Getting Started Using the DoD STIGs for Mainframe Security

SHARE - Phoenix 2019 - Session 24610, March 11, 2019

Phil Noplos - CISM, CISSP

WHO IS TODAY’S SPEAKER?

Bio - Phil Noplos, CISM, CISSP

SHARE
EDUCATE • NETWORK • INFLUENCE

- 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

SHARE
EDUCATE • NETWORK • INFLUENCE

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.

Value: 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

STIGs - What

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

STIGs - What

SHARE
EDUCATE • NETWORK • INFLUENCE

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

STIGs - What

SHARE
EDUCATE • NETWORK • INFLUENCE

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 - What

SHARE
EDUCATE • NETWORK • INFLUENCE

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

STIGs - What

	A	B	C	D	E	F	G	H	I	J
1	TOTALS	Version 6 Release 39								
2	January 25, 2019	ALL	z/OS	ACF2	RACF	TSS	Description	ACF2 w/z/OS	RACF w/z/OS	TSS w/z/OS
3	TOTAL # of PDIs	529	139	219	237	260	Total Vulnerabilities by Targets	358	376	399
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%	67.58%	72.57%	69.23%	% of Vulnerabilities currently automated	65.64%	68.88%	66.92%
11	Total Checks	619	172	265	290	307	Total number of Checks in all vulnerabilities	437	462	479
12	Checks to be Automated	599	157	263	287	307	Total number of Checks that can be automated	420	444	464
13	Checks That Cannot Be Automated	20	15	2	3	0	Total number of Checks that cannot be automated	17	18	15
14	% Checks to Be Automated	96.77%	91.28%	99.25%	98.97%	100.00%		96.11%	96.10%	96.87%
15	# 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%	71.86%	75.61%	72.31%		72.14%	74.55%	72.41%
19	% Checks Automated	71.57%	66.28%	71.32%	74.83%	72.31%		69.34%	71.65%	70.15%
20	Checks Needing Automation Scripts	156	43	74	70	85		117	113	128
21	% Checks Needing Automation Scripts	26.04%	27.39%	28.14%	24.39%	27.69%		27.86%	25.45%	27.59%
22										

STIGs are a mature framework to improved security posture

STIGs - What

SHARE
EDUCATE • NETWORK • INFLUENCE

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, WHY AND HOW

STIGs - Why

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?

STIGs - Why

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

RSM ENTERPRISE SOLUTIONS

Everything you wanted to know about mainframe security, pen testing and vulnerability scanning .. But were too afraid to ask!

Mark Wilson
markw@rsmpartners.com
Session Details: How to hack a mainframe

SHARE in Orlando 2015

Can CICS Be Hacked?
Are Yesterday's Practices Today's Exposure?

Leigh Compton
CICS Technical Specialist
IBM zGrowth Team

SHARE in Orlando 2015

Want to Hack a Mainframe System?

Mark Wilson
Technical Director
RSM Partners

RSM Partners
The z Specialists: Skills, Services & Support

z/OS Ethical Hacking
Vulnerability Scanning &
Pen Testing

Mark Wilson
RSM Partners

Session Number: 12275

HOW TO BREAK INTO
z/OS SYSTEMS

Stuart Henderson
the Henderson Group
Bethesda, MD
(301) 229-7187
www.stuhenderson.com

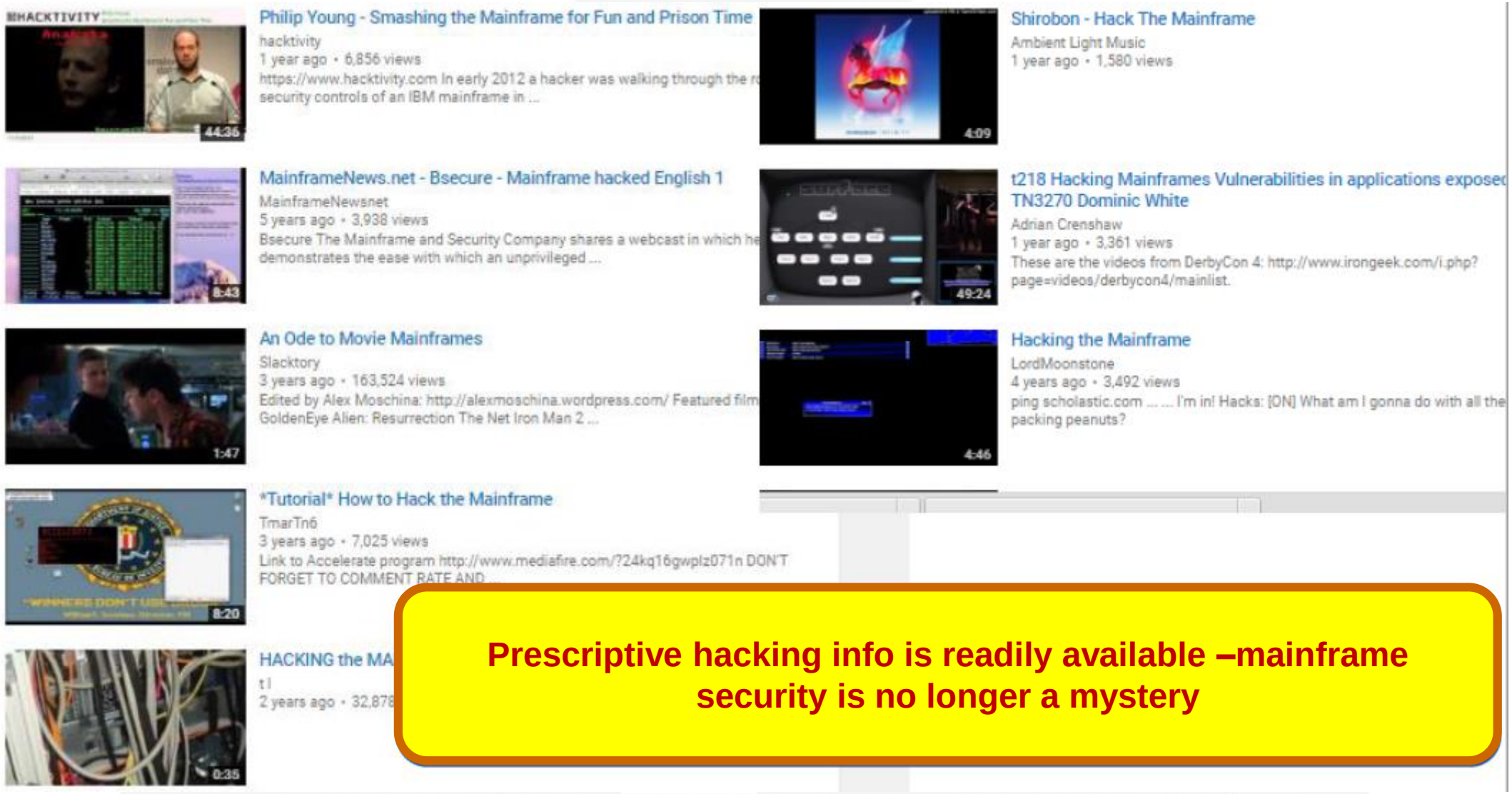
How Hackers Breached a
Government (and a Bank)

Philip Young
aka Soldier of Fortran
@mainframed767

Mainframe hacking has become real

STIGs - Why

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



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

STIGs - Why

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

Mainframe hacking has become real

STIGs - Why

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

STIGs - Why

SHARE
EDUCATE • NETWORK • INFLUENCE

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

STIGs - Why

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	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

STIGS – WHAT, WHY AND HOW

STIGs - How

SHARE
EDUCATE • NETWORK • INFLUENCE

Prepare

1. 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

STIGs - How

SHARE
EDUCATE • NETWORK • INFLUENCE

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

STIGs - How

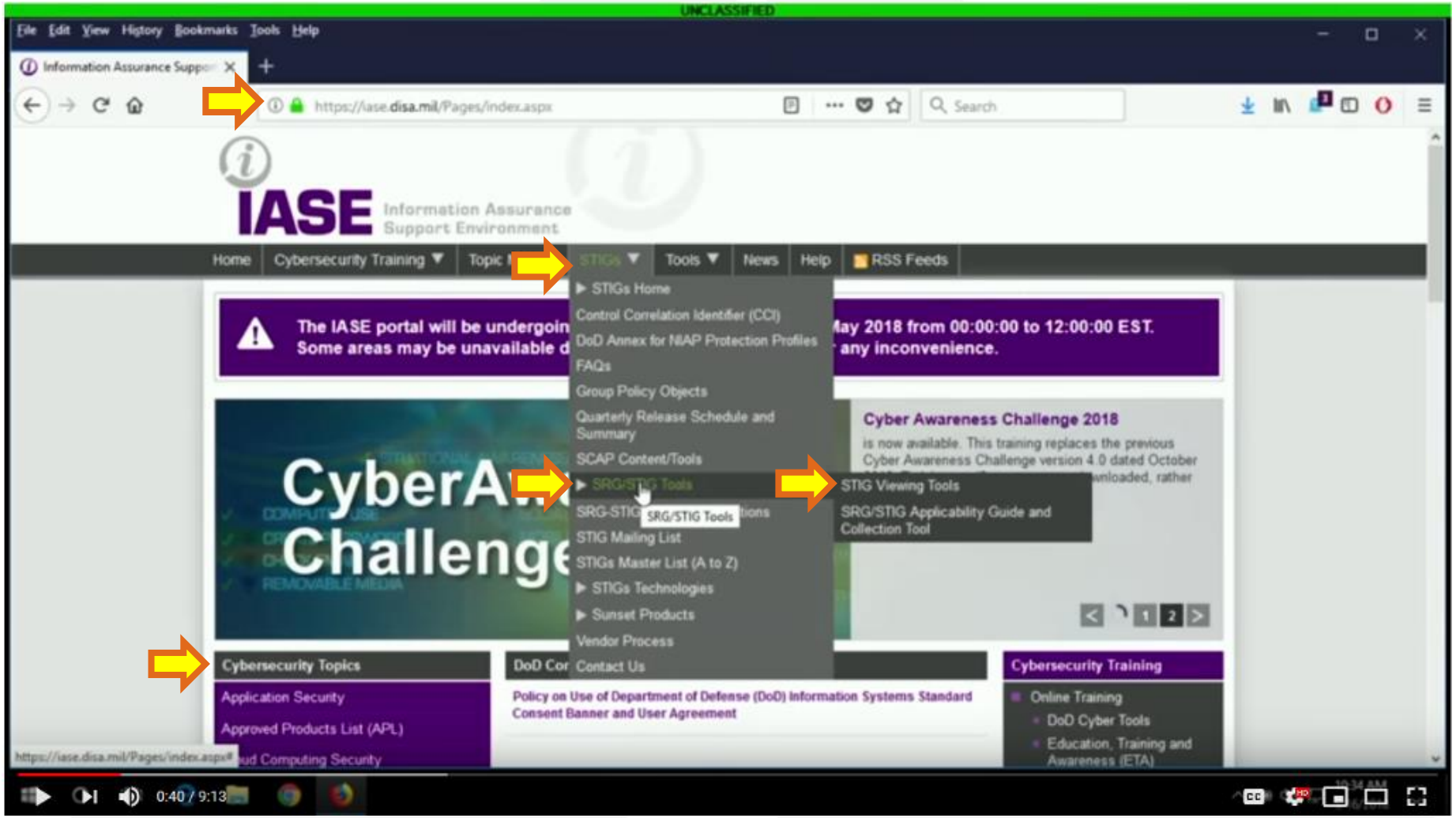
Play

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

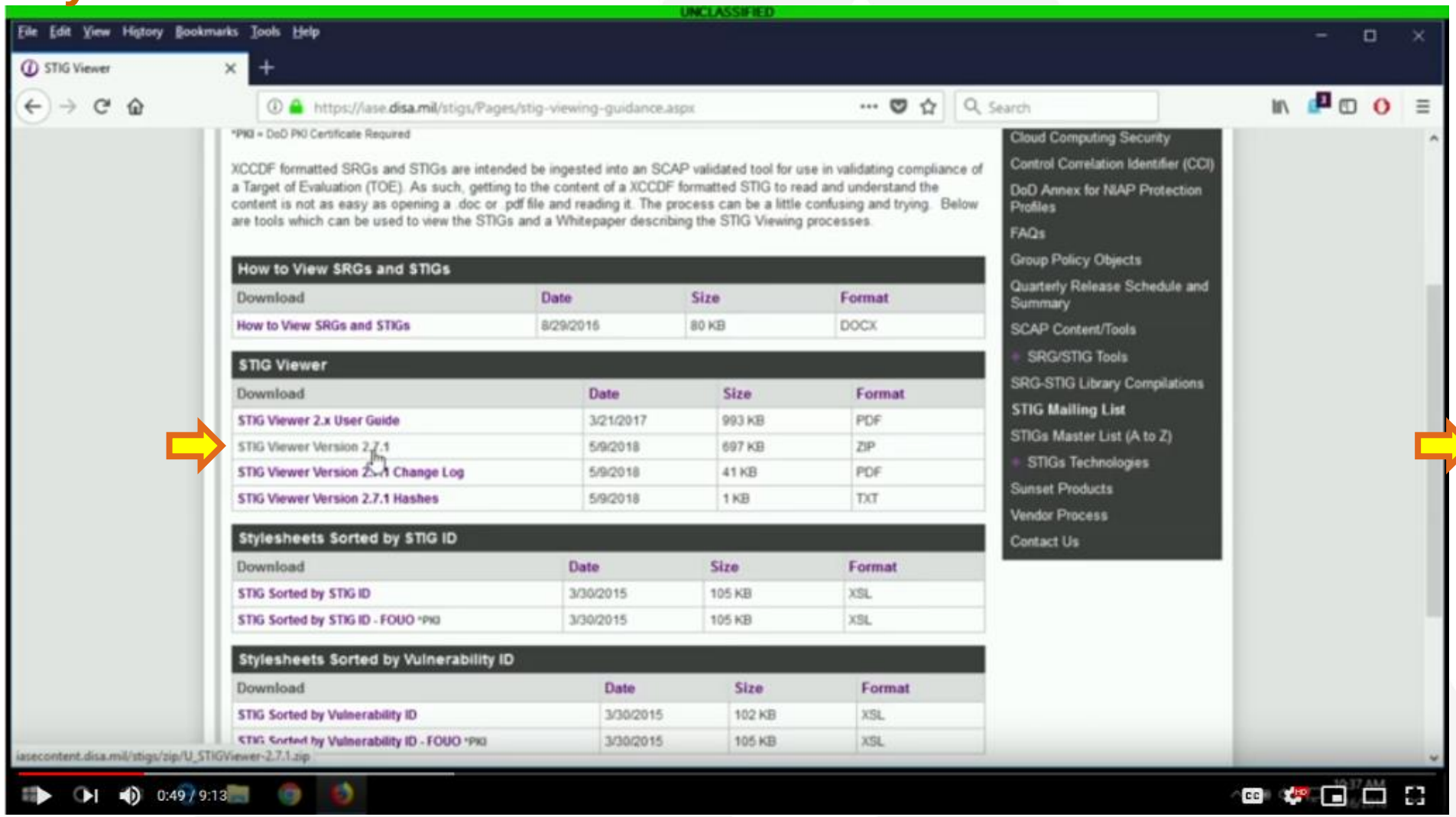
STIGs - How

Play – Download a viewer and the current STIGs



STIGs - How

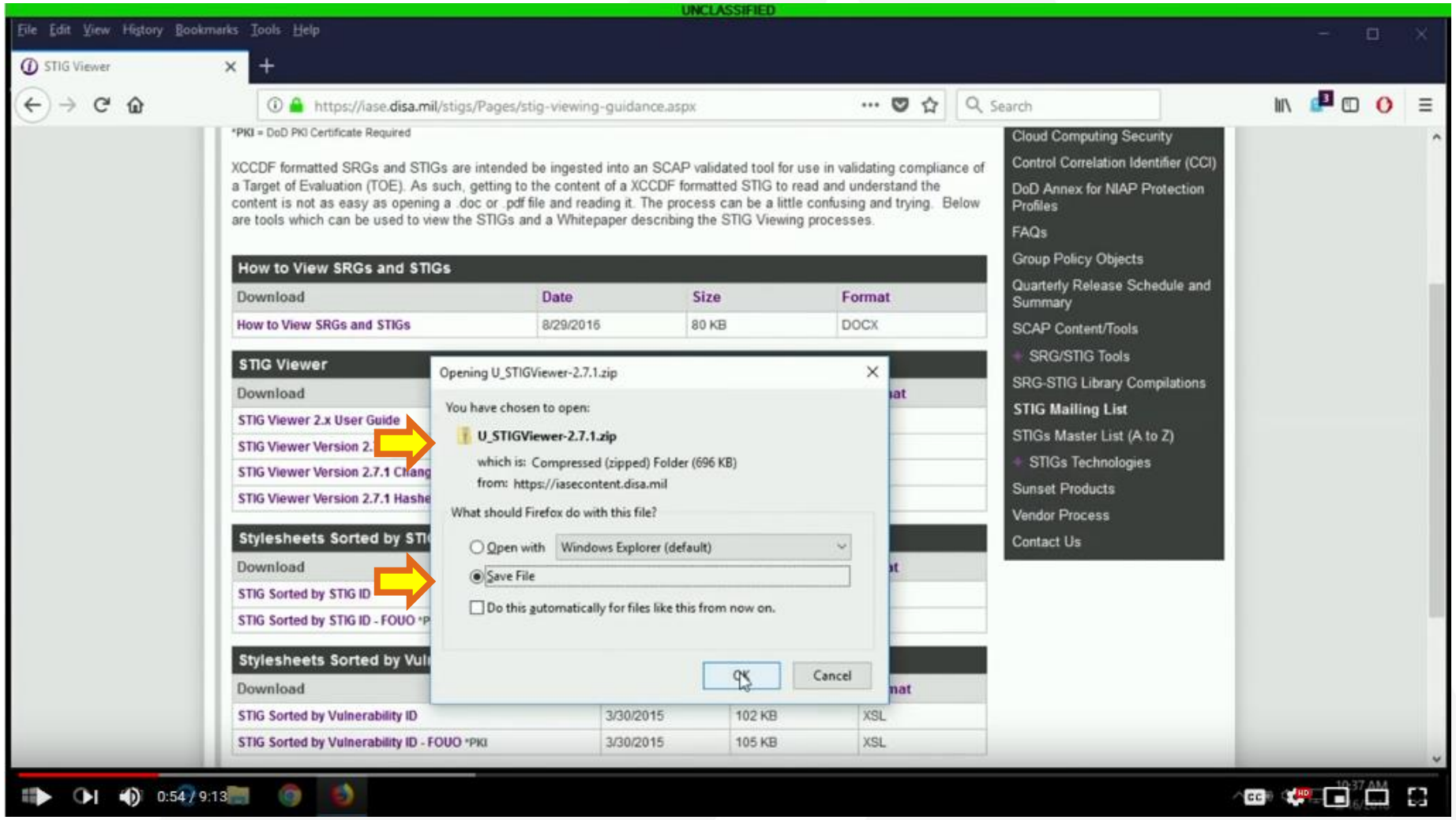
Play – Download a viewer and the current STIGs



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

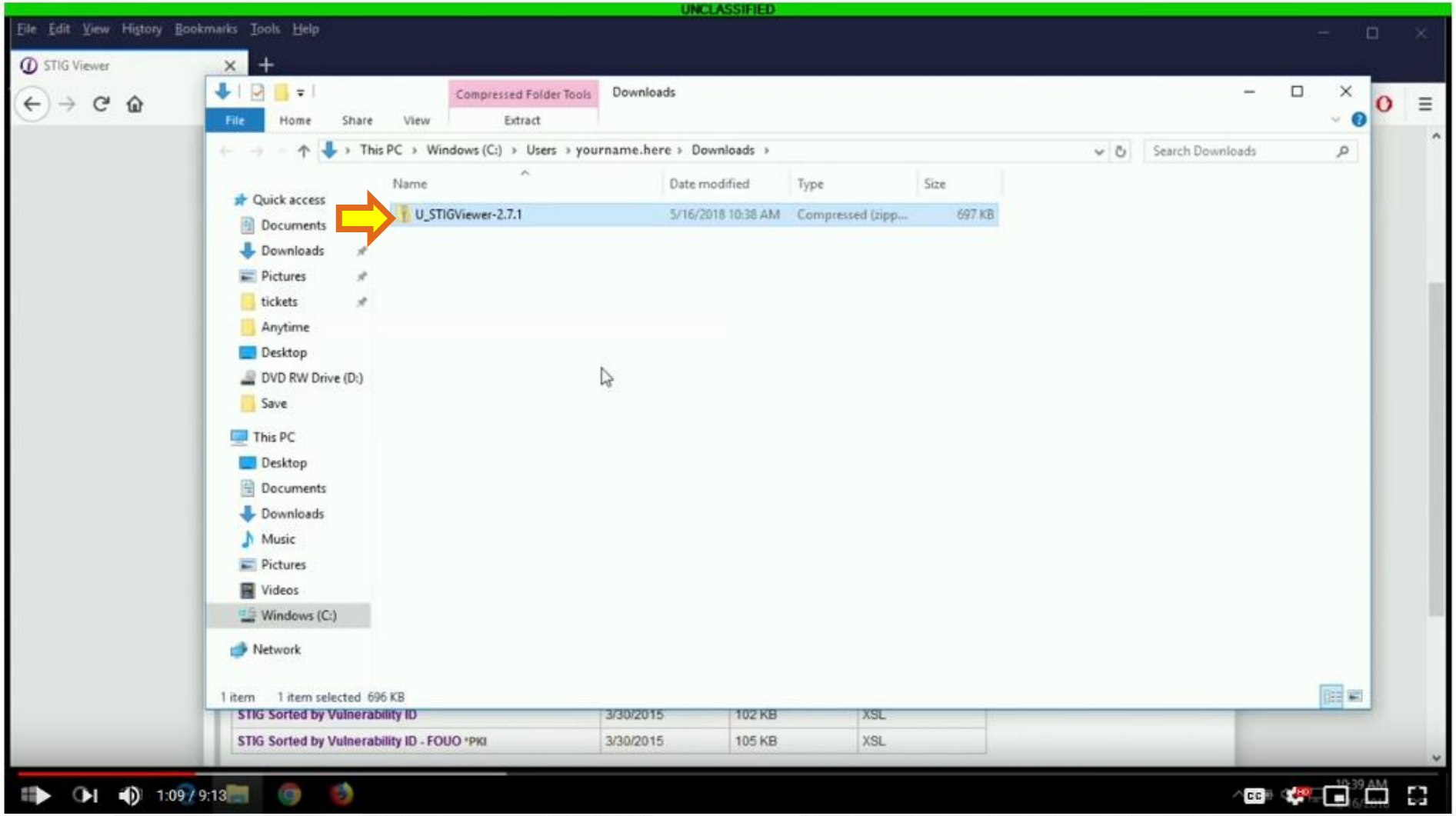
STIGs - How

Play – Download a viewer and the current STIGs



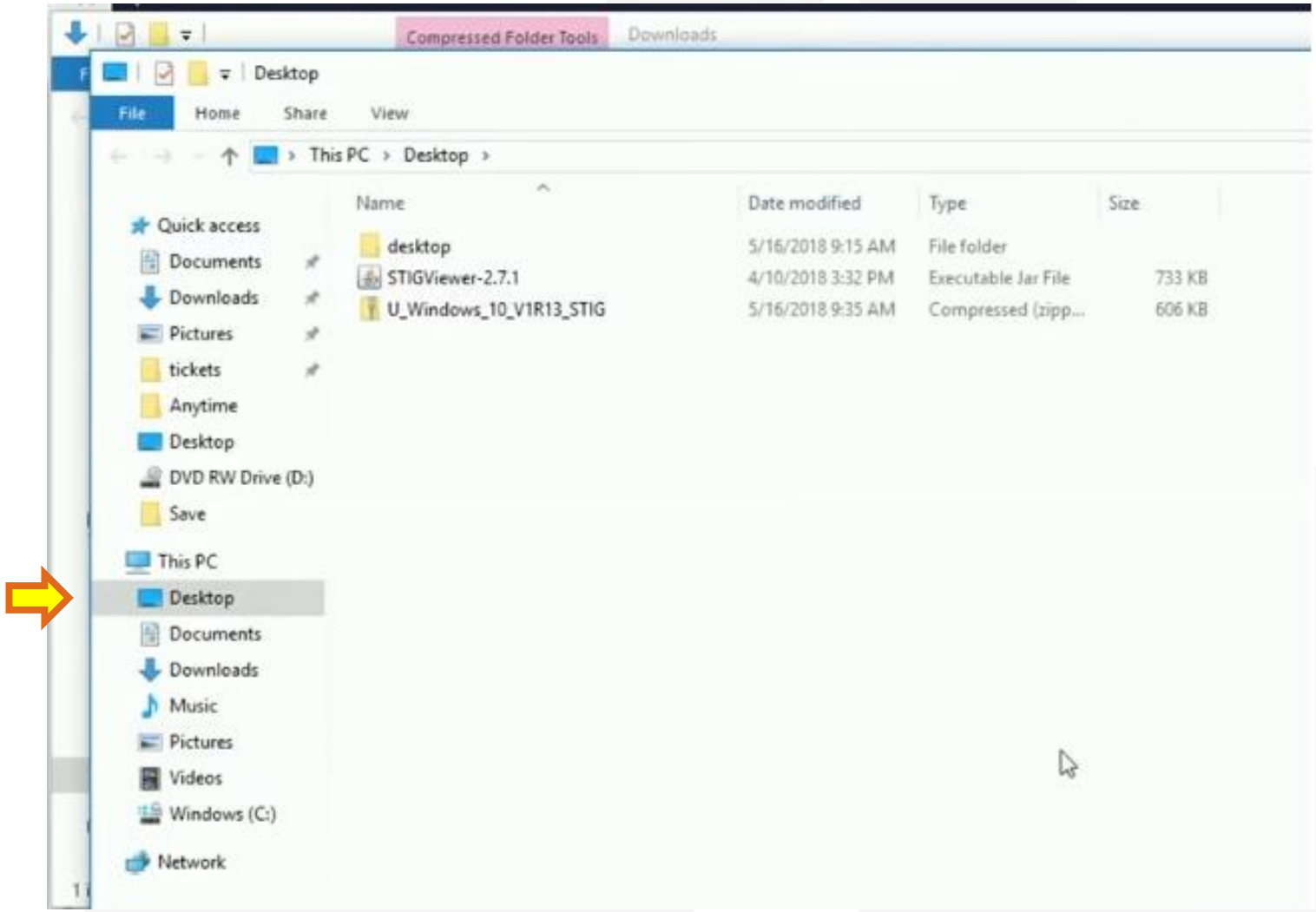
STIGs - How

Play – Download a viewer and the current STIGs



STIGs - How

Play – Download a viewer and the current STIGs



STIGs - How

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

STIG Viewer

HOME | STIGS | DOD 8500 | NIST 800-53 | COMMON CONTROLS HUB | ABOUT | Search...

https://www.stigviewer.com/

z/OS RACF STIG

Overview

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 Description

None

Available Profiles

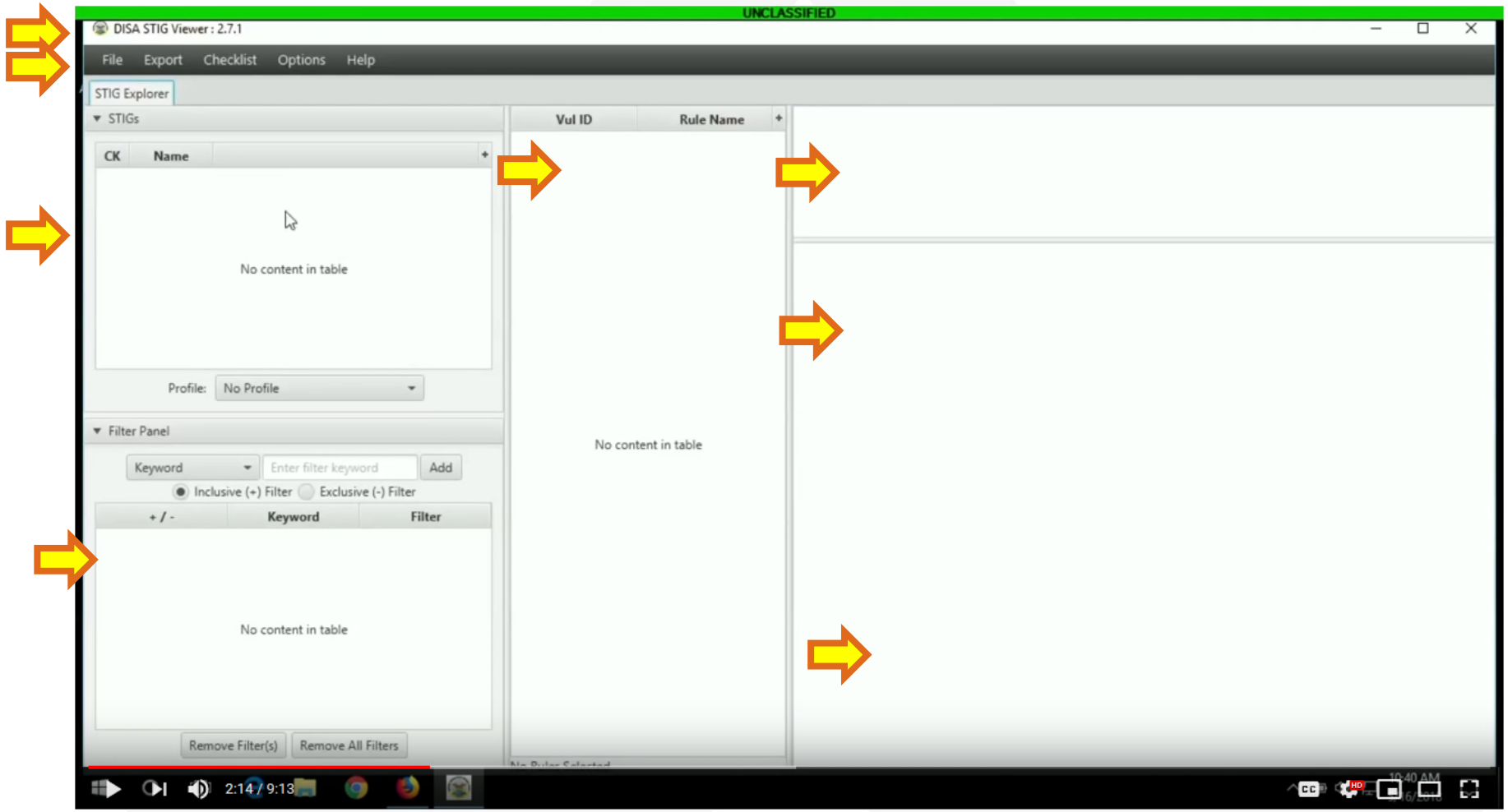
id	severity	title	description	iacontrols	ruleID	fixid	fixtext	checkid	checktext
V-3899	medium	The	SAF resource	None	SV-7265r2	F-18794r1	There are	C-3261r1_	a)Refer to the
V-3898	medium	HFS objec	HFS directori	['DCCS-1', 'DC	SV-3898r2	F-18956r1	Review	C-20978r1	a)Refer to the
V-6919	medium	JES2 input	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	LOGONIDs	SYS1.UADS is	['DCCS-1', 'DC	SV-184r3_	F-18939r1	The syster	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	Configuratio	['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

Findings (MAC III - Administrative Sensitive)

Finding ID	Severity	Title	Description
V-184	High	LOGONIDs must not be defined to SYS1.UADS for non-emergency use.	SYS1.UADS is a dataset where LOGONIDs will be maintained with applicable password information when the ACP is not functional. If an unauthorized user

STIGs - How

Play – Download a viewer and the current STIGs



STIGs - How

Play – Download a viewer and the current STIGs

IASE Information Assurance Support Environment

Home | Cybersecurity Training | Topic Map | STIGs | 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

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.

STIGs - How

Play – Download a viewer and the current STIGs

Extract To

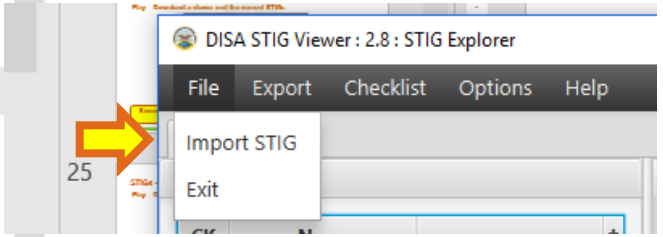
« OS- IBM zOS RACF STIG › U_zOS_RACF_V6R39_STIG.zip › U_zOS_RACF_V6R39_Manual_STIG

Search U_zOS_RACF_V6R39_M...

- 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-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_MIM_for_RACF_V6R3_Manual_STIG
- U_zOS_CA_VTAPE_for_RACF_V6R4_Manual_STIG
- U_zOS_Catalog_Solutions_for_RACF_V6R4_Manual_STIG
- U_zOS_CLSuperSession_for_RACF_V6R10_Manual_STIG
- U_zOS_Compuware_Abend-AID_for_RACF_V6R6_Manual_STIG

Name	Type	Compressed size
DoD-DISA-logos-as-JPEG.jpg	JPG File	112 KB
STIG_unclass.xsl	XSL Stylesheet	10 KB
U_OS_RACF_V6R39_STIG_Manual-xccdf.xml	XML Document	138 KB

- U_zOS_IBM_SDSF_for_RACF_V6R8_Manual_STIG
- U_zOS_ICSF_for_RACF_V6R5_Manual_STIG
- U_zOS_NetView_for_RACF_V6R8_Manual_STIG
- U_zOS_Quest_NC-Pass_for_RACF_V6R2_Manual_STIG
- U_zOS_RACF_V6R39_Manual_STIG
- U_zOS_ROSCOE_for_RACF_V6R7_Manual_STIG
- U_zOS_SRRAUDIT_for_RACF_V6R4_Manual_STIG
- U_zOS_TADz_for_RACF_V6R6_Manual_STIG



STIGs - How

Play – Download a viewer and the current STIGs

File Export Checklist Options Help

STIG Explorer

STIGs

CK	Name
✓	z/OS RACF STIG

Profile: No Profile

Filter Panel

Must match: All Any

Keyword | Enter filter keyword | Add

Inclusive (+) Filter Exclusive (-) Filter

+ / -	Keyword	Filter

Vul ID	Rule Name
V-7545	AAMV0012
V-7491	RACF0248
V-254	RACF0250
V-255	RACF0260
V-257	RACF0280
V-258	RACF0290
V-260	RACF0310
V-261	RACF0320
V-262	RACF0330
V-265	RACF0350
V-266	RACF0370
V-267	RACF0380
V-269	RACF0400
V-270	RACF0420
V-271	RACF0430
V-272	RACF0440
V-273	RACF0450
V-3900	ZWAS0040

z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019

Vul ID: V-7545 **Rule ID**: SV-8016r3_rule **STIG ID**: AAMV0012

Severity: CAT I **Classification**: Unclass

Group Title: AAMV0012

Rule Title: Unsupported system software is installed and
system.

Discussion: When a vendor drops support of System So
longer maintain security vulnerability patches to the soft
vulnerability patches, it is impossible to verify that the sy
contain code which could violate the integrity of the ope
environment.

Check Text: This check applies to all products that meet
criteria:

- Uses authorized and restricted z/OS interfaces by utiliz
Program Facility (APF) authorized modules or libraries.
- Require access to system datasets or sensitive informat
special or privileged authority to run.

For the products in the above category refer to the Vend
lifecycle information for current versions and releases. Th
should be added to the Vulnerability Questions within th
Management document for supported software product

Automated Analysis

Automated Analysis
Refer to the following report produced by the z/OS Data Collection:

- PDI(AAMV0012)

If the software products currently running on the reviewed system are at a version greater than or equal to the products listed in the vendor's Support Lifecycle information, this is not a finding.

Fix Text: For all products that meet the following criteria:

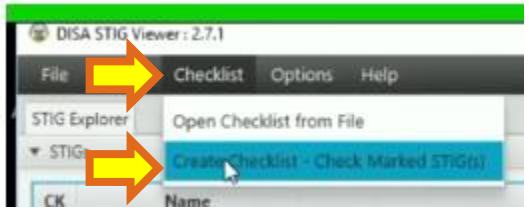
- Uses authorized and restricted z/OS interfaces by utilizing Authorized Program Facility (APF) authorized modules or libraries.
- Require access to system datasets or sensitive information or requires special or privileged authority to run.

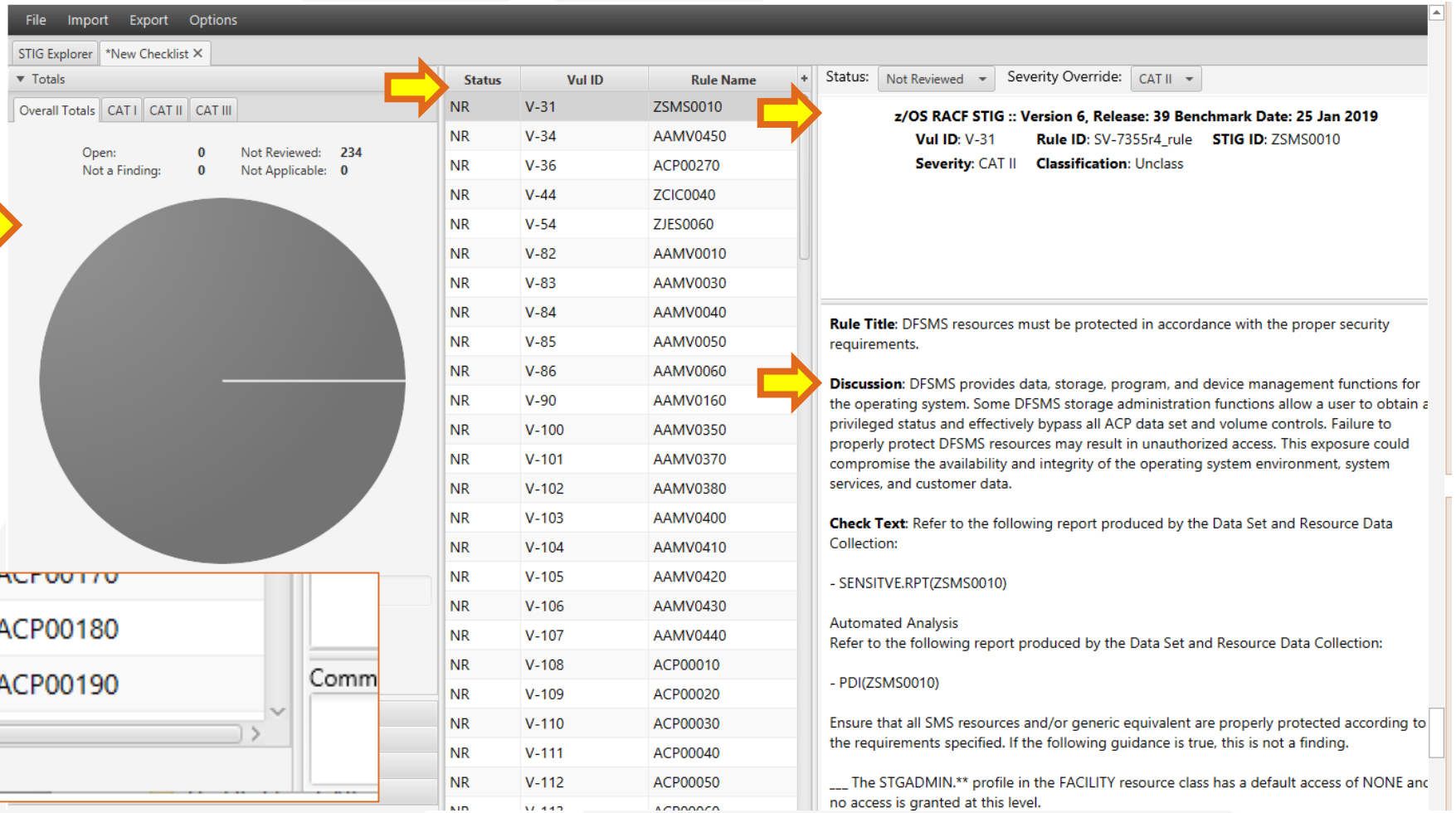
The ISSO will ensure that unsupported system software for the products in the above category is removed or upgraded prior to a vendor dropping support.

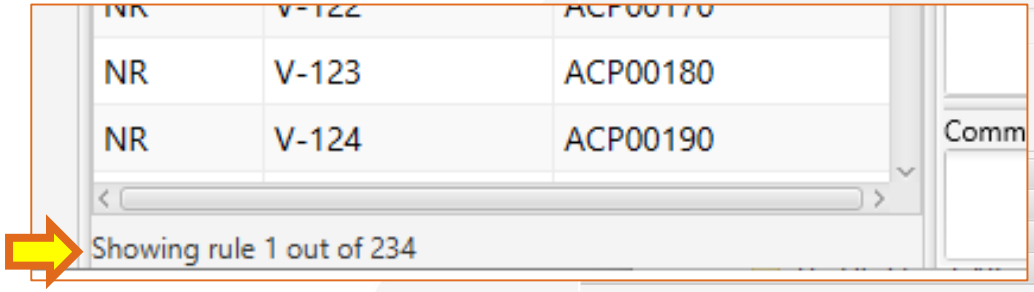
Authorized software which is NO longer supported is a CAT I – vulnerability

STIGs - How

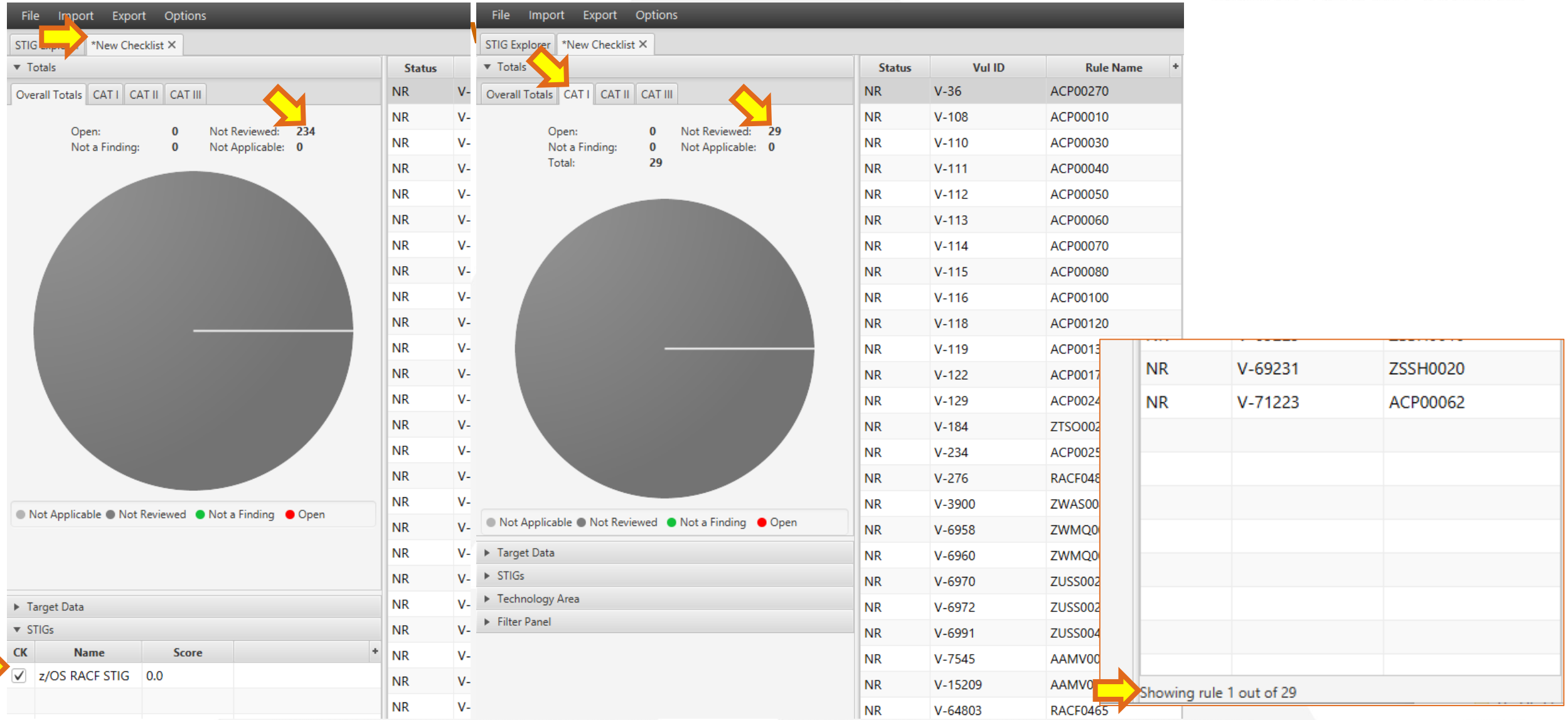
Play – Download a viewer and the current STIGs





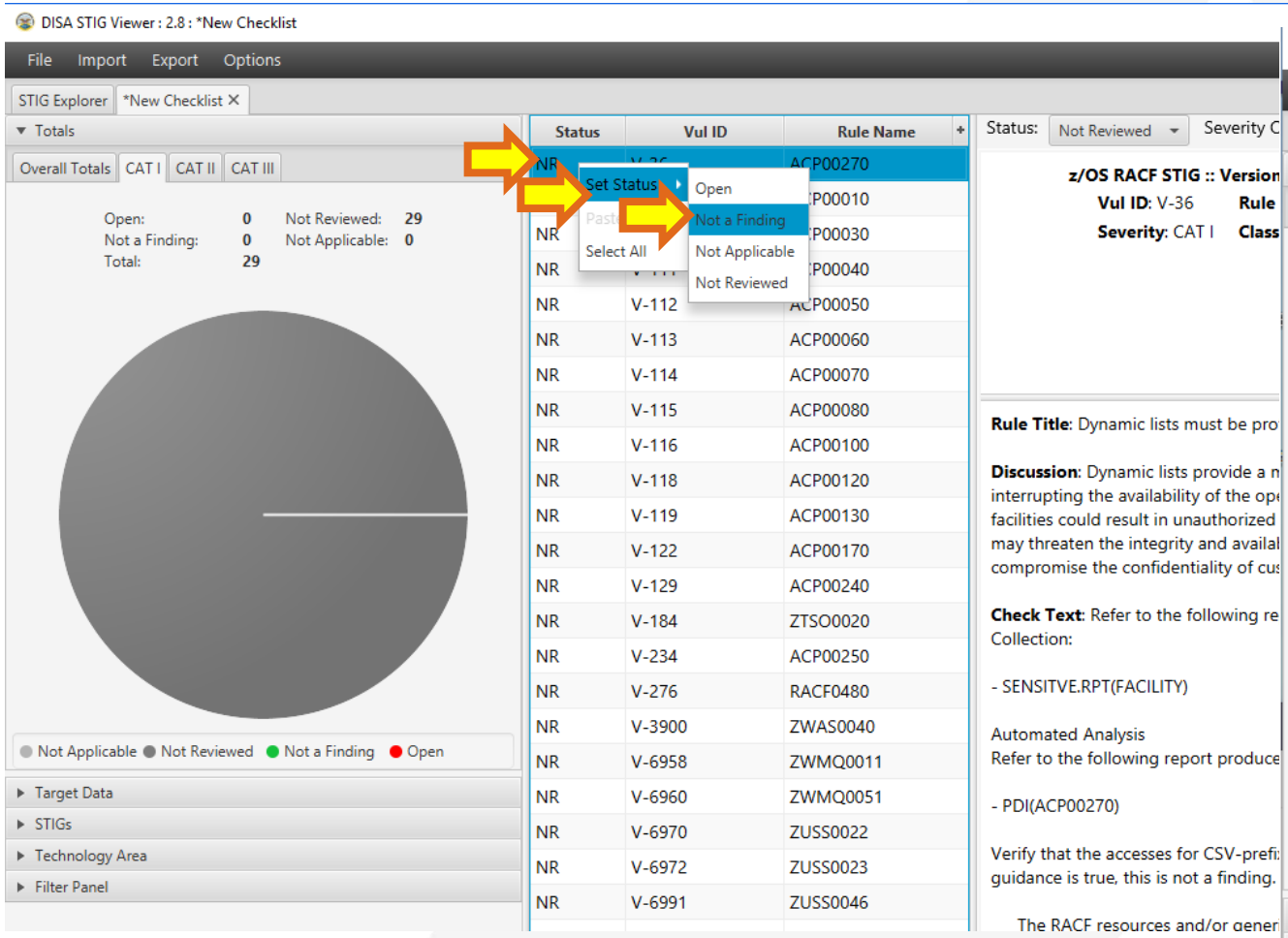


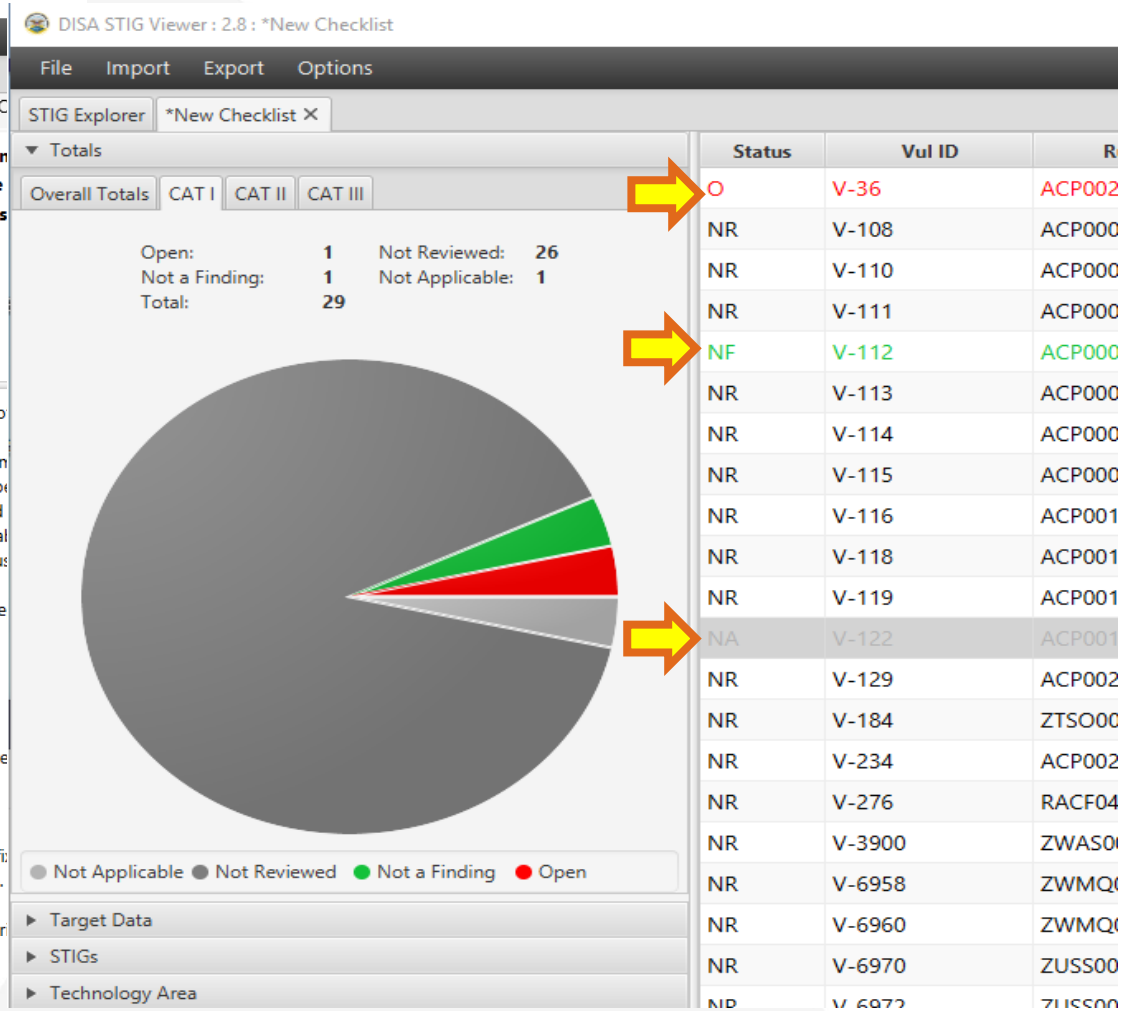
STIGs - How



STIGs - How

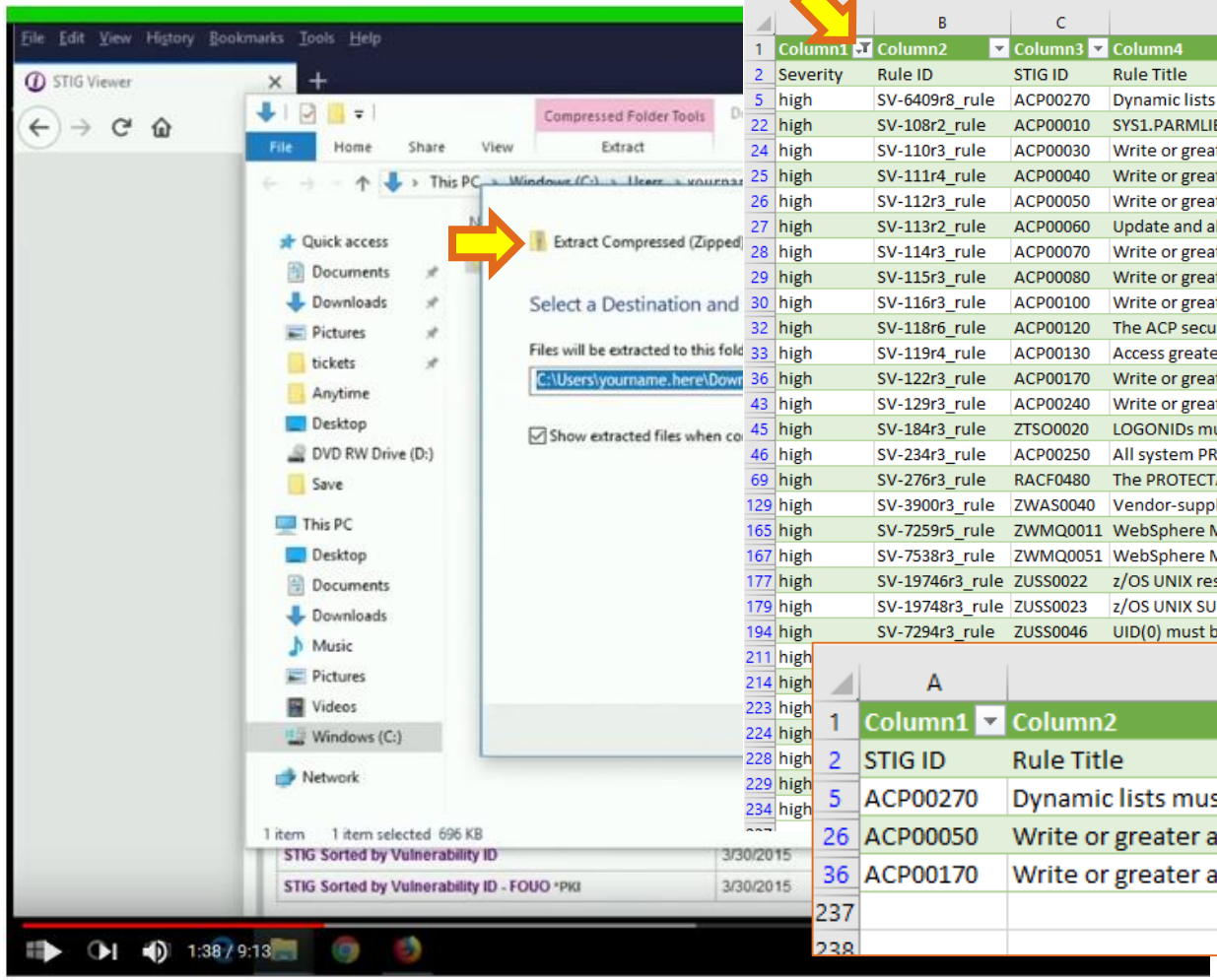
Play – Download a viewer and the current STIGs





STIGs - How

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



	B	C	D	E	F
1	Column1	Column2	Column3	Column4	Column5	Column6
2	Severity	Rule ID	STIG ID	Rule Title	STIG	Comments
5	high	SV-6409r8_rule	ACP00270	Dynamic lists must be protected in accordance with proper security requirements.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
22	high	SV-108r2_rule	ACP00010	SYS1.PARMLIB is not limited to only system programmers.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
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, Release: 39 Benchmark Date: 25 Jan 2019	
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, Release: 39 Benchmark Date: 25 Jan 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, Release: 39 Benchmark Date: 25 Jan 2019	
27	high	SV-113r2_rule	ACP00060	Update and allocate access to all APF -authorized libraries are not limited to system program	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
28	high	SV-114r3_rule	ACP00070	Write or greater access to all LPA libraries must be limited to system programmers only.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
29	high	SV-115r3_rule	ACP00080	Write or greater access to SYS1.NUCLEUS must be limited to system programmers only.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
30	high	SV-116r3_rule	ACP00100	Write or greater access to libraries that contain PPT modules must be limited to system prog	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
32	high	SV-118r6_rule	ACP00120	The ACP security data sets and/or databases must be properly protected.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
33	high	SV-119r4_rule	ACP00130	Access greater than Read to the System Master Catalog must be limited to system programm	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
36	high	SV-122r3_rule	ACP00170	Write or greater access to SYS1.UADS must be limited to system programmers only and read	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
43	high	SV-129r3_rule	ACP00240	Write or greater access to Libraries containing EXIT modules must be limited to system progr	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
45	high	SV-184r3_rule	ZTSO0020	LOGONIDs must not be defined to SYS1.UADS for non-emergency use.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
46	high	SV-234r3_rule	ACP00250	All system PROCLIB data sets must be limited to system programmers only	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
69	high	SV-276r3_rule	RACF0480	The PROTECTALL SETROPTS value specified must be properly set.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
129	high	SV-3900r3_rule	ZWAS0040	Vendor-supplied user accounts for the WebSphere Application Server must be defined to th	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
165	high	SV-7259r5_rule	ZWMQ0011	WebSphere MQ channel security must be implemented in accordance with security require	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
167	high	SV-7538r3_rule	ZWMQ0051	WebSphere MQ switch profiles must be properly defined to the MQADMIN class.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
177	high	SV-19746r3_rule	ZUSS0022	z/OS UNIX resources must be protected in accordance with security requirements.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
179	high	SV-19748r3_rule	ZUSS0023	z/OS UNIX SUPERUSER resource must be protected in accordance with guidelines.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
194	high	SV-7294r3_rule	ZUSS0046	UID(0) must be properly assigned.	z/OS RACF STIG :: Version 6, Release: 39 Benchmark Date: 25 Jan 2019	
211	high					
214	high					
223	high					
224	high					
228	high					
229	high					
234	high					

	A	B	C	D
1	Column1	Column2	Column3	Column4
2	STIG ID	Rule Title	Status	Comments
5	ACP00270	Dynamic lists must be protected in accordance with proper security requirements.	Open	
26	ACP00050	Write or greater access to SYS1.LPALIB must be limited to system programmers only.	Not A Finding	
36	ACP00170	Write or greater access to SYS1.UADS must be limited to system programmers only and read	Not Applicable	
237				
238				

STIGs - How

SHARE
EDUCATE • NETWORK • INFLUENCE

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

STIGs - How

SHARE
EDUCATE • NETWORK • INFLUENCE

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

STIGs - How

SHARE
EDUCATE • NETWORK • INFLUENCE

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

STIGs - How

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

STIGs - How

Propose

1. Justify – Need, benefit, cost, risk
2. Risk – express appropriately for your organization
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
7. Agree on metrics – measure results not activity, agree on definition of results both positive and negative (i.e., findings)

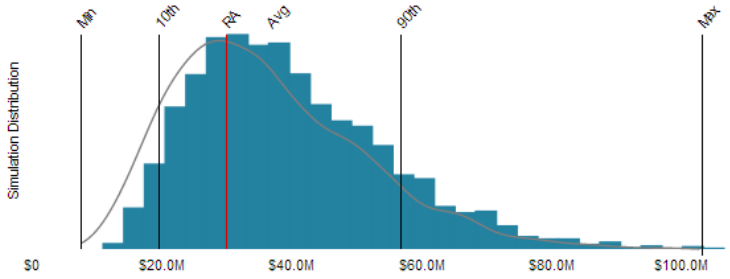
Treat Risk Using Methods That Fit Into Your Organization

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

Maximum	$103.2M
90th %	$56.9M
Average	$36.8M
10th %	$19.6M
Minimum	$7.7M

Risk Appetite	$30.0M

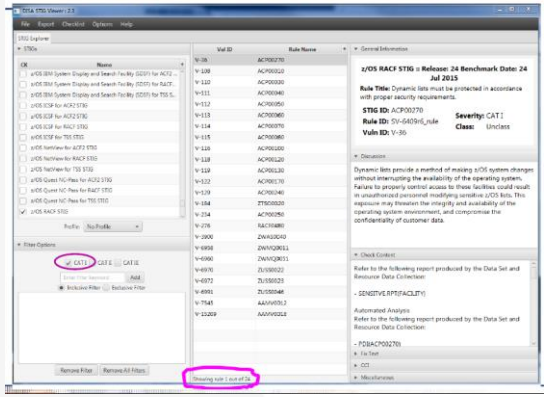
CapEx	$5.0M
OpEx	$2.5M



The average loss exposure for this analysis is $6.8M above the risk appetite.

RiskLens™

HIGH RISK STIG RULES CAN BE SELECTED



STIGs - How

SHARE
EDUCATE • NETWORK • INFLUENCE

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

STIGs - How

SHARE
EDUCATE • NETWORK • INFLUENCE

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

SHARE
EDUCATE • NETWORK • INFLUENCE

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.

- What: A secure framework to implement configuration management controls to prevent vulnerabilities due to errors and omissions
- Why: Now is the highest risk ever for mainframe, driving a need for improved security posture
- How: 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

Summary - Take Away Thoughts

SHARE
EDUCATE • NETWORK • INFLUENCE

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!

QUESTIONS

Q&A

Additional Questions later via email: philnoplos@aol.com

SHARE - Phoenix 2019 - Session 24610, March 11, 2019

Phil Noplos - CISM, CISSP

PLEASE ENTER YOUR SESSION EVALUATION!
THANK YOU!

APPENDIX

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 <https://iase.disa.mil/Pages/about.aspx>

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

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 <https://www.seguetech.com/stigs-security-program/>*

And for More on STIGs, see this SHARE 2015, Session #17735, presentation: *From <https://www.share.org/p/do/sd/topic=64&sid=11911> , 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_wZ36oI
- 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: *https://www.youtube.com/watch?v=QxVD6RIGIeo ,or webinar here: **https://www.sdsusa.com/security-software/automatic-mainframe-stig-monitoring/webinar/***
- BMC/Correlog for Monitoring and Alerting, see: *https://correlog.com*
- CA Auditor for z/OS and Compliance Event Manager, see: *https://www.ca.com/us/products/ca-auditor-zos.html*, and *https://www.youtube.com/playlist?list=PLynEdQRJawmzdBjZI276GRRt3SLqrPIEi*

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

Security Technical Implementation Guide (STIG) 101
From <https://rmf.org/stig-101/>

Command to start the viewer:

java -jar STIGViewer-2.8.jar

Appendix

Extra Goodies Come with the Viewer

U_zOS_V6R39_PDI_list.xlsx

ALL Vulnerabilities with elimination of duplicate Vulnerabilities

	Vul ID	STIG ID	Pri Cond	Sec Cond	Automate	Finished	Automate Check	Check Count	No Automa	Additional info
2										
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	V0000083	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.

U_zOS_V6R39_Cross_Ref_of_SRRAUDIT.xlsx

Authorized Group	Description
CICDAUDT	CICS Developers.
CICSAUDT	CICS Started Task.
CICSDEF	CICS regions default user ids (DFLTUSER).
CICUAUDT	CICS Utils (CONTROLO, BatIDs via CONTROLM, MAINVIEW
CONSOLES	The System Console user ids
DABAAUDT	Data Base Administrators
DAEMAUDT	Unix Daemon user ids
DASBAUDT	DASD batch, jobs that perform DASD Backups, Migrate
DASDAUDT	DASD Administrators
DPCSAUDT	Decentralized Production Control and Scheduling personnel
DUMPAUDT	STCs/Batch ids that perform Dump processing
EMERAUDT	Emergency TSO logon ids
FTPUSERS	FTP only interactive users
IOABAUDT	IOA batch users for operations
MCATBAT	Batch users requiring ALTER access to Master Catalog

STIG ID	Sensitve Member	Description	Logging Starts at	Group	Max Access
				SECAAUDT	ALTER
				SECBAUDT	ALTER
				SYSPAUDT	ALTER
				TSTCAUDT	ALTER
ACP00130	CATMRPT	MASTER SYSTEM CATALOG	WRITE	*	READ
				MCATBAT	ALTER
				SYSPAUDT	ALTER
				TSTCAUDT	ALTER
ACP00135	CATURPT	USER SYSTEM CATALOGS	ALTER	*	UPDATE
				MCATBAT	ALTER
				SYSPAUDT	ALTER
				TSTCAUDT	ALTER
ACP00140	SMPERPT	SMP/E DATA SETS		*	READ

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