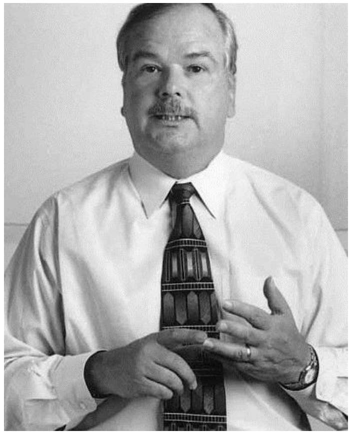
CorreLog

NY/TB RUG: The Mainframe isn't Dead: Call the Doctor not the Undertaker with Real-time Enterprise Alert Correlation

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

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 system technology and developers.



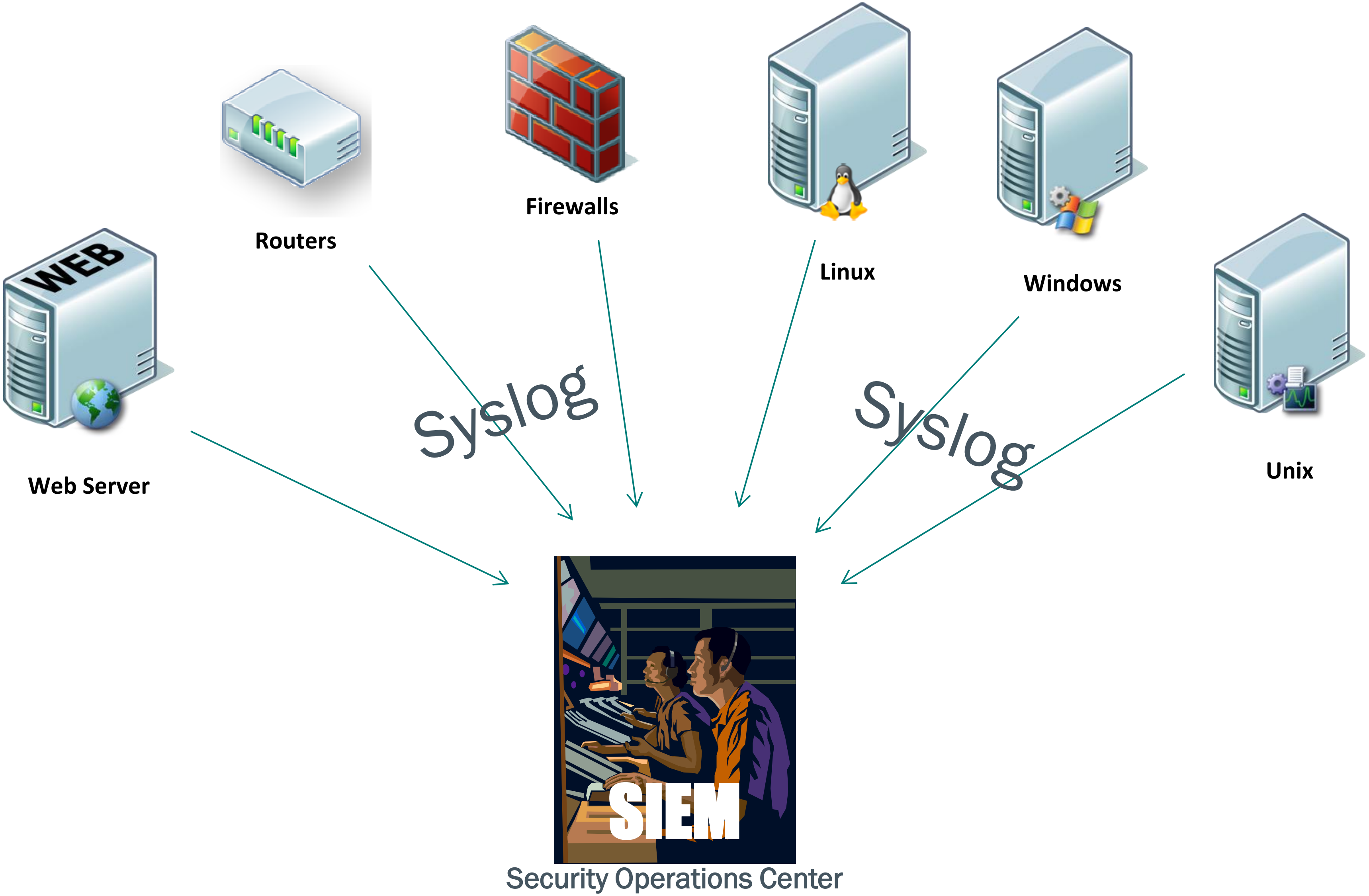
Agenda

- 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
- Brief Introduction to SIEM Systems
- Reference Material

Preface: Two Worlds of IT Security

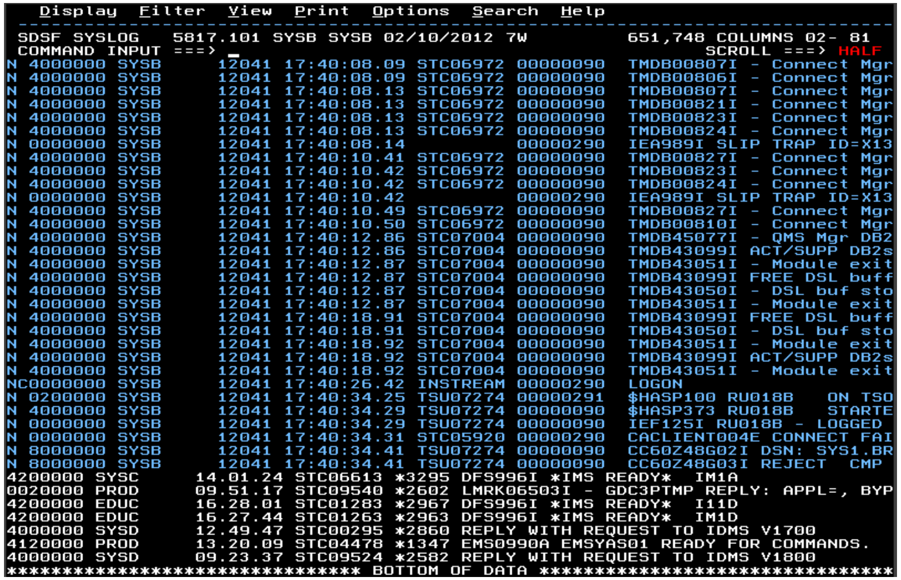
Security in the Mainframe World

Security in the Network World



The Two Meanings of “Syslog”

- z/OS SYSLOG: “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*



```
 SDSF SYSLOG   5817.101 SYSB SYSB 02/10/2012 7W         651,748 COLUMNS 02- 81
 COMMAND INPUT ===> _                                          SCROLL ===> HALF
N 4000000 SYSB     12041 17:40:08.09 STC06972 00000090  TMDB00807I - Connect Mgr
N 4000000 SYSB     12041 17:40:08.09 STC06972 00000090  TMDB00806I - Connect Mgr
N 4000000 SYSB     12041 17:40:08.13 STC06972 00000090  TMDB00807I - Connect Mgr
N 4000000 SYSB     12041 17:40:08.13 STC06972 00000090  TMDB00821I - Connect Mgr
N 4000000 SYSB     12041 17:40:08.13 STC06972 00000090  TMDB00823I - Connect Mgr
N 4000000 SYSB     12041 17:40:08.13 STC06972 00000090  TMDB00824I - Connect Mgr
N 0000000 SYSB     12041 17:40:08.14          00000290  IEA989I SLIP TRAP ID=X13
N 4000000 SYSB     12041 17:40:10.41 STC06972 00000090  TMDB00827I - Connect Mgr
N 4000000 SYSB     12041 17:40:10.42 STC06972 00000090  TMDB00823I - Connect Mgr
N 4000000 SYSB     12041 17:40:10.42 STC06972 00000090  TMDB00824I - Connect Mgr
N 0000000 SYSB     12041 17:40:10.42          00000290  IEA989I SLIP TRAP ID=X13
N 4000000 SYSB     12041 17:40:10.49 STC06972 00000090  TMDB00827I - Connect Mgr
N 4000000 SYSB     12041 17:40:10.50 STC06972 00000090  TMDB00810I - Connect Mgr
N 4000000 SYSB     12041 17:40:12.86 STC07004 00000090  TMDB45077I - QMS Mgr DB2
N 4000000 SYSB     12041 17:40:12.86 STC07004 00000090  TMDB43099I ACT/SUPP DB2s
N 4000000 SYSB     12041 17:40:12.87 STC07004 00000090  TMDB43051I - Module exit
N 4000000 SYSB     12041 17:40:12.87 STC07004 00000090  TMDB43099I FREE DSL buff
N 4000000 SYSB     12041 17:40:12.87 STC07004 00000090  TMDB43050I - DSL buf sto
N 4000000 SYSB     12041 17:40:12.87 STC07004 00000090  TMDB43051I - Module exit
N 4000000 SYSB     12041 17:40:18.91 STC07004 00000090  TMDB43099I FREE DSL buff
N 4000000 SYSB     12041 17:40:18.91 STC07004 00000090  TMDB43050I - DSL buf sto
N 4000000 SYSB     12041 17:40:18.92 STC07004 00000090  TMDB43051I - Module exit
N 4000000 SYSB     12041 17:40:18.92 STC07004 00000090  TMDB43099I ACT/SUPP DB2s
N 4000000 SYSB     12041 17:40:18.92 STC07004 00000090  TMDB43051I - Module exit
NC0000000 SYSB     12041 17:40:26.42 INSTREAM 00000290  LOGON
N 0200000 SYSB     12041 17:40:34.25 TSU07274 00000291  $HASP100 RU018B   ON TSO
N 4000000 SYSB     12041 17:40:34.29 TSU07274 00000090  $HASP373 RU018B   STARTE
N 0000000 SYSB     12041 17:40:34.29 TSU07274 00000090  IEF125I RU018B - LOGGED
N 0000000 SYSB     12041 17:40:34.31 STC05920 00000290  CACLIENT004E CONNECT FAI
N 8000000 SYSB     12041 17:40:34.41 TSU07274 00000090  CC60Z48G02I DSN: SYS1.BR
N 8000000 SYSB     12041 17:40:34.41 TSU07274 00000090  CC60Z48G03I REJECT  CMP
4200000 SYSC     14.01.24 STC06613 *3295 DFS996I *IMS READY*  IM1A
0020000 PROD     09.51.17 STC09540 *2602 LMRK06503I - GDC3PTMP REPLY: APPL=, BYP
4200000 EDUC     16.28.01 STC01283 *2967 DFS996I *IMS READY*  I11D
4200000 EDUC     16.27.44 STC01263 *2963 DFS996I *IMS READY*  IM1D
4000000 SYSD     12.49.47 STC00295 *2860 REPLY WITH REQUEST TO IDMS V1700
4120000 PROD     13.20.09 STC04478 *1347 EMS0990A EMSYAS01 READY FOR COMMANDS.
4000000 SYSD     09.23.37 STC09524 *2582 REPLY WITH REQUEST TO IDMS V1800
******************************** BOTTOM OF DATA ********************************
```

- That is not what the rest of the *IT industry* means by “Syslog”

“Syslog” – The Network Security Meaning

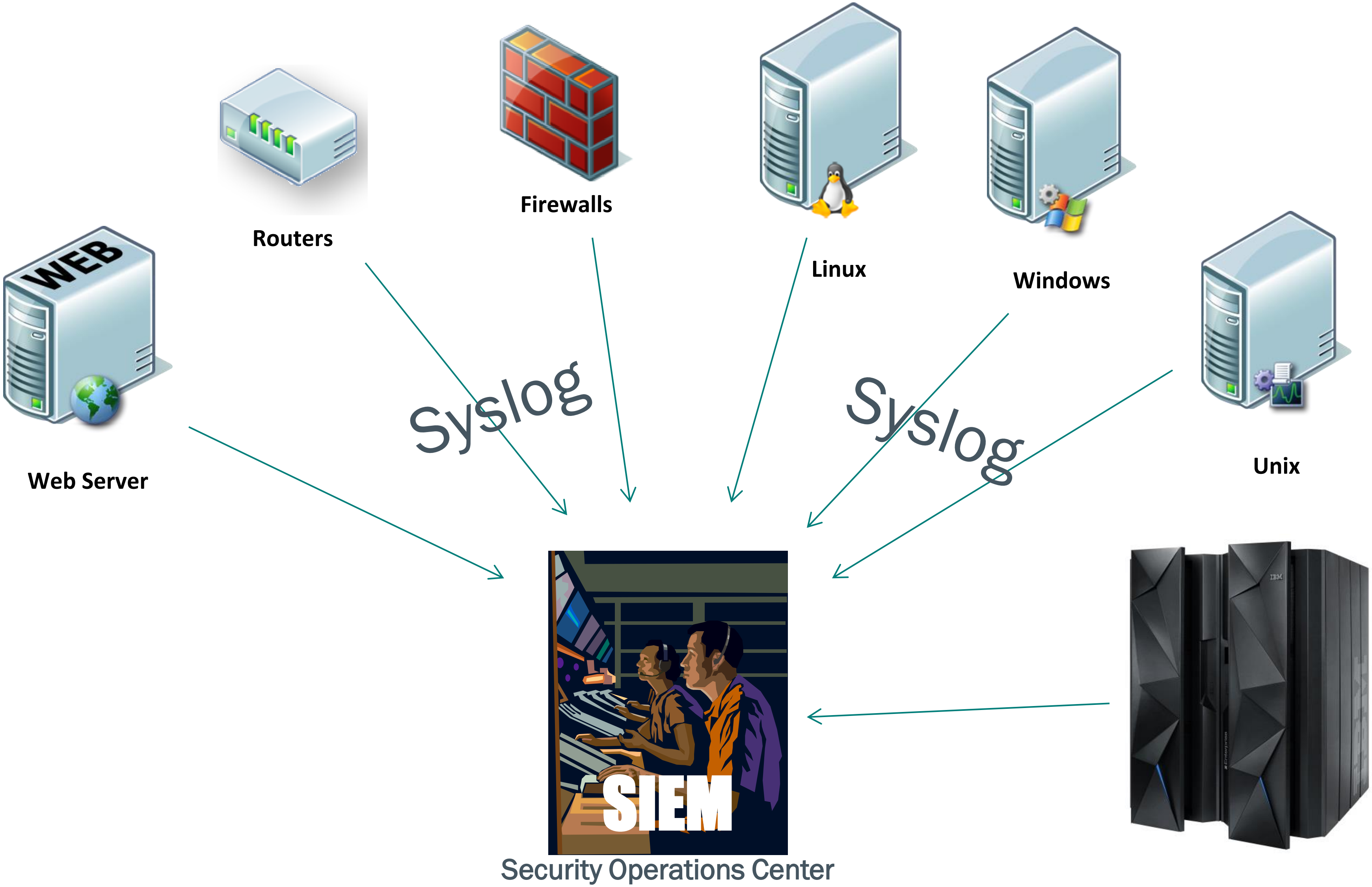
- “The BSD syslog Protocol”
  - IETF RFC 3164 and follow-ons RFC 5424, 5425, 5426 and 6587
  - Almost free-format text (ASCII) messages
  - **`<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8`**
  - Transmitted via UDP or TCP/IP with optional SSL/TLS encryption
  - Generated by most routers, firewalls, UNIX systems, etc.
    - No native Syslog capability: Windows and z/OS

What’s a SIEM?

- SIEM: Security Information and Event Management
  - SIEM aggregates event data produced by devices, systems and applications.
- Consists of
  - SIM — log management, analytics and compliance reporting
  - SEM — real-time monitoring and incident management for security-related events
- SIEM typically deployed to support three primary use cases:
  - Threat management — monitoring and reporting of user activity, data access and application activity
  - Compliance — log management and compliance reporting
  - A deployment that provides a mix of threat management and compliance capabilities
- Key SIEM functions
  - Collecting Syslog messages
  - Correlation
  - Alerting and reporting
  - Cost effective, tamper-proof storage

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

Mainframe in the Network Security World



Routers

Firewalls

Linux

Windows

Web Server

Unix

Syslog

Syslog

SIEM

Security Operations Center

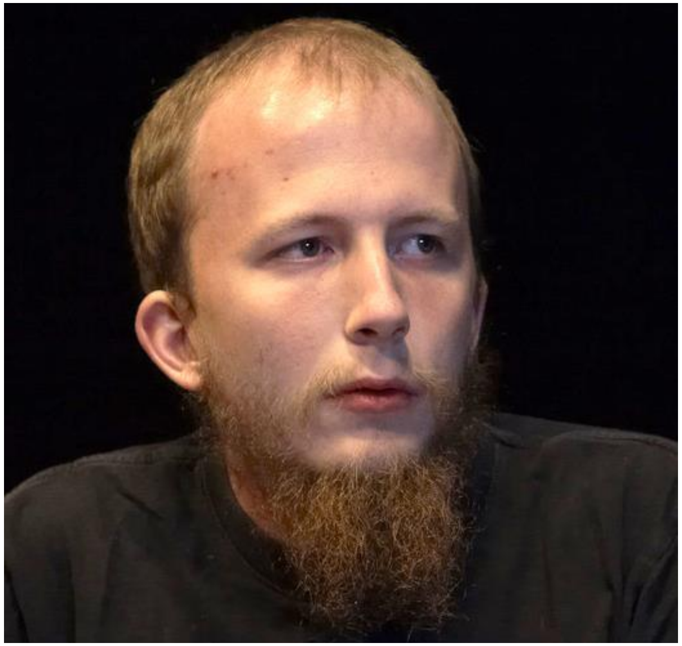
Aren’t Mainframes Inherently Secure?

- “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!

- Logica, service bureau in Sweden, March to September 2012
- Data including bank data, government agencies, credit cards – multiple LPARs
- Access via FTP and TN3270, possibly initially using accounts stolen from breached Web server
- Installed backdoor to allow easy ongoing access
- Downloaded RACF databases, used PC hacker password cracking tool* to decrypt 30,000 passwords
- Gottfrid Svartholm Warg, co-founder of The Pirate Bay, and an accomplice convicted June 2013

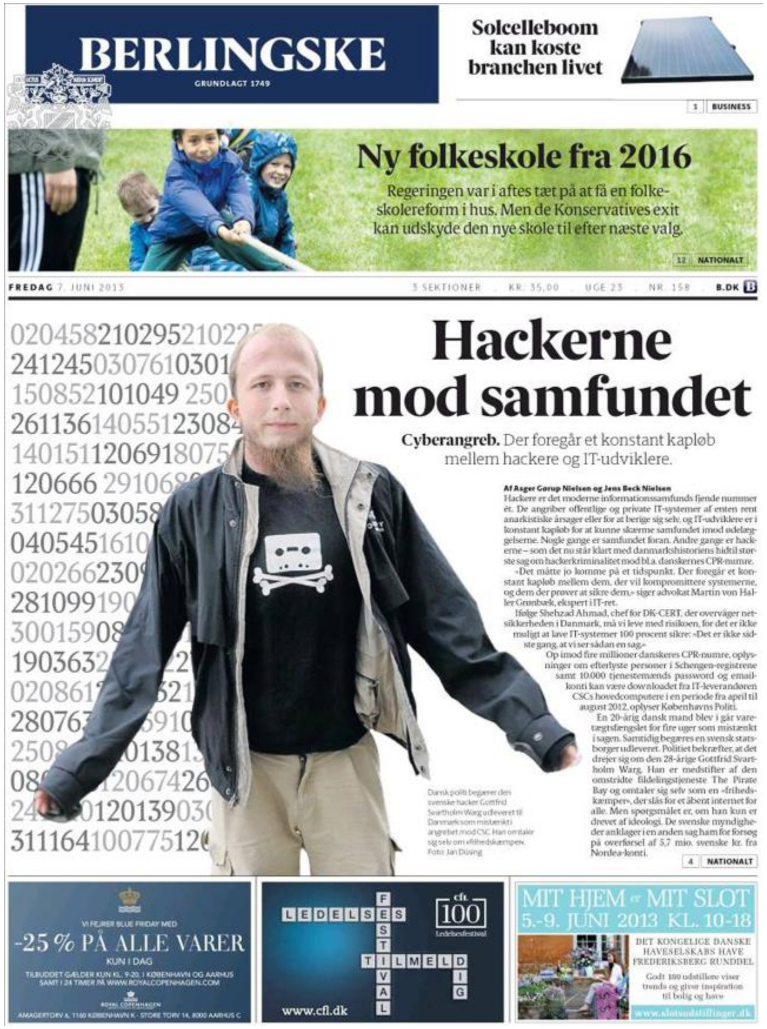


Source: Wikimedia

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

“Hackers against Society”

- Breach of CSC mainframe, April to August, 2012
- Downloaded and also may have modified information in the driver’s license registry and an international database of wanted persons
- Same mainframe also served Danish Tax Authority, the citizen ID number registry and other public agencies
- Warg charged and awaiting trial (as of January 2014)



BERLINGSKE
GRUNDLAGT 1749

Solcelleboom kan koste branchen livet

1 BUSINESS

Ny folkeskole fra 2016

Regeringen var i aftes tæt på at få en folkeskolereform i hus. Men de Konservatives exit kan udskyde den nye skole til efter næste valg.

12 NATIONALT

FREDAG 7. JUNI 2013 . 3 SEKTIONER . KR. 35,00 . UGE 23 . NR. 158 . B.DK

Hackerne mod samfundet

Cyberangreb. Der foregår et konstant kapløb mellem hackere og IT-udviklere.

Af Asger Gorup Nielsen og Jens Beck Nielsen

Hackere er det moderne informationssamfunds fjende nummer ét. De angriber offentlige og private IT-systemer af enten rent anarkistiske årsager eller for at berige sig selv, og IT-udviklere er i konstant kapløb for at kunne skærme samfundet imod ødelæggelserne. Nogle gange er samfundet foran. Andre gange er hackerne – som det nu står klart med danmarkshistoriens hidtil største sag om hackerkriminalitet mod bl.a. danskernes CPR-numre.

»Det måtte jo komme på et tidspunkt. Der foregår et konstant kapløb mellem dem, der vil kompromittere systemerne, og dem der prøver at sikre dem,« siger advokat Martin von Haller Grønbæk, ekspert i IT-ret.

Ifølge Shehzad Ahmad, chef for DK-CERT, der overvåger netsikkerheden i Danmark, må vi leve med risikoen, for det er ikke muligt at lave IT-systemer 100 procent sikre: »Det er ikke sidste gang, at vi ser sådan en sag.«

Op imod fire millioner danskeres CPR-numre, oplysninger om efterlyste personer i Schengen-registrene samt 10.000 tjenestemænds password og emailkonti kan være downloadet fra IT-leverandøren CSCs hovedcomputere i en periode fra april til august 2012, oplyser Københavns Politi.

En 20-årig dansk mand blev i går varetægtsfængslet for fire uger som mistænkt i sagen. Samtidig begæres en svensk statsborger udleveret. Politiet bekræfter, at det drejer sig om den 28-årige Gottfrid Svartholm Warg. Han er medstifter af den omstridte fildelingstjeneste The Pirate Bay og omtaler sig selv som en »frihedskæmper«, der slås for et åbent internet for alle. Men spørgsmålet er, om han kun er drevet af ideologi. De svenske myndigheder anklager i en anden sag ham for forsøg på overførsel af 5,7 mio. svenske kr. fra Nordea-konti.

Dansk politi begærer den svenske hacker Gottfrid Svartholm Warg udleveret til Danmark som mistænkt i angrebet mod CSC. Han omtaler sig selv om »frihedskæmper«. Foto: Jan Düsing

4 NATIONALT

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
- Warg and his accomplices moved freely among PC, Web, z/OS, UNIX – and Hercules
- Protect your mainframe by correlating the indicators

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

“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?
- Convert mainframe events to Syslog in real time
- Leverage the SIEM software you probably already own for real-time alerts
- PCI DSS, IRS Pub. 1075, SOX all require secure, archived log of accesses – why use expensive mainframe DASD?

z/OS Events Available Real-Time

- Everything RACF, ACF2 and Top Secret
- Start and end of TSO sessions, started tasks and batch jobs
- PDS modifications: who modified SYS1.PARMLIB?
- TCP/IP, TN3270 and FTP sessions and failures
- File modifications: QSAM and VSAM files written
- Everything DB2: a “Who’s Who” of PCI DSS
- Dataset renames

What IP Address Edited SYS1.PARMLIB?

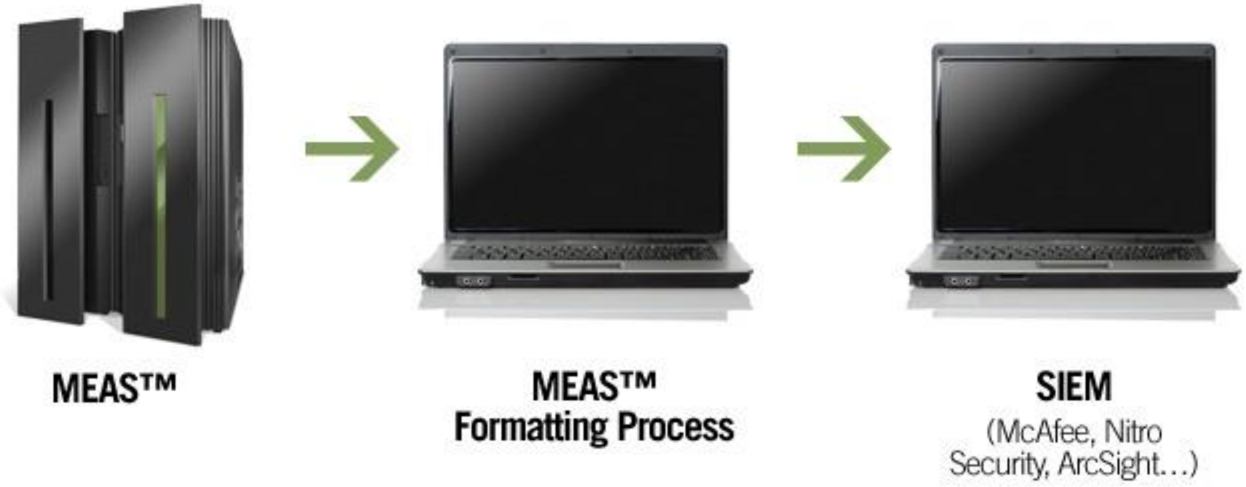
```
<69>Mar 26 05:18:00 mvssysb TCP/IP: Subtype: Telnet
SNA init - TermNm: TCPB2931 - RemtIP: 58.14.0.140

<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
```

Real-time Mainframe Events – How?

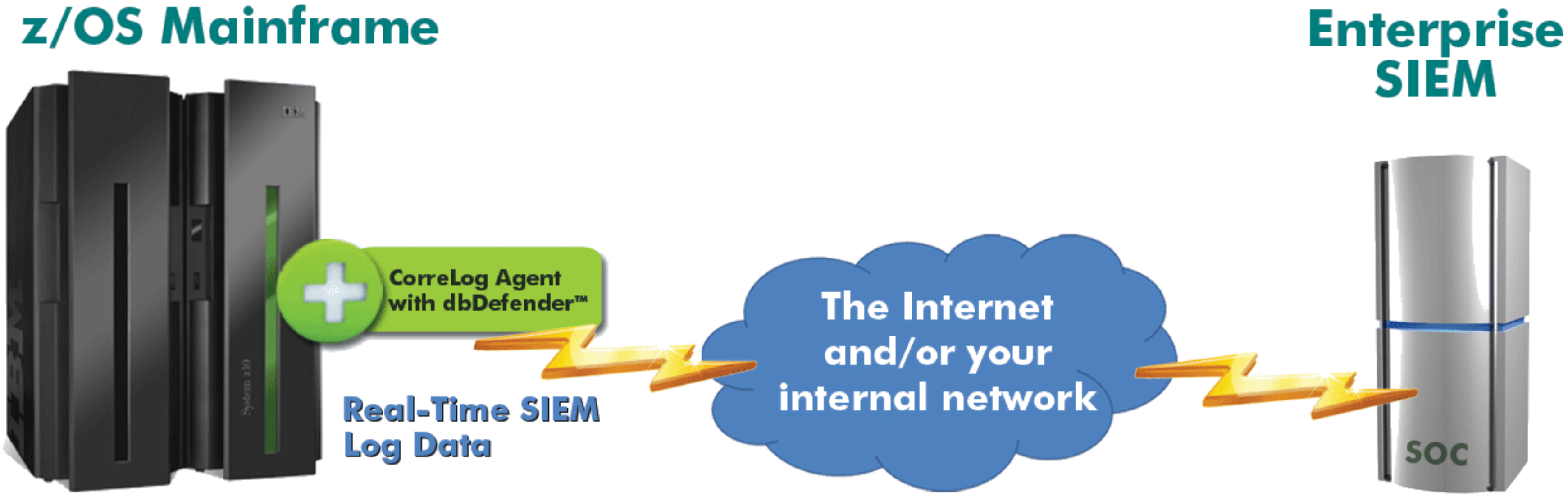
- “Big” Mainframe Products (may be near real-time)
  - IBM Security zSecure Alert
  - CA Compliance Manager
- Forwarding via Off-Mainframe Formatting PC
  - MEAS from InfoSec, Centreville, VA



Source: InfoSecInc.com

Real-time Mainframe Events

- Lightweight started task
  - CorreLog Agent for z/OS


z/OS Mainframe
CorreLog Agent with dbDefender™
Real-Time SIEM Log Data
The Internet and/or your internal network
Enterprise SIEM
SOC

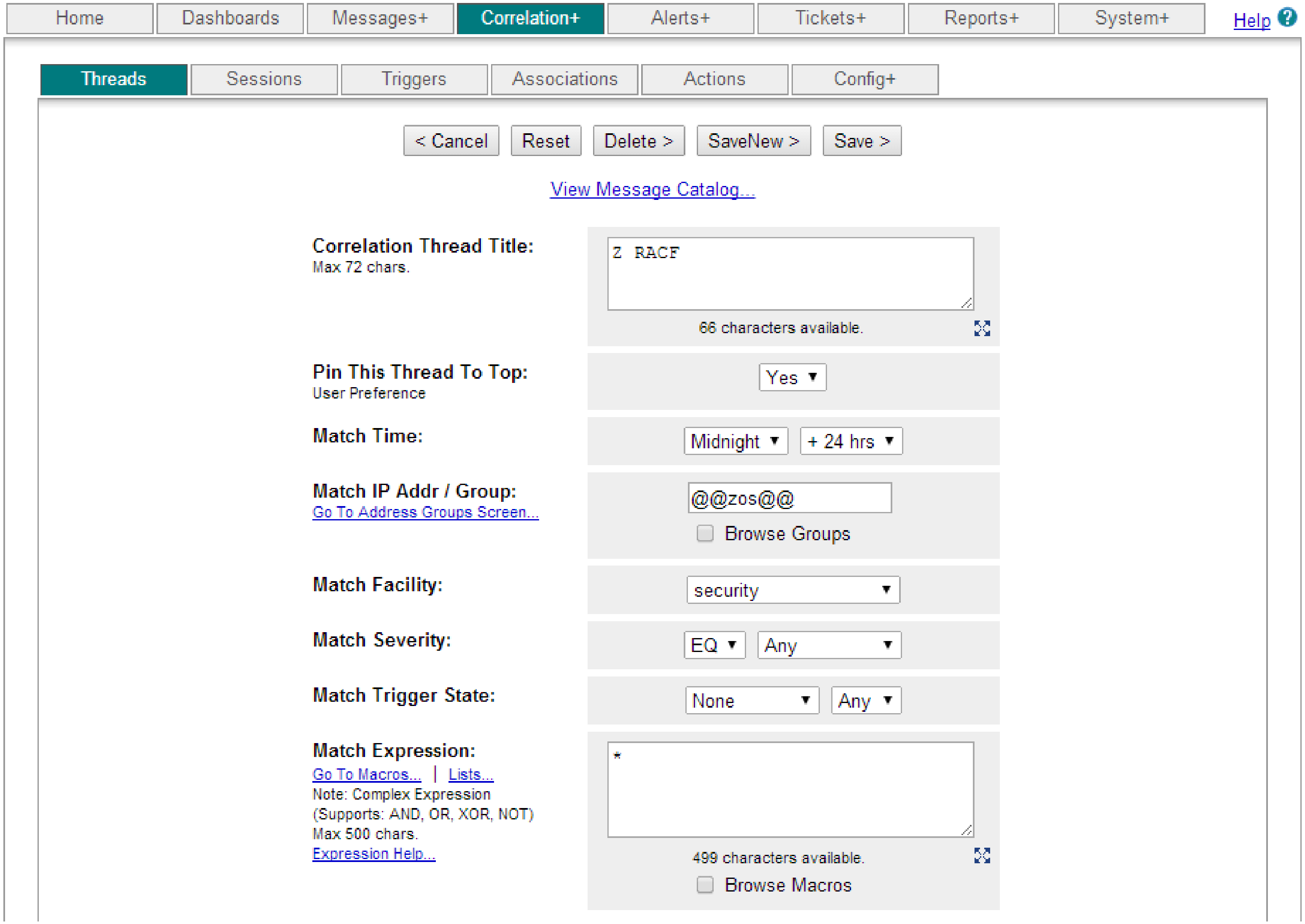
CorreLog

Brief Introduction to SIEMs

What do SIEMs do?

- Gartner: “Critical Capabilities for SIEM Technology”
  - Collect Syslog messages
  - Filtering
  - Correlation: establish relationships among messages and events with real-time alerting
  - Event normalization and taxonomy: logon, log on, signon, sign on, session start, session initiation, …
  - Log management: cost-effective storage, indexing, analysis and reporting
  - User and Application Monitoring
  - Compliance reporting

Correlation



Correlation Thread Title: Max 72 chars.
Z RACF
66 characters available.

Pin This Thread To Top: User Preference
Yes

Match Time: Midnight + 24 hrs

Match IP Addr / Group: Go To Address Groups Screen...
@@zos@@
□ Browse Groups

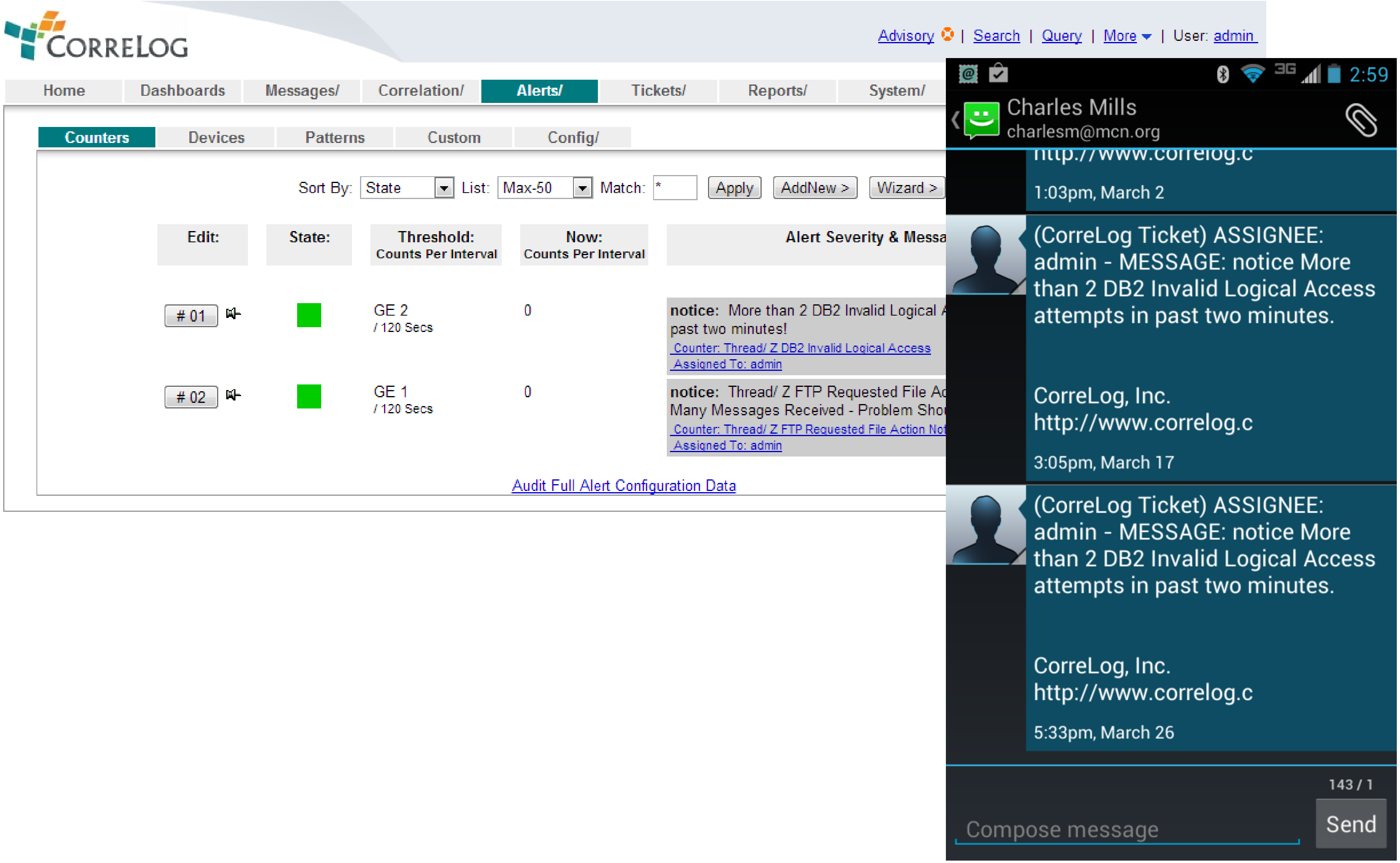
Match Facility: security

Match Severity: EQ Any

Match Trigger State: None Any

Match Expression: Go To Macros... | Lists...
Note: Complex Expression
(Supports: AND, OR, XOR, NOT)
Max 500 chars.
Expression Help...
*
499 characters available.
□ Browse Macros

Alert on Events by Text or E-Mail



CORRELOG
Advisory | Search | Query | More | User: admin
Home | Dashboards | Messages/ | Correlation/ | Alerts/ | Tickets/ | Reports/ | System/
Counters | Devices | Patterns | Custom | Config/
Sort By: State
List: Max-50
Match: *
Apply
AddNew >
Wizard >

Edit:	State:	Threshold: Counts Per Interval	Now: Counts Per Interval	Alert Severity & Messa
# 01	🟩	GE 2 / 120 Secs	0	**notice:** More than 2 DB2 Invalid Logical A past two minutes! Counter: Thread/ Z DB2 Invalid Logical Access Assigned To: admin
# 02	🟩	GE 1 / 120 Secs	0	**notice:** Thread/ Z FTP Requested File Ac Many Messages Received - Problem Sho Counter: Thread/ Z FTP Requested File Action Not Assigned To: admin

Audit Full Alert Configuration Data

http://www.correlog.c

1:03pm, March 2

(CorreLog Ticket) ASSIGNEE: admin - MESSAGE: notice More than 2 DB2 Invalid Logical Access attempts in past two minutes.

CorreLog, Inc.
http://www.correlog.c

3:05pm, March 17

(CorreLog Ticket) ASSIGNEE: admin - MESSAGE: notice More than 2 DB2 Invalid Logical Access attempts in past two minutes.

CorreLog, Inc.
http://www.correlog.c

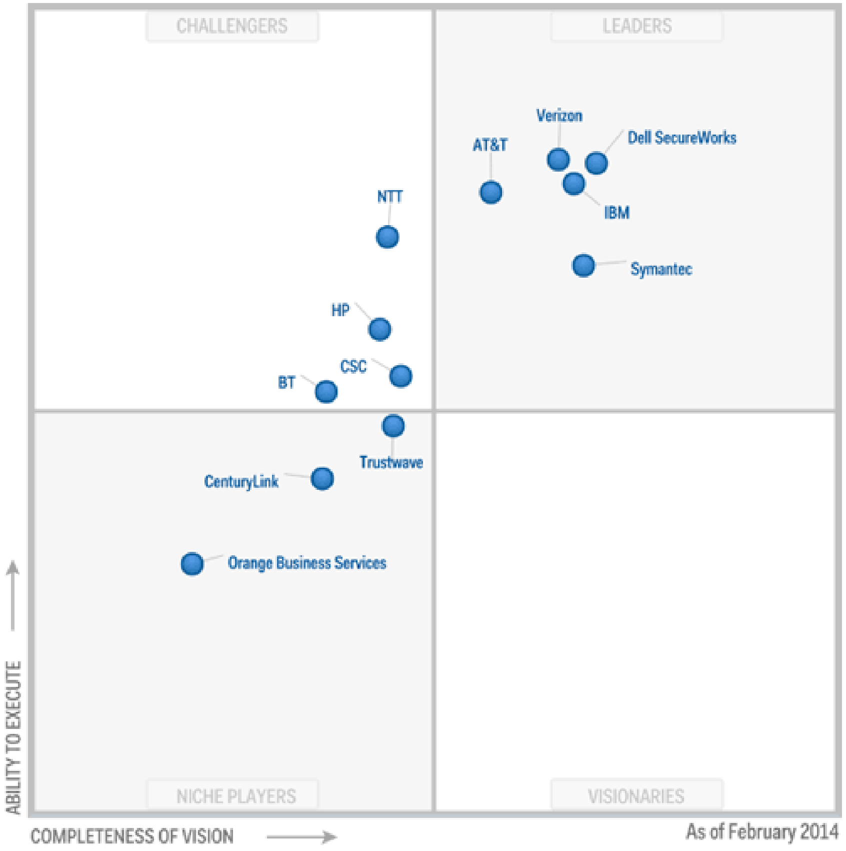
5:33pm, March 26

Types of SIEMs

- Conventional Software/Appliance/Virtual Appliance
  - Running on Linux, UNIX or Windows
  - HP ArcSight ESM
  - IBM Security QRadar
  - McAfee NitroView
  - LogRhythm
  - CorreLog Correlation Server
  - Splunk – does not call themselves a SIEM but customers use it as a SIEM, and Gartner positions it as a SIEM

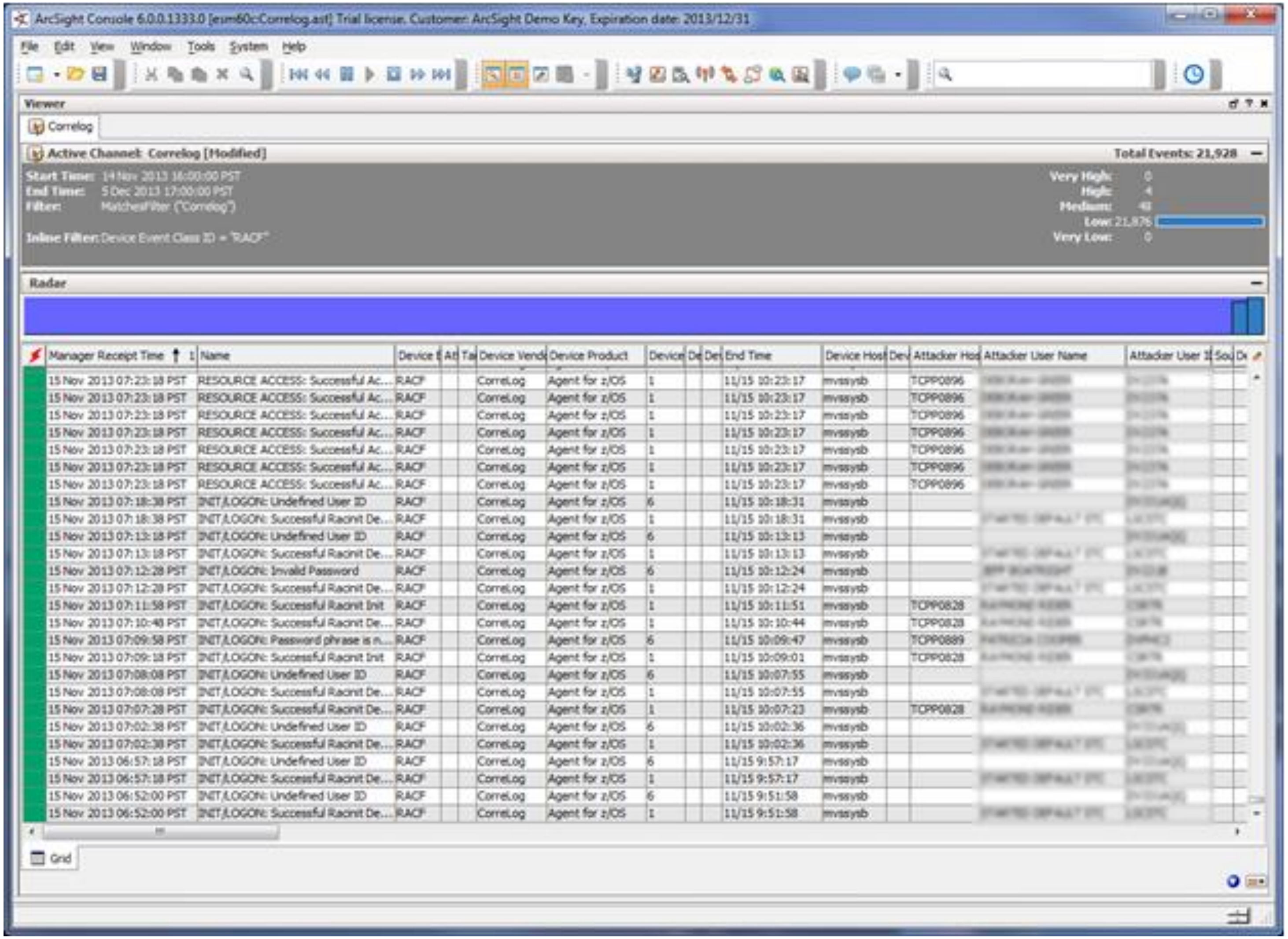
SIEM in the Cloud: MSSP

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



Source: Gartner (February 2014)

z/OS Events in HP ArcSight ESM



ArcSight Console 6.0.0.1333.0 [esm60c:Correlog.ast] Trial license. Customer: ArcSight Demo Key. Expiration date: 2013/12/31
File Edit View Window Tools System Help
Viewer
Correlog
Radar
Grid

Active Channel: Correlog [Modified]

Total Events: 21,928

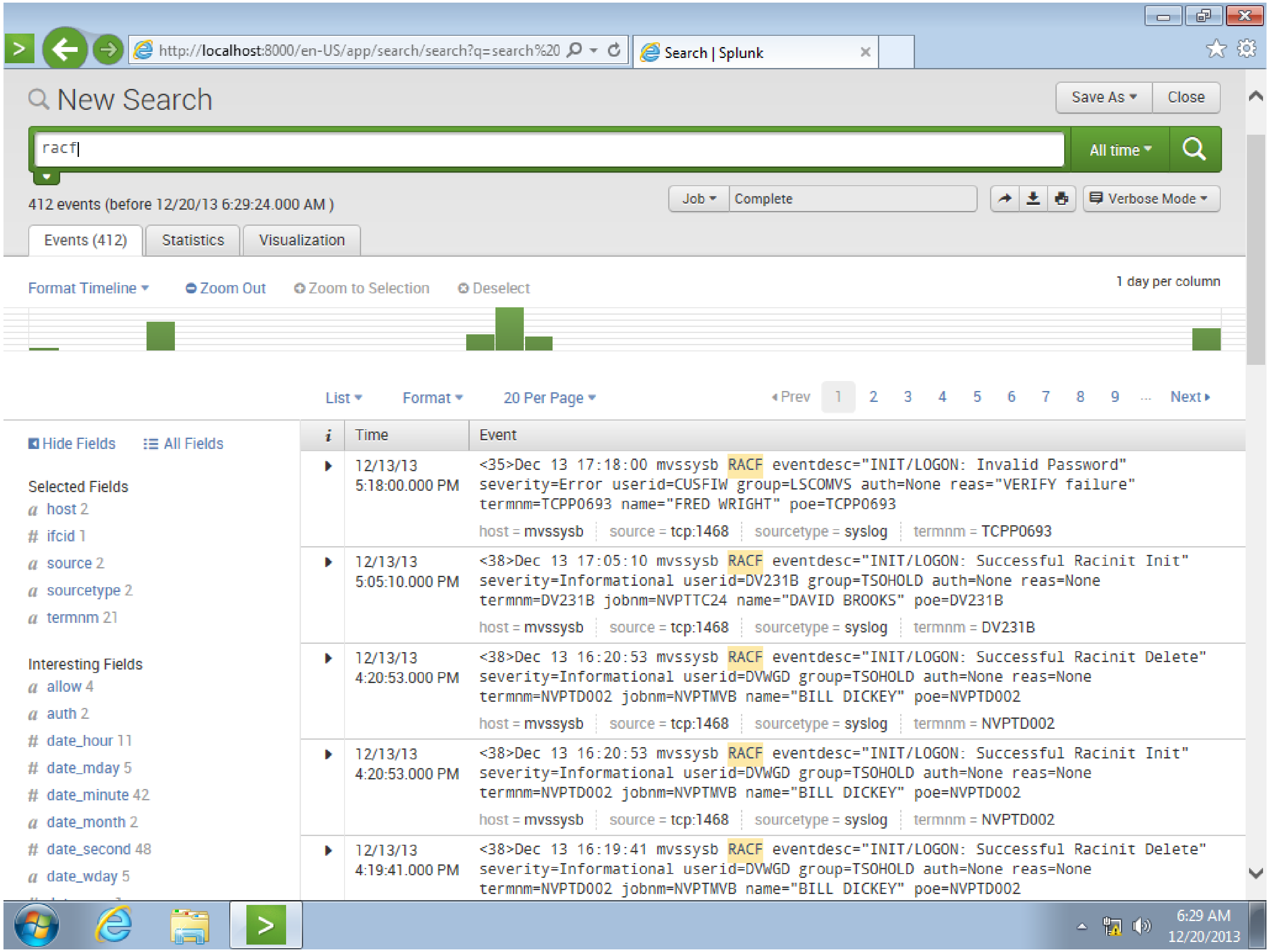
Start Time: 14 Nov 2013 16:00:00 PST
End Time: 5 Dec 2013 17:00:00 PST
Filter: MatchesFilter ("Correlog")

Inline Filter: Device Event Class ID = "RACF"

Very High: 0
High: 4
Medium: 48
Low: 21,876
Very Low: 0

Manager Receipt Time	Name	Device E	Att	Ta	Device Vend	Device Product	Device	De	Dev	End Time	Device Host	Dev	Attacker Hos	Attacker User Name	Attacker User I	Sou	De
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF			CorreLog	Agent for z/OS	1			11/15 10:23:17	mvssysb		TCPP0896	[redacted]	[redacted]		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF			CorreLog	Agent for z/OS	1			11/15 10:23:17	mvssysb		TCPP0896	[redacted]	[redacted]		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF			CorreLog	Agent for z/OS	1			11/15 10:23:17	mvssysb		TCPP0896	[redacted]	[redacted]		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF			CorreLog	Agent for z/OS	1			11/15 10:23:17	mvssysb		TCPP0896	[redacted]	[redacted]		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF			CorreLog	Agent for z/OS	1			11/15 10:23:17	mvssysb		TCPP0896	[redacted]	[redacted]		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF			CorreLog	Agent for z/OS	1			11/15 10:23:17	mvssysb		TCPP0896	[redacted]	[redacted]		
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF			CorreLog	Agent for z/OS	1			11/15 10:23:17	mvssysb		TCPP0896	[redacted]	[redacted]		
15 Nov 2013 07:18:38 PST	INIT/LOGON: Undefined User ID	RACF			CorreLog	Agent for z/OS	6			11/15 10:18:31	mvssysb				[redacted]		
15 Nov 2013 07:18:38 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 10:18:31	mvssysb			[redacted]	[redacted]		
15 Nov 2013 07:13:18 PST	INIT/LOGON: Undefined User ID	RACF			CorreLog	Agent for z/OS	6			11/15 10:13:13	mvssysb				[redacted]		
15 Nov 2013 07:13:18 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 10:13:13	mvssysb			[redacted]	[redacted]		
15 Nov 2013 07:12:28 PST	INIT/LOGON: Invalid Password	RACF			CorreLog	Agent for z/OS	6			11/15 10:12:24	mvssysb			[redacted]	[redacted]		
15 Nov 2013 07:12:28 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 10:12:24	mvssysb			[redacted]	[redacted]		
15 Nov 2013 07:11:58 PST	INIT/LOGON: Successful Racinit Init	RACF			CorreLog	Agent for z/OS	1			11/15 10:11:51	mvssysb		TCPP0828	[redacted]	[redacted]		
15 Nov 2013 07:10:48 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 10:10:44	mvssysb		TCPP0828	[redacted]	[redacted]		
15 Nov 2013 07:09:58 PST	INIT/LOGON: Password phrase is n...	RACF			CorreLog	Agent for z/OS	6			11/15 10:09:47	mvssysb		TCPP0889	[redacted]	[redacted]		
15 Nov 2013 07:09:18 PST	INIT/LOGON: Successful Racinit Init	RACF			CorreLog	Agent for z/OS	1			11/15 10:09:01	mvssysb		TCPP0828	[redacted]	[redacted]		
15 Nov 2013 07:08:08 PST	INIT/LOGON: Undefined User ID	RACF			CorreLog	Agent for z/OS	6			11/15 10:07:55	mvssysb				[redacted]		
15 Nov 2013 07:08:08 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 10:07:55	mvssysb			[redacted]	[redacted]		
15 Nov 2013 07:07:28 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 10:07:23	mvssysb		TCPP0828	[redacted]	[redacted]		
15 Nov 2013 07:02:38 PST	INIT/LOGON: Undefined User ID	RACF			CorreLog	Agent for z/OS	6			11/15 10:02:36	mvssysb				[redacted]		
15 Nov 2013 07:02:38 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 10:02:36	mvssysb			[redacted]	[redacted]		
15 Nov 2013 06:57:18 PST	INIT/LOGON: Undefined User ID	RACF			CorreLog	Agent for z/OS	6			11/15 9:57:17	mvssysb				[redacted]		
15 Nov 2013 06:57:18 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 9:57:17	mvssysb			[redacted]	[redacted]		
15 Nov 2013 06:52:00 PST	INIT/LOGON: Undefined User ID	RACF			CorreLog	Agent for z/OS	6			11/15 9:51:58	mvssysb				[redacted]		
15 Nov 2013 06:52:00 PST	INIT/LOGON: Successful Racinit De...	RACF			CorreLog	Agent for z/OS	1			11/15 9:51:58	mvssysb			[redacted]	[redacted]		

z/OS Events in Splunk



racf

412 events (before 12/20/13 6:29:24.000 AM)

Selected Fields

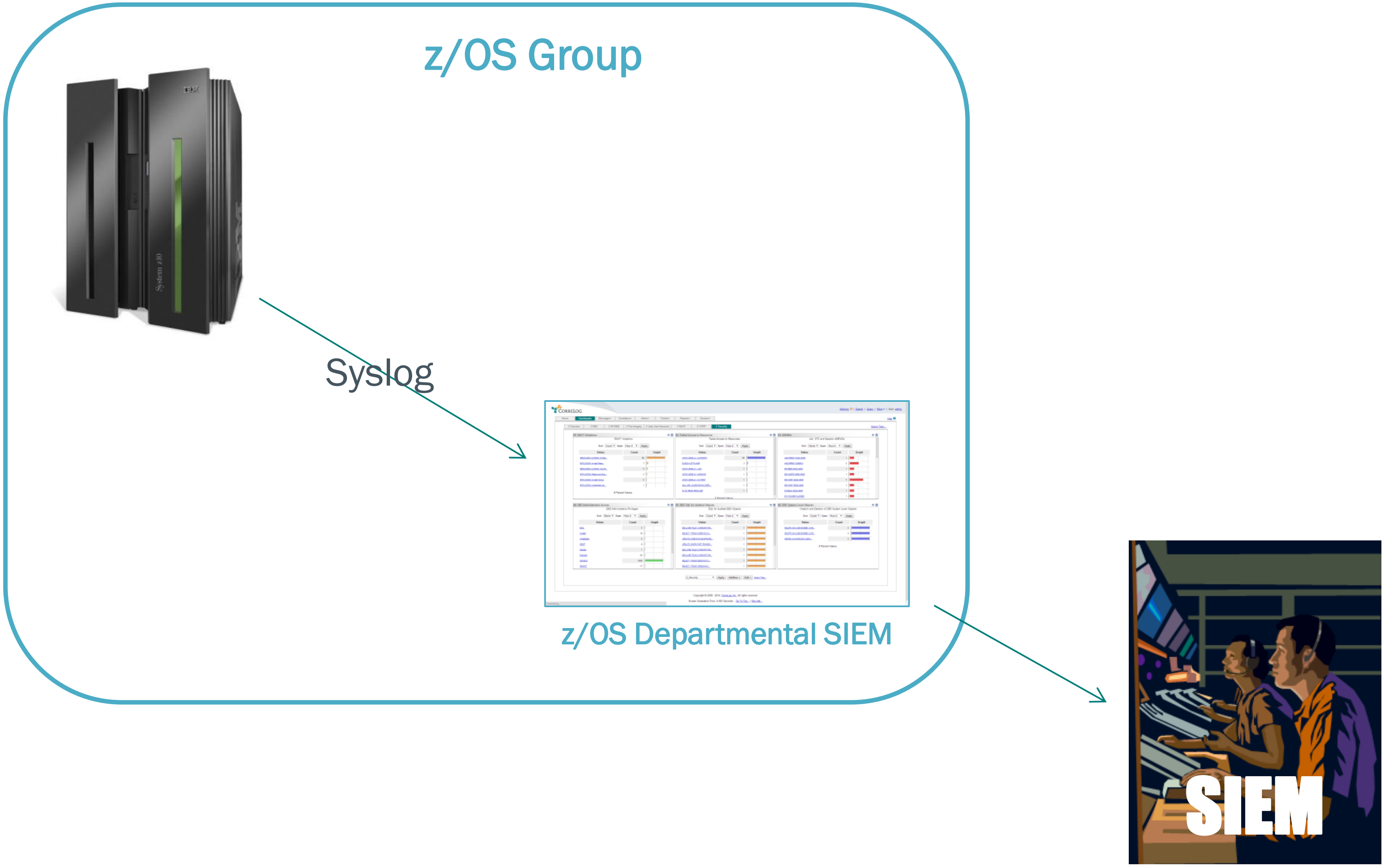
- a host 2
- # ifcid 1
- a source 2
- a sourcetype 2
- a termnm 21

Interesting Fields

- a allow 4
- a auth 2
- # date_hour 11
- # date_mday 5
- # date_minute 42
- a date_month 2
- # date_second 48
- a date_wday 5

i	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=CUSFIW group=LSCOMVS auth=None reas="VERIFY failure" termnm=TCPP0693 name="FRED WRIGHT" poe=TCPP0693 host = mvssysb source = tcp:1468 sourcetype = syslog termnm = TCPP0693
▶	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 termnm=DV231B jobnm=NVPTTC24 name="DAVID BROOKS" poe=DV231B host = mvssysb source = tcp:1468 sourcetype = syslog termnm = 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=DVWGD group=TSOHOLD auth=None reas=None termnm=NVPTD002 jobnm=NVPTMVB name="BILL DICKEY" poe=NVPTD002 host = mvssysb source = tcp:1468 sourcetype = syslog termnm = 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=DVWGD group=TSOHOLD auth=None reas=None termnm=NVPTD002 jobnm=NVPTMVB name="BILL DICKEY" poe=NVPTD002 host = mvssysb source = tcp:1468 sourcetype = syslog termnm = 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=DVWGD group=TSOHOLD auth=None reas=None termnm=NVPTD002 jobnm=NVPTMVB name="BILL DICKEY" poe=NVPTD002

z/OS Departmental SIEM



z/OS Group

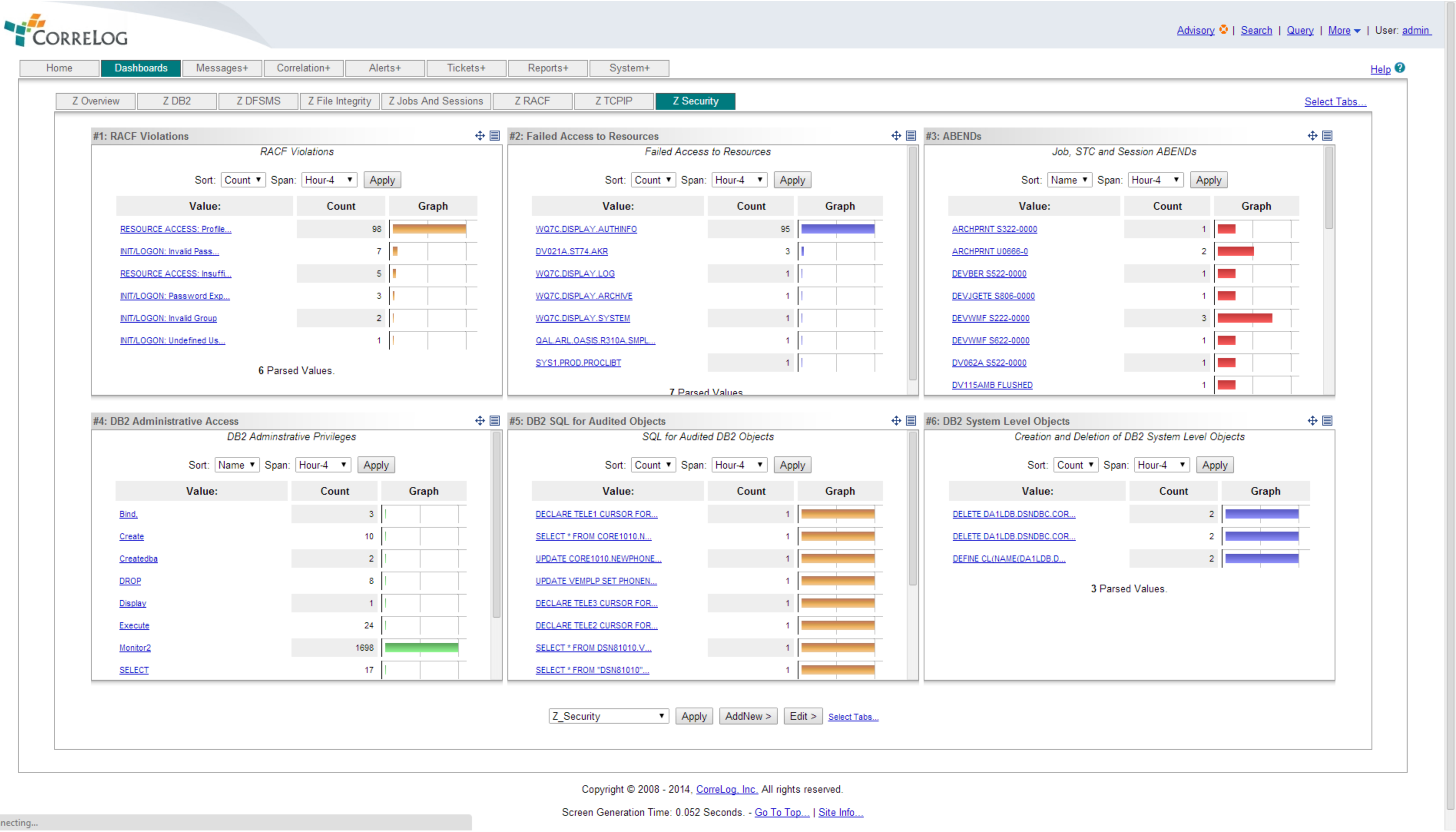
Syslog

z/OS Departmental SIEM

SIEM

Security Operations Center

Mainframe Events in a SIEM Dashboard



#1: RACF Violations

RACF Violations

Sort: Count ▾ Span: Hour-4 ▾ Apply

Value:	Count	Graph
RESOURCE ACCESS: Profile...	98	
INIT/LOGON: Invalid Pass...	7	
RESOURCE ACCESS: Insuffi...	5	
INIT/LOGON: Password Exp...	3	
INIT/LOGON: Invalid Group	2	
INIT/LOGON: Undefined Us...	1	

6 Parsed Values.

#2: Failed Access to Resources

Failed Access to Resources

Sort: Count ▾ Span: Hour-4 ▾ Apply

Value:	Count	Graph
WQ7C.DISPLAY.AUTHINFO	95	
DV021A.ST74.AKR	3	
WQ7C.DISPLAY.LOG	1	
WQ7C.DISPLAY.ARCHIVE	1	
WQ7C.DISPLAY.SYSTEM	1	
QAL.ARL.OASIS.R310A.SMPL...	1	
SYS1.PROD.PROCLIBT	1	

7 Parsed Values

#3: ABENDs

Job, STC and Session ABENDs

Sort: Name ▾ Span: Hour-4 ▾ Apply

Value:	Count	Graph
ARCHPRNT S322-0000	1	
ARCHPRNT U0666-0	2	
DEVBER S522-0000	1	
DEVJGETE S806-0000	1	
DEVWMF S222-0000	3	
DEVWMF S622-0000	1	
DV062A S522-0000	1	
DV115AMB FLUSHED	1	

#4: DB2 Administrative Access

DB2 Adminstrative Privileges

Sort: Name ▾ Span: Hour-4 ▾ Apply

Value:	Count	Graph
Bind,	3	
Create	10	
Createdba	2	
DROP	8	
Display	1	
Execute	24	
Monitor2	1698	
SELECT	17	

#5: DB2 SQL for Audited Objects

SQL for Audited DB2 Objects

Sort: Count ▾ Span: Hour-4 ▾ Apply

Value:	Count	Graph
DECLARE TELE1 CURSOR FOR...	1	
SELECT * FROM CORE1010.N...	1	
UPDATE CORE1010.NEWPHONE...	1	
UPDATE VEMPLP SET PHONEN...	1	
DECLARE TELE3 CURSOR FOR...	1	
DECLARE TELE2 CURSOR FOR...	1	
SELECT * FROM DSN81010.V...	1	
SELECT * FROM "DSN81010"...	1	

#6: DB2 System Level Objects

Creation and Deletion of DB2 System Level Objects

Sort: Count ▾ Span: Hour-4 ▾ Apply

Value:	Count	Graph
DELETE DA1LDB.DSNDBC.COR...	2	
DELETE DA1LDB.DSNDBC.COR...	2	
DEFINE CL(NAME(DA1LDB.D...	2	

3 Parsed Values.

Copyright © 2008 - 2014, CorreLog, Inc. All rights reserved.

Screen Generation Time: 0.052 Seconds. - Go To Top... | Site Info...

Connecting...

Reference Material

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
- Questions?
- Thank you!