

Getting Started Using the DoD STIGs for Mainframe Security

SHARE - Phoenix 2019 - Session 24610, March 11, 2019 Phil Noplos - CISM, CISSP

Copyright[®] by SHARE Association Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

©€\$≘ 1



WHO IS TODAY'S SPEAKER?

Bio - Phil Noplos, CISM, CISSP



- 50 years of Information Technology leadership roles at Financial, Health Care and Academic institutions across many aspects of information technology, including:
 - Operations
 - Application development
 - Systems programming
 - Data warehousing and
 - Cyber security (last 10 years)
- First mainframe = 360/40 (i.e. after "unit record" equipment)
- First SHARE volunteer project involvement in the 70's (in the GUIDE organization, co-authored HIPO publication)
- Today, in addition to speaking, I am a SHARE Affiliate member applicant and volunteer participant in SHARE Marketing Committee and SHARE Security Project.

I bring this perspective to today's session

Disclaimer



- Solely my opinions
- Not a vendor of any hardware or software products
- No affiliations with any commercial firm aside from my own PLN & Associates
- The references in this presentation to IBM, SDS, CA/Broadcom, Vanguard, Correlog/BMC, UCF, RiskLens, You Tube or other firms, or their respective products, are purely illustrative and imply neither a claim by me to any licensed usage rights to, nor my promotion of any of those firms or their products.

Today's Session – Value and Objective



Target Audience: Experienced security professionals who are at the stage of considering or planning the use of DISA STIGs for z/OS configuration management.

Purpose: Offer recommendations that will allow participants to confidently define, propose and initiate a useful and viable configuration management program to reduce security risk.

Scope: We will discuss the "What", "Why", and "How" elements of implementing a successful, STIGs-based, mainframe configuration management program to effect cyber risk reduction.



Reduce security risk of configuration-based vulnerabilities by implementing successful and sustainable configuration management.

Note:

This session is not a tool training lab session though several useful tools will be mentioned during the presentation.

Let's Get Started!



STIGS – WHAT, WHY AND HOW



Let's cite some security context for STIGs (Security Technical Information Guide) Risk Management Context:

Configuration/Asset Management is generally considered a basic element of information cyber risk management (e.g., by NIST 800-128 and 800-53, Security Control CM-6).

- One reason configuration management is fundamental is that threats often exploit vulnerabilities due to mis-configured infrastructure.
 - Exploitation is particularly dangerous when it occurs in privileged environments.
 - Privileged operation is typical for operating systems.

STIGs are a Cybersecurity framework from DoD for effective configuration management



NIST Context:

- The National Institute of Science and Technology operates a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, NIST's cybersecurity program supports its overall mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and related technology through research and development in ways that enhance economic security and improve our quality of life.
- The need for cybersecurity standards and best practices that address interoperability, usability and privacy continues to be critical for the nation. NIST's cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.

STIGs are tightly coupled to generally-accepted best security practices



DISA Context:

The Defense Information Systems Agency, is a combat support agency of the Department of Defense (DoD). The agency provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters,

STIGs are designed to meet US national defense security standards



STIGs:

Security Technical Implementation Guides, since 1998, have played a critical role enhancing the security posture of DoD's security systems. The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

The official IASE (Information Assurance Support Environment) definition of Security Technical Implementation Guide is:

"The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack."

STIGs are a mature framework to improved security posture



	A		С	D	E	F	G	Н	1	J
1	TOTALS	Version 6 Release 39								
	January 25, 2019	ALL	z/OS	ACF2	RACF	TSS	Description	ACF2	RACF	TSS
2	_							w/z/OS	w/z/OS	w/z/OS
3	TOTAL # of PDIs	529	139	219	237	260	Total Vulnerabilities by Targets	358		
4	TOTAL # of PDIs for Automation	511	124	217	236	260	Total Vulnerabilities that can be automated	341	360	384
5	TOTAL # of PDIs Automated	368	87	148	172	180	Currently automated	235	259	267
6	Cat I	44	23	6	7	16		29	30	39
7	Cat II	468	110	206	228	242		316	338	352
8	Cat III	17	6	7	2	2		13	8	8
9	% TOTAL Automation	96.60%	89.21%	99.09%	99.58%	100.00%	% of Vulnerabilities that can be automated	95.25%	95.74%	96.24%
10	% TOTAL Automated	69.57%	62.59%				% of Vulnerabilities currently automated	65.64%	68.88%	
11	Total Checks	619	172	265	290		Total number of Checks in all vulnerabilities	437	462	479
12	Checks to be Automated	599	157	263	287		Total number of Checks that can be automated	420	444	464
13	Checks That Cannot Be Automated	20	15	2	3		Total number of Checks that cannot be automated	17	18	15
	% Checks to Be Automated	96.77%	91.28%		98.97%	100.00%		96.11%		
	# Checks to PDI	1.17013	1.23741	1.21005	1.22363	1.18077		1.22067	1.22872	1.20050
16										
17	Checks with Automation Scripts	443	114	189	217	222		303	331	336
18	% Checks with Automation Scripts	73.96%	72.61%			72.31%		72.14%		
19	% Checks Automated	71.57%	66.28%		74.83%	72.31%		69.34%		
20	Checks Needing Automation Scripts	156	43	74	70	85		117	113	128
	% Checks Needing Automation Scripts	26.04%	27.39%	28.14%	24.39%	27.69%		27.86%	25.45%	27.59%
21										
22										

STIGs are a mature framework to improved security posture



Characterizing the STIGs a little more deeply, they:

	ARE	ARE NOT
>	Configuration Assessment and Tracking Tool	NOT - Activity or change monitoring or logging or SIEM tool
	Semi-automated	NOT – 100% turn key/plug n' play
	Available publicly – online, a DoD product	NOT – Proprietary (some add-on components are "classified" (FOUO))
	Linked to NIST standards	NOT – One-off opinions
	Framed in cybersecurity, risk-reduction terms	NOT – Expressed in exclusive sysprog terms
	Complemented by several cyber tools	NOT - Isolated
	Created and maintained to meet DoD needs	NOT – Representing all possible System/z products
	Mature and widely-used across US government	NOT – Newly invented (first STIGs were created in 1998)
⇒	A detailed collection of over 300 mainframe configuration standards/cyber-risk controls	NOT – Conceptual or ethereal

STIGs are a mature framework to improved security posture – why?



STIGS – WHAT, <u>WHY</u> AND HOW



Why Configuration Management? Why now? Specifically, WHY STIGs?

Threat

Mainframe hacks are unheard of – right? – nobody hacks the mainframe.

Our mainframe is "secure".

Mainframe data stays on the mainframe, so there is no likelihood of loss.

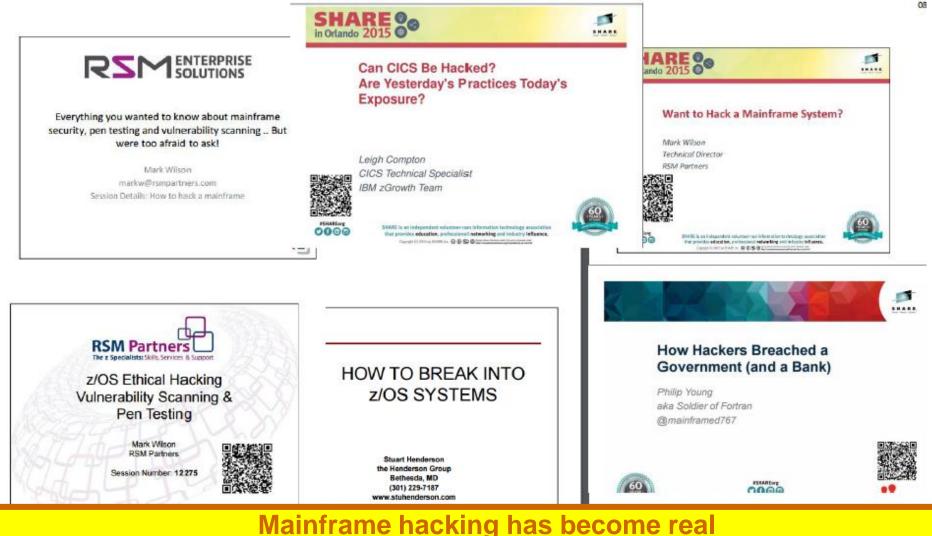
The mainframe has been in place so long, all needed controls have already been identified and addressed.

The mainframe is surrounded by firewalls – it's totally safe.

But – what are we actually seeing?

SHARE EDUCATE + NETWORK + INFLUENCE

Why Configuration Management? Why now? Specifically, WHY STIGs?





STIGs - Why Why Configuration Management? Why now? Specifically, WHY STIGs?



Philip Young - Smashing the Mainframe for Fun and Prison Time

hacktivity 1 year ago + 6.856 views

https://www.hacktivity.com In early 2012 a hacker was walking through the ro security controls of an IBM mainframe in ...



Shirobon - Hack The Mainframe Ambient Light Music

1 year ago + 1,580 views



MainframeNews.net - Bsecure - Mainframe hacked English 1 MainframeNewsnet 5 years ago + 3,938 views Bsecure The Mainframe and Security Company shares a webcast in which he demonstrates the ease with which an unprivileged ...



t218 Hacking Mainframes Vulnerabilities in applications exposed TN3270 Dominic White

Adrian Crenshaw 1 year ago • 3,361 views These are the videos from DerbyCon 4: http://www.irongeek.com/i.php? page=videos/derbycon4/mainlist.



An Ode to Movie Mainframes Slacktory 3 years ago + 163.524 views

3 years ago + 163,524 views Edited by Alex Moschina: http://alexmoschina.wordpress.com/ Featured filr GoldenEye Alien: Resurrection The Net Iron Man 2 ...

-	1			T	
m		100	Tiere **		
					4-46
					4:4/

Hacking the Mainframe

LordMoonstone 4 years ago • 3,492 views ping scholastic.com I'm in! Hacks: [ON] What am I gonna do with all the packing peanuts?



Tutorial How to Hack the Mainframe

TmarTnő 3 years ago • 7,025 views Link to Accelerate program http://www.mediafire.com/?24kq16gwplz071n DON'T FORGET TO COMMENT <u>BATE AND</u>



HACKING the MA

2 years ago + 32,878

Prescriptive hacking info is readily available –mainframe security is no longer a mystery



0

Why Configuration Management? Why now? Specifically, WHY STIGs?





Why Configuration Management? Why now? Specifically, WHY STIGs?

- Unix usage (Java, FTP, TCP/IP, other) increasing
- Direct data base connections increasing
- Mobile connections increasing
- Increasing 3rd Party partner connections increasing
- Cloud connections increasing
- Better hacker awareness, technology and skill (SET command for mainframes, MF Sniffer(python), NMAP, VTAM walker, John the Ripper, Metasploit... all for mainframe!)
- Quantum computing emerging as a powerful brute force attack weapon
- Increased dependency on electronic record (e.g., digital ledger with blockchain)
- Increased use of Open Source in applications—Thirty free Open Source Languages and Tools for z/OS. Mainframe coding made easy! These open source languages and tools enable anyone to program a mainframe (August 11, 2016)
- Increased diversity in connection methods

STIGs form a mature, practical Cybersecurity tool



Why Configuration Management? Why now? Specifically, WHY STIGs?

Why STIGs?	Why STIGs?	Why STIGs?
DISA and DoD sponsorship – robust, repeatable, mature and maintained by version to keep pace with new defense levels for new technology	Produces auditable evidentiary documentation and built-in metrics for leadership, auditors and business partners	Can filter by selected STIGs to align with tactical and strategic goals (e.g., red team/blue team exercises, audits, assessments, new technology, etc.)
Follows well-known and accepted NIST principles	Can be easily augmented by a range of complementary commercial tools	Provides prescriptive fixes
Can be scaled to meet higher priority needs – not monolithic	Produces summary-level and detailed progress tracking	Potential extension development (SCAP tool – future, event monitoring threads)
Can filter by NIST family	It's "free"	Provides prescriptive tests
Can filter by CAT I, II or III risk levels	Can filter by mainframe product	Can be scaled based on risk appetite

STIGs form a mature, practical Cybersecurity tool



Characteristic	Benefit				
DISA and DoD sponsorship – robust, repeatable, mature	Regular updates to a robust method adapts to change				
Follows well-known and accepted NIST principles	NIST is well-accepted and forms the basis for many other standards				
Can be scaled to meet higher priority needs – not monolithic	Many filters and independent testing provide flexibility				
Can filter by NIST family	Can match to current strategic initiatives				
Can filter by CAT I, II or III risk levels	Maximize the benefit with risk-based prioritization				
Produces auditable evidentiary documentation and built-in metrics for leadership, auditors, regulators and business partners	Provides crucial, time-based evidence				
Can be easily augmented by a range of complementary commercial tools	Tools from CA, SDS, IBM, Vanguard can be integrated and monitors can be interfaced				
Produces summary-level and detailed progress tracking	Useful for creating impactful and efficient metrics				
It's "free"	Well, not really, but there is no license or maintenance fee				
Can filter by mainframe product	Useful for focus and for delegation, especially remediation				
Can filter by selected STIGs to align with tactical and strategic goals	³ Focus assessments in areas of current interest for immediate payback				
Provides prescriptive fixes	Findings and corrective actions for detected variances are precisely defined				
Potential extension development (e.g., SCAP tool – future)	Watch this space for additional XML based automation in the future				
Provides prescriptive tests	Determination criteria for findings are precisely defined				
Can be scaled based on risk appetite	Organization risk appetites can vary across time and organization				
Copyright© by SHARE Association Except where otherwise noted, this work is licensed under a	Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/				



STIGS – WHAT, WHY AND <u>HOW</u>



Prepare

- What is your org's business case? Urgency? Strategic fit?
- 2. What org cultural parameters are in effect?
- 3. What will be required of your executive sponsor?

Propose

- 1. Justify
- 2. Risk/Risk Appetite
- 3. Cost
- 4. Timing
- 5. Align with Company goals
- 6. Agree on indeterminate results
- 7. Agree on scope, schedule & metrics

Play

- 1. Learning Curve
- 2. DISA/STIGs content and tools
- 3. Project documentation
- 4. Complementary tools
- 5. Sandbox vs Change Control

Produce Results

- 1. Advertise early successes
- 2. Adjust from early failures
- 3. Process and Tool Tuning
- 4. Iteration
- 5. Sandbox vs Change Control

Plan

- 1. Scope
- 2. Priority
- 3. Staffing/Capacity/Schedule
- 4. Separating Assessment from Remediation

Prevent

- 1. Real time monitoring/detection
- 2. Update Standards
- 3.

Let's Examine Each Step



Prepare

- 1. What is your org's business case? Urgency? Strategic fit?
 - The business case must explain why but a solid business case is essential to "how"
- 2. What org cultural parameters are in effect?
 - Big/small, mature/emerging, disciplined/free-form
 - Good/bad fit, existing processes
 - Metrics, SLAs, funding, budgets, tool interfaces, tool overlap, skills, resources
- 3. What will be required of your executive sponsor?

Hint: The Executive Sponsor will be essential in coordinating cross-department resource allocation. This type of resource allocation is particularly prevalent during remediation of assessment findings

When fully prepared, you will be able to express the value of STIGs to any audience in your organization



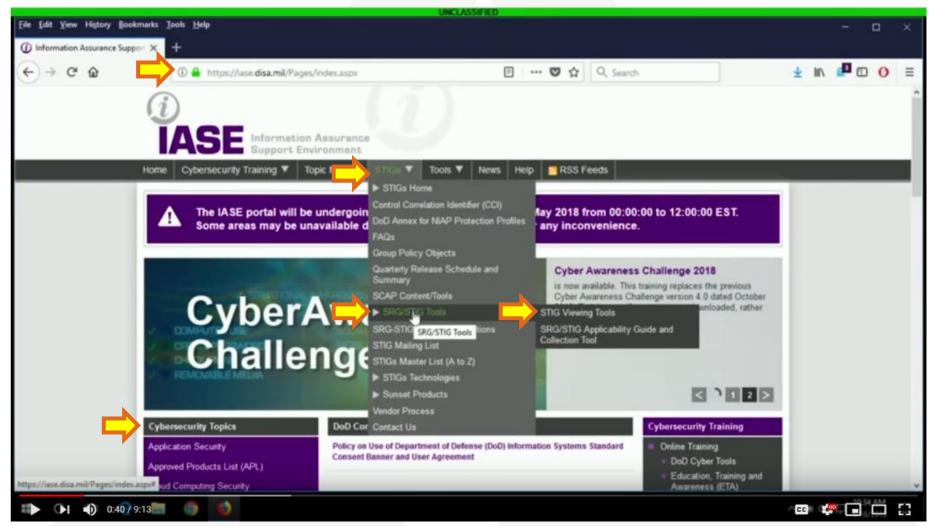
Play

- 1. Learning Curve download a viewer, download the current STIGs, read the STIGs, set up to accommodate quick iterations and practice
- 2. DISA/STIGs content and tools import and export files so you can manipulate the data, archive and retrieve results effectively
- 3. Project documentation is there an organizationally-prescribed format, or multiples depending on the audience? Consider collect/store/retrieve/archive
 - 4. Complementary tools how will you interface/integrate the STIGs with existing risk controls? Can you save time with additional tools by automation?
- 5. Sandbox vs Change Control where will you play? where will you produce "auditable" results? Keep them separated!

Become Familiar with the Concepts, Terminology and Tools by Playing. You Need and Deserve the Chance to Become an Expert



Play – Download a viewer and the current STIGs





Play – Download a viewer and the current STIGs

le Edit Yiew Higtory Bor	okmarks Tools Help		UNCLASSIFIED					
) STIG Viewer	× +							
€ → ℃ @	🕐 🔒 https://ase. disa.mil /stigs/Pag	es/stig-viewing-guidan	ce.aspx	··· 🛡 🕁 🔍	Search	li/ 🗗	0 0	=
	*PKI = DoD PKI Certificate Required XCCDF formatted SRGs and STIGs are inter a Target of Evaluation (TOE). As such, gettin content is not as easy as opening a .doc or are tools which can be used to view the STIG	ng to the content of a XCC pdf file and reading it. Th	CDF formatted STIG to re the process can be a little	ad and understand the confusing and trying. Below	Cloud Computing Security Control Correlation Identifier (CCI) DoD Annex for NIAP Protection Profiles FAQs Group Policy Objects			*
	How to View SRGs and STIGs	P	<i>6</i> 1		Quarterly Release Schedule and			
	Download How to View SRGs and STIGs	Date 8/29/2016	Size 80 KB	Format DOCX	Summary SCAP Content/Tools			
	STIG Viewer				* SRG/STIG Tools			
	Download	Date	Size	Format	SRG-STIG Library Compilations			
	STIG Viewer 2.x User Guide	3/21/2017	993 KB	PDF	STIG Mailing List			
	STIG Viewer Version 2.7.1	5/9/2018	697 KB	ZIP	STIGs Master List (A to Z)			
	STIG Viewer Version 2-4 Change Log	5/9/2018	41 KB	PDF	STIGs Technologies			
	STIG Viewer Version 2.7.1 Hashes	5/9/2018	1 KB	TOT	Sunset Products Vendor Process			
	Stylesheets Sorted by STIG ID				Contact Us			
	Download	Date	Size	Format				
	STIG Sorted by STIG ID	3/30/2015	105 KB	XSL.				
	STIG Sorted by STIG ID - FOUO *PHI	3/30/2015	105 KB	XSL				
	Stylesheets Sorted by Vulnerability	ID						
	Download	Date	Size	Format				
	STIG Sorted by Vulnerability ID	3/30/201	15 102 KB	XSL.				
secontent.disa.mil/stigs/zip/U	STIG Context by Vulnerability ID - FOUO *PRI STIGViewer-2.7.1.aip	3/30/20	15 105 KB	XSL				~
🕩 🕩 🜒 0:49)	9:13 📷 🌀 🚯				Ä	cc 🦑 🗖	317 AM	83

Current library version (02/08/2019) is V6R39), current viewer version (April, 2019) is 2.9

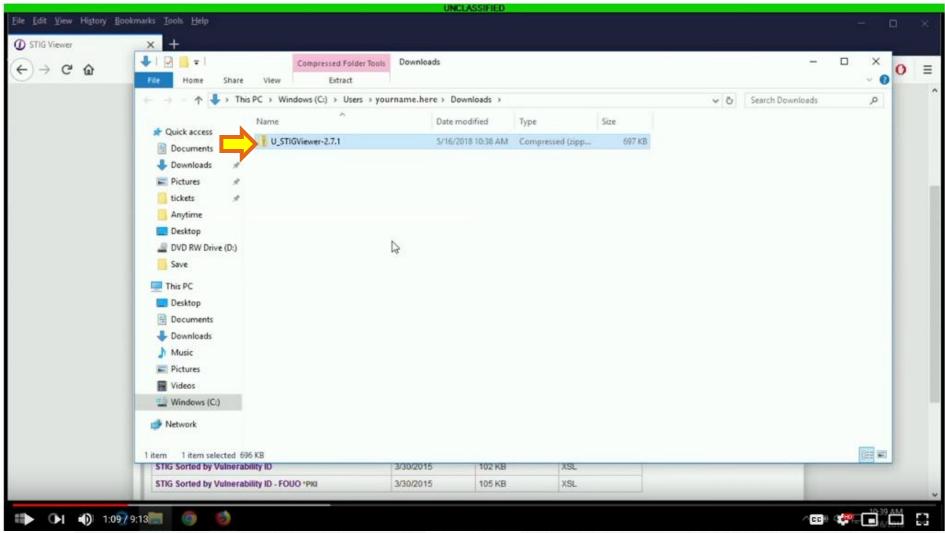


Play – Download a viewer and the current STIGs

le Edit Yiew History Boo	kmarks Iools Help					- D (
D STIG Viewer	× +					
€ → ℃ @	🛈 🔒 https://iase.disa.mil/stig	gs/Pages/stig-viewing-guida	nce.aspx	··· 🛡 🏠	7 Q. Search	lii\ 🔎 🗊 🚺
	*PKI = DoD PKI Certificate Required XCCDF formatted SRGs and STIGs at a Target of Evaluation (TOE). As such content is not as easy as opening a are tools which can be used to view th How to View SRGs and STIGs	, getting to the content of a X0 doc or .pdf file and reading it.	CDF formatted STIG to r The process can be a littl	read and understand the e confusing and trying.	DoD Annex for NIAP Protection	
	Download	Date	Size	Format	Quarterly Release Schedule and Summary	
	How to View SRGs and STIGs	8/29/2016	80 KB	DOCX	SCAP Content/Tools	
	Download STIG Viewer 2.x User Guide STIG Viewer Version 2. STIG Viewer Version 2.7.1 Chang STIG Viewer Version 2.7.1 Hashe	ening U_STIGViewer-2.7.1.zip u have chosen to open: U_STIGViewer-2.7.1.zip which is: Compressed (zipped from: https://iasecontent.diss /hat should Firefox do with this fi O_Qpen with Windows Exple Save File Do this gutomatically for file	umil le? vrer (default)	× iat	SRG/STIG Tools SRG-STIG Library Compilations STIG Mailing List STIGs Master List (A to Z) STIGs Technologies Sunset Products Vendor Process Contact Us	
	Stylesheets Sorted by Vuli Download	1-10000	٩٤	Cancel		
	STIG Sorted by Vulnerability ID STIG Sorted by Vulnerability ID - FOUO	3/30/2		XSL		
	Stas Sorted by Vulnerability ID - FOUO	*PKI 3/30/2	015 105 KB	XSL		



Play – Download a viewer and the current STIGs





Play – Download a viewer and the current STIGs

File Home Share	View								
← → - ↑ ■ > This PC > Desktop >									
Cuick access Comments Commen	Name desktop STIGViewer-2.7.1 U_Windows_10_V1R13_STIG	Date modified 5/16/2018 9:15 AM 4/10/2018 3:32 PM 5/16/2018 9:35 AM	Type File folder Executable Jar File Compressed (zipp	Size 733 KB 606 KB					
 Pictures Videos Windows (C:) 			G						



Findings (MAC III - Administrative Sensitive)

Severity Title LOGONIDs must not be defined to SYS1.UADS for n SYS1.UADS is a dataset where LOGONIDs will be maintained with applicable password information when the ACP is not functional. If an unauthorized user

on-emergency use.

Description

Q

z/OS RACF STIG

UCF STIG

STIGs - How

DOD 8500

NIST 800-53

Overview

Finding

ID V-184

HOME STIGS

Version	Date	Finding Count (234)				Downloads		
None	2018-04-04 🔽	CAT I (High): 29	CAT II (Med): 196	CAT III (Low): 9	Excel 🕑	JSON 🕒	XML 🕑	
STIG Des	STIG Description							
None								
Availabl	le Profiles 🔽							

COMMON CONTROLS HUB

id	severity	title	description	iacontrols	ruleID	fixid	fixtext	checkid	checktext
V-3899	medium	The	SAF resource	None	SV-7265r2	F-18794r1	There are	C-3261r1_	a)Refer to the
V-3898	medium	HFS object	HFS directori	['DCCS-1', 'DC	SV-3898r2	F-18956r1	Review	C-20978r1	a)Refer to the
V-6919	medium	JES2 input	JES2 input so	None	SV-7323r2	F-18545r1	Review	C-20612r1	a)Refer to the
V-6918	medium	RJE works	JES2 RJE work	['DCCS-1', 'DC	SV-7318r2	F-6627r1_	Ensure	C-3304r1_	a)Refer to the
V-184	high	LOGONID	SYS1.UADS is	['DCCS-1', 'DC	SV-184r3	F-18939r1	The system	C-20973r1	a)Refer to the
V-6916	medium	RJE works	JES2 RJE work	['DCCS-1', 'DC	SV-7314r2	F-18597r1	RJE	C-20669r1	RJE Userids
V-3897	medium	MVS data	MVS data set	['DCCS-1', 'DC	SV-3897r2	F-26597r1	The IAO	C-3258r1_	a)Refer to the
V-3896	low	SYS(x).Pa	Configuration	['DCCS-1', 'DC	SV-3896r2	F-18937r1	Review	C-3414r1_	
V-269	medium	The JES(XI	(RACF0400:	['DCCS-1', 'DC	SV-269r2_	F-17173r1	The IAO	C-17935r1	a)Refer to the
V 60001	high	The COURT	Use of weak	Mana	C1/ 000ED	F 75061-1	Editthe	C 70037-1	Locato the CCU

https://www.stigviewer.com/

Play – Download a viewer and the current STIGs (JAVA issues)

Search...

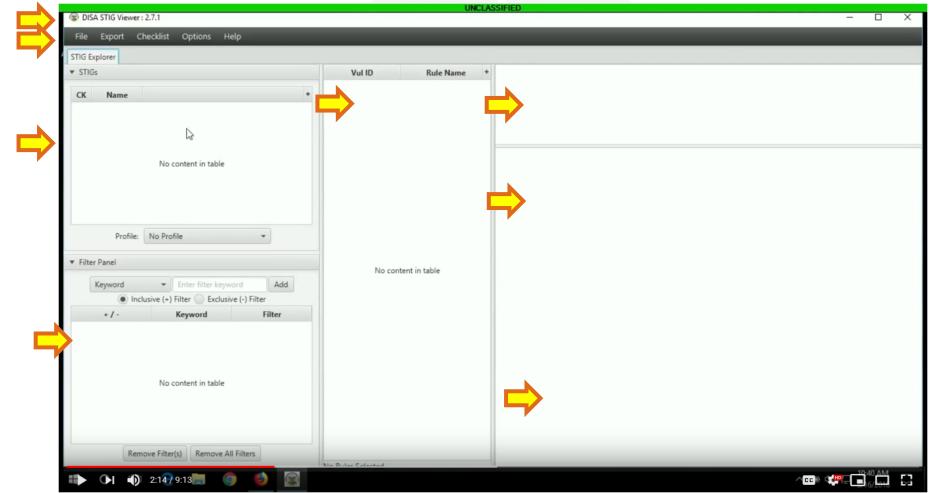
ABOUT







Play – Download a viewer and the current STIGs





Play – Download a viewer and the current STIGs

IASE Information Assurance Support Environment

Home Cybersecurity Training ▼ Topic Map ▼ STIGs ▼ Tools ▼ News Help 📉 RSS Feeds	s ▼ Tools ▼ News Help 🔂 RSS Feeds
---	---

Home > STIGs > Compilations

SRG-STIG Library Compilations

*PKI = DoD PKI Certificate Required

The SRG-STIG Library Compilation .zip files are compil Technical Implementation Guides (STIGs), Security Rea well as some other content that may be available throug

The Library Compilation .zip files will be updated and re capture all newly updated or released SRGs, STIGs, an individually downloadable from IASE as released. This c Compilation.

Two versions of the Library Compilation are produced, a

The file name preceded by FOUO_ is the FOUO versior designated as DoD sensitive information and therefore r general distribution under the Freedom of Information A The file name preceded by U_ is the NON-FOUO versio general public. These compilations may be used and di documents. The FOUO compilation as a whole and any customary FOUO handling and dissemination guideline See 'SRG-STIG Library Compilation READ ME' for more information to include download / extraction instructions, a FAQ, and a notice about access to the FOUO compilation by non-CAC holders.

NOTE: While every attempt will be made to provide a complete set of 'currently in force' SRGs, STIGs, and related tools, DISA makes no guarantee as to the completeness of the compilation or the "currently in force" status of the contents.

NOTE: While every attempt will be made to publish updated compilation files on the SRG-STIG Quarterly Update Release date, publication may lag due to competing workloads. Updated Compilation files will be published on or as soon as possible the published date. We apologize for any inconvenience this may impose.

Concerns or questions related to the contents or format of these compilation files should be directed to the DISA STIG Customer Support Desk at disa.stig_spt@mail.mil

SRG-STIG Library Compilation files for download

ł	Download	Date	Size	Format
⇒	Compilation - SRG-STIG Library - FOUO *PKI	1/28/2019	220 MB	ZIP
	Compilation - SRG-STIG Library - NON-FOUO	1/28/2019	205 MB	ZIP
	Compilation - SRG-STIG Library - READ ME	11/10/2016	34 KB	PDF

See 'SRG-STIG Library Compilation READ ME' for more information to include download / extraction instructions, a FAQ, and a notice about access to the FOUO compilation by non-CAC holders.





Play – Download a viewer and the current STIGs

 Control - Discription - Control - Discription - Control - Discription - Discripti - Discription - Discription - Discripti - Discripti - Discrip		
 U_SRG-STIG_Library_2019_01 U_ZOS_BMC_CONTROL-D_for_RACF_V6R7_Manual_STIG U_ZOS_BMC_CONTROL-M_for_RACF_V6R8_Manual_STIG U_ZOS_BMC_CONTROL-O_for_RACF_V6R7_Manual_STIG U_ZOS_BMC_CONTROL-O_for_RACF_V6R7_Manual_STIG U_ZOS_BMC_IOA_for_RACF_V6R7_Manual_STIG U_ZOS_BMC_MAINVIEW_for_ZOS_for_RACF_V6R6_Manual_STIG U_ZOS_CA_1_Tape_Management_for_RACF_V6R6_Manual_STIG U_ZOS_CA_Common_Services_for_RACF_V6R3_Manual_STIG U_ZOS_CA_Common_Services_for_RACF_V6R2_Manual_STIG U_ZOS_CA_MIICS_for_RACF_V6R3_Manual_STIG U_ZOS_CA_MIIM_for_RACF_V6R3_Manual_STIG U_ZOS_SRAUDIT_for_RACF_V6R4_Manual_STIG 	✓ [™] Search U_z	zOS_RACF_V6R39_M 🔎
 U_zOS_BMC_CONTROL-M_for_RACF_V6R8_Manual_STIG U_zOS_BMC_CONTROL-M_Restart_for_RACF_V6R5_Manual_STIG U_zOS_BMC_CONTROL-O_for_RACF_V6R7_Manual_STIG U_zOS_BMC_IOA_for_RACF_V6R7_Manual_STIG U_zOS_BMC_MAINVIEW_for_zOS_for_RACF_V6R7_Manual_STIG U_zOS_CA_1_Tape_Management_for_RACF_V6R6_Manual_STIG U_zOS_CA_Auditor_for_RACF_V6R3_Manual_STIG U_zOS_CA_Common_Services_for_RACF_V6R2_Manual_STIG U_zOS_CA_MICS_for_RACF_V6R3_Manual_STIG U_zOS_CA_MICS_for_RACF_V6R3_Manual_STIG U_zOS_CA_MIM_for_RACF_V6R3_Manual_STIG U_zOS_CA_MIM_for_RACF_V6R3_Manual_STIG U_zOS_CA_MIM_for_RACF_V6R3_Manual_STIG U_zOS_SRRAUDIT_for_RACF_V6R4_Manual_STIG U_zOS_SRRAUDIT_for_RACF_V6R4_Manual_STIG 	Туре	Compressed size
 U_zOS_CA_1_Tape_Management_for_RACF_V6R6_Manual_STIG U_zOS_CA_Auditor_for_RACF_V6R3_Manual_STIG U_zOS_CA_Common_Services_for_RACF_V6R2_Manual_STIG U_zOS_CA_MICS_for_RACF_V6R3_Manual_STIG U_zOS_CA_MIM_for_RACF_V6R3_Manual_STIG U_zOS_CA_MIM_for_RACF_V6R3_Manual_STIG U_zOS_CA_MIM_for_RACF_V6R3_Manual_STIG U_zOS_CA_MIM_for_RACF_V6R3_Manual_STIG U_zOS_RACF_V6R3P_Manual_STIG U_zOS_RACF_V6R3P_Manual_STIG U_zOS_RACF_V6R3P_Manual_STIG U_zOS_RACF_V6R3P_Manual_STIG 	JPG File XSL Stylesheet NI XML Document	112 KB 10 KB 138 KB
U_zOS_Catalog_Solutions_for_RACF_V6R4_Manual_STIG U_zOS_CLSuperSession_for_RACF_V6R10_Manual_STIG	IG File Export 25 Trit Tri	fiewer : 2.8 : STIG Explorer t Checklist Options Help



Play – Download a viewer and the current STIGs

File Export Checklist Options Help	_	_						
STIG Explorer								
r STIGs	Vul ID	Rule Name	* z/OS RACF STIG :: Version 6, Release: 39 Benchmark	Date: 25 Jan 2019				
CK Name	+ V-7545	AAMV0012	Vul ID: V-7545 Rule ID: SV-8016r3_rule STIG ID	D: AAMV0012				
✓ z/OS RACF STIG	-7491	RACF0248	Severity: CAT I Classification: Unclass					
	V-254	RACF0250		Automated Analysis				
	V-255	RACF0260	Group Title: AAMV0012	Refer to the following report produced by the z/OS Data Collection:				
	V-257	RACF0280	Rule Title: Unsupported system software is installed and	- PDI(AAMV0012)				
	V-258	RACF0290	system.					
	V-260	RACF0310	Discussion: When a vender drops support of System Sel	If the software products currently running on the reviewed system are at a				
	V-261	RACF0320	longer maintain security vulnerability patches to the soft	Version greater than or equal to the products listed in the vendor's Support				
	V-262	RACF0330	vulnerability patches, it is impossible to verify that the sy					
	V-265	RACF0350	contain code which could violate the integrity of the ope environment.	Fix Text: For all products that meet the following criteria:				
	V-266	RACF0370	Check Text: This check applies to all products that meet	Uses sutherized and sectorsted a /OC interfaces husutilizing Authorized				
	V-267	RACF0380	criteria:	 Uses authorized and restricted z/OS interfaces by utilizing Authorized Program Facility (APF) authorized modules or libraries. 				
	V-269	RACF0400		 Require access to system datasets or sensitive information or requires special or privileged authority to run. 				
	V-270	RACF0420	 Uses authorized and restricted z/OS interfaces by utiliz Program Facility (APF) authorized modules or libraries. 					
Profile: No Profile 👻	V-271	RACF0430	- Require access to system datasets or sensitive information	The ISSO will ensure that unsupported system software for the products in the above category is removed or upgraded prior to a vendor dropping				
 Filter Panel 	V-272	RACF0440	special or privileged authority to run.					
	V-273	RACF0450	For the products in the above category refer to the Vend					
Must match: All Any Keyword Character filter keyword	V-3900	ZWAS0040	lifecycle information for current versions and releases. The should be added to the Vulnerability Questions within the value of the Vulnerability Questions within the value o					
Inclusive (+) Filter Exclusive (-) Filter			Management document for supported software product					
+/- 🔺 Keyword Filter			Automated Analysis					
· CATI V								



Play – Download a viewer and the current STIGs

	and the second second second second	STIG Explorer *New Checklist ×					
File C	Checklist Options Help	▼ Totals		Status	Vul ID	Rule Name	+ Status: Not Reviewed - Severity Override: CAT II -
	Open Checklist from File	Overall Totals CAT I CAT II CA	AT III	NR	V-31	ZSMS0010	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019
Create Shecklist - Check Marked STIG(s)		Not Reviewed: 234	NR	V-34	AAMV0450	Vul ID: V-31 Rule ID: SV-7355r4_rule STIG ID: ZSMS0010	
CK Name		Open: 0 Not a Finding: 0		NR	V-36	ACP00270	Severity: CAT II Classification: Unclass
				NR	V-44	ZCIC0040	
				NR	V-54	ZJES0060	
				NR	V-82	AAMV0010	
				NR	V-83	AAMV0030	
				NR	V-84	AAMV0040	Rule Title: DFSMS resources must be protected in accordance with the proper security
				NR	V-85	AAMV0050	requirements.
				NR	V-86	AAMV0060	Discussion: DFSMS provides data, storage, program, and device management functions
							Discussion. Di sivis provides data, storage, program, and device management functions
				NR	V-90	AAMV0160	the operating system. Some DFSMS storage administration functions allow a user to obta
				NR NR	V-90 V-100	AAMV0160 AAMV0350	privileged status and effectively bypass all ACP data set and volume controls. Failure to
							privileged status and effectively bypass all ACP data set and volume controls. Failure to
				NR	V-100	AAMV0350	privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could
				NR NR	V-100 V-101	AAMV0350 AAMV0370	privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system
				NR NR NR	V-100 V-101 V-102	AAMV0350 AAMV0370 AAMV0380	privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data.
INK	V-122	ACPOUTTO		NR NR NR NR	V-100 V-101 V-102 V-103	AAMV0350 AAMV0370 AAMV0380 AAMV0400	privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure coul compromise the availability and integrity of the operating system environment, system services, and customer data. Check Text: Refer to the following report produced by the Data Set and Resource Data
-				NR NR NR NR	V-100 V-101 V-102 V-103 V-104	AAMV0350 AAMV0370 AAMV0380 AAMV0400 AAMV0410	 privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data. Check Text: Refer to the following report produced by the Data Set and Resource Data Collection: SENSITVE.RPT(ZSMS0010)
NR	V-122 V-123	ACP00170 ACP00180		NR NR NR NR NR	V-100 V-101 V-102 V-103 V-104 V-105	AAMV0350 AAMV0370 AAMV0380 AAMV0400 AAMV0410 AAMV0420	privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data. Check Text: Refer to the following report produced by the Data Set and Resource Data Collection:
NR	V-123	ACP00180	Comm	NR NR NR NR NR NR NR	V-100 V-101 V-102 V-103 V-103 V-104 V-105 V-106	AAMV0350 AAMV0370 AAMV0380 AAMV0400 AAMV0410 AAMV0420 AAMV0430	 privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data. Check Text: Refer to the following report produced by the Data Set and Resource Data Collection: SENSITVE.RPT(ZSMS0010) Automated Analysis Refer to the following report produced by the Data Set and Resource Data Collection:
-			Comm	NR NR NR NR NR NR NR NR	V-100 V-101 V-102 V-103 V-104 V-104 V-105 V-106 V-107	AAMV0350 AAMV0370 AAMV0380 AAMV0400 AAMV0410 AAMV0420 AAMV0430 AAMV0440	 privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data. Check Text: Refer to the following report produced by the Data Set and Resource Data Collection: SENSITVE.RPT(ZSMS0010) Automated Analysis
NR	V-123	ACP00180	Comm	NR NR NR NR NR NR NR NR NR	V-100 V-101 V-102 V-103 V-104 V-105 V-105 V-106 V-107 V-108	AAMV0350 AAMV0370 AAMV0380 AAMV0400 AAMV0410 AAMV0420 AAMV0430 AAMV0440 AAMV0410	 privileged status and effectively bypass all ACP data set and volume controls. Failure to properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data. Check Text: Refer to the following report produced by the Data Set and Resource Data Collection: SENSITVE.RPT(ZSMS0010) Automated Analysis Refer to the following report produced by the Data Set and Resource Data Collection: PDI(ZSMS0010) Ensure that all SMS resources and/or generic equivalent are properly protected according
NR NR	V-123	ACP00180	Comm	NR NR NR NR NR NR NR NR NR NR NR	V-100 V-101 V-102 V-103 V-104 V-105 V-105 V-106 V-107 V-108 V-108 V-109	AAMV0350 AAMV0370 AAMV0380 AAMV0400 AAMV0410 AAMV0420 AAMV0430 AAMV0440 AAMV0400 AAMV0420 AAMV0430 AAMV0440 AAMV0420 AAMV0420 AAMV0420 AAMV0420 AAMV0420 AAMV0420 AAMV0420 AAMV0420	 properly protect DFSMS resources may result in unauthorized access. This exposure could compromise the availability and integrity of the operating system environment, system services, and customer data. Check Text: Refer to the following report produced by the Data Set and Resource Data Collection: SENSITVE.RPT(ZSMS0010) Automated Analysis Refer to the following report produced by the Data Set and Resource Data Collection:

۲



File Import Export Options			File Import Export Options	_					
STIG			STIG Explorer *New Checklist ×						
▼ Totals	Status		▼ Totals	Status	Vul ID	Rule Na	me +		
Overall Totals CAT I CAT II CAT III	NR	V-	Overall Totals CAT I CAT II CAT III	NR	V-36	ACP00270			
Open: 0 Not Reviewed: 234 Not a Finding: 0 Not Applicable: 0	NR	V-	Open: 0 Not Reviewed: 29	NR	V-108	ACP00010			
	NR	V-	Not a Finding: 0 Not Applicable: 0	NR	V-110	ACP00030			
	NR	V-	Total: 29	NR	V-111	ACP00040			
	NR	V-		NR	V-112	ACP00050			
	NR	V-		NR	V-113	ACP00060			
	NR	V-		NR	V-114	ACP00070			
	NR	V-		NR	V-115	ACP00080			
	NR	V-		NR	V-116	ACP00100			
	NR	V-		NR	V-118	ACP00120			
	NR	V-		NR	V-119	ACP0013	II		
	NR	V-		NR	V-122	ACP0017	NR	V-69231	ZSSH0020
	NR	V-		NR	V-129	ACP0024	NR	V-71223	ACP00062
	NR	V-		NR	V-184	ZTSO002			
	NR	V-		NR	V-234	ACP0025			
	NR	V-		NR	V-276	RACF048			
Not Applicable Not Reviewed Not a Finding Open	NR	V-		NR	V-3900	ZWAS00			
Not Applicable Vot Kevlewed Vot a Finding Voten	NR	V-	Not Applicable In Not Reviewed In Not a Finding In Open	NR	V-6958	ZWMQ0			
	NR	V-	▶ Target Data	NR	V-6960	ZWMQ0	-		
	NR		► STIGs	NR	V-6970	ZUSS002			
▶ Target Data			 Technology Area 	NR	V-6972	ZUSS002			
▼ STIGs	NR	V-	 Filter Panel 	NR	V-6991	ZUSS004			
CK Name Score +	NR	V-		NR	V-7545	AAMV00	-		
✓ z/OS RACF STIG 0.0	NR	V-		NR	V-15209	AAMVO	Showing	rule 1 out of 29	
	NR	V-		NR	V-64803	RACF0465	showing		



Play – Download a viewer and the current STIGs

DISA STIG Viewer: 2.8: *New Checklist								
File Import Export Options					DISA STIG Viewer : 2.8 : *New Checklist			
STIG Explorer *New Checklist ×					File Import Export Options			
▼ Totals	Status	s Vul ID	Rule Name	Status: Not Reviewed - Severity C	STIG Explorer *New Checklist ×			
Overall Totals CAT I CAT II CAT III	NR		ACP00270	z/OS RACF STIG :: Version	▼ Totals	Status	Vul ID	R
Open: 0 Not Reviewed: 29		et Status P Open	P00010	Vul ID: V-36 Rule	Overall Totals CAT I CAT II CAT III	->0	V-36	ACP002
Not a Finding: 0 Not Applicable: 0	NR	elect All Not Applic	P00030	Severity: CAT I Class		NR	V-108	ACP000
Total: 29	NR -	Not Review	P00040		Open: 1 Not Reviewed: 26	NR	V-110	ACPOOD
	NR	V-112	ACP00050		Not a Finding: 1 Not Applicable: 1 Total: 29			
	NR	V-113	ACP00060			NR	V-111	
	NR	V-114	ACP00070			NF	V-112	ACP002 ACP000 ACP000 ACP000 ACP000 ACP000 ACP000 ACP001 ACP001 ACP001 ACP001 ACP001 ACP001 ACP001 ACP002 XTS000 ACP002 XTS000 ACP002 XTS000 XCP002 XWAQ0 ZWMQ0 ZUSS00
	NR	V-115	ACP00080	Rule Title: Dynamic lists must be pro		NR	V-113	
	NR	V-116	ACP00100	Kule File. Dynamic lists must be pro		NR	V-114	ACP000
	NR	V-118	ACP00120	Discussion: Dynamic lists provide a n interrupting the availability of the ope		NR	V-115	ACP000
	NR	V-119	ACP00130	facilities could result in unauthorized		NR	V-113 ACP000 V-114 ACP000 V-115 ACP000 V-116 ACP001 V-118 ACP001 V-119 ACP001	
	NR V-113 ACF00130 NR V-122 ACP00170 NR V-129 ACP00240	V-122	ACP00170	may threaten the integrity and availa		NR		
		ACP00240	compromise the confidentiality of cus					
	NR	V-184	21300020	Check Text: Refer to the following re		NR		
	NR V-234	V-234	ACP00250	Collection:		NA		ACP001
	NR	V-276	RACF0480	- SENSITVE.RPT(FACILITY)		NR	V-129	ACP002
	NR	V-3900	ZWAS0040	Automated Analysis		NR	V-184	ZTSO00
Not Applicable Not Reviewed Not a Finding Open	NR	V-6958	ZWMQ0011	Refer to the following report produce		NR	V-122 ACP001 R V-129 ACP002 R V-184 ZTSO00	
 Target Data 	NR	V-6960	ZWMQ0051	- PDI(ACP00270)		NR	V-276	ACP002 ACP000 ACP001 ACP001 ACP002 ZTSO00 ACP002 ZWAS04 ZWMQ4 ZWMQ4
► STIGs	NR	V-6970	ZUSS0022	- FDI(ACP00270)		NR	V-3900	
 Technology Area 	NR	V-6972	ZUSS0023	Verify that the accesses for CSV-prefi: guidance is true, this is not a finding.	Not Applicable Not Reviewed Not a Finding Open			
 Filter Panel 	NR	V-6991	ZUSS0046	guidance is true, this is not a multig.		NR	V-6958	
				The RACF resources and/or gener	Target Data	NR	V-6960	ZWMQ
					▶ STIGs	NR	V-6970	ZUSS00
					 Technology Area 	NID	V 6072	71 19900



Play – Read the STIGs, import and export files so you can manipulate the data, archive and retrieve results effectively

	terrete - Wester 1996		В	С	D		E	F
Eile Edit View History Boo	okmarks Tools Help	1 Column1	🕶 Column2	Column3	Column4	Column5		💌 Column6 💌
STIG Viewer	× +	2 Severity	Rule ID	STIG ID	Rule Title	STIG		Comments
	↓ I ⊇ = I Compresse	5 high	SV-6409r8_rule	ACP00270	Dynamic lists must be protected in accordance with proper security requirements.	z/OS RACF STIG :: Version 6, R	elease: 39 Benchmark Date: 25 Ja	an 2019
(←) → C* @		ed Folder Tools 22 high	SV-108r2_rule	ACP00010	SYS1.PARMLIB is not limited to only system programmers.	z/OS RACF STIG :: Version 6, R	elease: 39 Benchmark Date: 25 Ja	an 2019
\sim	File Home Share View E	high 24 high	SV-110r3_rule	ACP00030	Write or greater access to SYS1.SVCLIB must be limited to system programmers only.	z/OS RACF STIG :: Version 6, R	elease: 39 Benchmark Date: 25 Ja	an 2019
	+ + This PC - Windows (C-)	literr yournar 25 high	SV-111r4_rule	ACP00040	Write or greater access to SYS1.IMAGELIB must be limited to system programmers only.	z/OS RACF STIG :: Version 6, R	elease: 39 Benchmark Date: 25 Ja	an 2019
		26 high	SV-112r3_rule	ACP00050	Write or greater access to SYS1.LPALIB must be limited to system programmers only.	z/OS RACF STIG :: Version 6, R	elease: 39 Benchmark Date: 25 Ja	an 2019
	Cuick access	Compressed (Zipped no high	SV-113r2_rule	ACP00060	Update and allocate access to all APF -authorized libraries are not limited to system progra	nr z/OS RACF STIG :: Version 6, R	elease: 39 Benchmark Date: 25 Ja	an 2019
		28 nign	SV-114r3_rule	ACP00070	Write or greater access to all LPA libraries must be limited to system programmers only.		elease: 39 Benchmark Date: 25 Ja	
	🛅 Documents 💉 🔤	29 high	SV-115r3_rule	ACP00080	Write or greater access to SYS1.NUCLEUS must be limited to system programmers only.		elease: 39 Benchmark Date: 25 Ja	
	Downloads # Select a D	Destination and 30 high	SV-116r3_rule	ACP00100	Write or greater access to libraries that contain PPT modules must be limited to system pro			
	Fictures 🖈	32 high	SV-118r6_rule	ACP00120	The ACP security data sets and/or databases must be properly protected.		elease: 39 Benchmark Date: 25 Ja	
	DCKets #	extracted to this fold 33 high	SV-119r4_rule	ACP00130	Access greater than Read to the System Master Catalog must be limited to system program			
	Anytime C:\Users\yo	ourname.here\Dowr 36 high	SV-122r3_rule	ACP00170	Write or greater access to SYS1.UADS must be limited to system programmers only and rea			
	Parlana	43 high	SV-129r3_rule	ACP00240	Write or greater access to Libraries containing EXIT modules must be limited to system pro			
	Show ext	racted files when co 45 high	SV-184r3_rule	ZTSO0020	LOGONIDs must not be defined to SYS1.UADS for non-emergency use.		elease: 39 Benchmark Date: 25 Ja	
	DVD RW Drive (D:)	46 high	SV-234r3_rule	ACP00250	All system PROCLIB data sets must be limited to system programmers only		elease: 39 Benchmark Date: 25 Ja	
	Save	69 high	SV-276r3_rule		The PROTECTALL SETROPTS value specified must be properly set.		elease: 39 Benchmark Date: 25 Ja	
	This PC	129 high			Vendor-supplied user accounts for the WebSphere Application Server must be defined to			
		165 high	_		WebSphere MQ channel security must be implemented in accordance with security requir			
	Desktop	167 high	_		WebSphere MQ switch profiles must be properly defined to the MQADMIN class.		elease: 39 Benchmark Date: 25 Ja	
	Documents	177 high	SV-19746r3_rule		z/OS UNIX resources must be protected in accordance with security requirements.		elease: 39 Benchmark Date: 25 Ja	
		179 high	SV-19748r3_rule		z/OS UNIX SUPERUSER resource must be protected in accordance with guidelines.		elease: 39 Benchmark Date: 25 Ja	
	h Music	194 high	SV-7294r3_rule	20550046	UID(0) must be properly assigned.	Z/OS RACE STIG :: Version 6, R	elease: 39 Benchmark Date: 25 Ja	an 2019
	Pictures	211 high 214 high	Α		В		c c	D
	Videos	223 high	Column1 🔻	Column	a		🕶 Column3 🛛 🖵 Co	lumn4 💌 Colui
	Windows (C:)	224 high						
	Network	228 high 2	STIG ID	Rule Tit	le		Status Co	mments
	-	229 high 234 high 5	ACP00270	Dynami	c lists must be protected in accordance with proper security re	equirements.	Open	
	1 item 1 item selected 696 KB	26	ACP00050	Write o	r greater access to SYS1.LPALIB must be limited to system prog	grammers only.	Not A Finding	
	STIG Sorted by Vulnerability ID STIG Sorted by Vulnerability ID - FOUO *PKI	3/30/2015 3/30/2015 36	ACP00170	Write o	r greater access to SYS1.UADS must be limited to system prog	rammers only and rea	d Not Applicable	
	s no sorted by vulnerability iD - FOOO *PKI	20000010			<u> </u>	,		
		237						
1:38/	9:13 🔄 🌀 🛃	239						

Copyright® by SHARE Association Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/



Play - Project documentation – is there an organizationally-prescribed format, or multiples depending on the audience?

- Extract to spreadsheet and graphs
- Import data into presentation tool
- Import data into SIEM tool
- Other local options, perhaps different choices for different audiences

Determine what format and content of standard reporting will be required in your organization – Get agreement - Develop tool Interfaces as needed



Play - Complementary tools – how will you interface/integrate the STIGs with existing risk controls? Can you save time with additional tools by automation?

- STIGs are a compliance framework
- Many options exist to enhance documentation and archiving
- Each additional option will require attention:
 - Reports
 - Dashboards
 - Real Time Monitoring

Become Familiar with the Concepts, Terminology and Tools by Playing. You Need and Deserve the Chance to Become an Expert



Play - Sandbox vs Change Control – where will you play? – where will you produce "auditable" results? Keep them separated!

- Need a minimum of two environments production and development
 - Production reporting
 - Need archiving
 - Need auditability
 - Need standardization
 - Need replicability
 - May need specific additional security privileged tools, sensitive data
 - Development (play in the sandbox)
 - Need speed and flexibility

Become Familiar with the Concepts, Terminology and Tools by Playing. You Need and Deserve the Chance to Become an Expert

Copyright® by SHARE Association Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/



Plan

1. Scope

2. Priority factors to consider

Risk – H, M, L	High monetary impact	Timing
Daily loss by application	High customer impact	SOC2 or audit needs
Downstream critical apps	Compliance requirements	
Risk appetite	SLAs and penalties	
Target restriction times	Sensitive data	

- 3. Staffing/Capacity/Schedule
- 4. Separating Assessment from Remediation two distinct steps timing, skills, actors, actions, change controls

Focus finite resources, first, on the controls that are most important to your organization



Propose

- 1. Justify Need, benefit, cost, risk
- 2. Risk express appropriately for your organization

Maxin 90th Averag 10th Minim

Risk Ap

Capl

OpE

- 3. Cost suggest phases to avoid sticker shock
- 4. Timing Will leadership be receptive
- 5. Align with Company goals Security, resiliency, customer trust, compliance, business continuity
- 6. Agree on handling of indeterminate results process STIGs, more data needed, third party input
 - Agree on metrics measure results not activity, agree on definition of results both positive and negative (i.e., findings)

Treat Risk Using Methods That Fit Into Your Organization

		Potential Severity Rating								
		Minor	Moderate	Significant	Catastrophic					
Likelihood severity occurs	Very Likely	Moderate	High	Extreme	Extreme					
	Likely	Low	Moderate	High	Extreme					
elihood se	Unlikely	Very Low	Low	Moderate	High					
Like	Rare	Very Low	Very Low	Low	Moderate					

			<i>2</i> 1 1		æ		÷.	HIGH RISK S	STIG R	ULES CA	N BE SELECTED
imum	\$103.2M	4	e lar	25 120	our		Nº.	CITA ETD Viewer 2.1	-	_	1-1010
	-							He Esport Overslint Options Help-			
6 la 0/	\$56.9M							1832 Explorer			
th %	\$06.9M	E						+ 130a	Vel ID	Rule Norte	* Germi Intonetion
		- ¥						CK Name	* v-108	ACP00270 ACP00010	z/OS RACF STIG = Release: 24 Benchmark Date: 24
	000.014							arOS IBM System Display and Search Facility (SDD) for ACF2	v-110	ACP00030	Jul 2015
age	\$36.8M	1 2 1	Y					 arDS IBM System Display and Search Facility (SDS7) for RACE. 	v-110 v-111	ACP00040	Rule Title: Dynamic lists must be protected in accordance
-	+	<u></u>						2/05 BM System Display and Search Facility (SDSP) for TSS 5	9-112	K20050	with proper security requirements.
		ā	/					POSICIFIC ROP ACTION	v-113	AC700360	STIG ID: ACP00270 Severity: CAT I
th %	\$19.6M	E E	/					2/05/02/ No King File	9-114	AC700070	Rule ID: SV-6409r6_rule
	\$10.0m	.9	/					NOT ITSE AN THE STIC	V-115	40200060	Vuln ID: V-36
		5						1/05 NetView for 4/072 \$135	v-116	ACPOSIDO	
imum	\$7.7M	3						2/05 NetView for RACE STIG	V-118	ACP00120	* Decasion
	•••••	Simu	/					2/OS frect/sew for TSS \$139	w-119	AC900130	Dynamic lists provide a method of making a/OS system change
		o v						a/OS Quest NG-Pasa for ACR2 STIS	¥-522	ACR0570	without interrupting the availability of the operating system. Failure to properly control access to these facilities could result
						_		In IOS Quest NC Pass for BACF STIC	9-129	ACP08240	in unauthorized personnel modifying sensitive 2/OS lists. This
								AVGE Queen NC Pass for TSE STED	9-154	27500020	exposure may threaten the integrity and availability of the
ppetite	\$30.0M							V 2/05 R4CF STIE		ACP00250	operating system environment, and compromise the confidentiality of customer data.
								Peter NoPolle +	¥-276	RACFOARD	contract and a contract and
			· · · · ·					* Elter Carlors	V-3900	ZWA50040	
		S0	\$20.0M	\$40.0M	\$60.0M	\$80.0M	\$100.0M	* Haroper	v-6950	ZWM20011	* Deck Control
IDEX	\$5.0M	* -						CATE CATE CATE	9-6960	ZWMQ2051	
IPLA	33.010							Inter Proc Removed Add	V-6970	20/950022	Refer to the following report produced by the Data Set and Resource Data Collection:
	60.514							Instantion Filter Endpairies Filter	V-6972	20/550023	
pEx	\$2.5M	The a	average loss expo	osure for this ar	nalvsis is \$6.8M ;	above the risk	appetite		V-6921	20550046	- SENSITVE RPT(FACILITY)
			are age leve onp				appente.		V-7545 V-1520P	AAN/VEDL2	Automated Analysis
									4-1204	AND YOULD	Refer to the following report produced by the Data Set and Resource Data Collection:
											- POBACP092701
		\sim									+ fixled
			D1-1-1					Carrier Carrier			+ 03
			RiskLens"					Remove Friter Remove All Frites	Desiving sale 1 out of 2	24	* Mechanizati
								m		-	and the second



Produce Results

- ➡ 1. Advertise early successes
 - 2. Adjust from early failures
 - 3. Process and Tool Tuning especially collect, store, reduce, report, retrieve and archive data
 - 4. Iteration with reproducible results
 - 5. Sandbox vs Change Control

Hot topics and current events are a great way to demonstrate early success – deliver on schedule



Prevent

- 1. Real time:
 - Monitoring
 - Detection/Screening
 - Alerting
 - Correction
- 2. Update Standards
- 3. Secure Content Automation Protocol (SCAP) tools (future)

Feed Exception Results to Remediators, the SOC, the Standard SIEM Tool



SUMMARY – TAKE AWAY THOUGHTS

Today's Session – Value and Objective



Target Audience: Experienced security professionals who are at the stage of considering or planning the use of DISA STIGs for z/OS configuration management.

- Purpose: Offer recommendations that will allow participants to confidently define, propose and initiate a useful and viable configuration management program to reduce security risk.
- Scope: We will discuss the "What", "Why", and "How" elements of implementing a successful, STIGs-based, mainframe configuration management program to effect cyber risk reduction.
 - <u>What</u>: A secure framework to implement configuration management controls to prevent vulnerabilities due to errors and omissions
 - <u>Why</u>: Now is the highest risk ever for mainframe, driving a need for improved security posture
 - <u>How</u>: Organize a "Program" that includes the steps Prepare, Play, Plan, Propose, Produce and Prevent

Value:

Reduce security risk of configuration-based vulnerabilities by implementing viable and sustainable configuration management.

Note:

This session is not a tool training lab session though several useful tools will be mentioned during the presentation.

Let's review a few take-away thoughts

Copyright© by SHARE Association Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

Summary - Take Away Thoughts



- 1. DoD STIGs provide a useful framework of risk-reduction controls
- 2. Sustainable implementation requires a significant, well-executed, effort
 - Prepare
 - Play
 - Plan
 - Propose
 - Produce Results
 - Prevent
- 3. Implementation must address all three elements of:
 - People
 - Process
 - Technology

Have Fun!

Copyright® by SHARE Association Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/



QUESTIONS





Additional Questions later via email: philnoplos@aol.com

Copyright© by SHARE Association Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 license. http://creativecommons.org/licenses/by-nc-nd/3.0/

SHARE - Phoenix 2019 - Session 24610, March 11, 2019 Phil Noplos - CISM, CISSP

PLEASE ENTER YOUR SESSION EVALUATION! THANK YOU!





APPENDIX



Glossary



IASE: The Information Assurance Support Environment (IASE) provides one-stop access to Cybersecurity information, policy, guidance and training for cybersecurity professionals throughout the DoD. Some portions of the site are also available to the remainder of the Federal Government and the general public. These resources are provided to enable the user to comply with rules, regulations, best practices and federal laws. DISA is mandated to support and sustain the IASE as directed by DoDI 8500.01 and DODD 8140.01

From <<u>https://iase.disa.mil/Pages/about.aspx</u>> From <<u>https://iase.disa.mil/stigs/Pages/index.aspx</u>>

STIGs: The Security Technical Implementation Guides (STIGs) are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

See More on STIGs: From <<u>https://www.seguetech.com/stigs-security-program/</u>>

And for More on STIGs, see this SHARE 2015, Session #17735, presentation: *From* <<u>https://www.share.org/p/do/sd/topic=64&sid=11911</u>>, including a pretty good glossary of terms.

Training Choices:

- For basic training info about STIGS, the STIG viewer and SCAP tools, search for "DoD STIGs" on You Tube
- For a little more in-depth treatment: use Google Scholar to search for "mainframe STIGs"

Automation Tool Options

- For training on running a JAR file on Windows 10, see: https://www.youtube.com/watch?v=Glhw_wZ36ol
- IBM, zSecure, see next page
- Vanguard, Configuration Manager, see SHARE 2014 Session #15967
- SCAP Tools none known for mainframe yet see: Security Content Automation Protocol, From

<https://en.wikipedia.org/wiki/Security_Content_Automation_Protocol>

- SDS Iron Sphere, see: <u>https://www.youtube.com/watch?v=QxVD6RIGIeo</u>, or webinar here: <u>https://www.sdsusa.com/security-software/automatic-mainframe-stig-monitoring/webinar/</u>
- BMC/Correlog for Monitoring and Alerting, see: https://correlog.com
- CA Auditor for z/OS and Compliance Event Manager, see: <u>https://www.ca.com/us/products/ca-auditor-zos.html</u>, and <u>https://www.youtube.com/playlist?list=PLynEdQRJawmzdBjZl276GRRt3SLgrPIEi</u>

Appendix

SHARE EDUCATE + NETWORK + INFLUENCE

More Training Options for zSecure

IBM Security zSecure Audit Rule-based Compliance Evaluation and Customization (TK273G) Screen clipping taken: 2/26/2019 12:35 PM https://www.flane.de/en/course/ibm-tk273g

https://www.ingrammicrotraining.com

IBM Security zSecure on developerWorks

From

<<u>https://www.ibm.com/developerworks/community/blogs/d9705ece-5557-4f4c-9208-</u> 3258d1eb85f9/entry/Upcoming_zSecurity_Master_Skills_Bootcamp?lang=en></u>

Security Technical Implementation Guide (STIG) 101

From <<u>https://rmf.org/stig-101/</u>>

Command to start the viewer: java -jar STIGViewer-2.8.jar

Appendix



Extra Goodies Come with the Viewer

U_	zOS_V6R39_P	DI_list.xlsx - F	D	E	F	G	Н	I	J	K	
	ALL Vulnerabilities with elimination of duplicate Vulnerabilities										
	Vul ID	STIG ID	Pri Cond	Sec Cond	Automate	Finished	Automate	Check	No	Additional info	
2	-	-		· •	-	-T	Check 💌	Count 💌	Automa 🔻		
3	V0000082	AAMV0010	z/OS		1		1	1		SMP/E or CMP	
4	V0007545	AAMV0012	z/OS		1	1	1	1		Vulnerability question	
5	V0007546	AAMV0014	z/OS		1	1	1	1		Vulnerability question	
6	V0015209	AAMV0018	z/OS		1	1	1	1		Vulnerability question	
7	V000083	AAMV0030	z/OS		1	1	1	1			
8	V0000084	AAMV0040	z/OS		1	1	1	1			
9	V0000085	AAMV0050	z/OS		1	1	1	1		DUPES script handles this.	
	10000000	A A B B (00000	100		4		^			B 10 11 1	

U_zOS_V6R39	9_Cross_Ref_of_SRRAUDIT.xlsx	STIG ID	Sensitve Member	Description	Logging Storts at	Crown	Max Acces
Authorized		STIGID	wember	Description	Starts at	Group	
Group	Description						ALTER
CICDAUDT	CICS Developers.	-					ALTER
CICSAUDT	CICS Started Task.					SYSPAUDT	ALTER
CICSDEF	CICS regions default user ids (DFLTUSER).	-				TSTCAUDT	ALTER
CICUAUDT	CICS Utils (CONTROLO, BatIDs via CONTROLM, MAINVIEW	ACP00130	CATMRPT	MASTER SYSTEM CATALOG	WRITE	*	READ
CONSOLES		1				MCATBAT	ALTER
DABAAUDT	Data Base Administrators	-1				SYSPAUDT	ALTER
DAEMAUDT	Unix Daemon user ids	-				TSTCAUDT	ALTER
DASBAUDT	DASD batch, jobs that perform DASD Backups, Migrate	ACP00135	CATURPT	USER SYSTEM CATALOGS	ALTER	*	UPDATE
DASDAUDT	DASD Administrators					MCATBAT	ALTER
DPCSAUDT	Decentralized Production Control and Scheduling personnel					SYSPAUDT	ALTER
DUMPAUDT	STCs/Batch ids that perform Dump processing					TSTCAUDT	ALTER
EMERAUDT	Emergency TSO logon ids	ACP00140	SMPERPT	SMP/E DATA SETS		*	READ
FTPUSERS	FTP only interactive users	1					
IOABAUDT	IOA batch users for operations						
LIGATOAT							

MCATBAT Batch users requiring ALTER access to Master Catalog

Appendix



Extra Goodies Come with the Viewer

STIG ID	Resource Class	Resource	Logging Start at	Group	Max Access
ACF0870 PROGRAM		AHLGTF	READ	STCGAUDT	ALTER
		BLSROPTR	READ	DASBAUDT	ALTER
				DASDAUDT	ALTER
				SYSPAUDT	ALTER
		CSQ1LOGP	READ	MQSAAUDT	ALTER
		CSQJU003	READ	MQSAAUDT	ALTER
		CSQJU004	READ	MQSAAUDT	ALTER
		CSQUCVX	READ	MQSAAUDT	ALTER
		CSQUTIL	READ	AUDTAUDT	ALTER
				MQSAAUDT	ALTER
		DEBE	READ	DASDAUDT	ALTER
				TAPEAUDT	ALTER
		DITTO	READ	DASDAUDT	ALTER
				TAPEAUDT	ALTER
		FDRZAPOP	READ	SYSPAUDT	ALTER
		GIMSMP	READ	AUDTAUDT	ALTER
				DABAAUDT	ALTER
				SYSPAUDT	ALTER
		HHLGTF	READ	STCGAUDT	ALTER
		ICKDSF	READ	DASDAUDT	ALTER
				SYSPAUDT	ALTER
		ICPIOCP	READ	SYSPAUDT	ALTER
		IDCSC01	READ	SYSPAUDT	ALTER
		IEHINITT	READ	TAPEAUDT	ALTER