17442: 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

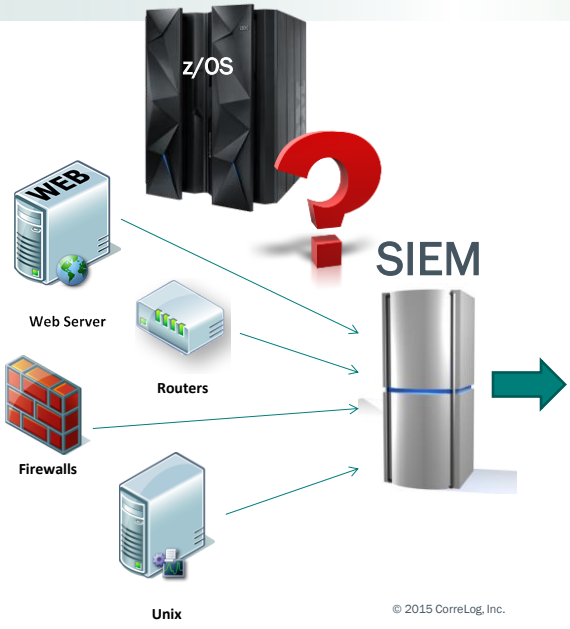
- SIEM You Already Own + CorreLog SIEM Agent = Improved z/OS and Enterprise Security
- Above + CorreLog Visualizer = Improved Security + “Log Analysis”

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

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 or 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 Transfers
- Everything needed from DB2 for PCI DSS
- Audited CICS Transactions
- Partner events: NewEra, Vanguard, …
- Console messages, IMS, …
- All real-time – no periodic FTP

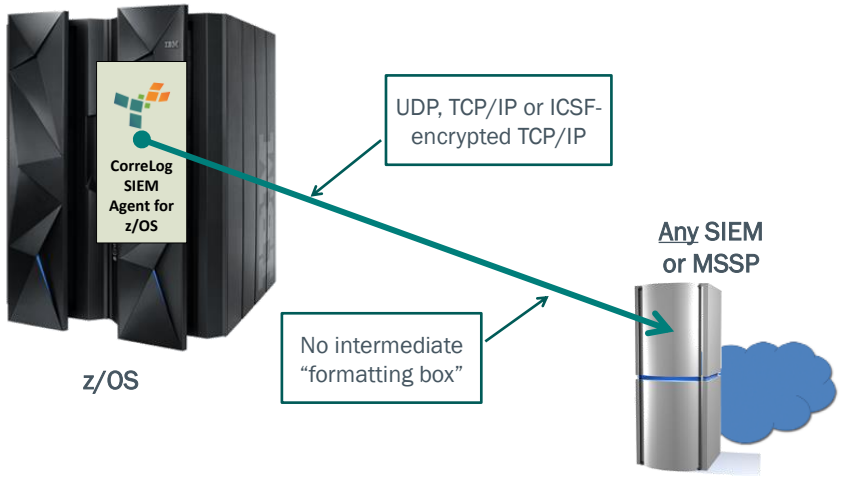
CORRELOG

SIEM/MSSP Agnostic

- HP ArcSight CEF Certified
- IBM Security QRadar "Ready for Security Intelligence"
- Intel Security (McAfee Nitro) Partner
- RSA (EMC) Security Analytics (enVision) Certified
- NTT Solutionary Partner
- Dell SecureWorks
- LogRhythm
- Splunk

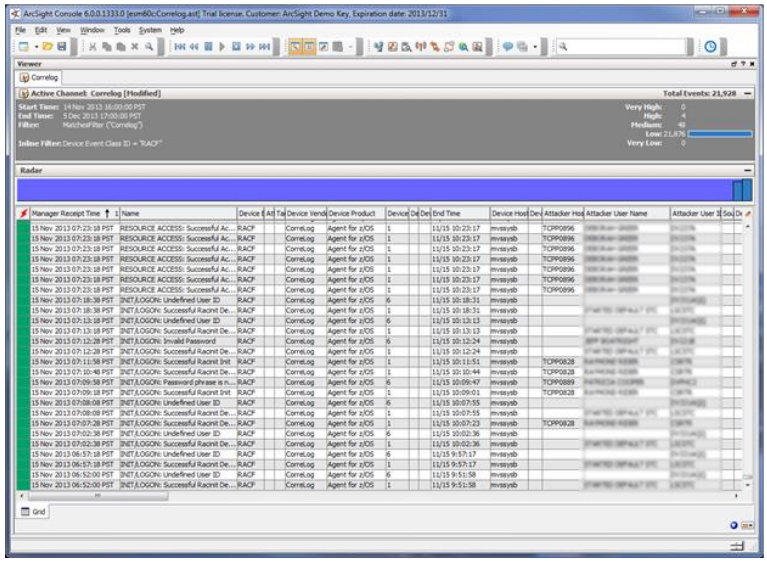
CORRELOG

The CorreLog SIEM Agent for z/OS

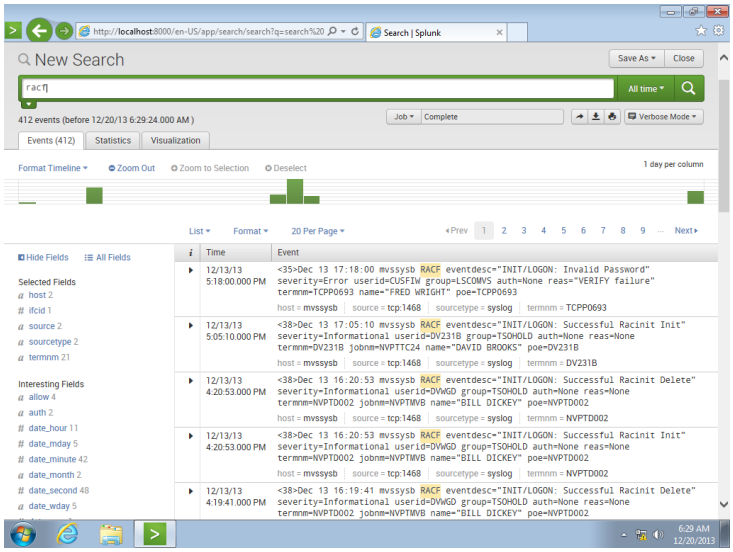


CORRELOG

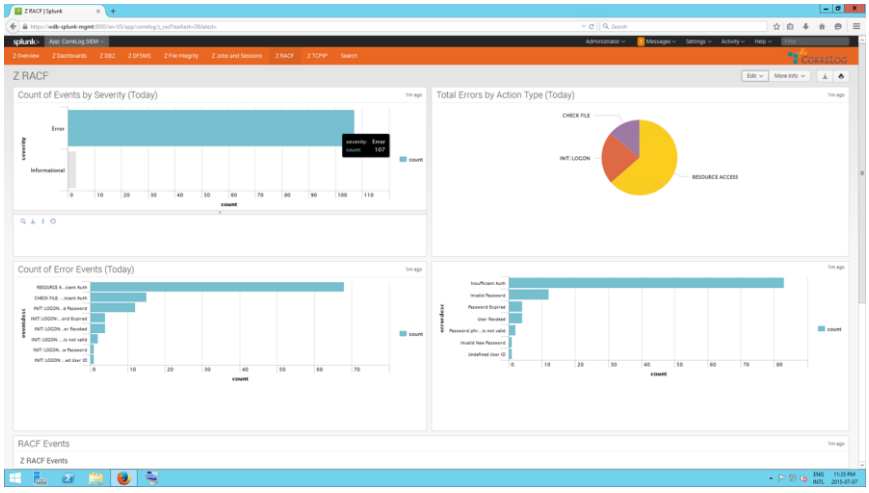
RACF Events in ArcSight



RACF Events in Splunk Search



RACF Events in Splunk Dashboard



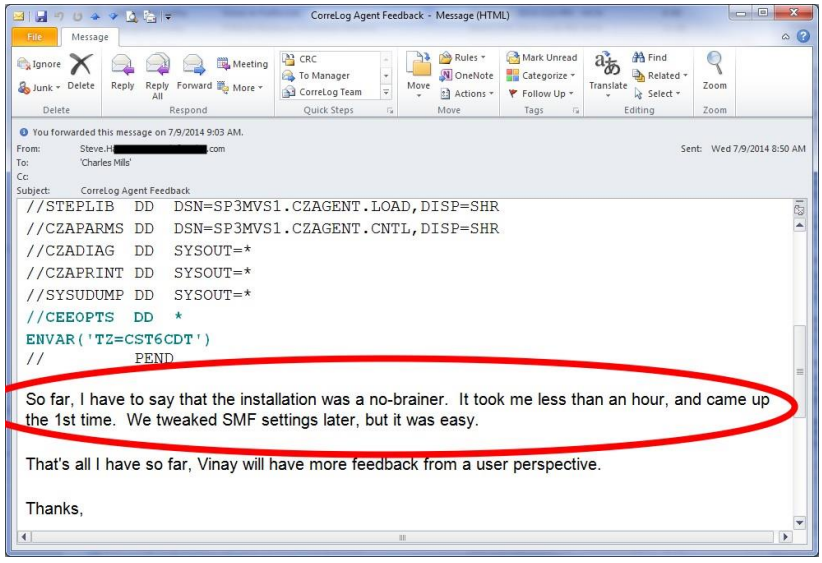
CORRELOG

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 Agent Feedback - Message (HTML)

File | Message

Ignore | Junk | Delete | Reply | Reply All | Forward | Meeting | More | CRC | To Manager | CorreLog Team | Move | Rules | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

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

From: Steve.H[redacted].com
To: 'Charles Mills'
Cc:
Subject: CorreLog Agent Feedback
Sent: Wed 7/9/2014 8:50 AM

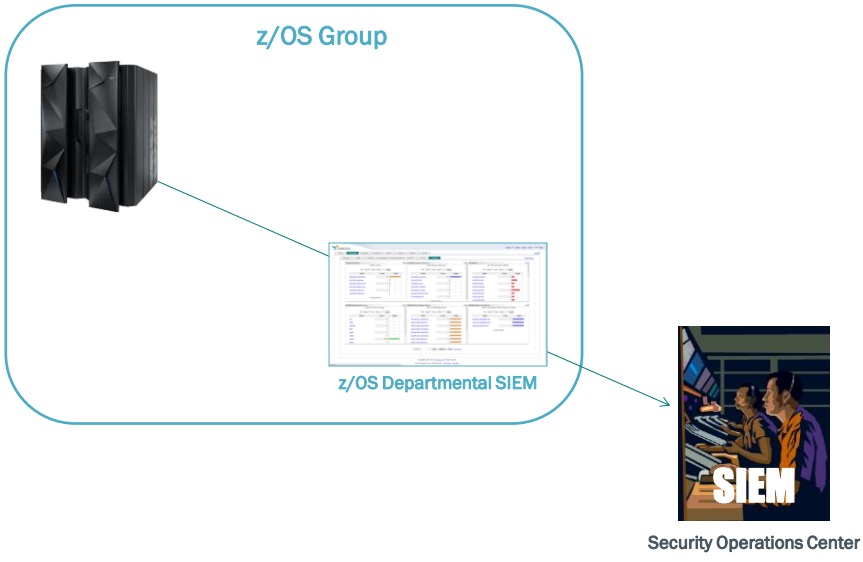
```
//STEPLIB  DD  DSN=SP3MVS1.CZAGENT.LOAD,DISP=SHR
//CZAPARMS DD  DSN=SP3MVS1.CZAGENT.CNTL,DISP=SHR
//CZADIAG  DD  SYSOUT=*
//CZAPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//CEEOPTS  DD  *
ENVAR('TZ=CST6CDT')
//          PEND
```

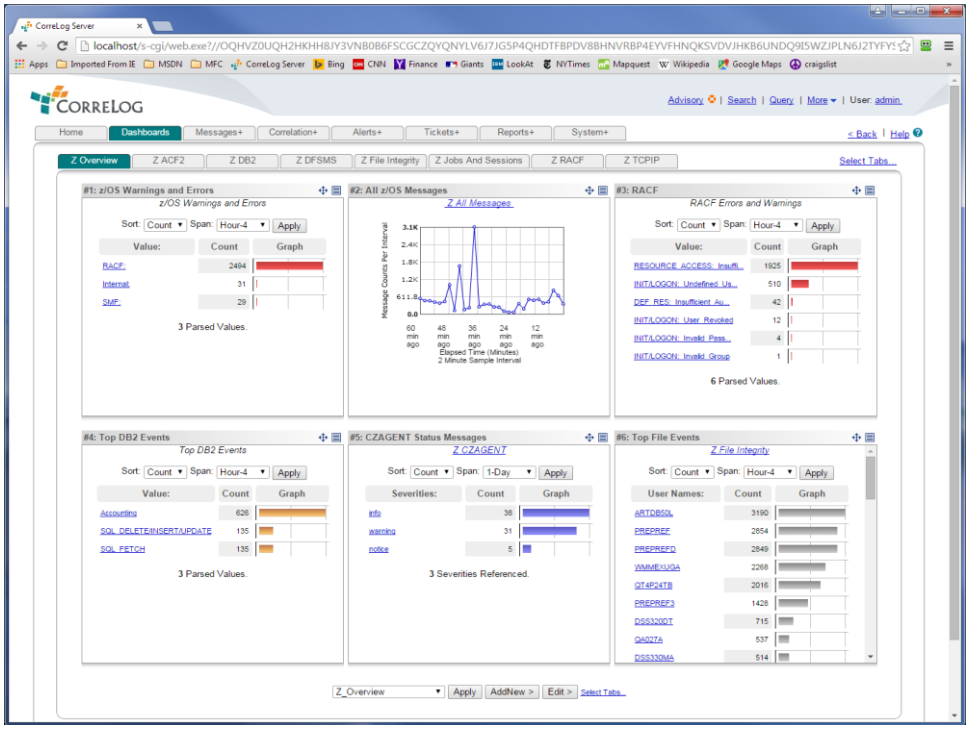
So far, I have to say that the installation was a no-brainer. It took me less than an hour, and came up the 1st time. We tweaked SMF settings later, but it was easy.

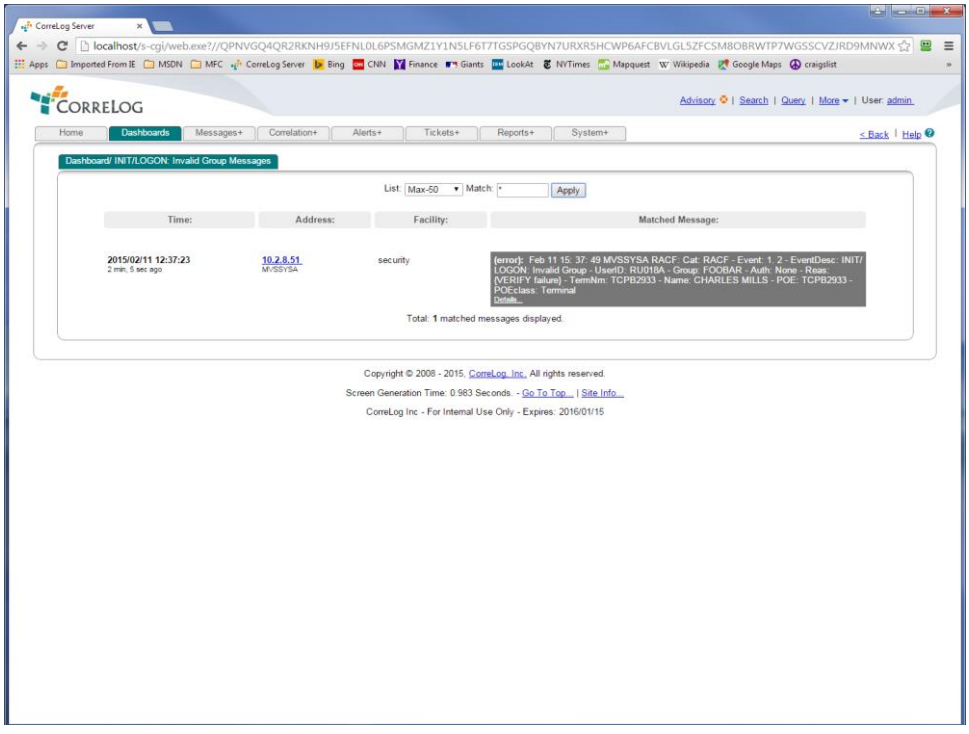
That's all I have so far, Vinay will have more feedback from a user perspective.

Thanks,

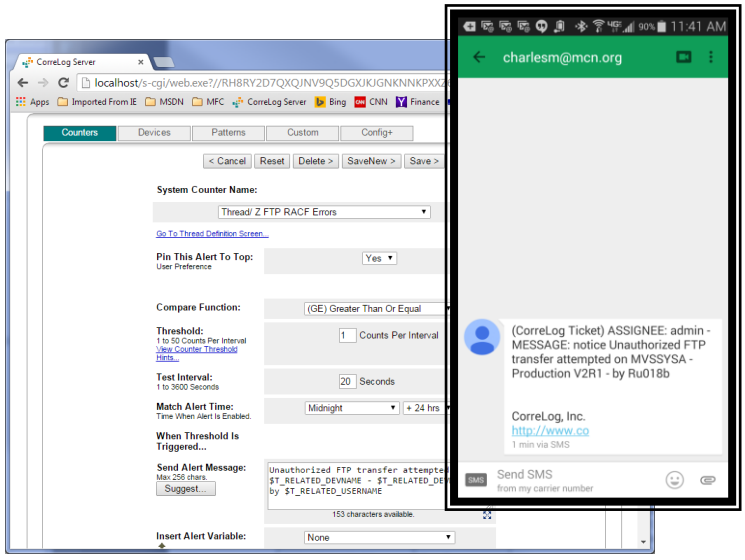
CorreLog Visualizer for z/OS




CorreLog Server
localhost/s-cgi/web.exe?//OQHVZ0UQH2HKHH8JY3VNB0B6FSCGCZQYQNYLV6J7JG5P4QHDTFBPDV8BHNVRBP4EYVFHNQKSVDVJHKB6UNDQ9I5WZJPLN6J2TYFY5
CORRELOG
Advisory | Search | Query | More | User: admin
Home
Dashboards
Messages+
Correlation+
Alerts+
Tickets+
Reports+
System+
< Back | Help
Z Overview
Z ACF2
Z DB2
Z DFSMS
Z File Integrity
Z Jobs And Sessions
Z RACF
Z TCPIP
Select Tabs...
#1: z/OS Warnings and Errors
z/OS Warnings and Errors
Sort: Count Span: Hour-4 Apply
Value: Count Graph
RACF 2494
Internal 31
SMF 29
3 Parsed Values.
#2: All z/OS Messages
Z All Messages
Message Counts Per Interval
Elapsed Time (Minutes)
2 Minute Sample Interval
#3: RACF
RACF Errors and Warnings
Sort: Count Span: Hour-4 Apply
Value: Count Graph
RESOURCE ACCESS: Insufficient Access Authority 1925
INIT/LOGON: Undefined User 510
DEF RES: Insufficient Authority 42
INIT/LOGON: User Revoked 12
INIT/LOGON: Invalid Password 4
INIT/LOGON: Invalid Group 1
6 Parsed Values.
#4: Top DB2 Events
Top DB2 Events
Sort: Count Span: Hour-4 Apply
Value: Count Graph
Accounting 626
SQL DELETE/INSERT/UPDATE 135
SQL FETCH 135
3 Parsed Values.
#5: CZAGENT Status Messages
Z CZAGENT
Sort: Count Span: 1-Day Apply
Severities: Count Graph
info 38
warning 31
notice 5
3 Severities Referenced.
#6: Top File Events
Z File Integrity
Sort: Count Span: Hour-4 Apply
User Names: Count Graph
ARTDB50L 3190
PREPREF 2654
PREPREFD 2849
WMMEXUGA 2268
QT4P24TB 2016
PREPREF3 1428
DSS320DT 715
QA027A 537
DSS320MA 514
Z_Overview Apply AddNew > Edit > Select Tabs...


CorreLog Server
localhost/s-cgi/web.exe?//QPNVGQ4QR2RKNH9J5EFNL0L6PSMGMZ1Y1N5LF6T7TGSPGQ8YN7URXR5HCWP6AFCBVLGL5ZFCSM8OBRWTP7WGSSCVZJRD9MNWX
CORRELOG
Advisory | Search | Query | More | User: admin
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, 5 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: FOOBAR - Auth: None - Reas: (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: 0.983 Seconds. - Go To Top... | Site Info...
CorreLog Inc - For Internal Use Only - Expires: 2016/01/15

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: leverages the SIEM you already own
  - 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

CORRELOG

For more information

- www.correlog.com
- charles.mills@correlog.com
- SHARE Technology Exchange booth 411 (Back wall – left aisle)
- 17369: Bridge the Gap: How to Use an Enterprise Product You Already Own to Enhance z/OS Security – Monday – Download the handouts

CORRELOG

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.