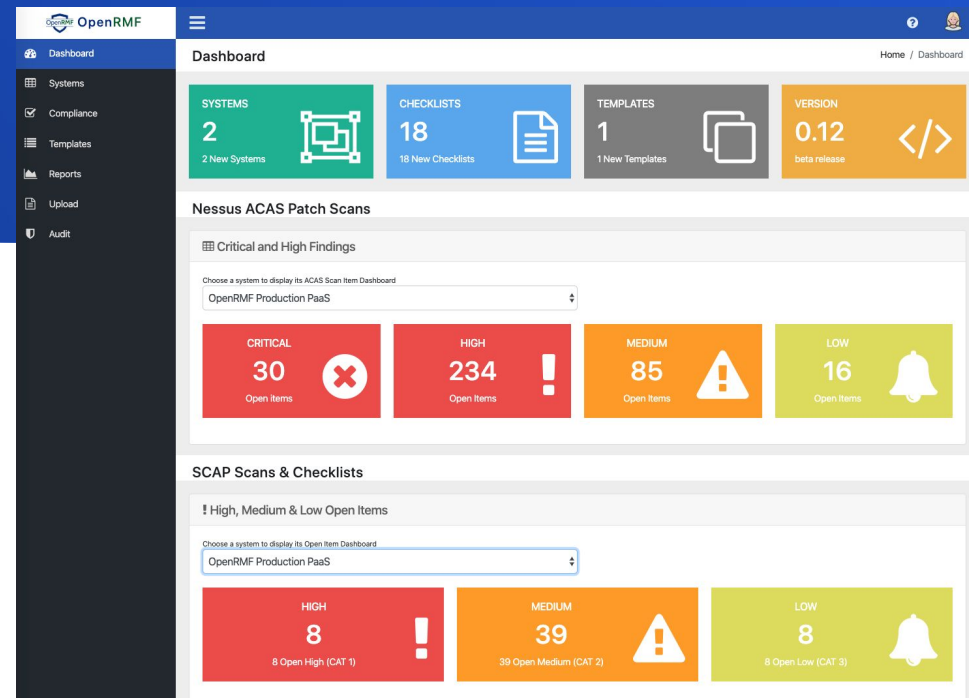


OpenRMF - Innovation and Automation for DISA STIGs and scans, Nessus scans and NIST Controls

<https://www.openrmf.io>

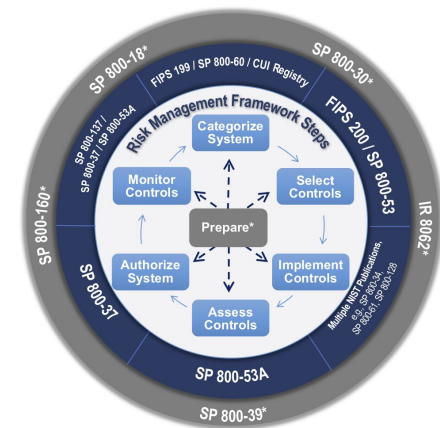
The only web-based open source tool to help you edit and manage your DISA STIG Checklists, Nessus Scans, NIST Controls, and correlate them automatically!

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



Current Challenges Implementing RMF

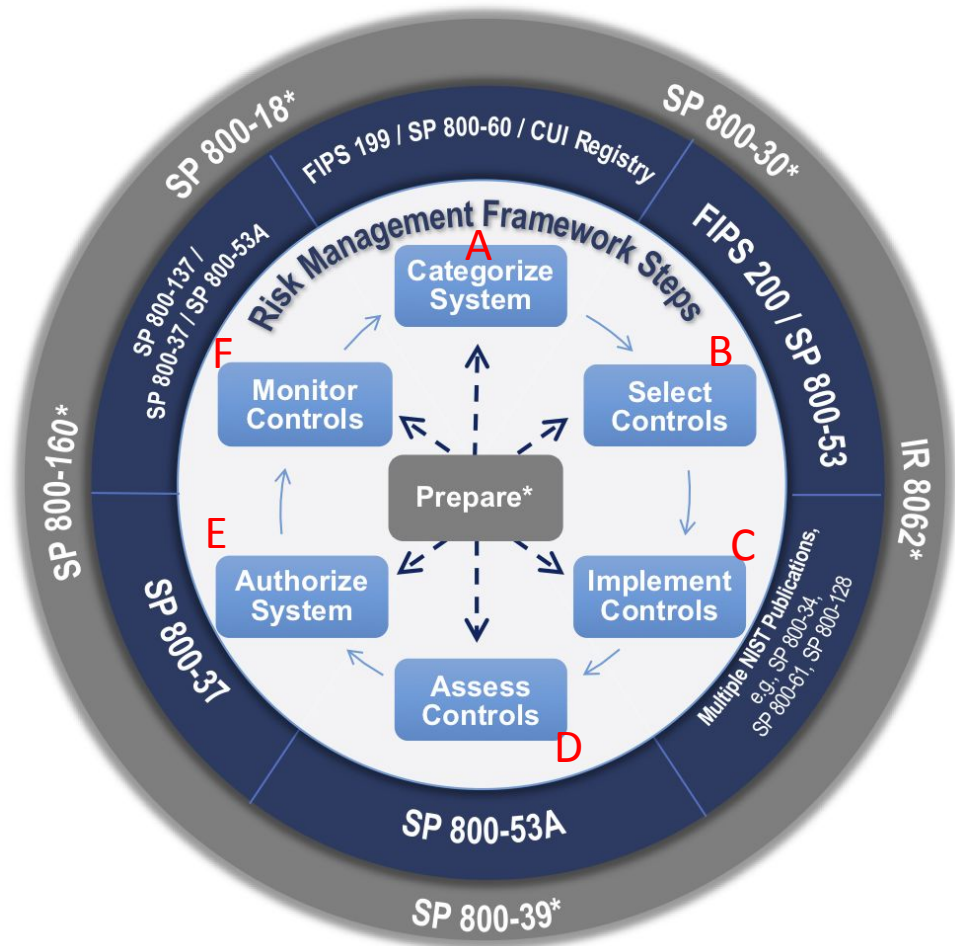
- Slow process driven by disparate systems
- Compliance with STIGs means checklists are numerous and not related directly to NIST control families
- Information shared via Email, DISA STIG Viewer, Excel, and shared folders – no single source of truth
- Limited management oversight into the IA status 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 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



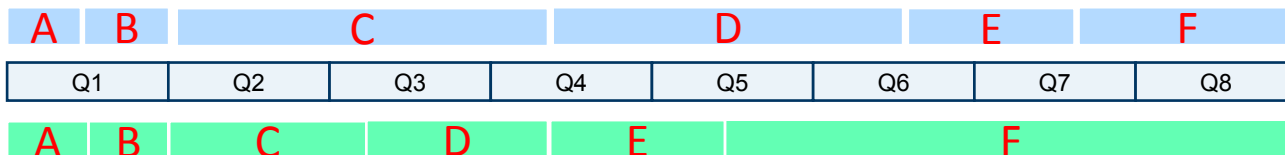
The RMF Process – 6 Steps

Time Consumers

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



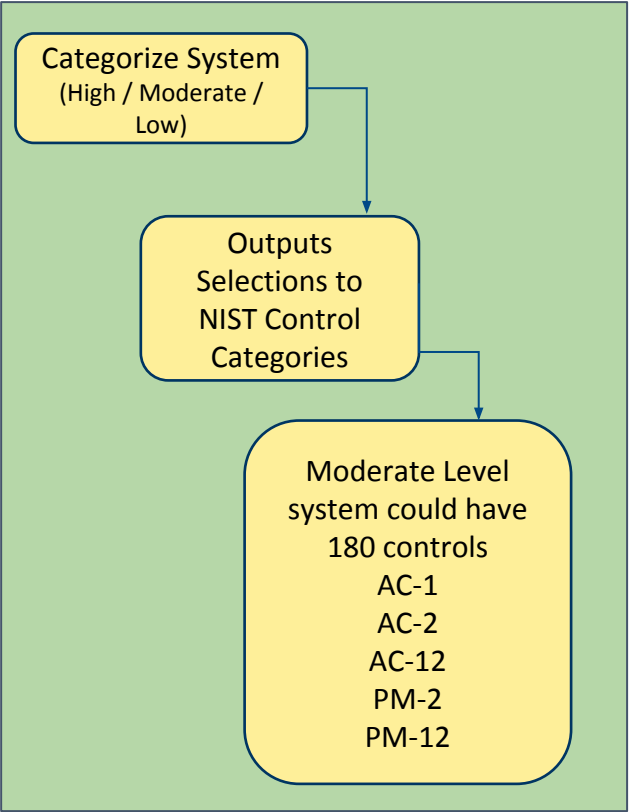
Current Timeframe



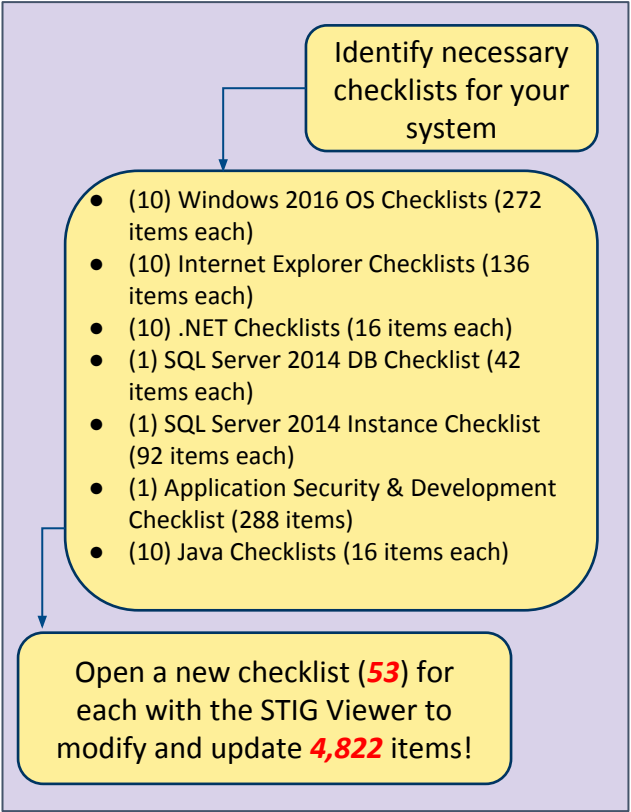
Complexity of RMF in your System

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

eMass Process

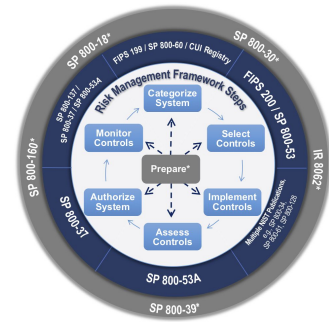


DISA STIG Process

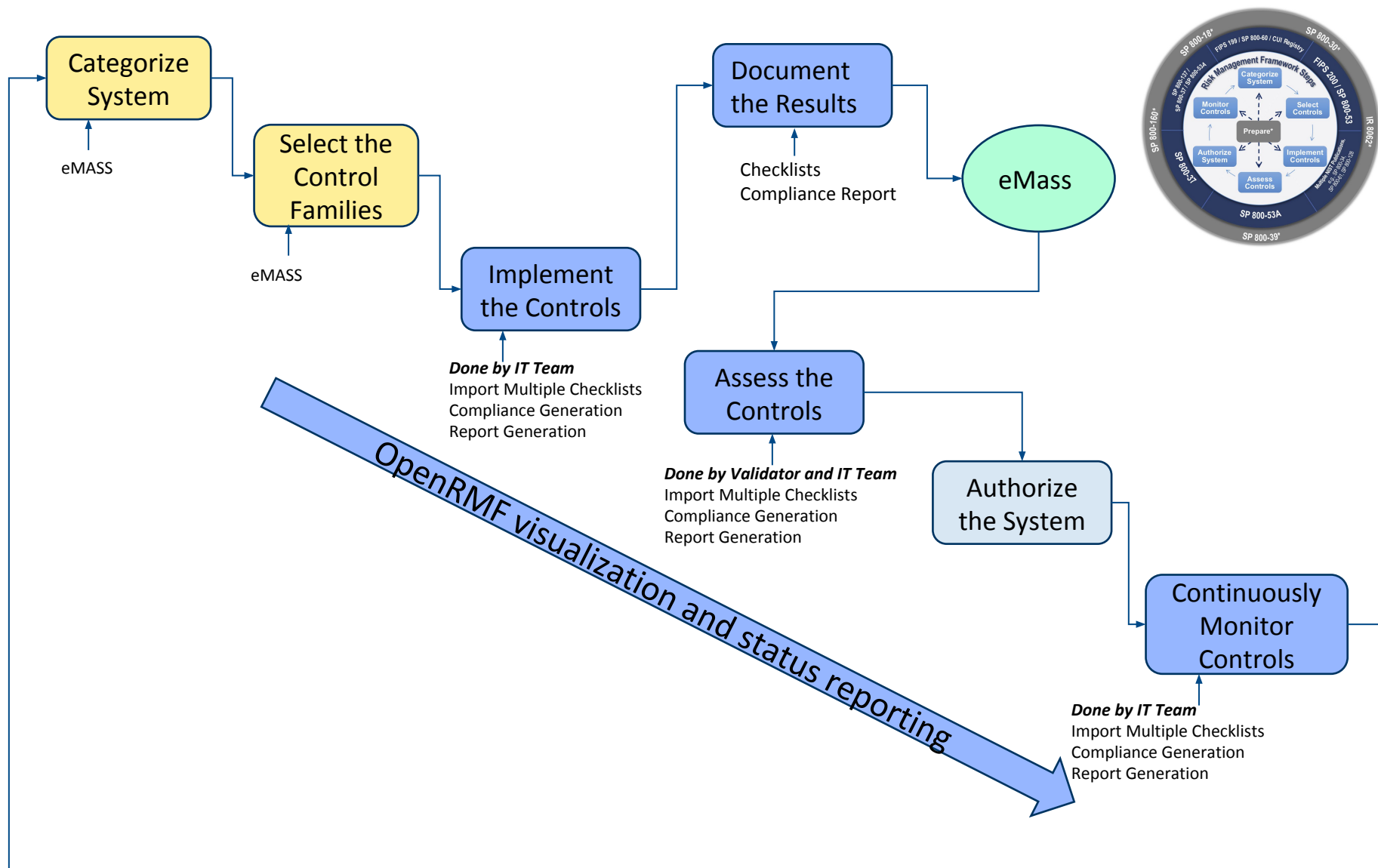


**No Automated
Correlation**

Completely Manual!



RMF Process with OpenRMF Automation



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!
- 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/>

Coming Soon...

- March 2020 v 0.12 (*in progress*)
 - (*done!*) Automatically create your Test Plan Summary
 - Automatically create your POA&M
 - Automatically create your Risk Assessment Report
 - (*done!*) Live Editing of Checklists Online
 - (*done!*) Better reporting and filtering of data

- ~ September 2020 - v 1.0 Enterprise Features
 - Versioning of Checklists
 - More Detailed Reporting
 - Multi-Tenant
 - Versioning and Merging of Nessus ACAS scan data
 - Enterprise Connectors to external systems

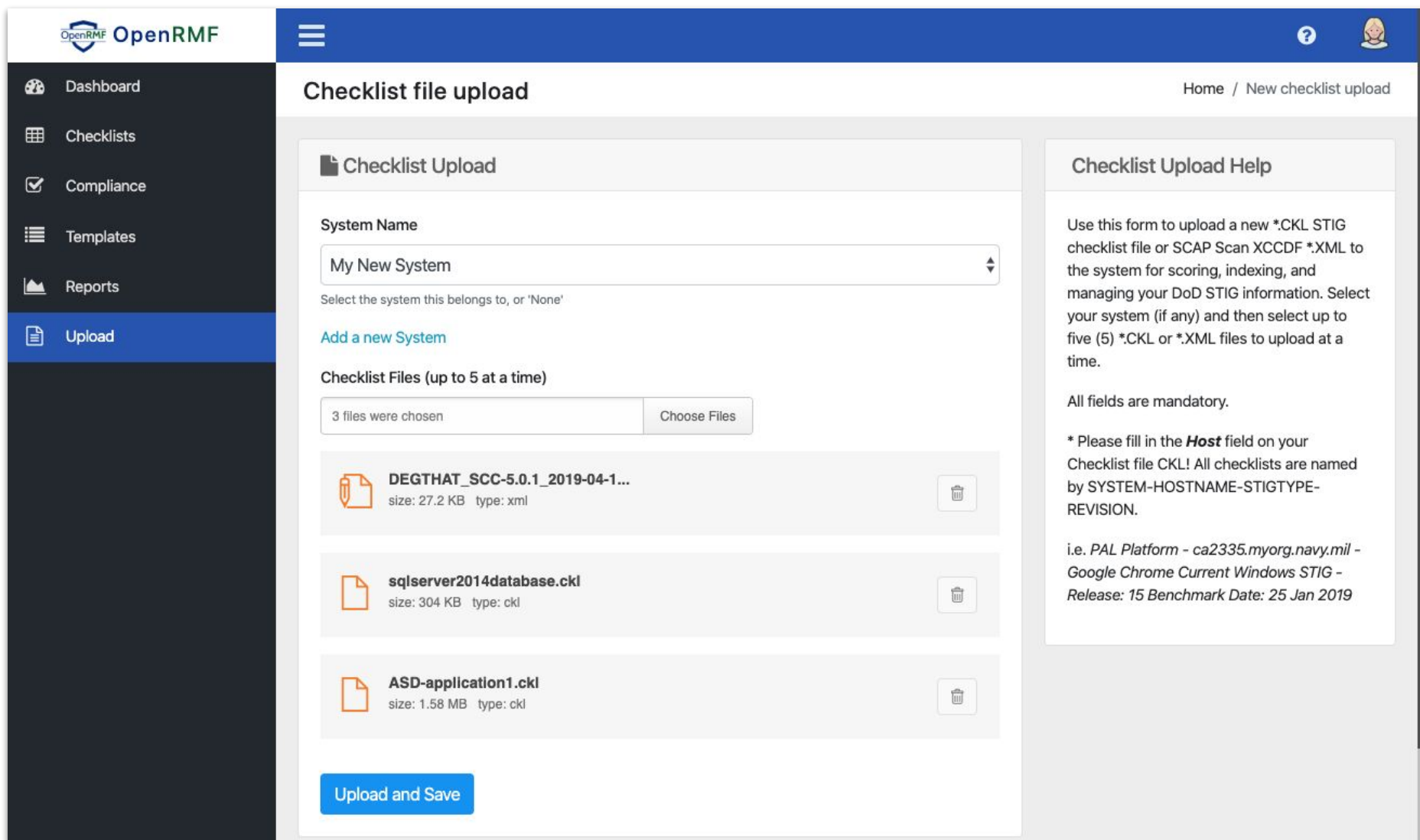
“Using the OpenRMF tool, we reduced the three weeks to generate our compliance report down to 5 minutes. And OpenRMF found an error in our compliance we did manually.” – former employee of MSG

“With the OpenRMF Tool, we quickly found 2 servers with the exact same hostname we did not see by looking at each checklist individually.” - Neany

“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

OpenRMF v 0.12 Screenshots

Screen Shots – OpenRMF Checklist Upload



The screenshot displays the OpenRMF web application interface for uploading checklist files. On the left is a dark sidebar with navigation links: Dashboard, Checklists, Compliance, Templates, Reports, and Upload (highlighted in blue). The main content area has a blue header with the OpenRMF logo, a hamburger menu, and user icons. Below the header, the page title is 'Checklist file upload' with a breadcrumb trail 'Home / New checklist upload'. The central form is titled 'Checklist Upload' and includes a 'System Name' dropdown menu currently set to 'My New System', with a note to 'Select the system this belongs to, or 'None''. Below this is a link to 'Add a new System'. The 'Checklist Files (up to 5 at a time)' section shows a file selection summary '3 files were chosen' and a 'Choose Files' button. Three files are listed: 'DEGTHAT_SCC-5.0.1_2019-04-1...' (27.2 KB, xml), 'sqlserver2014database.ckl' (304 KB, ckl), and 'ASD-application1.ckl' (1.58 MB, ckl). Each file entry has a trash icon for deletion. At the bottom of the form is a blue 'Upload and Save' button. To the right of the form is a 'Checklist Upload Help' section containing instructions on how to use the form to upload *.CKL or *.XML files, a note that all fields are mandatory, and a warning to fill in the 'Host' field with examples like 'ca2335.myorg.navy.mil'.

Checklist Upload

System Name



My New System



Select the system this belongs to, or 'None'



[Add a new System](#)

Checklist Files (up to 5 at a time)

3 files were chosen [Choose Files](#)

 **DEGTHAT_SCC-5.0.1_2019-04-1...**
size: 27.2 KB type: xml 

 **sqlserver2014database.ckl**
size: 304 KB type: ckl 

 **ASD-application1.ckl**
size: 1.58 MB type: ckl 

[Upload and Save](#)

Checklist Upload Help

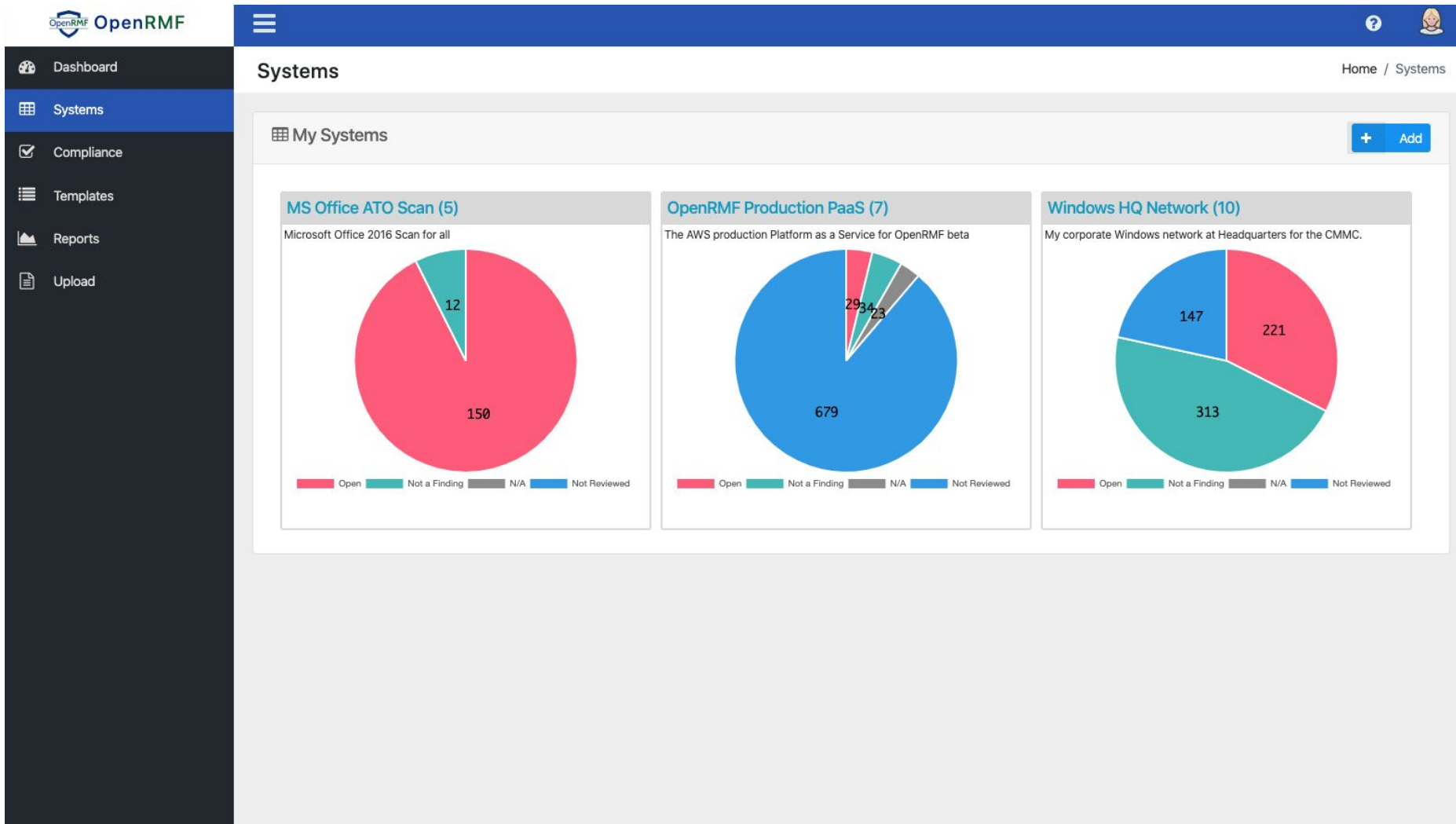
Use this form to upload a new *.CKL STIG checklist file or SCAP Scan XCCDF *.XML to the system for scoring, indexing, and managing your DoD STIG information. Select your system (if any) and then select up to five (5) *.CKL or *.XML files to upload at a time.

All fields are mandatory.

* 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

Screen Shots – OpenRMF Checklists by System



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: OpenRMF Production PaaS

Checklists: 8

Description: The AWS production Platform as a Service for OpenRMF beta

Nessus Scan: [Download](#) | [Summary Export](#) | [Host Export](#)

Test Plan Summary: [Generate Excel File](#)

Latest POA&M: (future)

Last Risk Assessment Report: (future)

Audit Information:

Created: 12/01/2019 11:31 am

Last Updated: 02/02/2020 8:25 pm

Last Compliance Check: 02/20/2020 9:50 am

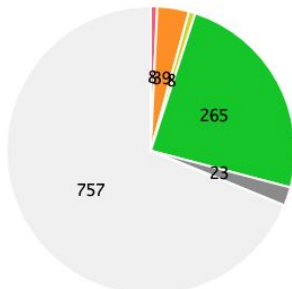
Edit

Compliance

Upload

Delete

System Status



757 265 23 8 8

CAT 1 Open CAT 2 Open CAT 3 Open Not a Finding Not Reviewed

Save Chart

Checklist Filter

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

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

Apply

Checklists

Show 50 entries

Search:

	Title	OPEN	NAF	N/A	N/R
	COMPUTER.DOMAIN-WIN SVR 2012/2012 R2 Member SVR STIG-R17 dated 25 Oct 2019 last updated on 02/21/2020 7:04 am	27	230	0	78
	jbossapp.member.local-JBoss EAP 6.3 STIG-R3 dated 25 Jan 2019 last updated on 02/21/2020 7:12 am	4	6	3	54
	oco2.worker2.edmz.mil-REL 7 STIG-R2 dated 25 Jan 2019				

© 2019 Cingulara LLC. © 2019 Tutela LLC. All Rights Reserved.

<https://www.openrmf.io>

13

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

Severity Breakdown

Severity	Count
Open	27
Not a Finding	230
Not Reviewed	78

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

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

Category Breakdown

Category	Count
CAT I	33
CAT II	243
CAT III	59

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

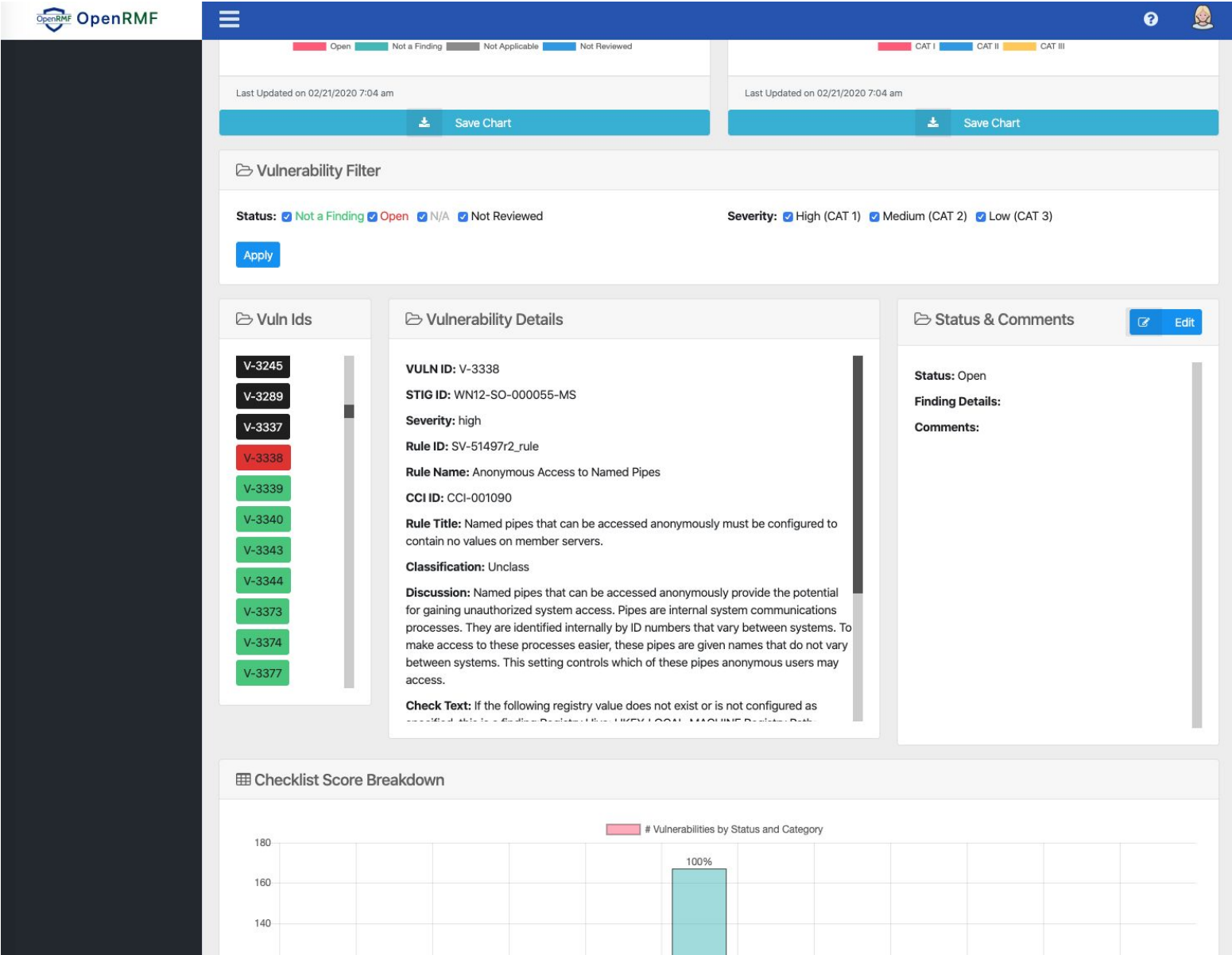
Save Chart

© 2019 Cingulara LLC. © 2019 Tutela LLC. All Rights Reserved.

<https://www.openrmf.io>

14

Screen Shots – OpenRMF Individual Checklist



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	

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

Screen Shots – OpenRMF Reports



Dashboard

Systems

Compliance

Templates

Reports

Upload


Audit

Home / Reports

Reports


Available Reports

Nessus Patch Listing




Run Report

System Pie Charts




Run Report

System Checklist Listing




Run Report

RMF Controls Listing











Run Report

Host Vulnerability Report



Run Report

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

	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

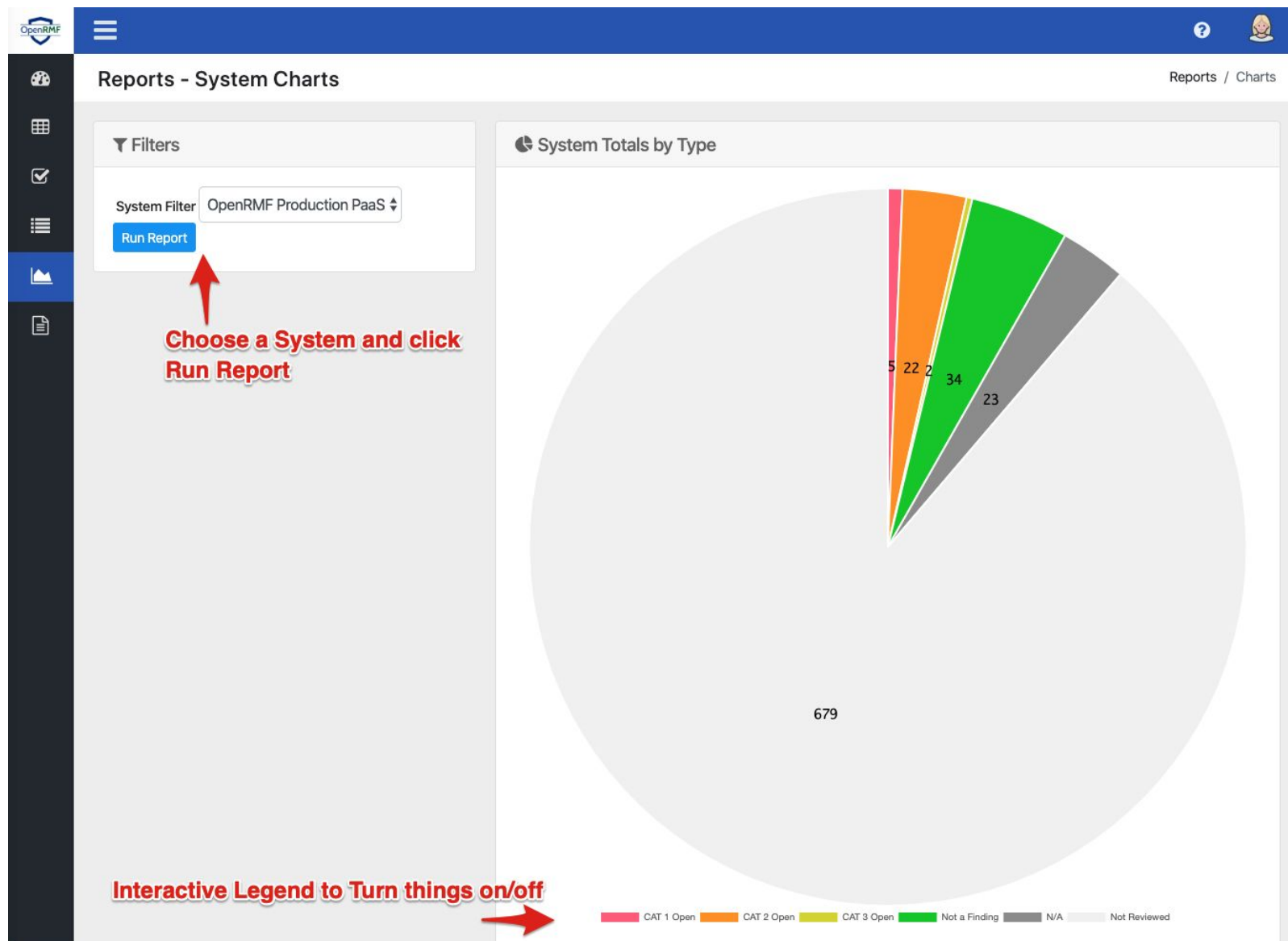
remote

Publication Date

2005/06/01

+	168.138.17.78	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	2 - Medium
+	168.138.17.78	57688	SSL Self-Signed Certificates	General	2 - Medium

Screen Shots – OpenRMF System Reports



Screen Shots – OpenRMF Checklist Reports



Home / Reports

Filters

System Filter

OpenRMF Production PaaS

Checklist

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

Run 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

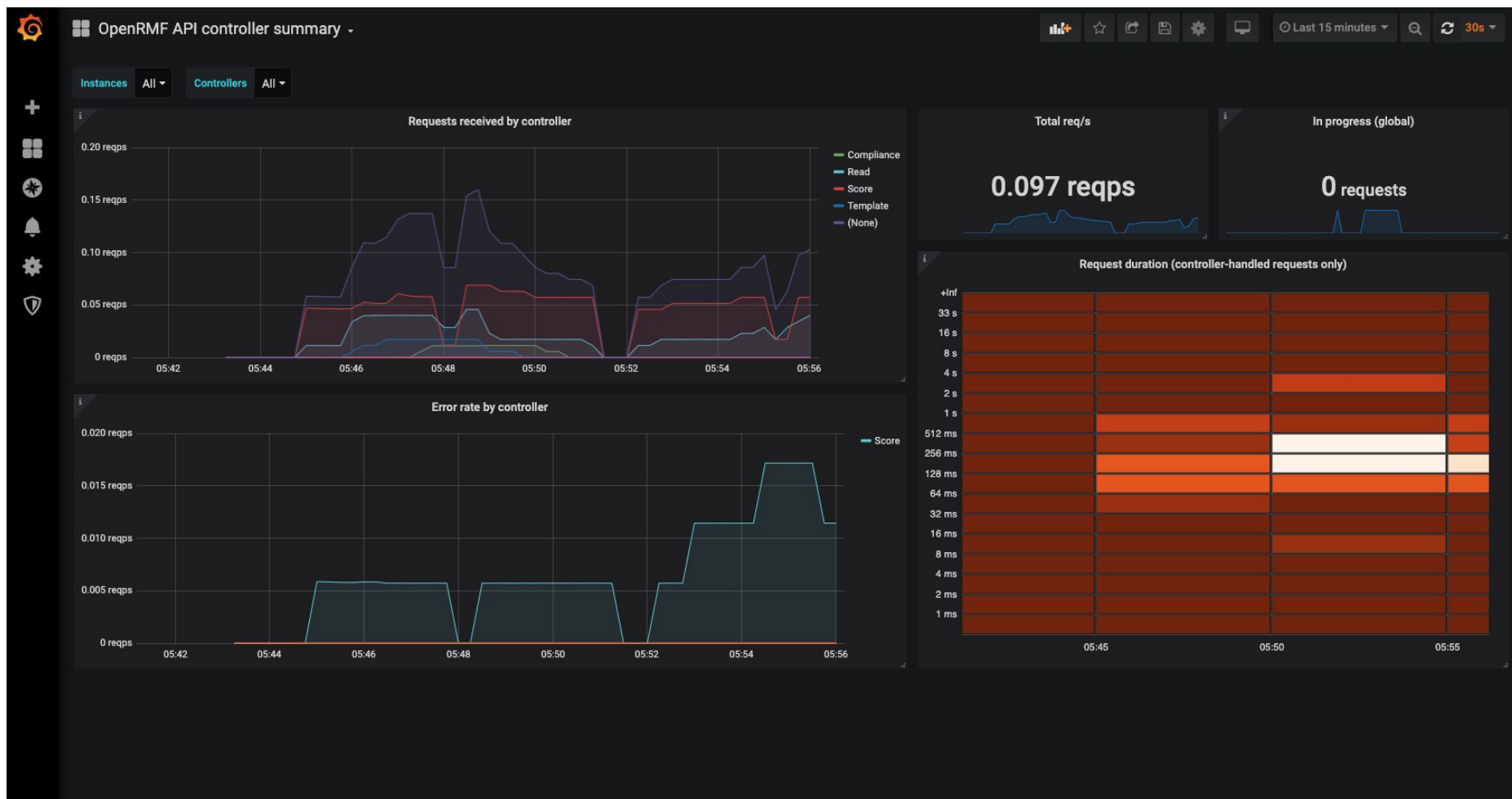
Discussion

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.

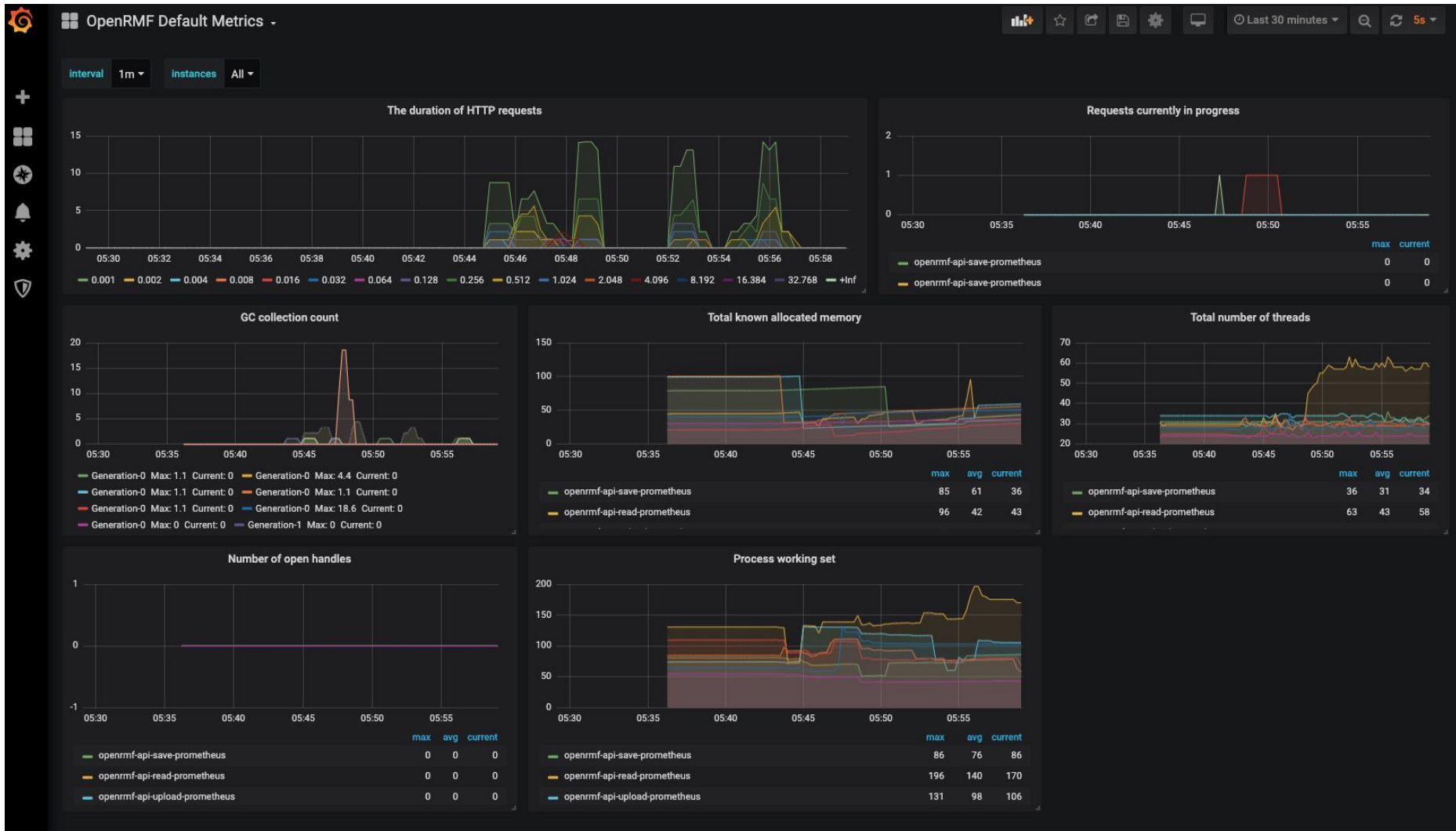
Check Content

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=" or "password=" If the web application prompts the user to save their password or if a username or password value exists within a cookie or

Screen Shots – OpenRMF Metrics (Grafana)



Screen Shots – OpenRMF Metrics (Grafana)



Screen Shots – OpenRMF Metrics (Grafana)

