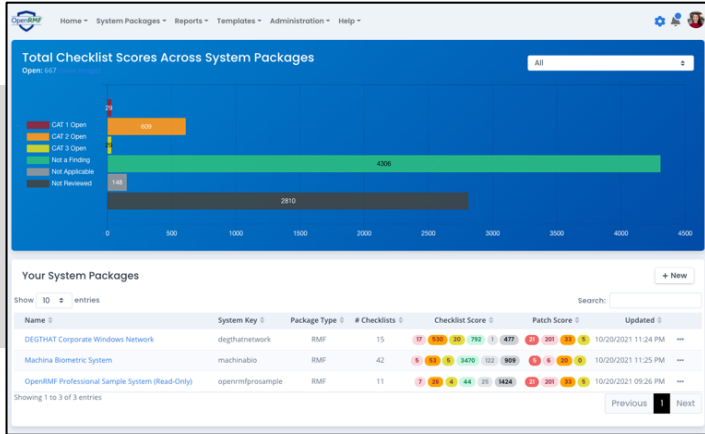


OpenRMF® Professional by Soteria Software

Cyber Compliance Automation

RMF and FedRAMP Tracking and Automation for your team, program office, organization or enterprise! Have a single source-of-truth for your scans, checklists, and system package information that is web-based and securely accessible. Reduce time to submit your ATO by 40+%!



System Package Dashboard

- Show system packages only where you have access
- Quickly view patch score vulnerabilities by severity
- Quickly view total checklist vulnerabilities by severity and category

Track Scans and Checklists Easily

- Upload SCAP, Checklist and Nessus/ACAS scans
- Track changes, vulnerability score updates, and history automatically
- Automate upload through our open API
- Easily answer data calls around RMF and Vulnerabilities

The Checklists table displays a list of system packages and their associated checklists. Columns include Host, Type, Version, Release, Score, Tags, and Updated. The table lists various checklists for different system packages, including McAfee VirusScan, Microsoft DotNet Framework, MSIE 11 STIG, WIN 10 STIG, WIN Defender Antivirus STIG, WIN Firewall with Advanced Security STIG, Cisco IOS Switch L2S STIG, Cisco IOS Switch NDM STIG, Microsoft Word 2016 STIG, and McAfee VirusScan 8.8 Local Client STIG.

The Compliance Summary Map shows a grid of colored boxes representing different compliance categories: AC, AT, AU, CA, CM, CP, IA, IR, MA, MP, PE, PL, PM, PS, RA, SA, SC. Below the map is the Checklist Compliance Listing table, which shows a list of controls and their associated checklists. The table includes columns for #, Control, Title, Checklist, and Overall Status. The table lists several controls related to account management and automated audit actions, with their respective checklists and overall status (e.g., Open, Not a Finding).

Generate Compliance Quickly

- Generate compliance against RMF or FedRAMP level
- Include tailoring and overlays
- View Checklists Vulnerabilities filtered for each NIST control and sub-control



OpenRMF® Professional by Soteria Software

What is OpenRMF® Professional?

A secure, collaborative, web-based application for tracking cyber compliance for your ATO, ATC, IATT or Type Accreditation system package from start to finish. Automatically read in patch and SCAP scans, create checklists, track vulnerabilities, and generate compliance with ease. Notify team members of work performed across the team for the entire system package.

☰ Ease Collection of Data

Tools for tracking cyber compliance data:

- Quick upload/import of SCAP, checklists, and scans
- Bulk Editing for consistency across multiple checklists
- Bulk Lock vulnerabilities or entire checklists for protection

🔄 Tracking Your Data

Automatic configuration management and history tracking:

- Track checklist vulnerability numbers across checklists changes, by severity and status, over time
- Track patch vulnerabilities over time, by device and severity

✅ Generate Compliance and Status

Show True Compliance:

- Generate compliance with inherited security controls, levels and tailoring
- Dive into checklists, filtered by the NIST control or sub-control being viewed

Enhanced Reporting for Data Calls

- Each checklist and patch scan generates reporting data
- Easily answer data calls on open vulnerabilities, patches, ports and protocols, from a source-of-truth
- Export reports, charts or PowerPoint Summary data

System Package Vulnerabilities Report

Choose your System Package: Machina Biometric System

Choose your Severity: CAT 1 / High, CAT 2 / Medium, CAT 3 / Low

Choose your Status: Open, Not a Finding, Not Applicable, Not Reviewed

→ Run Report

Vuln ID	STIG ID	Rule ID	Hostname	Severity	Status	Type
V-101113	CISCL2-000020	SV-1102171_rule	CiscoSwitch	CAT1	Open	Cisco IOS Switch L2S Security Technical Implementation Guide-V1-R1 dated 08 May 2020
V-101123	CISCL2-000080	SV-1102271_rule	CiscoSwitch	CAT1	Open	Cisco IOS Switch L2S Security Technical Implementation Guide-V1-R1 dated 08 May 2020
V-101135	CISCL2-000140	SV-1102391_rule	CiscoSwitch	CAT1	Open	Cisco IOS Switch L2S Security Technical Implementation Guide-V1-R1 dated 08 May 2020
V-101137	CISCL2-000150	SV-1102411_rule	CiscoSwitch	CAT1	Open	Cisco IOS Switch L2S Security Technical Implementation Guide-V1-R1 dated 08 May 2020
V-101299	CISCL2-000490	SV-1104031_rule	CiscoSwitch	CAT1	Open	Cisco IOS Switch NDM Security Technical Implementation Guide-V1-R1 dated 08 May 2020

Integrate with other Applications

- Automatically create system packages and checklists, pull vulnerability data, and download information through our API
- Integrate with your existing applications
- Use OpenRMF® Professional as your data source



General / System Package Snapshot

DEGTHAT Corporate Windows Network

# Checklists	CAT 1 / High Open	CAT 2 / Medium Open	CAT 3 / Low Open
14	17	408	19
Patch Critical	Patch High	Patch Medium	Patch Low
30	233	63	12

CALL 855-RMF-0848 | EMAIL sales@soteriasoft.com | www.soteriasoft.com | @soteriasoft

Improve speed, efficiency, and trust in your data with automated import, reporting, dashboards, notifications, compliance generation and integration of scans and checklists through our open API. Greatly reduce your time to ATO approval with OpenRMF Professional!

OpenRMF® Professional by Soteria Software

OpenRMF® Professional Features

Feature	
Role Based Access Control by System Package	✓
Open API for Automation and Integration	✓
100% Web-based	✓
Upload SCAP, Checklist, and Nessus scans	✓
Generate Compliance to NIST Sub-control Level	✓
Bulk Edit Vulnerabilities	✓
Bulk Lock Vulnerabilities	✓
Track History of Changes to Data	✓
Track Changes to Vulnerability Score over Time	✓
Show Proof of Continuous Monitoring	✓
Automated POAM to Track Changes to Data	✓
Authentication with CAC, PIV, Windows AD, LDAP, or Login/Password	✓
Works in cloud, on premise, on a laptop	✓
Works in a disconnected environment	✓
Integrated Logging and Auditing	✓
Export Data to Industry Formats	✓
Generate Report Data for Ad-hoc Data Calls	✓

Our OpenRMF® Professional application was born from the idea that we **must** apply better automation to the RMF and FedRAMP processes. We need better cyber accuracy with our massive amount of data we collect and we need to remove the manually intensive labor that can be done through automation. This frees up cyber personnel resources for other value-added tasks such as hardening systems, researching vulnerabilities and tracking risk to make better informed decisions.

With over 30 years' experience in dealing with information assurance and cybersecurity related issues, Soteria Software is helping reduce the outdated manual processes in tracking and achieving cyber compliance. While at the same time enabling your cyber personnel to track all your system packages in a structured, secure way.

