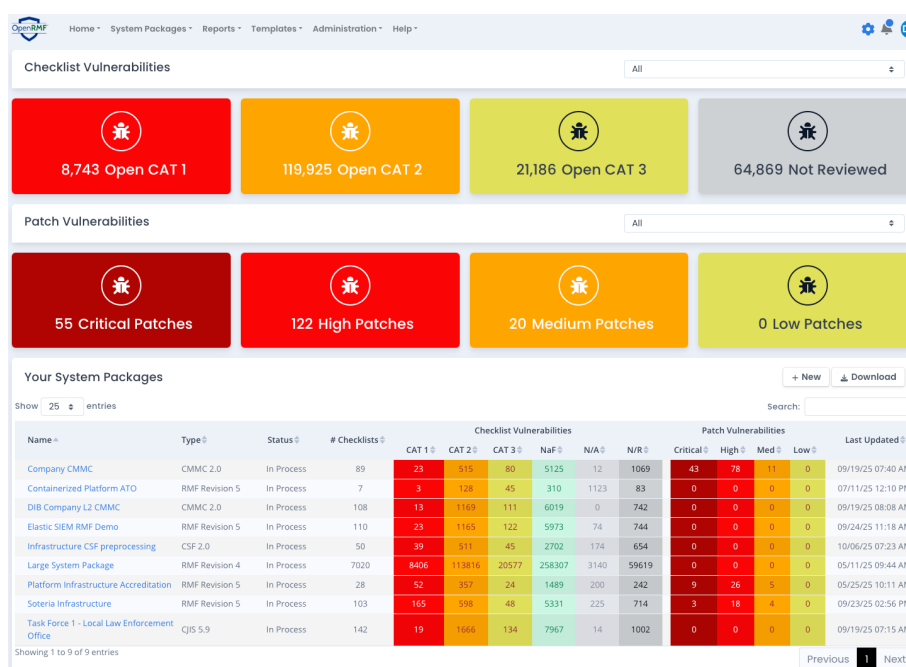


See The OpenRMF® Professional Difference

What makes our solution right for you and your team



OpenRMF® Professional is a revolution in cyber compliance automation for any cyber compliance framework including Risk Management Framework (RMF), FedRAMP, CMMC, CSF and any more.

Our solution ingests all your scan data, checklists, compliance statements, inherited controls and other information and automatically relates that to your framework's required controls. You can instantly automate updating your POAM status. Keep track of all checklist data from raw scan updates, manual updates or our bulk vulnerability edit feature. Setup compliance statements. Bring in inherited controls. Track all history of changes automatically for the who, what, when, why for configuration management. All from one solution that is web based, has role based access as well as group permissions, tracks auditing at multiple levels, and even has a journal feature for a running history from day 1.

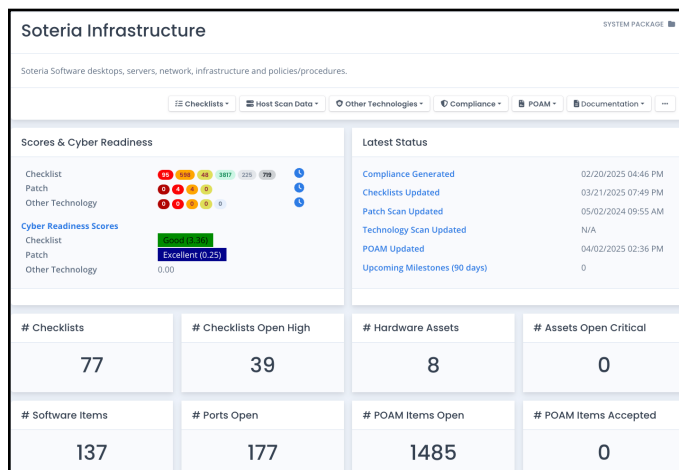
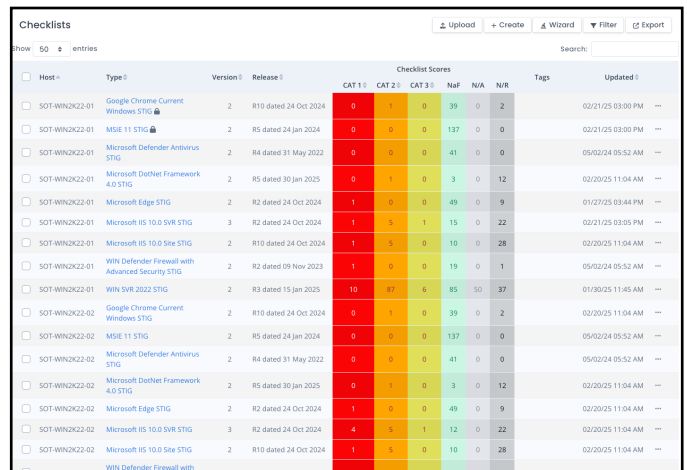
Cyber compliance is a team event. At least it should be. And it is continuously in motion. The whole team needs to know their part of the "playbook" and what role they play. Having one spot for viewing all this information in a way that makes sense to YOUR PART of the team makes this process much easier, faster, and a lot less stressful.

1. AUTOMATING CYBER COMPLIANCE AROUND THE SCANS YOU ALREADY PERFORM

Our OpenRMF® Professional ingests scans you are already doing. Then automates around them FOR YOU! You can use your raw SCAP scans or audit compliance CIS benchmark scans and quickly see where you are with regard to required compliance. Do the same with your patch vulnerability scans, software scans, and container image scans.

Use the web interface or our API to automate even further. You are already doing the scans. Make them work for you! As we always say...

Do the Work. Automate the Paperwork!

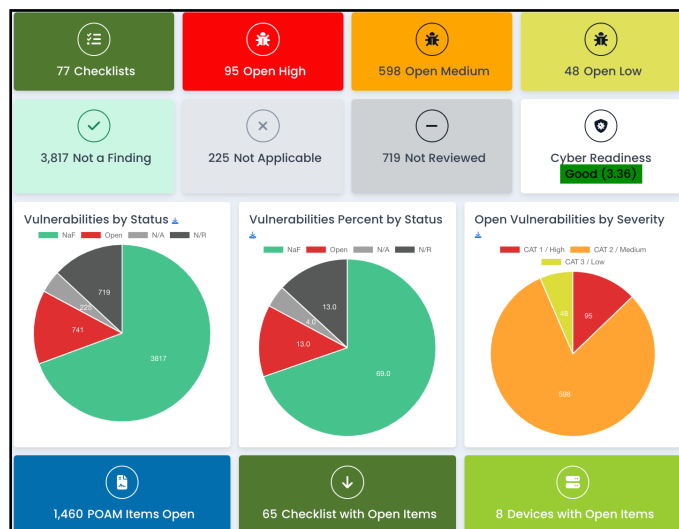



Checklists

Upload + Create Wizard Filter Export

Show 50 entries

Host	Type	Version	Release	CAT 1	CAT 2	CAT 3	Nat	N/A	N/R	Tags	Updated
SOT-WIN2K22-01	Google Chrome Current Windows STIG	2	R10 dated 24 Oct 2024	0	1	0	39	0	2		02/21/25 03:00 PM
SOT-WIN2K22-01	MSIE 11 STIG	2	R5 dated 24 Jan 2024	0	0	0	137	0	0		02/21/25 03:00 PM
SOT-WIN2K22-01	Microsoft Defender Antivirus STIG	2	R4 dated 31 May 2022	0	0	0	41	0	0		05/02/24 05:52 AM
SOT-WIN2K22-01	Microsoft DotNet Framework 4.0 STIG	2	R5 dated 30 Jan 2025	0	1	0	3	0	12		02/20/25 11:04 AM
SOT-WIN2K22-01	Microsoft Edge STIG	2	R2 dated 24 Oct 2024	1	0	0	49	0	9		01/27/25 03:44 PM
SOT-WIN2K22-01	Microsoft IS 10.0 SVR STIG	3	R2 dated 24 Oct 2024	1	0	1	15	0	22		02/21/25 03:05 PM
SOT-WIN2K22-01	Microsoft IS 10.0 Site STIG	2	R10 dated 24 Oct 2024	1	0	0	10	0	28		02/20/25 11:04 AM
SOT-WIN2K22-01	WIN Defender Firewall with Advanced Security STIG	2	R2 dated 09 Nov 2023	1	0	0	19	0	1		05/02/24 05:52 AM
SOT-WIN2K22-01	WIN SVR 2022 STIG	2	R3 dated 15 Jan 2025	10	87	6	85	50	37		01/30/25 11:45 AM
SOT-WIN2K22-02	Google Chrome Current Windows STIG	2	R10 dated 24 Oct 2024	0	1	0	39	0	2		02/20/25 11:04 AM
SOT-WIN2K22-02	MSIE 11 STIG	2	R5 dated 24 Jan 2024	0	0	0	137	0	0		05/02/24 05:52 AM
SOT-WIN2K22-02	Microsoft Defender Antivirus STIG	2	R4 dated 31 May 2022	0	0	0	41	0	0		05/02/24 05:52 AM
SOT-WIN2K22-02	Microsoft DotNet Framework 4.0 STIG	2	R5 dated 30 Jan 2025	0	1	0	3	0	12		02/20/25 11:04 AM
SOT-WIN2K22-02	Microsoft Edge STIG	2	R2 dated 24 Oct 2024	1	0	0	49	0	9		02/20/25 11:04 AM
SOT-WIN2K22-02	Microsoft IS 10.0 SVR STIG	3	R2 dated 24 Oct 2024	4	0	1	12	0	22		02/20/25 11:04 AM
SOT-WIN2K22-02	Microsoft IS 10.0 Site STIG	2	R10 dated 24 Oct 2024	1	0	0	10	0	28		02/20/25 11:04 AM



2. HYPER AUTOMATION AROUND YOUR COMPLIANCE DATA TO MAKE IT WORK FOR YOU

Now that your data is ingested, we automate even further. Automatically fill out your POAM and keep it up-to-date based on your latest uploaded/updated data on scans and compliance statements. Automatically track trends on vulnerabilities from all scans, including software and container scans if you need that.

Automate your cyber compliance scores (a.k.a. CCRI) instantly based on your most up-to-date data. Automatically track the number of open vulnerability items per area and the number of active checklists. Automatically related every single checklist — vulnerability — CCI, compliance statement, and inherited or common control to all cyber compliance controls you have to meet.

And keep track of that trend over time with snapshots. Have boilerplate pre-filled checklists with common answers and locked vulnerabilities so false positives are a thing of the past. And save every single edit of all data to have traceability on who did what/where/when/why/how across your cyber compliance data.

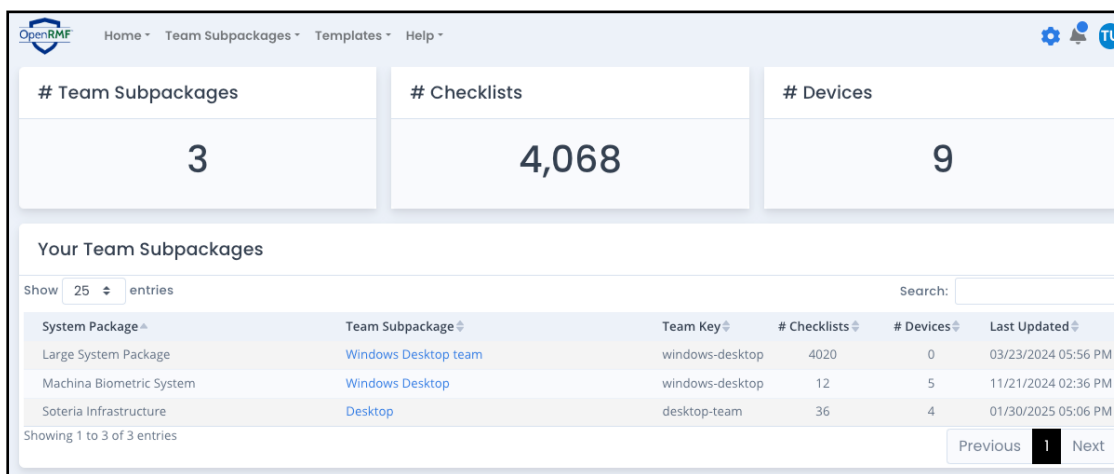


3. TEAM COLLABORATION AROUND YOUR CYBER COMPLIANCE DATA AND PROCESSES

With your information in one single “pane of glass”, now your team can collaborate easier and perform their jobs faster. Cyber compliance and the cyber compliance frameworks look like magic to those not in the cyber space. OpenRMF Professional is designed to be collaborative from day 1 to help alleviate this challenge.

You see your specific data, your impact, and the information in your accreditation package relates to anyone where an analyst, cyber specialist, system administrator, program manager, assessor or anyone that needs to see that information.

View the compliance data across all checklists, statements, and inherited information. See a checklist filtered by a certain framework control or subcontrol. Show what has been fix, what has not, and the severity of the problem. Filter checklists to show only those with open vulnerabilities. No matter what your role or what you are looking to do, we have a view for you to use.



The screenshot shows the OpenRMF Professional dashboard. At the top, there are navigation links: Home, Team Subpackages, Templates, and Help. On the right, there are icons for settings, notifications, and a user profile. The main content area is divided into three sections: # Team Subpackages (3), # Checklists (4,068), and # Devices (9). Below these, there is a section titled 'Your Team Subpackages' with a table of data. The table has columns for System Package, Team Subpackage, Team Key, # Checklists, # Devices, and Last Updated. There are three entries in the table. At the bottom of the table, it says 'Showing 1 to 3 of 3 entries'. There are also 'Previous' and 'Next' buttons.

System Package	Team Subpackage	Team Key	# Checklists	# Devices	Last Updated
Large System Package	Windows Desktop team	windows-desktop	4020	0	03/23/2024 05:56 PM
Machina Biometric System	Windows Desktop	windows-desktop	12	5	11/21/2024 02:36 PM
Soteria Infrastructure	Desktop	desktop-team	36	4	01/30/2025 05:06 PM

4. EASY INSTALLATION, SETUP, AND USE ON DAY 1

Installation and setup can be done in 15 minutes. You do not need several weeks to configure massive numbers of questions, workflows, gates, and have a Masters Degree in the application tooling to get it to work. You also do not need an OpenRMF® Professional specialist to install and run this solution. Anyone on your current team that is good at installing software and following guides can get this running for you easily.

You can pull down an OVA, run Ansible scripts or even do a manual installation if you prefer. We have documentation on installation, configuration, and usage. We also have a video on demand site with tutorials to go along with the documentation to make this process simple to follow.

Download and evaluate for yourself at <https://www.soteriasoft.com/>