959 - Name:
MARIE BERGERON - POE: TCPA2959

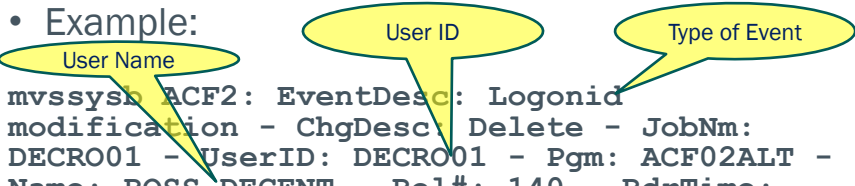
© 2015 CorreLog, Inc.



ACF2 Security Events

- Logon ID Modification, Dataset & Program Security Journal, Invalid Password Authority, Resource Access Violation, Restricted Logon ID and similar mainframe security events

- Example:



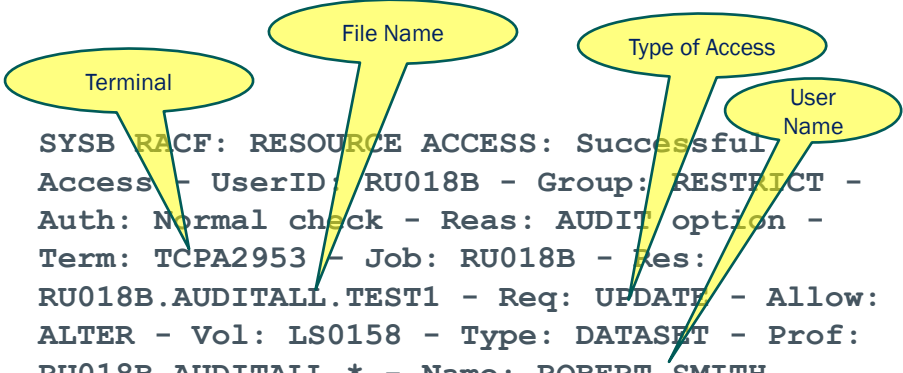
 mvssysb ACF2: EventDesc: Logonid
 modification - ChgDesc: Delete - JobNm:
 DECRO01 - UserID: DECRO01 - Pgm: ACF02ALT -
 Name: ROSS DECENT - Rel#: 140 - RdrTime:
 2012-07-03T16:19:43.880 - ASID: XE34 -
 DelTime: 2012-07-03T17:19:51.028 - UID:
 OMVSDGRPAAABDECRO01

© 2015 CorreLog, Inc.



File Integrity Monitoring

- Be alerted to modifications of critical system files
- Filter out system temporaries and SPFTEMP



 SYSB RACF: RESOURCE ACCESS: Successful
 Access - UserID: RU018B - Group: RESTRICT -
 Auth: Normal check - Reas: AUDIT option -
 Term: TCPA2953 - Job: RU018B - Res:
 RU018B.AUDITALL.TEST1 - Req: UPDATE - Allow:
 ALTER - Vol: LS0158 - Type: DATASET - Prof:
 RU018B.AUDITALL.* - Name: ROBERT SMITH

© 2015 CorreLog, Inc.



TCP/IP and FTP Events

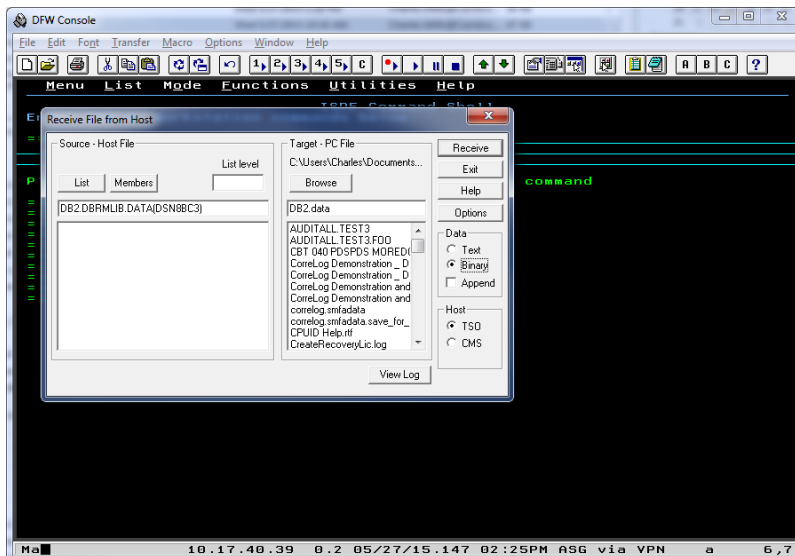
```
<69>Mar 26 17:32:46 mvssysb TCP/IP: Subtype: FTP server
complete - Stack: TCPIP - Op: Retrieve - FileType: SEQ -
RemtDataIP: ::ffff:10.31.0.209 - UserID: RX239JB -
DStype: HFS - Start: 11037 22:32:45.21 - Dur: 0.78 -
Bytes: 56324 - SessID: FTPD100335 - DSN:
/u/rx239jb/Source/Fields.C - Security: {Mech: None -
CtlProt: None - DataProt: None - Login: Password}
```

```
<69>Mar 25 18:53:21 mvssysb TCP/IP: Subtype: FTP server
logon fail - Stack: TCPIP - AS: FTPD1 - UserID: DV174A -
RemtIP: ::ffff:10.10.8.66 - LogonUserID: DV174A - Reas:
Password invalid - SessID: FTPD100026 - Security: {Mech:
None - CtlProt: None - DataProt: Undefined - Login:
Password}
```

© 2015 CorreLog, Inc.



IND\$File Events



New! IND\$defender

- IND\$FILE is a useful tool but completely unaudited
- May 28 16:18:10 MVSSYSB CorreLog: SubT: IND\$FILE Audit - SubCmd: GET - DSN: SYSP.DB2.DBRMLIB.DATA - Mem: DSN8BC3 - Type: Partitioned - RdrTime: 2015-05-28T20:16:41.164 - UserID: DEV013 - Name: CHARLES MILLS - Group: RESTRICT - RemtIP: 129.42.38.1 - JobID: TSU00637 - TermNm: NVA00076 - Dur: P00:00:02.660

© 2015 CorreLog, Inc.



UNIX File System Events

Full path name

z/OS Job Name

OMVS UID

```

Jun 20 14:33:35 mvssysb zFS: APID: 67305918 - Cat: zFS -
OGroup: 675 - JobNm: MDRZ620A - PGroup: 84083495 - PID:
84083495 - Group: ZDEV - Start: 2014-06-20T11:56:49.390 -
Uid: DV001 - SessID: 84083495 - StepNm: MDRZSYS - SubT:
File close - Ouid: 500021 - In: 4255 - DirBlks: 10 -
DevNo: 0069 - Inode: 133 - BlksRead: 2 - FName:
/source/views/$shared$.views.xml - Reads: 3 - Close:
2014-06-20T14:33:34.879 - Token: 6943232 - Open: 2014-06-
20T14:33:34.856 - Type: Regular
  
```

© 2015 CorreLog, Inc.



UNIX File System Events

Full path name

z/OS Job Name

OMVS UID

```
Jun 20 14:33:35 mvssysb zFS: APID: 67305918 - Cat: zFS -
OGroup: 675 - JobNm: MDRZ620A - PGroup: 84083495 - PID:
84083495 - Group: ZDEV - Start: 2014-06-20T11:56:49.390 -
Uid: DV001 - SessID: 84083495 - StepNm: MDRZSYS - SubT:
File close - OUid: 500021 - In: 4255 - DirBlks: 10 -
DevNo: 0069 - Inode: 133 - BlksRead: 2 - FName:
/source/views/$shared$.views.xml - Reads: 3 - Close:
2014-06-20T14:33:34.879 - Token: 6943232 - Open: 2014-06-
20T14:33:34.856 - Type: Regular
```

© 2015 CorreLog, Inc.



Operational Events

```
<29>Mar 04 04:42:01 mvssysb SMF:
End - Work: STC - Sysname: SYSB -
JobNm: MITDB41T - JobID: STC07802 -
Step#: 1 - Group: DFLTSTC - UID:
LSCSTC - RC: U0011-0
```

© 2015 CorreLog, Inc.



DB2 Events

<110>Mar 24 15:29:00 mvssysb DB2: Subsys: DA1L -
IFCID: **Audit administrative authorities** - UserID:
RU018B - AuthID: RU018B - CorrID: RU018BD3 - Auth:
SYSADM - Priv: SELECT - ObjType: Table or view -
Cmd: SELECT * FROM SYSIBM.SYSTABLES - SrcQual:
SYSIBM - Src: SYSTABLES

<110>Mar 24 15:44:20 mvssysb DB2: Subsys: DA1L -
IFCID: **Authorization failures** - UserID: RU018A -
AuthID: RU018A - CorrID: RU018ADS - Priv: SELECT -
ObjType: Table or view - SrcQual: CORE1010 - Src:
NEWPHONE - Node: JES2SYSB - Group: RESTRICT - POE:
INTRDR - Sql: SELECT * FROM CORE1010.NEWPHONE

© 2015 CorreLog, Inc.



Introduction to SIEMs

Types of SIEMs

- Conventional Software/Appliance/Virtual Appliance
 - Running on Linux, UNIX or Windows
 - HP ArcSight ESM
 - IBM Security Qradar
 - LogRhythm
 - AlienVault (Open Source)
 - McAfee (Intel Security) NitroView
 - RSA (EMC) Security Analytics (enVision)
 - CorreLog Correlation Server
 - Splunk – do not call themselves a SIEM but customers use as a SIEM, and Gartner positions as a SIEM



© 2015 CorreLog, Inc.



SIEM in the Cloud: MSSP



- Managed Security Service Provider
 - Some are hybrids with on-site “concentrator” appliance
 - Dell SecureWorks
 - IBM Managed Security Services
 - Verizon
 - NTT Solutionary



Correlation

The screenshot shows the 'Correlation' configuration page in the CorreLog Server web interface. The page is titled 'Correlation Thread' and includes several configuration options:

- Correlation Thread Title:** Z FTP RACF Errors (55 characters available)
- Pin This Thread To Top:** Yes
- Match Time:** Midnight + 24 hrs
- Match IP Addr / Group:** @zoz@@ (Browse Groups checkbox is unchecked)
- Match Facility:** security
- Match Severity:** GE error
- Match Trigger State:** None Any
- Match Expression:** "POEClass: Terminal" AND NOT "POE: TCP" (461 characters available)

Buttons at the top include Cancel, Reset, Delete, SaveNew, and Save. A 'View Message Catalog' link is also present. At the bottom, there are links for 'View This Thread's Dependents' and 'Regenerate Catalog Information'.

Real-Time Text Alerts

The screenshot shows the 'Counters' configuration page in the CorreLog Server web interface. The page is titled 'System Counter Name' and includes several configuration options:

- System Counter Name:** Thread/ Z FTP RACF Errors
- Pin This Alert To Top:** Yes
- Compare Function:** (GE) Greater Than Or Equal
- Threshold:** 1 Counts Per Interval
- Test Interval:** 20 Seconds
- Match Alert Time:** Midnight + 24 hrs
- When Threshold Is Triggered:** (No specific selection)
- Send Alert Message:** Unauthorized FTP transfer attempted by \$T_RELATED_USERNAME (153 characters available)
- Insert Alert Variable:** None

Buttons at the top include Cancel, Reset, Delete, SaveNew, and Save. A 'Go To Thread Definition Screen' link is also present. At the bottom, there is a 'Suggest' button.

Overlaid on the right is a mobile phone screen showing an SMS alert from CorreLog, Inc. The message reads: "(CorreLog Ticket) ASSIGNEE: admin - MESSAGE: notice Unauthorized FTP transfer attempted on MVSSYSA - Production V2R1 - by Ru018b". The phone screen also shows the time 11:41 AM and the contact name charlesm@mcn.org.

Compliance Scorecards

PCI DSS Score Card Report

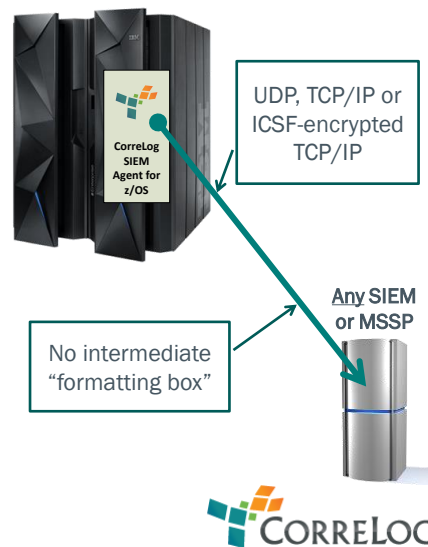
Match Requirement: *

[Download HTML Report](#) | [Download Text Report](#) | [Download CSV Report](#)

Requirement	Description	Msgs Today	Msgs Yesterday	Last 7 Days	Last 30 days	Daily Avg	Status
PCI-DSS 1.0	Install and maintain a firewall configuration to protect cardholder data. Firewall Packet Dropped Events	0	0	0	0	0	NO-DATA
PCI-DSS 2.0	Do not use vendor-supplied defaults for system passwords and other security parameters. Successful Admin Logon Events	6	0	21	55	3	OK
PCI-DSS 3.0	Protect stored cardholder data. Active Directory Account Changes Active Directory Group Changes Windows Blocked Connections	0	0	0	0	0	NO-DATA
PCI-DSS 4.0	Encrypt transmission of cardholder data across open, public networks. Virus Scanner Events	0	0	0	0	0	NO-DATA
PCI-DSS 5.0	Use and regularly update anti-virus software. Virus Scanner Events	0	0	0	0	0	NO-DATA
PCI-DSS 6.0	Develop and maintain secure systems and applications. Irregular System Messages	47	165	940	1584	83	OK
PCI-DSS 7.0	Restrict access to cardholder data by business need-to-know. Correlation Alerts	2	0	4	7	1	OK
PCI-DSS 8.0	Assign a unique ID to each person with computer access. Successful Logon Events	32	16	206	2696	134	OK
PCI-DSS 9.0	Restrict physical access to cardholder data. Network Share Access	0	0	0	0	0	NO-DATA

z/OS to SIEM Integration

- ArcSight and QRadar include free or low-cost connectors
 - Frequent FTP
 - Limited functionality
- Splunk-specific agent from Syncsort
- CorreLog SIEM Agent for z/OS
 - SIEM Agnostic
 - 100% Real-time



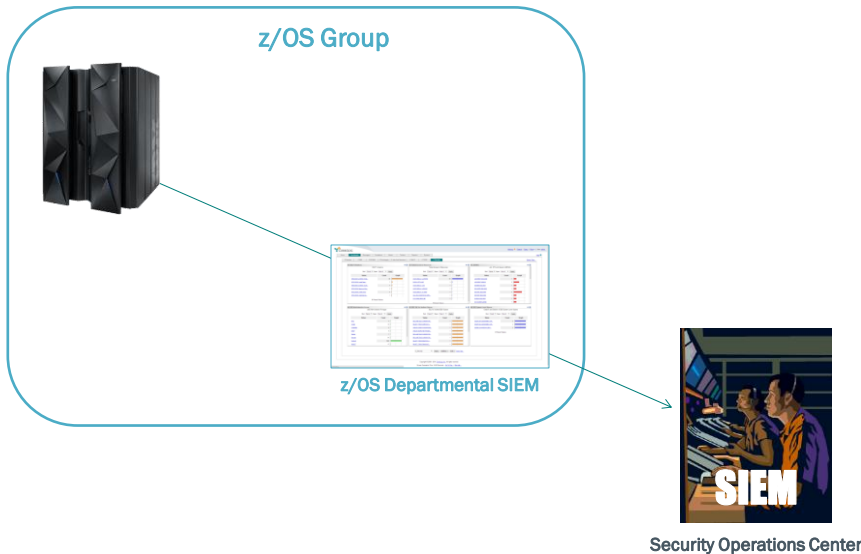
z/OS Events in Splunk

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** Contains the query 'racf'.
- Results:** 412 events (before 12/20/13 6:29:24.000 AM).
- Timeline:** A bar chart showing event frequency over time.
- Event List:**

Time	Event
12/13/13 5:18:00.000 PM	<35-Dec 13 17:18:00 mvssysb RACF eventdesc="INIT/LOGON: Invalid Password" severity=Error userId=CUSFTM group=LSCOMVS auth=None reas="VERIFY failure" term=TCPPO693 name="FRED WRIGHT" poe=TCPPO693 host = mvssysb source = tcp1468 sourcetype = syslog term= TCPPO693
12/13/13 5:05:10.000 PM	<38-Dec 13 17:05:10 mvssysb RACF eventdesc="INIT/LOGON: Successful Racinit Init" severity=Informational userId=DV231B group=TSOHOLD auth=None reas=None term=DV231B job=NVPTTC24 name="DAVID BROOKS" poe=DV231B host = mvssysb source = tcp1468 sourcetype = syslog term= DV231B
12/13/13 4:20:53.000 PM	<38-Dec 13 16:20:53 mvssysb RACF eventdesc="INIT/LOGON: Successful Racinit Delete" severity=Informational userId=DWGD group=TSOHOLD auth=None reas=None term=NVPTD002 job=NVPTMB name="BILL DICKEY" poe=NVPTD002 host = mvssysb source = tcp1468 sourcetype = syslog term= NVPTD002
12/13/13 4:20:53.000 PM	<38-Dec 13 16:20:53 mvssysb RACF eventdesc="INIT/LOGON: Successful Racinit Init" severity=Informational userId=DWGD group=TSOHOLD auth=None reas=None term=NVPTD002 job=NVPTMB name="BILL DICKEY" poe=NVPTD002 host = mvssysb source = tcp1468 sourcetype = syslog term= NVPTD002
12/13/13 4:19:41.000 PM	<38-Dec 13 16:19:41 mvssysb RACF eventdesc="INIT/LOGON: Successful Racinit Delete" severity=Informational userId=DWGD group=TSOHOLD auth=None reas=None term=NVPTD002 job=NVPTMB name="BILL DICKEY" poe=NVPTD002

CorreLog Visualizer for z/OS



Mainframe Values Events in z/OS Visualizer

The screenshot displays the CORRELOG z/OS Visualizer interface with several dashboards:

- 1) RACF Violations:** A table showing RACF violations with columns for Value, Count, and Graph. Values include RACF001, RACF002, RACF003, RACF004, RACF005, RACF006, RACF007, RACF008, RACF009, RACF010, RACF011, RACF012, RACF013, RACF014, RACF015, RACF016, RACF017, RACF018, RACF019, RACF020, RACF021, RACF022, RACF023, RACF024, RACF025, RACF026, RACF027, RACF028, RACF029, RACF030, RACF031, RACF032, RACF033, RACF034, RACF035, RACF036, RACF037, RACF038, RACF039, RACF040, RACF041, RACF042, RACF043, RACF044, RACF045, RACF046, RACF047, RACF048, RACF049, RACF050, RACF051, RACF052, RACF053, RACF054, RACF055, RACF056, RACF057, RACF058, RACF059, RACF060, RACF061, RACF062, RACF063, RACF064, RACF065, RACF066, RACF067, RACF068, RACF069, RACF070, RACF071, RACF072, RACF073, RACF074, RACF075, RACF076, RACF077, RACF078, RACF079, RACF080, RACF081, RACF082, RACF083, RACF084, RACF085, RACF086, RACF087, RACF088, RACF089, RACF090, RACF091, RACF092, RACF093, RACF094, RACF095, RACF096, RACF097, RACF098, RACF099, RACF100.
- 2) Failed Access to Resources:** A table showing failed access to resources with columns for Value, Count, and Graph. Values include RACF001, RACF002, RACF003, RACF004, RACF005, RACF006, RACF007, RACF008, RACF009, RACF010, RACF011, RACF012, RACF013, RACF014, RACF015, RACF016, RACF017, RACF018, RACF019, RACF020, RACF021, RACF022, RACF023, RACF024, RACF025, RACF026, RACF027, RACF028, RACF029, RACF030, RACF031, RACF032, RACF033, RACF034, RACF035, RACF036, RACF037, RACF038, RACF039, RACF040, RACF041, RACF042, RACF043, RACF044, RACF045, RACF046, RACF047, RACF048, RACF049, RACF050, RACF051, RACF052, RACF053, RACF054, RACF055, RACF056, RACF057, RACF058, RACF059, RACF060, RACF061, RACF062, RACF063, RACF064, RACF065, RACF066, RACF067, RACF068, RACF069, RACF070, RACF071, RACF072, RACF073, RACF074, RACF075, RACF076, RACF077, RACF078, RACF079, RACF080, RACF081, RACF082, RACF083, RACF084, RACF085, RACF086, RACF087, RACF088, RACF089, RACF090, RACF091, RACF092, RACF093, RACF094, RACF095, RACF096, RACF097, RACF098, RACF099, RACF100.
- 3) ABE/DCs:** A table showing ABE/DCs with columns for Value, Count, and Graph. Values include ABE001, ABE002, ABE003, ABE004, ABE005, ABE006, ABE007, ABE008, ABE009, ABE010, ABE011, ABE012, ABE013, ABE014, ABE015, ABE016, ABE017, ABE018, ABE019, ABE020, ABE021, ABE022, ABE023, ABE024, ABE025, ABE026, ABE027, ABE028, ABE029, ABE030, ABE031, ABE032, ABE033, ABE034, ABE035, ABE036, ABE037, ABE038, ABE039, ABE040, ABE041, ABE042, ABE043, ABE044, ABE045, ABE046, ABE047, ABE048, ABE049, ABE050, ABE051, ABE052, ABE053, ABE054, ABE055, ABE056, ABE057, ABE058, ABE059, ABE060, ABE061, ABE062, ABE063, ABE064, ABE065, ABE066, ABE067, ABE068, ABE069, ABE070, ABE071, ABE072, ABE073, ABE074, ABE075, ABE076, ABE077, ABE078, ABE079, ABE080, ABE081, ABE082, ABE083, ABE084, ABE085, ABE086, ABE087, ABE088, ABE089, ABE090, ABE091, ABE092, ABE093, ABE094, ABE095, ABE096, ABE097, ABE098, ABE099, ABE100.
- 4) DB2 Administrative Access:** A table showing DB2 administrative access with columns for Value, Count, and Graph. Values include DB2001, DB2002, DB2003, DB2004, DB2005, DB2006, DB2007, DB2008, DB2009, DB2010, DB2011, DB2012, DB2013, DB2014, DB2015, DB2016, DB2017, DB2018, DB2019, DB2020, DB2021, DB2022, DB2023, DB2024, DB2025, DB2026, DB2027, DB2028, DB2029, DB2030, DB2031, DB2032, DB2033, DB2034, DB2035, DB2036, DB2037, DB2038, DB2039, DB2040, DB2041, DB2042, DB2043, DB2044, DB2045, DB2046, DB2047, DB2048, DB2049, DB2050, DB2051, DB2052, DB2053, DB2054, DB2055, DB2056, DB2057, DB2058, DB2059, DB2060, DB2061, DB2062, DB2063, DB2064, DB2065, DB2066, DB2067, DB2068, DB2069, DB2070, DB2071, DB2072, DB2073, DB2074, DB2075, DB2076, DB2077, DB2078, DB2079, DB2080, DB2081, DB2082, DB2083, DB2084, DB2085, DB2086, DB2087, DB2088, DB2089, DB2090, DB2091, DB2092, DB2093, DB2094, DB2095, DB2096, DB2097, DB2098, DB2099, DB2100.
- 5) DB2 SQL for Audited Objects:** A table showing DB2 SQL for audited objects with columns for Value, Count, and Graph. Values include DB2001, DB2002, DB2003, DB2004, DB2005, DB2006, DB2007, DB2008, DB2009, DB2010, DB2011, DB2012, DB2013, DB2014, DB2015, DB2016, DB2017, DB2018, DB2019, DB2020, DB2021, DB2022, DB2023, DB2024, DB2025, DB2026, DB2027, DB2028, DB2029, DB2030, DB2031, DB2032, DB2033, DB2034, DB2035, DB2036, DB2037, DB2038, DB2039, DB2040, DB2041, DB2042, DB2043, DB2044, DB2045, DB2046, DB2047, DB2048, DB2049, DB2050, DB2051, DB2052, DB2053, DB2054, DB2055, DB2056, DB2057, DB2058, DB2059, DB2060, DB2061, DB2062, DB2063, DB2064, DB2065, DB2066, DB2067, DB2068, DB2069, DB2070, DB2071, DB2072, DB2073, DB2074, DB2075, DB2076, DB2077, DB2078, DB2079, DB2080, DB2081, DB2082, DB2083, DB2084, DB2085, DB2086, DB2087, DB2088, DB2089, DB2090, DB2091, DB2092, DB2093, DB2094, DB2095, DB2096, DB2097, DB2098, DB2099, DB2100.
- 6) DB2 System Level Objects:** A table showing DB2 system level objects with columns for Value, Count, and Graph. Values include DB2001, DB2002, DB2003, DB2004, DB2005, DB2006, DB2007, DB2008, DB2009, DB2010, DB2011, DB2012, DB2013, DB2014, DB2015, DB2016, DB2017, DB2018, DB2019, DB2020, DB2021, DB2022, DB2023, DB2024, DB2025, DB2026, DB2027, DB2028, DB2029, DB2030, DB2031, DB2032, DB2033, DB2034, DB2035, DB2036, DB2037, DB2038, DB2039, DB2040, DB2041, DB2042, DB2043, DB2044, DB2045, DB2046, DB2047, DB2048, DB2049, DB2050, DB2051, DB2052, DB2053, DB2054, DB2055, DB2056, DB2057, DB2058, DB2059, DB2060, DB2061, DB2062, DB2063, DB2064, DB2065, DB2066, DB2067, DB2068, DB2069, DB2070, DB2071, DB2072, DB2073, DB2074, DB2075, DB2076, DB2077, DB2078, DB2079, DB2080, DB2081, DB2082, DB2083, DB2084, DB2085, DB2086, DB2087, DB2088, DB2089, DB2090, DB2091, DB2092, DB2093, DB2094, DB2095, DB2096, DB2097, DB2098, DB2099, DB2100.

© 2015 Correlog, Inc.

Point-and-Click Drill-Down to Detail

The screenshot displays the CORRELOG web interface showing a detailed view of a security message. The message details are as follows:

Time:	Address:	Facility:	Matched Message:
2015/01/14 11:39:43 5 hr, 6 min, 12 sec ago	10.2.8.51 MVSYSVA	security	[error]- Jan 14 14 40:00 MVSYSVA RACF: Cat: RACF - Event: 2.1 - EventDesc: RESOURCE ACCESS: Insufficient Auth - UserID: RU018A - Group: RESTRICT - Auth: Normal check - Reas: (User audited) - RdTime: 2015-01-14 11:39:59.520 - TermNm: DA020833 - JobNm: RU018A - Res: RU018B - CORRELOG: CNTL - Req: READ - Allow: NONE - Vol: LSI504 - Type: DATASET - Prof: RU018B - ** - Owner: RU018B - Name: CHARLES MILLS - POE: DA020833 - POEclass: Terminal - Details
2015/01/14 11:38:14 5 hr, 7 min, 41 sec ago	10.2.8.51 MVSYSVA	security	[error]- Jan 14 14:38:32 MVSYSVA RACF: Cat: RACF - Event: 2.1 - EventDesc: RESOURCE ACCESS: Insufficient Auth - UserID: RU018A - Group: RESTRICT - Auth: Normal check - Reas: (User audited) - RdTime: 2015-01-14 11:38:32.31240 - TermNm: DA020833 - JobNm: RU018A - Res: RU018B - CORRELOG: CNTL - Req: READ - Allow: NONE - Vol: LSI504 - Type: DATASET - Prof: RU018B - ** - Owner: RU018B - Name: CHARLES MILLS - POE: DA020833 - POEclass: Terminal - Details
2015/01/14 11:34:48 5 hr, 11 min, 7 sec ago	10.2.8.51 MVSYSVA	security	[error]- Jan 14 14:35:05 MVSYSVA RACF: Cat: RACF - Event: 2.1 - EventDesc: RESOURCE ACCESS: Insufficient Auth - UserID: RU018A - Group: RESTRICT - Auth: Normal check - Reas: (User audited) - RdTime: 2015-01-14 11:35:04.570 - TermNm: DA020833 - JobNm: RU018A - Res: RU018B - CORRELOG: CNTL - Req: READ - Allow: NONE - Vol: LSI504 - Type: DATASET - Prof: RU018B - ** - Owner: RU018B - Name: CHARLES MILLS - POE: DA020833 - Details
2015/01/14 11:27:10	10.2.8.51	security	[error]- Jan 14 14:27:07 MVSYSVA RACF: Cat: RACF - Event: 2.1 -

CorreLog z/OS Agent + Visualizer

- Compatible with – will “front end” – any enterprise SIEM
- Point-and-click window into z/OS events
 - Security, TSO, started tasks, ABENDs, FTP, DB2
- Real-time: up-to-the-second, timely data
- “Log analysis”
- “Big SIEM” features like correlation, point-and-click, reports, text alerts, etc.

© 2015 CorreLog, Inc.



In conclusion ...

- We have covered
 - The two worlds of IT security
 - Why and How to get real-time event alerts by making your mainframe part of your overall enterprise security posture
 - A brief introduction to SIEMs
- Thank you!



Questions?



© 2015 CorreLog, Inc.



For more information ...

- www.CorreLog.com
- Charles.Mills@CorreLog.com
- SHARE in Seattle March 1 to 6, 2015
 - 16933: z/OS Log Analysis Product Shoot-Out
Tuesday 1:45 PM-2:45 PM
 - “16529: Mainframe Security – Should You Worry? Call the Doctor, Not the Undertaker!”
Thursday, 1:45 PM-2:45 PM
 - SHARE Technology Exchange, Booth 609

© 2015 CorreLog, Inc.



Legal

- Trademarks
 - CorreLog® is a registered trademark, and dbDefender is a 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, Q1®, QRadar®, RACF, System z, Tivoli®, z/OS®, zSecure®, zSeries®
 - ACF2® and Top Secret® are registered trademarks of CA Inc.
 - ArcSight is a trademark of Hewlett-Packard Development Company, L.P.
 - Gartner® is a registered trademark of Gartner, Inc.
 - LogRhythm is a trademark of LogRhythm, Inc.
 - McAfee® is a registered trademark of McAfee, Inc.
 - PCI Security Standards Council is a trademark of The PCI Security Standards Council LLC.
 - Splunk® is a registered trademark of Splunk, Inc.
 - UNIX® is a registered trademark of The Open Group.
 - Vanguard Integrity Professionals is a trademark of Vanguard Integrity Professionals
 - Windows® is a registered trademark of Microsoft Corporation.
 - 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.