OpenRMF Professional v2.5!

Introducing OpenRMF Professional v2.5, the latest in Cyber Compliance Automation from Soteria Software. We have taken the massively manual process for Risk Management Framework (RMF) and Federal Risk and Authorization Management Program (FedRAMP) and automated much of the work for you and your team. So, you can get back to what is really important: *Hardening Your Systems*!

OpenRMF Professional combines the use of Patch Scans, Security Content Automation Protocol (SCAP) scans and manual checklists in a web-based solution that gives you a single source-of-truth for your data. Our application uses role-based access control by system package, compliance generation, a templating engine for structured checklist answers and status, historical tracking of vulnerability numbers as well as internal configuration management of your checklist data all available by a web browser.

With easy ways to edit checklists, the new bulk edit and bulk lock/unlock of vulnerabilities, and a live plan of action and milestones (POA&M) with traceability back to the checklist or patch vulnerability, OpenRMF Professional is a *must have* for your cyber compliance team.

Save hours of time with the automation and reporting built into OpenRMF Professional. Reduce errors on data input, overwriting vulnerability status, false positives, and manual compliance generation with our included suite of functionality all available with your web browser.

THE OpenRMF SOLUTION

OpenRMF Professional's collaborative environment eliminates much of the manual labor and isolated work involved in aligning the NIST controls, checklists and patch scans, and then manages all information in a secure central database structure. This allows automatic generation and updating of the POA&M, Test Plan Summary, STIG Checklists and various other security reports for Risk Management Framework (RMF) and Federal Risk and Authorization Management Program (FedRAMP) processes.

Having a web-based central repository for all RMF and FedRAMP data that has role-based security for each system, eases the cybersecurity processes using a single source of truth. It eliminates errors, manually intensive individual tracking, and rework and reduces the stress on your team for data calls and timelines. It also provides leadership with direct insight into the status of all system security and risk information which eliminates the mystery around implementing the RMF process.

With the latest updates to OpenRMF Professional you can easily:

- **Create teams to edit their own checklists and SCAP data as well as patch and device information:** with our Team Subpackage concept, you can create teams within your system ATO package and assign checklists and/or hardware devices per team. This allows the team to review and edit checklists as well as device information, ports/protocols/services information, as well as software listings per device. Let the team manage their own data without viewing others' data or running compliance or POA&M listings. Gain all the automation of OpenRMF Professional for your team but segment their data only for them! While the larger group can do all the same functions plus manage the POA&M, compliance, mitigations, reports and more!
- **Easily Edit Vulnerabilities:** quicker selection and editing of vulnerability data on checklists.
- **Export Patch Score Information:** easily export the patch score information per device into MS Excel for reporting, data calls, tracking, and more.
- **Software Filter and History updates:** we added the history tracking tools in OpenRMF Professional for the software listing per device. Now you can track edits as well as specify if it is an application, OS level, or support and driver. And then filter your listing to what you need to see easily.

Once an ATO or FedRAMP level is achieved, OpenRMF Professional continues with continuous monitoring and tracking of POA&M items, overall risk of systems and applications, and tracking updated scans and checklists throughout the life of the system package.

More information can be found at https://www.soteriasoft.com/.

Contact Us: Please email us at **sales@soteriasoft.com** or visit https://www.soteriasoft.com/

SOTERIA SOFTWARE
CYBER COMPLIANCE AUTOMATION

OpenRMF

System Package Features

- Role-based Access Control
- Compliance Generation
- Control Tailoring
- Test Plan Summary
- Bulk Lock/Unlock Vulnerabilities
- RMF or FedRAMP Control Listing
- SSP Control to Vulnerability Matrix
- Automated POA&M Tracking
- PowerPoint Summary Download
- Bulk Edit Vulnerabilities
- Overlays
- Mitigation Statements
- Team Notifications
- Track Overall Open Item Numbers
- Milestone Event Tracking

Team Subpackage Features

- Manage subsets of checklists for a team
- Manage subsets of devices for a team
- Allow teams to view / edit only their data
- Track changes and history of edits
- Edits tracked at the system package level
- POA&M automation still tied in

Checklist Features

- Upload SCAP to generate Checklist
- Track checklist update history
- Upload Checklist
- Upgrade checklists to latest version
- Track individual Checklist Score
- Edit vulnerability status, comments, and details

Patch Features

- Import .nessus patch files
- Automated Ports, Protocols, Services listing from scans
- Automated Hardware Device listing
- Track patch open items for continuous monitoring reporting
- Automated Software listing

Checklist Templating Features

- Included DISA Public Checklists
- Create Custom Checklist Templates
- Create Organization Templates
- Import DISA PKI-only Checklists
- Create System Package Templates
- Lock Vulnerabilities

Reporting Features

- Open Checklist Vulnerabilities
- System Activity
- Open Patch Vulnerabilities
- POAM Risk Cube
- Checklist Upgrades Required
- RMF v. FedRAMP Controls

General Features

- Docker or Kubernetes
- Login by CAC, Windows AD, LDAP, or User/Password
- OVA Virtual Machine Images
- Responsive Design
- 100% Web-based
- Detailed Auditing

Contact Us: Please email us at **sales@soteriasoft.com** or visit https://www.soteriasoft.com/