

SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

16898: A Forensic Analysis of Security Events on System z, Without the Use of SMF Data

Brian Marshall

Vice President, Research and Development

Vanguard Integrity Professionals

Monday March 2, 2015



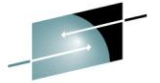
#SHAREorg



SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.



Well, today it's all about data!



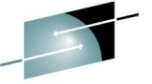
SHARE
Educate • Network • Influence
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

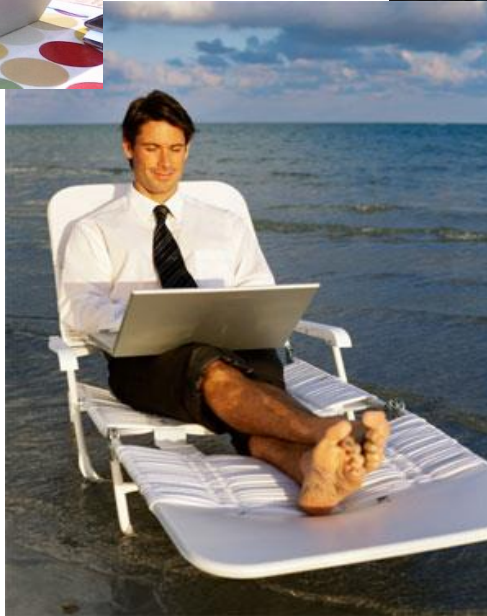


So, where is your data today?



SHARE
Educate • Network • Influence

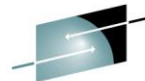
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Wherever you are.....

Complete your session evaluations online at www.SHARE.org/Seattle-Eval





SHARE
Educate • Network • Influence
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

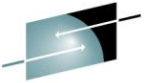
Your data on the move with tablets....



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

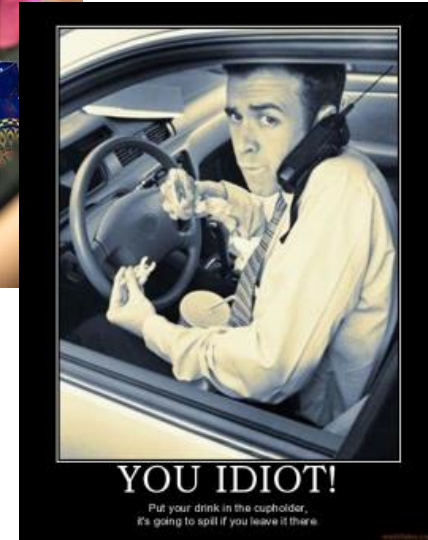


...and oh so many devices!



SHARE
Educate • Network • Influence

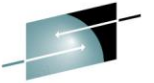
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Is your data in the cloud?



SHARE
Educate • Network • Influence

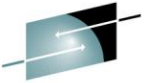
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



In the hands of criminals?



SHARE
Educate • Network • Influence

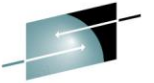
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

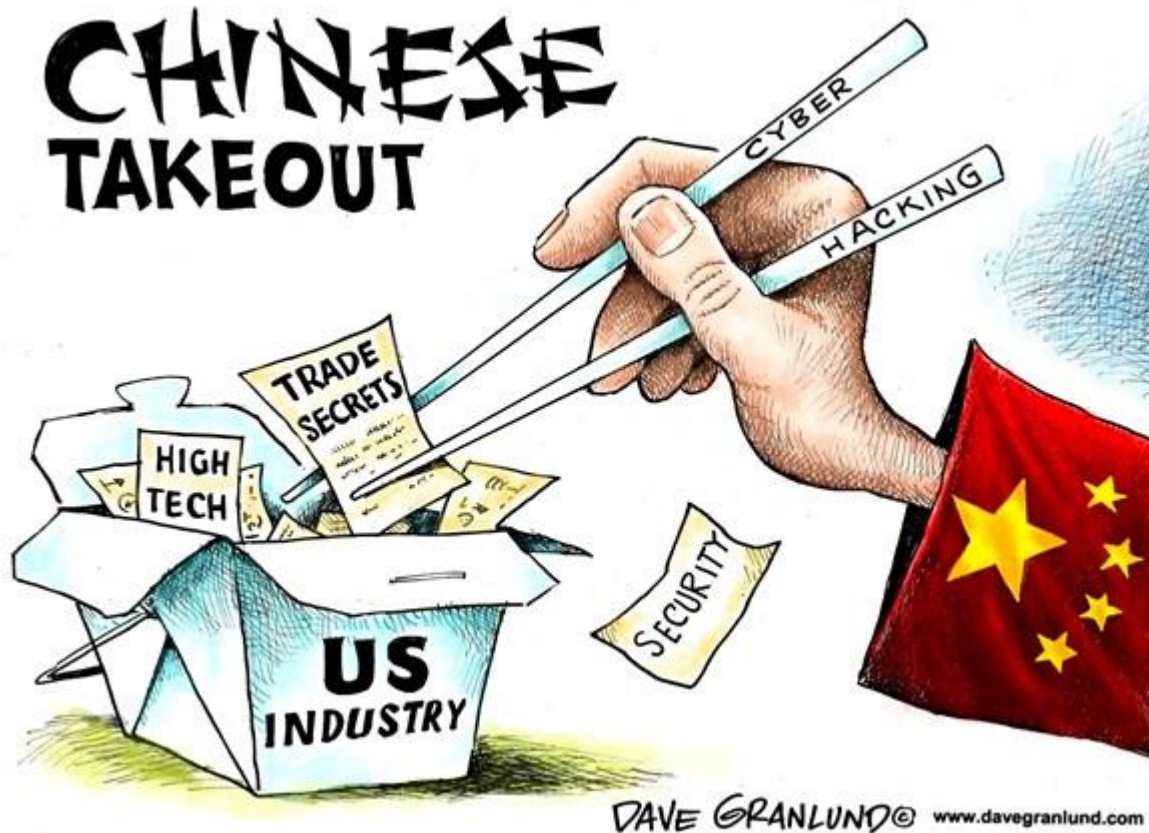


In the hands of other nations?



SHARE
Educate • Network • Influence

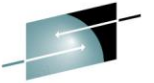
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



In the hands of some government agency?



SHARE
Educate • Network • Influence

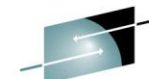
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



We hear it every day!



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

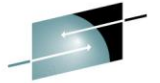


Because the truth is....

You are about to be compromised

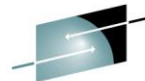
OR

You have already been compromised



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Maybe you have better security.....

The web became significantly more malicious, both as an attack vector and as the primary support element of other trajectories (i.e. social, mobile, e-mail, etc.).

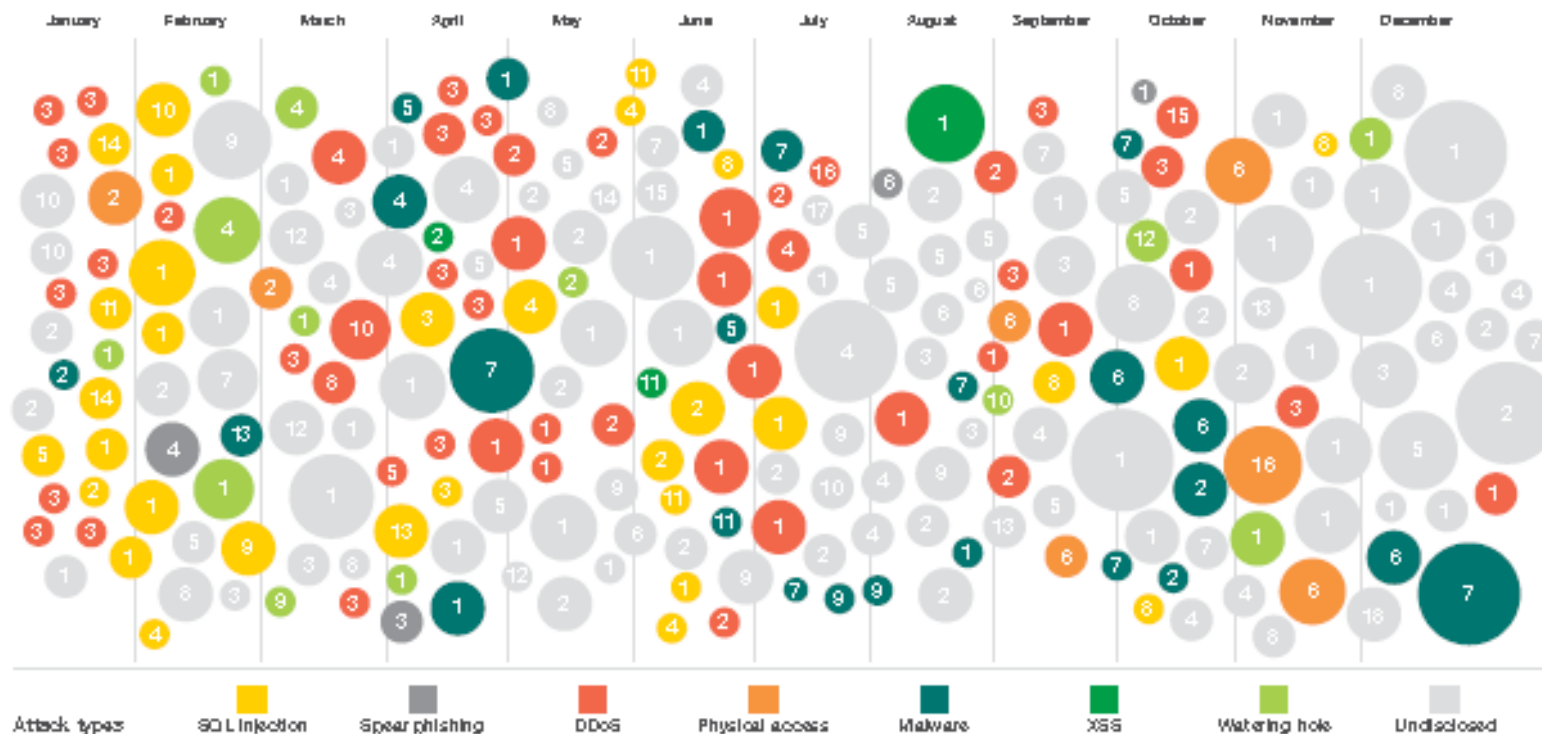


A diagram of a fiber optic cable. It shows a rectangular cross-section divided into a central core and an outer cladding. Two white arrows represent light rays traveling through the core. One ray is at the top, and the other is at the bottom. Both rays are angled towards the center and reflect off the interface between the core and cladding, demonstrating total internal reflection. The core is shaded light blue, and the cladding is shaded dark blue.

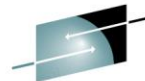
S H A R E
Educate • Network • Influence

Sampling of 2013 security incidents by attack type, time and impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



State of police will make no bid/impact of incident in terms of cost to business



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Biggest IT Myths

- Hey, it won't happen to us!
- Buy this tool <insert tool here> and it will solve all of your problems.
- Let's get the policy in place and we are good to go.
- I passed my IT audit, I must be secure.



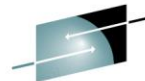
Complete your session evaluations online at www.SHARE.org/Seattle-Eval



Their M.O.

The cyber spies typically enter targeted computer networks through “spearfishing” attaches, in which company official receives a creatively disguised email and it tricked into clicking on a link or attachment that then opens a secret door for hackers.





SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

They can't get to me, I'm secure.

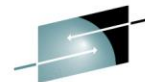
- Hackers go after suppliers to get into larger companies.
- Smaller companies tend not to have the funding, staff, or knowledge need to formalize – let alone maintain – more secure policies and procedures all combining to make them the path of least resistance....and the bad guys have discovered this.



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



But I run a mainframe. I'm not vulnerable.



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS



Complete your session evaluations online at www.SHARE.org/Seattle-Eval

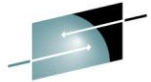


Black Hat 2013



- While most IT security teams tend to lump mainframe systems into the category of legacy systems unnecessary or impossible to scrutinize during regular audits, that couldn't be farther from the truth, says a researcher at Black Hat USA
- On Mainframes.. I see them described as legacy all the time: 'Oh, we don't need to implement this policy because it's a legacy system.' Calling a mainframe legacy is like calling Windows 2012 Server legacy because parts of the Window NT kernel are still in the code. Or it's like calling my car legacy because it's still got tires," said Philip "Soldier of Fortran" Young, explaining that most enterprise mainframes today run off the IBM z/OS platform
- As part of the Black Hat presentation on Mainframe Vulnerabilities to being breached, a website with a number of tools to aid with the hacking of a mainframe was released including VERY SPECIFIC mainframe vulnerabilities (ACEE zapper, USS elevated permission code, TN3270 sniffers)
- <https://github.com/mainframed>

In Response to Black Hat 2013 Mainframe “Hackable” Presentation



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Home News Commentary Slideshows Video Events

 How To Cushion The Impact Of A Data Breach

darkREADING
Protect The Business Enable Access

Advanced Threats Applications Attacks & Breaches Compliance Database End
Monitoring Perimeter Risk Security Analytics Services SMB Threat Intel

IBM X-Force® 2012 Annual Trend and Risk Report
→ Download and read about emerging security threats and trends.



Excerpt from his response:

*The person responsible for mainframe database security, don't have a lot to worry about. And if you were worried about these attacks, **you can disable FTP** to thwart malicious code uploads. **Or firewall off the mainframe from Web access**, as seems common.*

COMMENTARY

Mainframes Hackable, But Do You Care?



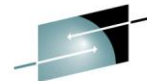
Adrian Lane

[See more from Adrian](#)

Connect directly with Adrian: [RSS](#) [Bio](#) | [Contact](#)

Adrian Lane is an analyst/CTO with Securosis LLC

*Any one want to guess why Adrian Lane is **JUST WRONG???***



SHARE
Educate • Network • Influence

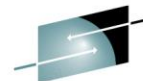
VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

In Response to Black Hat 2013

Adrian Lane states in the article:

- The reason we don't hear about DB2 hacks is that, "Because Nobody uses it".
 - *Wow*
- Mainframes come with "a Supplementary UNIX environment". - *How many of us run a z/OS system without UNIX? Does this negate or even mitigate the vulnerability?*
- About the mainframe: "Mainframes do not attract attackers." - *I guess security by obscurity is alive and well.*
- If you are worried about security, you need only wall off the mainframe from all internet access.
 - *I guess all those applications (Airline Reservations, ACH transfers, Inventory Management Systems, Banking, Financial and Government applications) DO NOT NEED to run with connectivity to the world.*

Logica and Nordea Bank Mainframe Breach 2013



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

COMPUTERWORLD

– it-nyheter døgnet rundt

IDG – verdens største mediehus innen it

Security | Software | IT Management | Virtualization | Operating systems | Hardware Systems | Cor

[IDG News Service](#) >

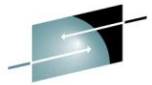
Pirate Bay co-founder charged with hacking IBM mainframes, stealing money

o Loek Essers

16.04.2013 kl 16:02 | IDG News Service\Amsterdam Bureau

+1 0

Tweet 2



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Lessons Learned

Bill for data breach was
expensive...Investigations aren't cheap!

Findings:

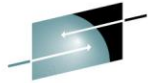
- Pirate Bay co-founder Gottfrid Svartholm Warg was charged with hacking the IBM mainframe of Logica, a Swedish IT firm that provided tax services to the Swedish government, and the IBM mainframe of the Swedish Nordea Bank, according to the Swedish public prosecutor.
- “This is the biggest investigation into data intrusion ever performed in Sweden”, said the public prosecutor Henrik Olin.
- It is not really clear why Logica was hacked said Olin. But the intruders stole expensive personal and vehicle data, including security numbers.
- They attempted to steal over \$900K from Nordea customer accounts.

But Wait!!!

In September of 2013, Gottfrid Svartholm was cleared of hacking into the Swedish bank Nordea because it was impossible to prove that he had illegally gained access to their mainframe even though \$990,000 was stolen and even though his conviction for hacking into the Banks IT provider Logica was upheld.



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

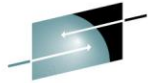


So what now???

- I have SMF running.
- I track my privileged users right?
- I don't have unnecessary libraries in APF list.
- I follow the NIST security guidelines for securing my system.
- I pass all of my audits.

I must be secure!!!!

So what now???



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

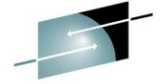
Are you sure???



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



So what now???



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Of course not, but you can be more sure.

Complete your session evaluations online at www.SHARE.org/Seattle-Eval



How?



With Vanguard Offline and Correlog.

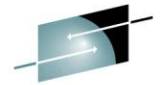
Complete your session evaluations online at www.SHARE.org/Seattle-Eval



What is Vanguard Offline?

Vanguard Offline is a product that captures all access requests passed to RACF, saves each unique access in a VSAM file, which then allows customers to execute RACF commands against a test copy of the RACF database and thereby evaluate the impact of those commands given historical authorization information.

What is Vanguard Offline?

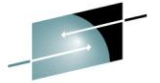


SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

- Vanguard Offline also provides reporting against all of the historical data and allows you to essentially data mine the access requests to RACF database
- Reporting can be done against the raw access records, OR can be replayed against a copy of the racf database for real time (batch or online) reporting of changes to access
- Data capture is achieved through the use of RACF exits

ICHRCX02 (AUTH)



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

A RACROUTE REQUEST=AUTH determines whether a user is authorized to obtain use of a resource

ICHRFX02 and ICHRFX04 (FASTAUTH)

RACROUTE REQUEST=FASTAUTH examines the auditing and global options in effect for the resource while determining the access authority of the caller. There are two types of these exits: ICHRFX02 and ICHRFX04

ICHRIX02 (VERIFY(x))

A RACROUTE REQUEST=VERIFY or RACROUTE REQUEST=VERIFYX request is used to determine whether a user ID is defined to RACF® and whether the user has supplied a valid password or password phrase and group name ICHRIX02

So what can we get from these exits?

Who – Userid

What – resource

Where – Terminal ID

When – Date and Time of access

How – Covering Profile (or other method that allowed access)

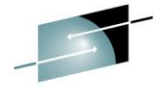
Access Requested

Access Allowed

Access History Reports

Access History reports are available organized in several ways:

- Access Summary by Access
- Access Summary by User
- Access Summary by Group
- Access Summary by Class
- Access Summary by System
- Access Detail by Masking
- Access Detail (Complete List)
- Access Detail (Denied Access)



SHARE
Educate • Network • Influence

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

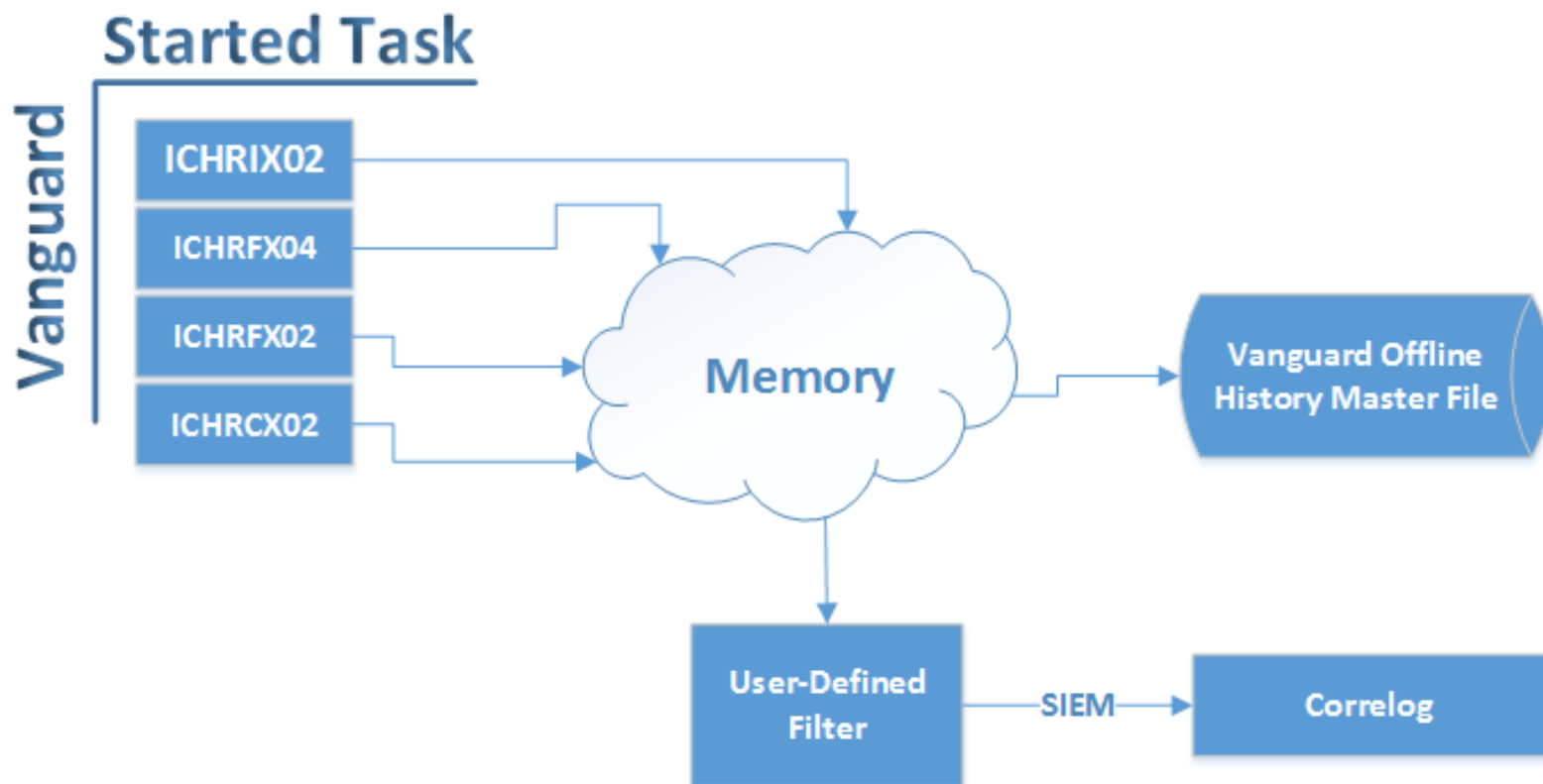
Access History Reports

- Summarize all access data in the VOF history master file
- “Drill down” to view specific access records
- Direct mode – from VOF history master file
- Extract mode – from flat file created with the VOF history master file

What is the value?

- Provides a safe offline environment for testing changes in access
- Lowers the risk of making changes to access to production systems
- Provides reports to view details of individual access records
- Allows for complete reporting of who accessed what or attempted to access what, w/o having to peruse days/weeks/months or years of SMF data
- Can be used as a forensic tool or as a method to ensure that access is/is not granted any longer.

How It Works



CorreLog Agent for z/OS

Bridging the z/OS Gap in Your SIEM



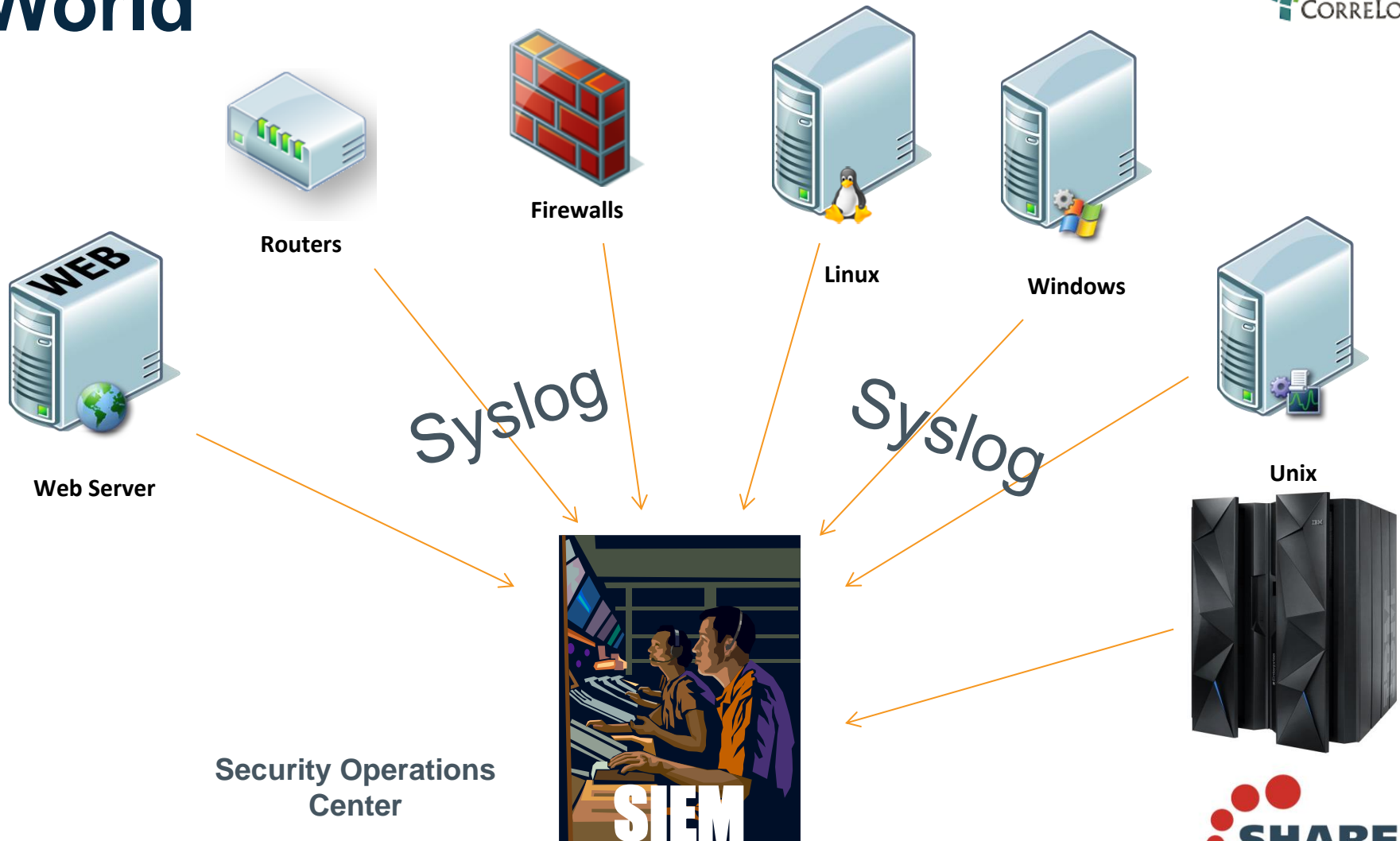
#SHAREorg



SHARE is an independent volunteer-run information technology association that provides **education, professional networking and industry influence.**



Mainframe in the Network Security World

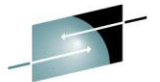


SIEM Integration

- Flexible enough to integrate with any SIEM or MSSP
- Customers running with LogRhythm, ArcSight, IBM QRadar, Dell SecureWorks, CorreLog SIEM, NTT Solutionary, Splunk and more
- SIEMs provide correlation, forensic archive, real-time alerts, reporting, etc.
- Very flexible configuration – out of the box compatibility



z/OS Events in ArcSight ESM



SHARE
Educate • Network • Influence



ArcSight Console 6.0.0.1333.0 [esm60cCorrelog.asi] Trial license. Customer: ArcSight Demo Key. Expiration date: 2013/12/31

File Edit View Window Tools System Help

Viewer

Correlog

Active Channel: Correlog [Modified]

Start Time: 14 Nov 2013 16:00:00 PST
End Time: 5 Dec 2013 17:00:00 PST
Filter: MatchedFilter ("Correlog")
Inline Filter: Device Event Class ID = "RACF"

Total Events: 21,928

Very High: 0
High: 4
Medium: 43
Low: 21,875
Very Low: 0

Radar

Manager Receipt Time	Name	Device ID	Device Vendor	Device Product	Device ID	Device End Time	Device Host	Attacker Host	Attacker User Name	Attacker User ID	Source	Destination
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF	Correlog	Agent for z/OS	1	11/15 00:23:17	mvssysb	TCPP0896	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF	Correlog	Agent for z/OS	1	11/15 00:23:17	mvssysb	TCPP0896	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF	Correlog	Agent for z/OS	1	11/15 00:23:17	mvssysb	TCPP0896	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF	Correlog	Agent for z/OS	1	11/15 00:23:17	mvssysb	TCPP0896	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF	Correlog	Agent for z/OS	1	11/15 00:23:17	mvssysb	TCPP0896	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF	Correlog	Agent for z/OS	1	11/15 00:23:17	mvssysb	TCPP0896	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:23:18 PST	RESOURCE ACCESS: Successful Ac...	RACF	Correlog	Agent for z/OS	1	11/15 00:23:17	mvssysb	TCPP0896	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:18:38 PST	INTEL.LOGON: Undefined User ID	RACF	Correlog	Agent for z/OS	6	11/15 00:18:31	mvssysb					
15 Nov 2013 07:18:38 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 00:18:31	mvssysb					
15 Nov 2013 07:13:18 PST	INTEL.LOGON: Undefined User ID	RACF	Correlog	Agent for z/OS	6	11/15 00:13:13	mvssysb					
15 Nov 2013 07:13:18 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 00:13:13	mvssysb					
15 Nov 2013 07:12:28 PST	INTEL.LOGON: Invalid Password	RACF	Correlog	Agent for z/OS	6	11/15 00:12:24	mvssysb					
15 Nov 2013 07:12:28 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 00:12:24	mvssysb					
15 Nov 2013 07:11:58 PST	INTEL.LOGON: Successful Racnit Init	RACF	Correlog	Agent for z/OS	1	11/15 00:11:51	mvssysb	TCPP0828	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:10:40 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 00:10:44	mvssysb	TCPP0828	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:09:58 PST	INTEL.LOGON: Password phrase is n...	RACF	Correlog	Agent for z/OS	6	11/15 00:09:47	mvssysb	TCPP0889	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:09:18 PST	INTEL.LOGON: Successful Racnit Init	RACF	Correlog	Agent for z/OS	1	11/15 00:09:01	mvssysb	TCPP0828	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:08:08 PST	INTEL.LOGON: Undefined User ID	RACF	Correlog	Agent for z/OS	6	11/15 00:07:55	mvssysb					
15 Nov 2013 07:08:08 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 00:07:55	mvssysb					
15 Nov 2013 07:07:28 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 00:07:23	mvssysb	TCPP0828	100.0.0.0	100.0.0.0	100.0.0.0	100.0.0.0
15 Nov 2013 07:02:38 PST	INTEL.LOGON: Undefined User ID	RACF	Correlog	Agent for z/OS	6	11/15 00:02:36	mvssysb					
15 Nov 2013 07:02:38 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 00:02:36	mvssysb					
15 Nov 2013 06:57:18 PST	INTEL.LOGON: Undefined User ID	RACF	Correlog	Agent for z/OS	6	11/15 9:57:17	mvssysb					
15 Nov 2013 06:57:18 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 9:57:17	mvssysb					
15 Nov 2013 06:52:00 PST	INTEL.LOGON: Undefined User ID	RACF	Correlog	Agent for z/OS	6	11/15 9:51:58	mvssysb					
15 Nov 2013 06:52:00 PST	INTEL.LOGON: Successful Racnit De...	RACF	Correlog	Agent for z/OS	1	11/15 9:51:58	mvssysb					

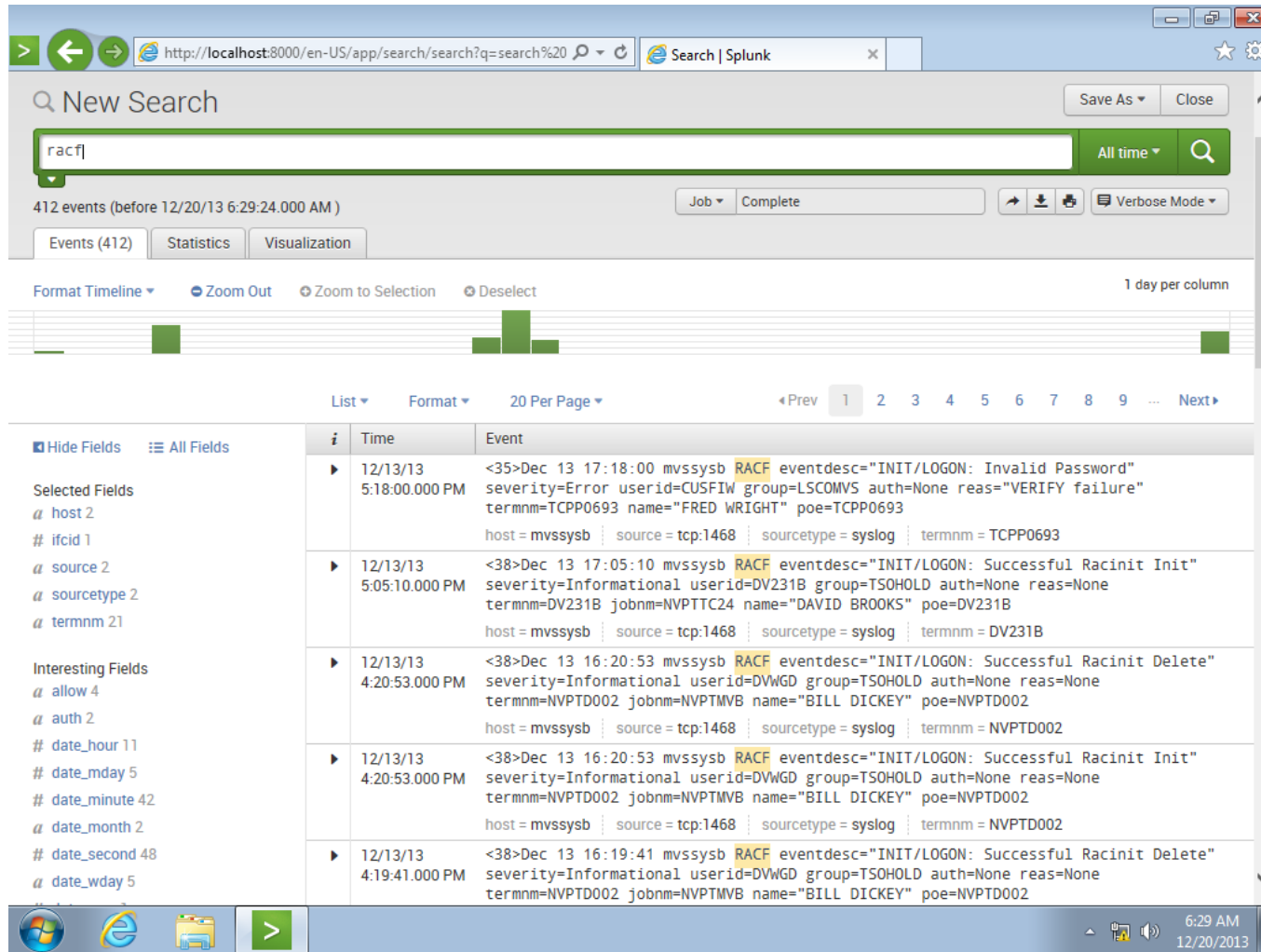
Grid



Complete your session evaluations online at www.SHARE.org/Seattle-Eval



z/OS Events in Splunk



The screenshot shows the Splunk web interface with the search query 'racf'. The results show 412 events. The interface includes a search bar, a timeline view, and a list of events. The events are filtered by 'All time' and 'Verbose Mode' is selected. The events are displayed in a table with columns for Time and Event.

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

Complete your session evaluations online at www.SHARE.org/Seattle-Eval

Thank You



Stop by and visit us at Booth 607!

Complete your session evaluations online at www.SHARE.org/Seattle-Eval