OpenRMF 1.4 - Innovation, Automation and Collaboration for DISA STIGs and scans, Nessus scans, OpenSCAP and NIST Controls

https://www.openrmf.io

The only web-based open source tool to help you edit and manage your DISA STIG Checklists, Nessus Scans, NIST Controls, and correlate them automatically!

- Upload Checklists (CKL or XCCDF SCAP)
- Run Compliance and Information Reports
- Filter on Open Items remaining
- Edit and Manage Checklists by System

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Current Challenges Implementing RMF

- Slow process driven by disparate systems
- Compliance with STIGs means checklists are numerous and not automatically related directly to NIST control families
- Information shared via Email, DISA STIG Viewer, Excel, and shared folders – no single source of truth
- Limited management oversight into the IA status and security posture
- Must install Java to use the DISA STIG viewer to edit Checklists
- Teams need actionable data from Nessus ACAS scans easily
- IT Teams must manage the checklists manually
- Checklists are managed and edited ***manually***, one at a time
- Leadership sees Cybersecurity as “black magic” and “too hard”
- Leadership does not see value in Cybersecurity – only hardship
- No correlation of errors and deltas across checklists

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

The RMF Process – 6 Steps

Time Consumers

A. Categorize the System
B. Select the Control Families
OpenRMF here → C. Implement the Controls
OpenRMF here → D. Assess the Controls
E. Authorize the System
OpenRMF here → F. Monitor Controls

Current Timeframe

A	B	C		D		E	F
Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
A	B	C	D	E	F		

OpenRMF

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Complexity of RMF in your System

Example: 1 system consisting of 10 Windows Servers with 1 Application

eMass Process

Categorize System (High / Moderate / Low)

Outputs Selections to NIST Control Categories

Moderate Level system could have 180 controls
AC-1
AC-2
AC-12
PM-2
PM-12

DISA STIG Process

Identify necessary checklists for your system

- (10) Windows 2016 OS Checklists (272 items each)
- (10) Internet Explorer Checklists (136 items each)
- (10) .NET Checklists (16 items each)
- (1) SQL Server 2014 DB Checklist (42 items each)
- (1) SQL Server 2014 Instance Checklist (92 items each)
- (1) Application Security & Development Checklist (288 items)
- (10) Java Checklists (16 items each)

Open a new checklist (***53***) for each with the STIG Viewer to modify and update ***4,822*** items!

No Automated Correlation

Completely Manual!

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Current RMF Process

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

RMF Process with OpenRMF Automation

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Saving Time and Frustration

Task	Currently (manual)	OpenRMF
Import SCAP scans to create a checklist	2 - 5 minutes per scan i.e. 200 checklists = a few days	4 seconds * up to 10 at a time
Create a Starting POA&M on Open and Not Reviewed Items	1 day minimum, depending on the size of the system	5 seconds
Create a Test Plan Summary to 90%	1 day minimum, depending on the size of the system	5 seconds
Upgrade a Checklist to the new Release (Quarterly)	1 hour minimum, depending on the # of items in the checklist	10 seconds per checklist
Keeping Track of the # of Open Items, Not a Finding, Not Reviewed, and N/A by Severity (Category) across all checklists in a complete system	*Too hard to keep current, not done usually*	5 seconds to view 5 seconds to Excel

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

OpenRMF Features

- 100% Open Source tool
- Automatically Relate DISA STIGs with NIST RMF Control Families and Categories Seamlessly
- Automatically Organize Checklists by System
- Single Source of Truth for all System Checklists
- Edit your Checklist data Live through a web browser! Includes ***Bulk Edit*** in v 1.1.
- Run Nessus scan, Checklist, Vulnerability and Controls reports across your whole System
- Management Insight into IA Status and Security Posture
- On premise, local machine, or in the cloud
- 100% Browser based
- Role Based Access Control
- Easily Find Errors and Deltas Across Checklists
- Run Nessus scan, Checklist, and Controls reports
- Removes the IA Mystery!

More information at https://www.openrmf.io/

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

OpenRMF Updates in 2020 and 2021

- **May 2020 - v 1.0 OpenRMF Core (OSS)**
  - Performance Improvements
- **June 2020 - v 1.1 OpenRMF Core (OSS)**
  - Rootless containers, updated UI Components, Bulk Edit for Vulnerabilities
- **July 2020 - v 1.2 OpenRMF Core (OSS)**
  - .NET Core 3.1, Updated server components, Keycloak theme, Compliance Results Filtering
- **Nov 2020 - v 1.3**
  - Severity Override usage in Checklist Scores
  - Various Bug Fixes
- **Dec 2020 - v 1.3.1**
  - Upgrade Checklist process allows upgrading to new Checklists with Vulnerability renumbering
  - Fix on CCI subcontrol references for Compliance Generation
- **February 2020 - v 1.4**
  - Adding OpenSCAP scan result support to create/update STIG Checklists
- **Mar 2021 - v 2.0 Enterprise Features**
  - Multi-Tenant, Versioning of Checklists, Versioning and Merging of Nessus ACAS scan data
  - More Detailed Reporting, Enterprise Connectors to external systems
  - Live POA&M with Automatic updates via Patch Scans, SCAP Scans, and STIG Vulnerability updates
  - System Team Notifications

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

OpenRMF Testimonials

- "The work you all have put into this project is phenomenal! I can't say enough great things about the team and the amazing accomplishments you all have achieved in a very, very short period of time. Now that's what I call CodeHustle!"
- "Using the OpenRMF tool, we reduced the ***three weeks*** to generate our compliance report down to ***5 minutes***. And OpenRMF found an error in our compliance we did manually." – former employee of MSG
- Nick, an ISSO for AWS that supports Joint Forces after seeing and using OpenRMF: *"Hey, guys, look! You've been doing RMF wrong this whole time."*
- "I'm super happy that OpenRMF handles that upgrade of those STIGs and the copy/paste does not have to happen!"
- "Using the list of checklists per system, we were able to update management on our number of open items across all checklists within our system in seconds." - Tutela

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

OpenRMF Core OSS Screenshots

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Dashboard

OpenRMF

- Dashboard
- Systems
- Compliance
- Templates
- Reports
- Upload
- Audit

Dashboard

Home / Dashboard

SYSTEMS	CHECKLISTS	TEMPLATES	VERSION
1	2	0	1.4.0
1 New Systems	2 New Checklists	0 New Templates	OpenRMF OSS

Nessus ACAS Patch Scans

Critical and High Findings

Choose a system to display its ACAS Scan Item Dashboard

Client Boomer

CRITICAL	HIGH	MEDIUM	LOW
11	11	26	0
Open items	Open Items	Open Items	Open Items

SCAP Scans & Checklists

! High, Medium & Low Open Items

Choose a system to display its Open Item Dashboard

Client Boomer

HIGH	MEDIUM	LOW
5	127	5
5 Open High (CAT 1)	127 Open Medium (CAT 2)	5 Open Low (CAT 3)

© 2020 Cingular LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Checklist Upload

OpenRMF

- Dashboard
- Systems
- Compliance
- Templates
- Reports
- Upload
- Audit

Checklist file upload

Home / New checklist upload

Checklist Upload

System Name

OpenRMF PaaS

Select the system this belongs to. Add a new one if needed.

Add a new System

Checklist Files (up to 10 at a time)

Choose files To Upload | Choose Files

Upload and Save

Checklist Upload Help

Use this form to upload a new *.CKL STIG checklist file or SCAP Scan XCCDF *.XML to the system for scoring, indexing, and managing your DoD STIG information. Select your system (if any) and then select up to ten (10) *.CKL or *.XML files to upload at a time. Note that currently, the ***Nessus SCAP scan files are in beta***. DoD SCAP files should work fine.

All fields are mandatory. Once Checklist per CKL file.

* Please fill in the ***Host*** field on your Checklist file CKL! All checklists are named by SYSTEM-HOSTNAME-STIGTYPE-REVISION.

i.e. *PAL Platform - ca2335.myorg.navy.mil - Google Chrome Current Windows STIG - Release: 15 Benchmark Date: 25 Jan 2019*

Template Upload

Title

Enter title

Specify a good title for this Template

Description

Enter a Description

Specify a good description for this Template

Template Checklist File

Choose files To Upload | Choose Files

Template Upload Help

Use this form to upload a new *.CKL STIG checklist template for download and use for any system. A template is used as a starting point or a baseline for that checklist that your administrators, developers, cybersecurity personnel and managers can use to include known statuses and information for that particular checklist.

Example: you have an infrastructure package and a platform-as-a-service package that your application(s) run on. That infrastructure and PaaS have known good checklists as a baseline that application owners use as a starting point and adjust the remaining vulnerability items accordingly.

All fields are mandatory.

© 2020 Cingular LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Checklists by System

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF System Record

OpenRMF

- Dashboard
- Systems
- Compliance
- Templates
- Reports
- Upload
- Audit

System Information and Checklists

Home / System / Checklists

System Information

List All Systems

Title: Windows HQ Network
Checklists: 11
Description: This is the corporate network system
Nessus Scan: Download | Summary Export | Host Export

Generate Test Plan
Generate POAM
Generate RAR

Audit Information:

Created: 02/23/2020 4:45 pm
Last Updated: 03/15/2020 6:36 am
Last Compliance Check: 02/23/2020 4:48 pm

Edit | Compliance | Upload | Delete

System Status

Save Chart

Checklist Filter

Status: Not a Finding, Open, N/A, Not Reviewed

Severity: High (CAT 1), Medium (CAT 2), Low (CAT 3)

Host Name: Enter the host name

* Does a contains search so can be a partial host name

Apply

Checklists

Show 50 entries

Search:

Title	OPEN	NAF	N/A	N/R
DEGTHAT-Google Chrome Current WIN STIG-V1-R18 dated 24 Jan 2020 last updated on 02/23/2020 4:46 pm	17	6	0	19
CAT 1:	1	0	0	0
CAT 2:	14	6	0	18
CAT 3:	2	0	0	1

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Individual Checklist

OpenRMF

- Dashboard
- Systems
- Compliance
- Templates
- Reports
- Upload
- Audit

My Checklist

Home / Checklist

Asset Information

List All Checklists

System: OpenRMF Production PaaS
Host: COMPUTER.DOMAIN
Title: Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide
Version: 2
Release: Release: 17 Benchmark Date: 25 Oct 2019
FQDN:
Tech Area:
Asset Type: Computing
Role: None

Last Updated on 02/21/2020 7:04 am

Edit | Download | Export | Delete

COMPUTER.DOMAIN-WIN SVR 2012/2012 R2 Member SVR STIG-R17 dated 25 Oct 2019

	OPEN	NOT A FINDING	NOT APPLICABLE	NOT REVIEWED
Total	27	230	0	78
CAT 1	4	22	0	7
CAT 2	17	167	0	59
CAT 3	6	41	0	12

* Click on the numbers to filter the Vulnerabilities below

Severity Breakdown

Last Updated on 02/21/2020 7:04 am

Save Chart

Category Breakdown

Last Updated on 02/21/2020 7:04 am

Save Chart

Vulnerability Filter

Status: Not a Finding, Open, N/A, Not Reviewed

Severity: High (CAT 1), Medium (CAT 2), Low (CAT 3)

Apply

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Individual Checklist

OpenRMF

Open | Not a Finding | Not Applicable | Not Reviewed

Last Updated on 02/21/2020 7:04 am

Save Chart

CAT I | CAT II | CAT III

Last Updated on 02/21/2020 7:04 am

Save Chart

Vulnerability Filter

Status: Not a Finding, Open, N/A, Not Reviewed

Severity: High (CAT 1), Medium (CAT 2), Low (CAT 3)

Apply

Vuln Ids

V-3245
V-3289
V-3337
V-3338
V-3339
V-3340
V-3343
V-3344
V-3373
V-3374
V-3377

Vulnerability Details

VULN ID: V-3338

STIG ID: WN12-SO-000055-MS

Severity: high

Rule ID: SV-51497r2_rule

Rule Name: Anonymous Access to Named Pipes

CCI ID: CCI-001090

Rule Title: Named pipes that can be accessed anonymously must be configured to contain no values on member servers.

Classification: Unclass

Discussion: Named pipes that can be accessed anonymously provide the potential for gaining unauthorized system access. Pipes are internal system communications processes. They are identified internally by ID numbers that vary between systems. To make access to these processes easier, these pipes are given names that do not vary between systems. This setting controls which of these pipes anonymous users may access.

Check Text: If the following registry value does not exist or is not configured as

Status & Comments

Edit

Status: Open

Finding Details:

Comments:

Checklist Score Breakdown

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Generate Compliance

OpenRMF

- Dashboard
- Systems
- Compliance
- Templates
- Reports
- Upload

Compliance

Home / Compliance

Compliance Generator

System Filter

OpenRMF Production PaaS

System Impact Level

Moderate

Contains PII / Privacy Data?

☑

Generate

Compliance Help

Generate a Compliance Report across all the checklists in your system to verify your status on satisfying all relevant controls. Follow the steps below to generate and validate your checklists for the chosen Impact Level.

1. Choose your System
2. Choose your Impact Level (Low, Moderate, High)
3. Check if you contain PII, PHI, or Privacy Data
4. Click the Generate button
5. Review the controls and checklists
6. Click the checklist to view the Vulnerabilities for that control
7. Page through the results at the bottom of the table
8. Use the Search box to filter results as you type

Compliance Summary

Summary per family for your System Compliance. Details are below in the next section.

✔ Green = Not A Finding / Not Applicable. Blue = Not Reviewed. ✖ Red = Open.

✖ AC | ⊘ AP | ⊘ AR | AT | ✖ AU | CA | ✖ CM | CP | ⊘ DI | ⊘ DM | ✖ IA

⊘ IP | ⊘ IR | ✖ MA | MP | ⊘ PE | ⊘ PL | PM | ⊘ PS | ⊘ RA | SA | ✖ SC

⊘ SE | ✖ SI | ⊘ TR

Compliance Details

Below find the results. Green = Not A Finding / Not Applicable. Blue = Not Reviewed. Red = Open.

Show 50 entries

Search:

#	Control	Title	Checklists
1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Compliance Details

OpenRMF

Compliance Details

Below find the results. Green = Not A Finding / Not Applicable. Blue = Not Reviewed. Red = Open.

Show 50 entries

Search:

#	Control	Title	Checklists
1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	
3	AC-2	ACCOUNT MANAGEMENT	COMPUTER.DOMAIN-WIN SVR 2012/2012 R2 Member SVR STIG-R17 dated 25 Oct 2019
4	AC-2	ACCOUNT MANAGEMENT	ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019
5	AC-2	ACCOUNT MANAGEMENT	web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019
7	AC-3	ACCESS ENFORCEMENT	COMPUTER.DOMAIN-WIN SVR 2012/2012 R2 Member SVR STIG-R17 dated 25 Oct 2019
8	AC-3	ACCESS ENFORCEMENT	jbossapp.member.local-JBoss EAP 6.3 STIG-R3 dated 25 Jan 2019
9	AC-3	ACCESS ENFORCEMENT	ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019
10	AC-3	ACCESS ENFORCEMENT	sql1.myorg.navy.mil-MSSQL 2014 Database STIG-R6 dated 26 Jan 2018
11	AC-3	ACCESS ENFORCEMENT	web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019
13	AC-4	INFORMATION FLOW ENFORCEMENT	web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019
14	AC-4	INFORMATION FLOW ENFORCEMENT	workstation.myorg.navy.mil-Google Chrome Current WIN STIG-R15 dated 25 Jan 2019
15	AC-5	SEPARATION OF DUTIES	
17	AC-6	LEAST PRIVILEGE	COMPUTER.DOMAIN-WIN SVR 2012/2012 R2 Member SVR STIG-R17 dated 25 Oct 2019
18	AC-6	LEAST PRIVILEGE	jbossapp.member.local-JBoss EAP 6.3 STIG-R3 dated 25 Jan 2019
19	AC-6	LEAST PRIVILEGE	ocp2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019
20	AC-6	LEAST PRIVILEGE	web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019
22	AC-7	UNSUCCESSFUL LOGON ATTEMPTS	COMPUTER.DOMAIN-WIN SVR 2012/2012 R2 Member SVR STIG-R17 dated 25 Oct 2019

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Reports

© 2020 Cingular LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Nessus Reports

Reports - Nessus Scan Report

Home / Reports

Filters

System Filter: OpenRMF Production PaaS | Run Report

Choose your System and click Run Report

Nessus Scan Report: 168.138.17.78

Show 50 entries

Search:

	Host	Plugin Id	Plugin Name	Family	Severity
+	168.138.17.78	57690	Terminal Services Encryption Level is Medium or Low	Misc.	2 - Medium
−	168.138.17.78	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows	2 - Medium

Click the + to get more detailed information

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Plugin Type

remote

Publication Date

2005/06/01

+	168.138.17.78	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	2 - Medium

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF System Reports

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Checklist Reports

Reports - Checklist Report

Home / Reports

Filters

System Filter ← **Choose the System**

OpenRMF Production PaaS

Checklist ← **Choose the Checklist**

web1.myorg.mil-ASD STIG-R9 dated 25 Jan 2019

Run Report ← **Run the Report**

Asset Information

System: OpenRMF Production PaaS
Host: web1.myorg.mil
Title: Application Security and Development Security Technical Implementation Guide
Release: Release: 9 Benchmark Date: 25 Jan 2019
FQDN:
Tech Area:
Asset Type: Computing
Role: None

Show 50 entries

Search:

	Vuln ID	Severity	Rule ID	STIG ID	Status	Title	CCI
	V-69239	medium	SV-83861r1_rule	APSC-DV-000010	Open	The application must provide a capability to limit the number of logon sessions per user.	CCI-000054
	V-69241	medium	SV-83863r1_rule	APSC-DV-000060	Not Reviewed	The application must clear temporary storage and cookies when the session is terminated.	CCI-002361

Click for more detail

Discussion

Persistent cookies are a primary means by which a web application will store application state and user information. Since HTTP is a stateless protocol, this persistence allows the web application developer to provide a robust and customizable user experience. However, if a web application stores user authentication information within a persistent cookie or other temporary storage mechanism, this information can be stolen and used to compromise the users account. Likewise, HTML 5 provides the developer with a client storage capability where application data larger than the 4K cookie size limit can be stored on the local client. While this can be beneficial to the developer, this is considered insecure storage and should not be used for storing sensitive session or security tokens. A cross site scripting attack can put this data at risk. Web applications must clear sensitive data from files and storage areas on the client when the session is terminated.

Check Content

Review application design documentation and interview application administrator to identify how the application makes use of temporary client storage and cookies. Identify cookie and web storage locations on the client. Clear all browser cookies and web cache. Log on to the application and perform several standard operations, noting if the application ever prompts the user to accept a cookie. If prompted by the browser to save the user ID and password (decline to save the user ID and password), this is a finding. Log out of the application and close the browser. Reopen the browser and examine the stored cookies. The cookies displayed should be related to the application website. The procedure to view cookies will vary according to the browser used. Some modern browsers are making use of SQLite databases to store cookie data so use of a SQLite db reader/browser may be required. Open the cookies related to the application website and search for any identification or authentication information. While authentication information can vary on a per application basis, this is most often specified as "username=x" or "password=x". If the web application prompts the user to save their password, or if a username or password value exists within a cookie or

© 2020 Cingulara LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Metrics (Grafana)

© 2020 Cingular LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Metrics (Grafana)

© 2020 Cingular LLC. © 2020 Tutela LLC. All Rights Reserved.

Screen Shots – OpenRMF Metrics (Grafana)

© 2020 Cingular LLC. © 2020 Tutela LLC. All Rights Reserved.