CORRELOG

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”

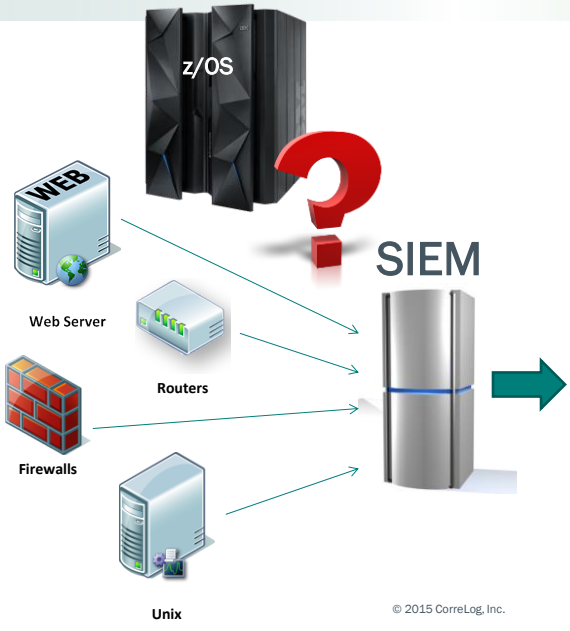
CORRELOG

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

CORRELOG

What do SIEMs do?



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

CORRELOG

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

CORRELOG

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

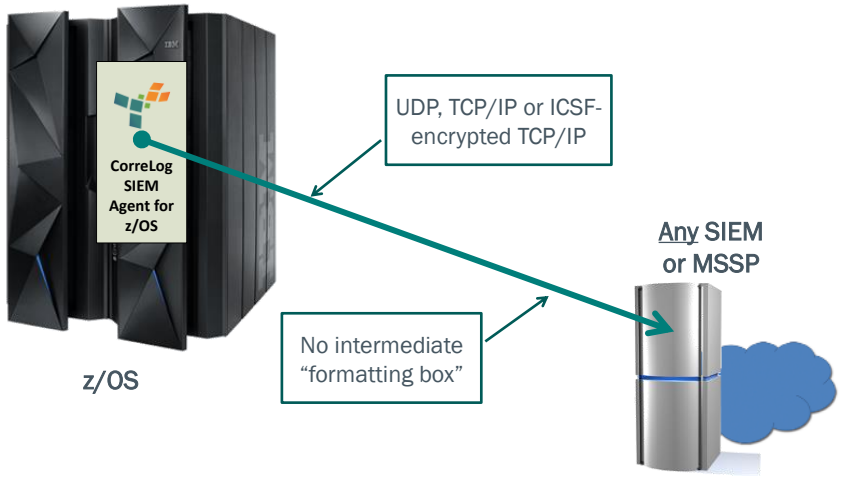
CORRELOG

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

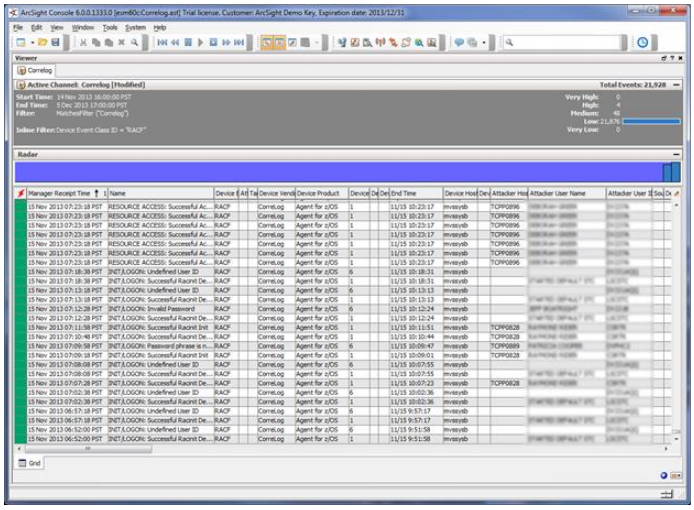
CORRELOG

The CorreLog SIEM Agent for z/OS



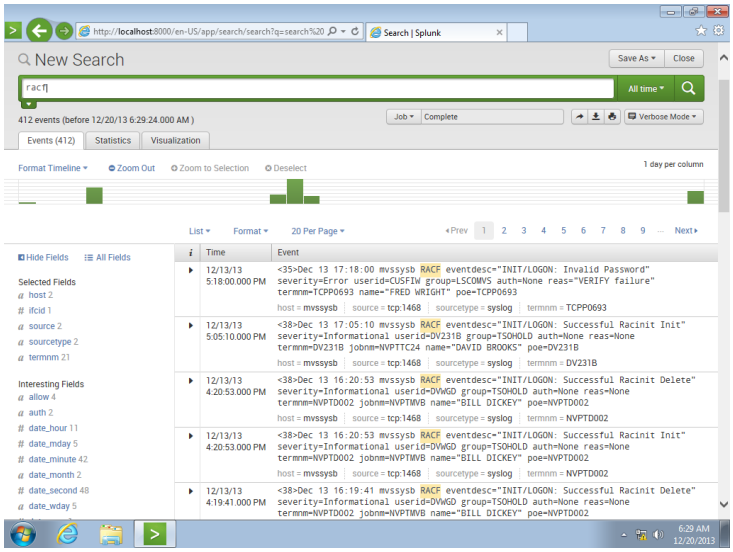
CORRELOG

z/OS RACF Events in ArcSight



CORRELOG

z/OS RACF Events in Splunk

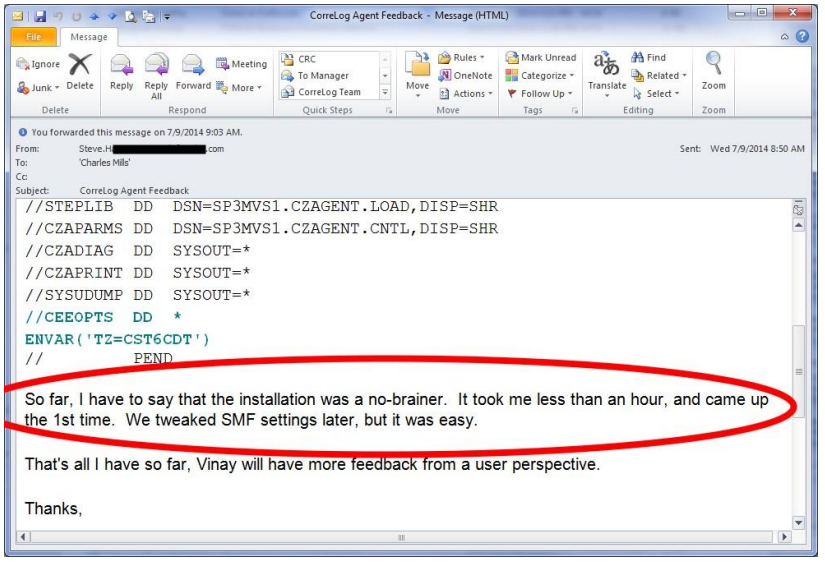


System Programming

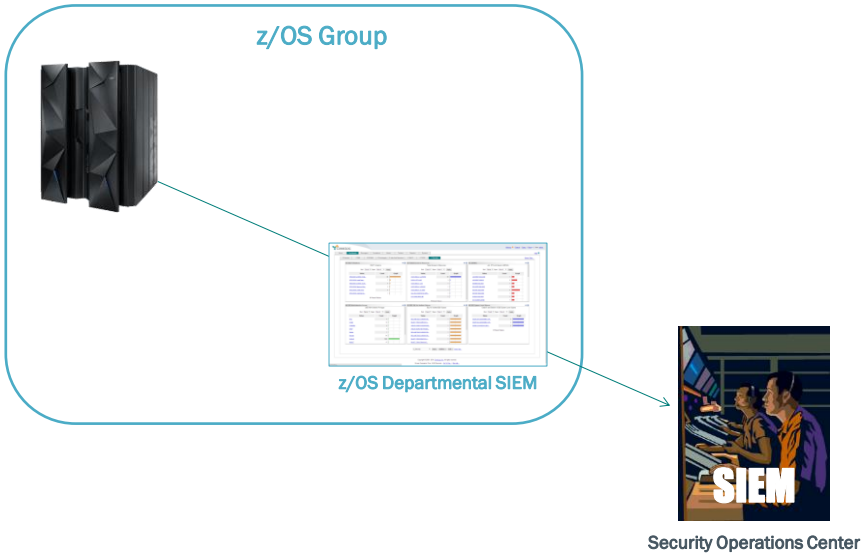
- DASD Requirements: 150 tracks
  - Load, parm and sample libraries – that's it
- Maintenance requirements: none
- Single started task – easy to automate
- No "hooks" – all supported interfaces
- Stability: last disruptive problem at a customer was July, 2012
- CPU: on a z196 about $\frac{1}{10000}$ 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

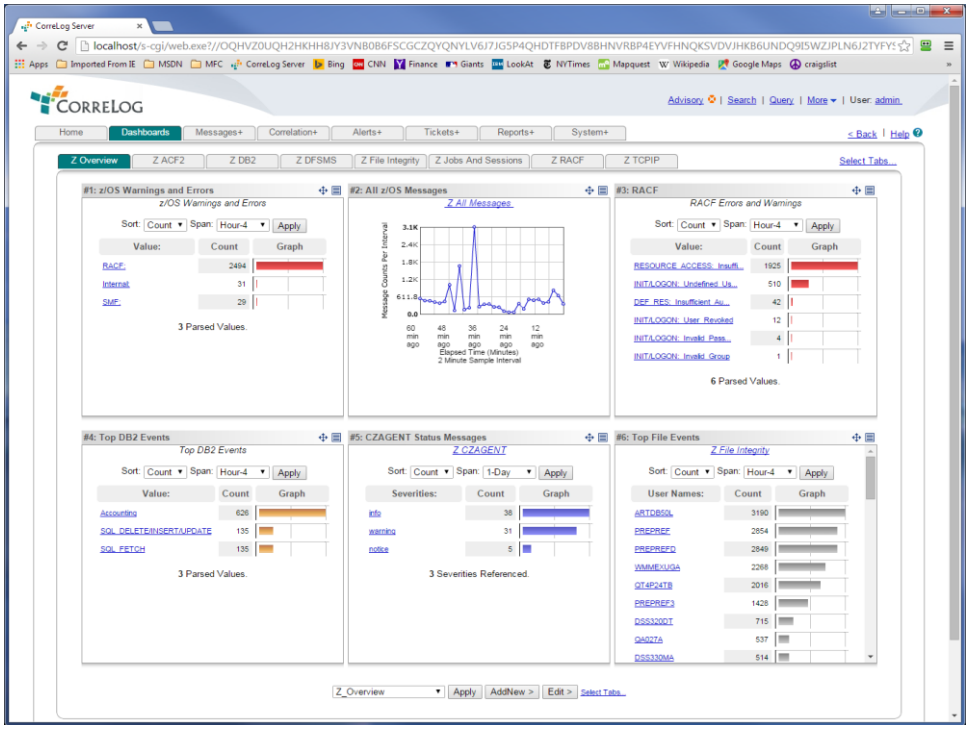
CORRELOG

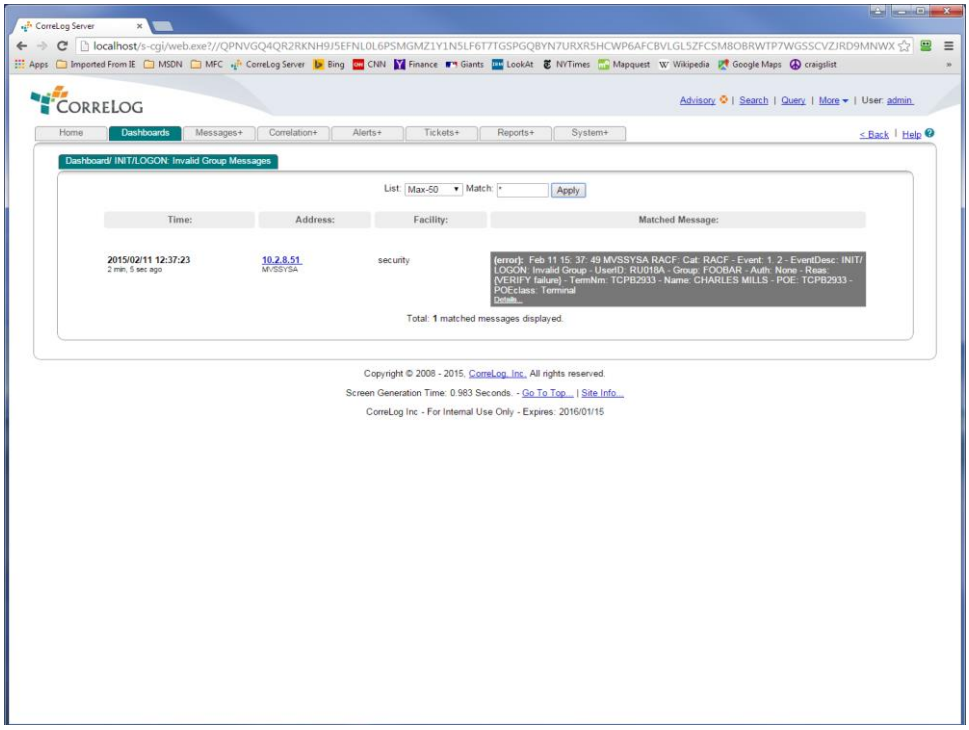
Installation a "No-Brainer"



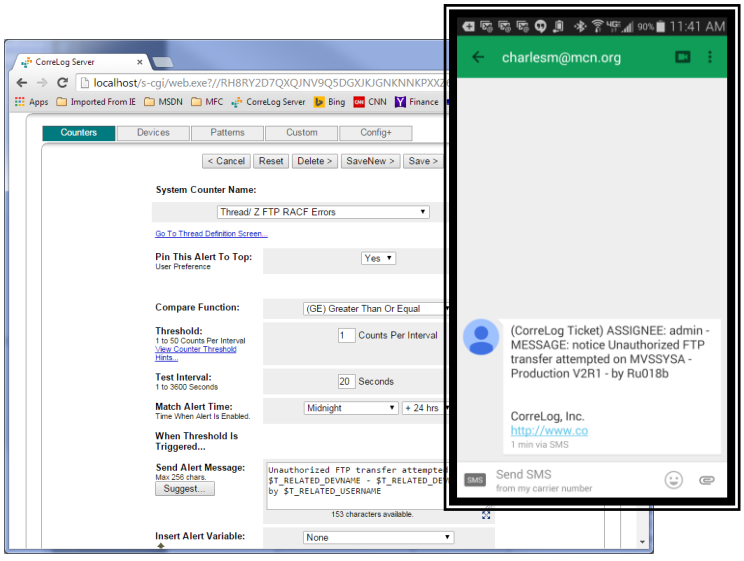
CorreLog Visualizer for z/OS







Real-Time Text Alerts



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

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

Thank you

CORRELOG

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.

CORRELOG