



16933: z/OS Log Analysis Product Shoot-Out: CorreLog, Syncsort/Splunk and IBM

CorreLog SIEM Agent for z/OS

Charles Mills
Director of Advanced Projects
CorreLog, Inc.

Agenda

- Software You Already Own + CorreLog SIEM Agent = Improved z/OS and Enterprise Security
- Above + CorreLog Visualizer = Improved Security + “Log Analysis”



What's a SIEM?

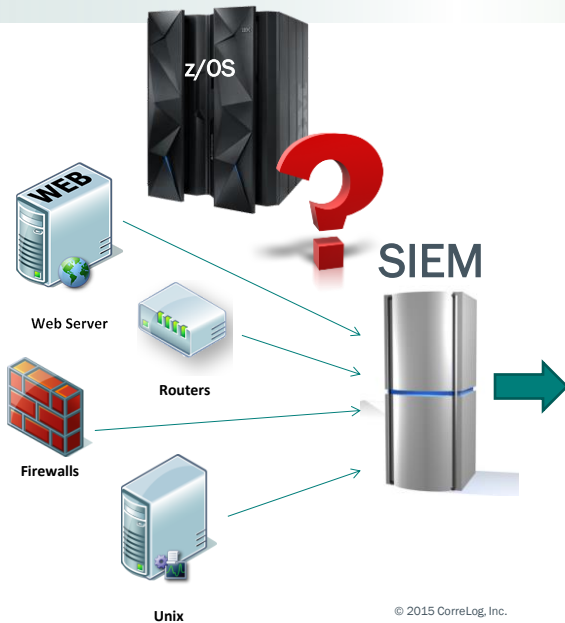
- Security Information and Event Management
- 73 Vendors!
 - HP ArcSight
 - IBM Security QRadar
 - Intel Security (McAfee Nitro) ESM
 - LogRhythm
 - CorreLog Correlation Server
 - Splunk
- SIEM in the Cloud: MSSP (Managed Security Service Provider)
 - Dell SecureWorks
 - NTT Solutionary
 - HP, IBM, Verizon, AT&T, Symantec, ...
- You probably already spent or are spending \$\$\$,\$\$\$ on a SIEM
 - Why? Security and/or Compliance: PCI DSS, HIPAA, GLBA, SOX, IRS Pub. 1075



© 2015 CorreLog, Inc.



What do SIEMs do?



- Sophisticated correlation
- IP Location
- Real-time Text alerts
- Service desk integration
- Query and Search
- Reports
- Compliance
- Forensic archive

© 2015 CorreLog, Inc.



Why Integrate z/OS into your SIEM?

- Compliance: PCI DSS, HIPAA, GLBA, SOX, IRS Pub. 1075
 - Need to include the box with 70% of the data
 - CISOs and Auditors 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

© 2015 CorreLog, Inc.



What z/OS Events?

- 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
- Everything required of DB2 for PCI DSS
- Audited CICS Transactions
- Partner events: NewEra, Vanguard, ...
- Console messages, IMS events, ...
- All real-time – no periodic FTP

© 2015 CorreLog, Inc.



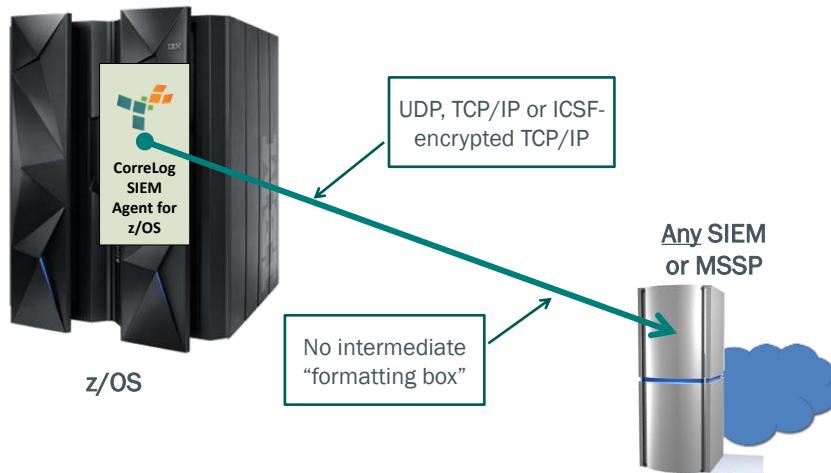
SIEM/MSSP Agnostic

- HP ArcSight CEF Certified
- IBM Security QRadar “Ready for Security Intelligence”
- Intel Security (McAfee Nitro) Partner
- NTT Solutionary Partner
- Dell SecureWorks
- LogRhythm
- Splunk



© 2015 CorreLog, Inc.

The CorreLog SIEM Agent for z/OS



© 2015 CorreLog, Inc.



z/OS RACF Events in ArcSight

Manager	Receipt Time	Name	Device	Device Version	Device Product	Device ID	Device Name	Device Host	Device Attacker Host	Attacker User Name	Attacker User ID
RCACF	15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RCACF	Correlog	Agent for z/OS	1	11/15 00:23:17	invsyab	TCPP0696
RCACF	15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RCACF	Correlog	Agent for z/OS	1	11/15 00:23:17	invsyab	TCPP0696
RCACF	15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RCACF	Correlog	Agent for z/OS	1	11/15 00:23:17	invsyab	TCPP0696
RCACF	15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RCACF	Correlog	Agent for z/OS	1	11/15 00:23:17	invsyab	TCPP0696
RCACF	15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RCACF	Correlog	Agent for z/OS	1	11/15 00:23:17	invsyab	TCPP0696
RCACF	15 Nov 2013 07:18:38 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	6	11/15 00:18:31	invsyab	TCPP0696
RCACF	15 Nov 2013 07:13:18 PST	INIT/LOGON: Undefined User ID	RCACF	Correlog	Agent for z/OS	6	11/15 00:13:13	invsyab	TCPP0696
RCACF	15 Nov 2013 07:13:18 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 00:13:13	invsyab	TCPP0696
RCACF	15 Nov 2013 07:12:38 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 00:12:24	invsyab	TCPP0696
RCACF	15 Nov 2013 07:11:58 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 00:11:51	invsyab	TCPP0696
RCACF	15 Nov 2013 07:10:48 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 00:10:44	invsyab	TCPP0696
RCACF	15 Nov 2013 07:09:58 PST	INIT/LOGON: Password phrase is n...	RCACF	Correlog	Agent for z/OS	6	11/15 00:09:47	invsyab	TCPP0696
RCACF	15 Nov 2013 07:03:28 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 00:03:24	invsyab	TCPP0696
RCACF	15 Nov 2013 07:08:08 PST	INIT/LOGON: Undefined User ID	RCACF	Correlog	Agent for z/OS	6	11/15 00:07:55	invsyab	TCPP0696
RCACF	15 Nov 2013 07:08:08 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 00:07:55	invsyab	TCPP0696
RCACF	15 Nov 2013 07:02:38 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 00:02:32	invsyab	TCPP0696
RCACF	15 Nov 2013 07:02:38 PST	INIT/LOGON: Undefined User ID	RCACF	Correlog	Agent for z/OS	6	11/15 00:02:36	invsyab	TCPP0696
RCACF	15 Nov 2013 07:02:38 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 00:02:36	invsyab	TCPP0696
RCACF	15 Nov 2013 06:57:18 PST	INIT/LOGON: Undefined User ID	RCACF	Correlog	Agent for z/OS	6	11/15 0 57:17	invsyab	TCPP0696
RCACF	15 Nov 2013 06:52:00 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	6	11/15 0 51:58	invsyab	TCPP0696
RCACF	15 Nov 2013 06:52:00 PST	INIT/LOGON: Successful Racinit De...	RCACF	Correlog	Agent for z/OS	1	11/15 0 51:58	invsyab	TCPP0696

© 2015 CorreLog, Inc.



z/OS RACF Events in Splunk

Time	Event
12/13/13 5:18:00 PM	<35>Dec 13 17:18:00 mvssysy RACF eventdesc="INIT/LOGON: Invalid Password" severity=Error userId=CUSFTM group=LSCOWS auth=None reas="VERIFY failure" term=TCPP0693 name="FRED WRIGHT" poe=TCPP0693 host = mvssysy source = tcp:1468 sourcetype = syslog term= TCPP0693
12/13/13 5:05:10 PM	<38>Dec 13 17:05:10 mvssysy RACF eventdesc="INIT/LOGON: Successful Racinit Init" severity=Informational userId=DV231B group=TS0HOLD auth=None reas=None term=NV231B jobn=NVPTTC24 name="DAVID BROOKS" poe=DV231B host = mvssysy source = tcp:1468 sourcetype = syslog term= DV231B
12/13/13 4:20:53 PM	<38>Dec 13 16:20:53 mvssysy RACF eventdesc="INIT/LOGON: Successful Racinit Delete" severity=Informational userId=DWGD group=TS0HOLD auth=None reas=None term=NVPTD002 jobn=NVPTMB name="BILL DICKEY" poe=NVPTD002 host = mvssysy source = tcp:1468 sourcetype = syslog term= NVPTD002
12/13/13 4:20:53 PM	<38>Dec 13 16:20:53 mvssysy RACF eventdesc="INIT/LOGON: Successful Racinit Init" severity=Informational userId=DWGD group=TS0HOLD auth=None reas=None term=NVPTD002 jobn=NVPTMB name="BILL DICKEY" poe=NVPTD002 host = mvssysy source = tcp:1468 sourcetype = syslog term= NVPTD002
12/13/13 4:19:41 PM	<38>Dec 13 16:19:41 mvssysy RACF eventdesc="INIT/LOGON: Successful Racinit Delete" severity=Informational userId=DWGD group=TS0HOLD auth=None reas=None term=NVPTD002 jobn=NVPTMB name="BILL DICKEY" poe=NVPTD002

System Programming

- DASD Requirements: 150 tracks
 - Load, parm and sample libraries – that's it
- Maintenance requirements: none
- Single started task – easy to automate
- No “hooks” – all supported interfaces
- Stability: last disruptive problem at a customer was July, 2012
- CPU: on a z196 about $\frac{1}{10000}$ of a CPU second per event forwarded
 - Proportionally less on a faster box
 - “Which events” easy to configure
- Installation
 - SMP/E or non-SMP/E
 - No IPL
 - Ships pre-configured

© 2015 CorreLog, Inc.



Installation a “No-Brainer”

You forwarded this message on 7/9/2014 9:03 AM.

From: Steve M [mailto:steve.m@correlog.com]
 To: 'Charles Mile'
 Cc:
 Subject: CorreLog Agent Feedback

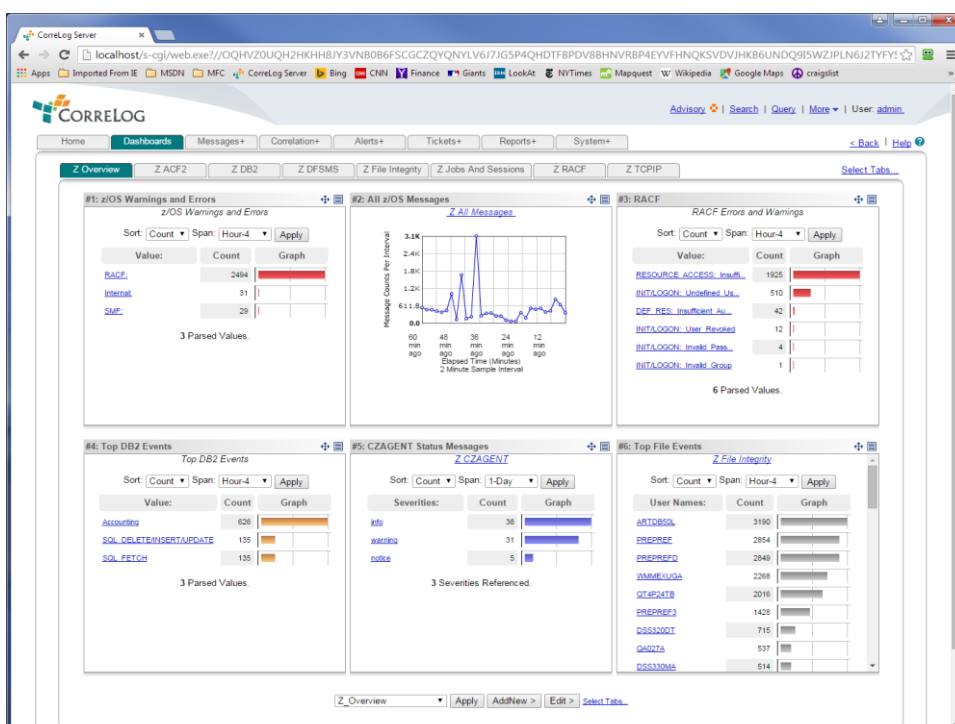
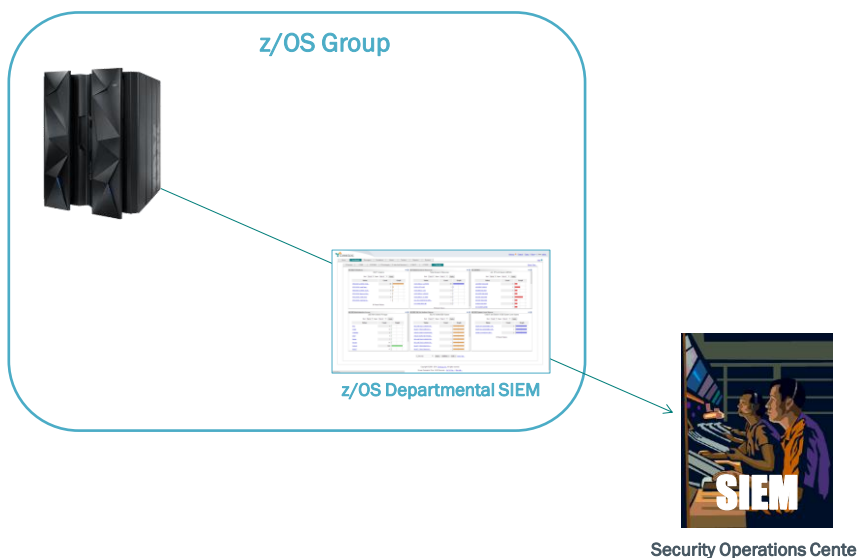
```
//STEPLIB DD DSN=SP3MVS1.CZAGENT.LOAD,DISP=SHR
//CZAPARMS DD DSN=SP3MVS1.CZAGENT.CNTL,DISP=SHR
//CZADIAG DD SYSOUT=*
//CZAPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//CEEOPTS DD *
ENVAR ('TZ=CST6CDT')
// PEND
```

So far, I have to say that the installation was a no-brainer. It took me less than an hour, and came up the 1st time. We tweaked SMF settings later, but it was easy.

That's all I have so far, Vinay will have more feedback from a user perspective.

Thanks,

CorreLog Visualizer for z/OS



CorreLog Server

localhost/s-cgi/web.exe?/QPNVGQ4R2RKNH9J5EFNL0L6PSMGMZ1Y1N5LF677GSPGQBYN7URXR5HCWP6AFCBVLGL5ZFC5M80BRWPT7WGS5CVZJR9MNNWX

Home Dashboards Messages+ Correlation+ Alerts+ Tickets+ Reports+ System+ < Back Help

Dashboard/ INIT/LOGON: Invalid Group Messages

List: Max-50 Match: Apply

Time:	Address:	Facility:	Matched Message:
2015/02/11 12:37:23 2 min, 0 sec ago	10.2.8.51 MVSSYSA	security	(error): Feb 11 15: 37: 49 MVSSYSA RACF: Cat: RACF - Event: 1 - 2 - EventDesc: INIT/LOGON: Invalid Group - UserID: RU018A - Group: FOOTBAR - Auth: None - Reason: VERIFY (failure) - TermNm: TCPB2933 - Name: CHARLES MILLS - POE: TCPB2933 - POEClass: Terminal Details

Total: 1 matched messages displayed

Copyright © 2008 - 2015, CorreLog, Inc. All rights reserved.
Screen Generation Time: 0.963 Seconds - [Go To Top](#) | [Site Info](#)
CorreLog Inc. - For Internal Use Only - Expires: 2016/01/15

Real-Time Text Alerts

CorreLog Server

localhost/s-cgi/web.exe?/RH8RY2D7QXQ/INV9Q5DGKJGKGNKPKXX

Counters Devices Patterns Custom Config+

< Cancel Reset Delete > SaveNew > Save >

System Counter Name:
Thread/ Z FTP RACF Errors

Pin This Alert To Top:
User Preference Yes

Compare Function:
(GE) Greater Than Or Equal

Threshold:
1 Counts Per Interval

Test Interval:
20 Seconds

Match Alert Time:
Time When Alert is Enabled: Midnight + 24 hrs

When Threshold is Triggered:

Send Alert Message:
Max 255 chars
Unauthorized FTP transfer attempted by \$T_RELATED_DEVNAME - \$T_RELATED_DE by \$T_RELATED_USERNAME

Insert Alert Variable:
None

153 characters available.

charlesm@mcn.org

(CorreLog Ticket) ASSIGNEE: admin - MESSAGE: notice Unauthorized FTP transfer attempted on MVSSYSA - Production V2R1 - by Ru018b

CorreLog, Inc.
<http://www.cq>
1 min via SMS

Send SMS
from my carrier number

In conclusion

- SIEM You Already Own + CorreLog SIEM Agent = Improved z/OS and Enterprise Security
- Your SIEM + CorreLog SIEM Agent + CorreLog Visualizer = Improved Security + “Log Analysis”
- Differentiators
 - Easy to install and maintain
 - SIEM/MSSP agnostic; certified with top SIEMs
 - Mature, stable product; installed around the world
 - Exclusive z/OS Visualizer – no charge by data volume, unlike competitors
 - Economical. Lightweight; designed to complement the SIEM you already own; no use of mainframe resources for what your SIEM already does
- CorreLog also publishes a z/OS DB2 Agent for McAfee DAM

© 2015 CorreLog, Inc.



For more information

- www.correlog.com
- charles.mills@correlog.com
- “16529: Mainframe Security – Should You Worry? Call the Doctor, Not the Undertaker!”
Thursday, March 5, 2015: 1:45 PM-2:45 PM
Issaquah A
- SHARE Technology Exchange booth 609

© 2015 CorreLog, Inc.



Thank you



© 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.

© 2015 CorreLog, Inc.

