SOTERIA
SOFTWARE
CYBER COMPLIANCE AUTOMATION

OpenRMF® Professional Concept of Operations

Automating Cyber Compliance

Updated July 18, 2022

Background

The process of cyber compliance for your organization across various frameworks is extremely important. Tracking your vulnerabilities, software patches, operating system patches as well as ports and protocols open can be extremely time consuming and produce inaccurate results when only performed manually. Using disjointed checklists, scans, PDFs, and countless spreadsheets for the importance of your cybersecurity and relating it to a group of devices and software is painful. And continuous monitoring requires this to be done over and over again.

Soteria Software is working to revolutionize the cyber compliance landscape through automation for its government and commercial clients. Through automation around known good standard processes to ingest, track and correlate this data you can reduce the time and cost spent on tedious manual scanning and reporting, and return your workforce to the value-added service of securing your infrastructure and software based on the information produced through automation.

Problem – Disjointed Data and Many Manual Steps

It is a common idea that tracking your cyber compliance is extremely important and extremely time consuming. Running Security Content Automation Protocol (SCAP) scans, audit compliance scans, and then updating checklists for manual items you cannot automate is a lot to handle manually. Add in PDF reports or other data listings for your operating system patch vulnerabilities lets you tie in operating system problems as well. And if you are producing software manually or through a DevSecOps process or software factory, you have even more vulnerability and checklist data to track to know your cyber compliance readiness.

All of these processes are required to know the true compliance of your application, systems, or network infrastructure. That is not the issue. The issue is the amount of labor hours, time, and cost to track all this information and keep it up-to-date properly. And trust that what you are tracking and producing is timely and correct. And relate all the different types of configuration and vulnerability data across disjointed areas of your applications, operating systems and infrastructure.

What is needed is automation and efficiency around these industry practices. A way to automate known, good processes around scanning, relating data to your cyber control requirements, and tracking open issues through a plan of action and milestones (POAM) that is kept up-to-date as things change automatically.

What you need is OpenRMF® Professional.

Solution - OpenRMF® Professional

The OpenRMF® Professional solution is cyber compliance automation achieved. It performs automation against your ingested SCAP scans, audit compliance scans, checklist files, operating system patch scans and other vulnerability scans to give you a complete picture of all your compliance information. Group this data into system packages to relate the correct software, devices, and infrastructure and then grant privileges on access and update across your team or agency. You can further compartmentalize this data into team subpackages so users only see the data they are allowed to see, while the backend automation keeps everything related and up-to-date.

From this data you can generate and track your compliance status, run data calls and reports from truthful data, track open items with an integrated POAM, and link to project management applications to track the tasks and workload required to keep this data updated and relevant. You also can generate required documentation such as the System Security Plan (SSP), Security Assessment Report (SAR) and Risk Assessment Report (RAR) from trusted data within OpenRMF® Professional in seconds.

Your vulnerability data and compliance information is extremely sensitive. That is why OpenRMF® Professional is ***not*** a software-as-a-service (SaaS) application. This is software you download and run on your own laptop, server, virtual machine, or secured virtual cloud infrastructure. You can even run this in a 100% disconnected environment.

Manage Your System Package Information

OpenRMF® Professional groups data into system packages to relate the correct software, devices, and infrastructure and then grant privileges on access and update across your team or agency. In U.S. Federal government terms this would be an Authorization to Operate (ATO), Authorization to Connect (ATC), or type accreditation for a system or software application as examples. Each system package has an owner and permissions for your users, which allows a single application to securely help you manage multiple system packages and cyber compliance accreditation projects in a standard, structured way.

When your SCAP or Audit Compliance scans of devices are ingested, OpenRMF® Professional tracks the results and puts the data into predefined DISA or CIS checklists based on checklist templates. You can customize these checklist templates with pre-filled boilerplate information based on your needs to standardize and structure your information appropriately.

All this data is tracked historically so you can see changes on checklists, patch scan vulnerabilities, software scan vulnerabilities as well as compliance and POAM entries all within a secure web based application. And your information is exportable to common formats for checklist (CKL) files and spreadsheets (XLSX) as well for common documentation, reporting, data calls, and submission to government or commercial approvals.

Tracking All Scan Results and Vulnerabilities

The checklists and scan data in OpenRMF® Professional allow you to easily see all vulnerability data related to your system package along the groups of devices and applications. Whether it is SCAP scan ingested to create or update checklists, audit compliance scans based on DISA or CIS benchmarks, operating system patch vulnerability scans, software scans, container scans or other vulnerability data you can easily ingest and relate that data to your specific system package in OpenRMF® Professional. Any change to your data is tracked and the open vulnerability numbers (a.k.a. the score) are also tracked for changes.

For those items that cannot be scanned automatically, you can edit your checklists manually. And any process, procedure, technology, documentation or even cloud services can be tracked using our Custom Checklist creator to get full documentation across all items required for your compliance.

Once the data is uploaded through our web interface or via our API, it is displayed at the system package level accordingly. The score totals as well as individually are shown by checklist, by device, or by project and source. The patch scan data is used to not only track patch vulnerabilities and patch scan scores. It is also used to list the software, hardware device, and ports, protocols and services coming from that patch scan.

Now that the data is loaded, it can be reported on very easily. You also can bulk edit checklist data to make sure all data is structured and recorded the same. And you can lock vulnerabilities in checklists or entire checklists so they are not updated by users manually, automatically, or even to stop false positives from changing your data incorrectly.

Easily Generate and Tracking Cyber Compliance

With the click of a button in OpenRMF® Professional you generate your cyber compliance against risk management framework (RMF) or Federal Risk and Authorization Management Program (FedRAMP) as well as through tailoring and compliance overlays for a true compliance picture. This tedious manual process is now automated to not only quicken the process. It also automates it and structures it so it is correct every single time.

As you make changes to your data through scans and edits, updating and adding compliance statements, or adding custom checklists you generate updated compliance and track your compliance data over time historically as well. You also can add inherited or common controls as well to get a complete view of your cyber compliance data that is trustworthy and up-to-date. As those inherited or common controls you depend on are updated, your team is notified to ensure changes are reviewed and updated compliance is generated and tracked correctly.

Third Party Assessment Organizations (3PAO)

Third Party Assessment Organizations are charged with validating and verifying cyber compliance data across RMF, FedRAMP and other frameworks. And normally this is done using the same old same old – PDFs, XLSX, CKL, text files, screenshots, and DOCX explanations.

Now, using OpenRMF® Professional these 3PAOs can easily setup a new system package, drop in all SCAP, Audit Compliance, Patch Vulnerability and Full Audit scans from industry leading applications like Tenable Nessus, Rapid7 Nexpose, or the DISA and OpenSCAP tools and quickly see where organizations and companies are related to required compliance.

In under 10 minutes with all the scans collected, a 3PAO can fully show compliance, track POAM items, generate documentation, run reports and generate charts from all the scan data. This saves WEEKS of time doing this by hand across checklist files, PDF reports, Excel spreadsheets, and various other file formats and emails. You can identify gaps, note where mitigations can help with issues, and give end user agencies or customers valid data on where software and systems are related to compliance. All from a tool that gives you consistency, accuracy, truthfulness, transparency and does so at a rapid pace.

With our licensing model, you can have a single installation with the included 5 active system packages (full ATO, ATC, IATT) and perform many different assessments. Then mark them as “read only” to keep for archive and reporting purposes. Then release that system package from your license and move on to the next!

Assessors Validating RMF and FedRAMP

Those charged with doing assessments for system packages normally sift through mounds of papers, PDFs, checklists, Excel spreadsheets (i.e. Excel Hell!), a test plan summary and then raw scans to go through MANUALLY and assess a group's software or platform. Doing that over and over again with each visit to a site or remote location to gauge compliance with various security frameworks.

Using OpenRMF® Professional, these same assessors can receive a Test Plan Summary exported from the owners of the system package. And then they can load all SCAP, Audit Compliance, Patch Vulnerability and Full Audit scans from various Tenable Nessus, Rapid7 Nexpose, DISA SCAP and OpenSCAP scanners to see all relevant information from the most up-to-date scans. Along with generating compliance reports and tracking POAM items, the assessor can also generate SSP, SAR, RAR and other summary information. From this data they can very quickly see the compliance level, note areas of risk, track open vulnerabilities as well as the critical PPSM data in a matter of minutes. Those week long assessments shrink down to a couple few days and massively reduce the stress level of the job as well.

Again with our licensing model, you can have a single installation with the included 5 active system packages (full ATO, ATC, IATT) and perform many different assessments. Then mark them as "read only" to keep for archive and reporting purposes. Then release that system package from your license and move on to the next!

Cyber Reporting for Forward Deployed Networks

For people who have forward deployed networks that they still must track and report on, OpenRMF® Professional can be included on the deployed network to help gather the scans from disparate sources on the network. And then report back in a consolidated view based on requirements, data calls, compliance, POAM status, and the like in a much easier manner. No more sending back large PDF files, checklists, raw SCAP scans, and not knowing answers to cyber security and compliance questions.

Whether the forward deployed networks are their own accreditation or part of a larger accreditation, having automation through OpenRMF® Professional allows easy reporting and status. Add in automation via GitLab pipelines or other mechanisms via the OpenRMF® Professional open API, and you also lessen your manual intervention on gathering and reporting on these deployed networks as well. This works for intermittent connectivity over SATCOM, hardware networks 100% connected or anything in between.

Keep Updated with a Live Automated POAM

A major feature in OpenRMF® Professional is the live POAM. The POAM once generated links to all your automated scan and manual checklist data automatically, keeping it up-to-date based on the latest updates and edits to your data. And each entry in the POAM is tracked for edits and history of the changes are saved. You also can add manual entries of POAM items for those not tied to your specific scan, checklist or vulnerability data.

The POAM when done manually is very hard to keep up-to-date whether you have a small team and number of devices or if those numbers are very large. With OpenRMF® Professional and its automation engine, your POAM is kept as up-to-date as the latest data is. You can always export the POAM to a XLSX file for viewing, reporting, and uploading into the approving authority system as well.

Quickly Respond to Data Calls, CVEs, Zero Days

Having all your information from scans, checklists, vulnerabilities and compliance in OpenRMF® Professional allows you to quickly respond to data calls, vulnerability announcements, and zero day issues quickly and easily. This data can be shown and filtered on the screen, exported to XLSX, or searched and queried from external systems using our open API.

Whether it is vulnerability information, operating system patches, ports or services open, network boundaries crossed, or software scan vulnerabilities to track OpenRMF® Professional is tracking, ingesting, correlating and displaying all your cyber compliance data securely in one place. That lets you have trust in your information and make accurate, timely decisions to safeguard your data and systems.

Integrate with Other Industry Leading Software

You can also track the workload and tasks associated with your cyber compliance processes with OpenRMF® Professional through our integration with project management software. Using tools such as Atlassian Jira, ServiceNow, GitLab and GitHub you can create tasks from within OpenRMF® Professional, link them to the page you are referencing automatically, and synchronize the updates of those tasks easily. So not only can you track the data. You can track the workload and people around the data through these integrations.

OpenRMF® Professional also integrates with Nessus to directly list and import your audit compliance and patch vulnerability scan results. And you can directly import software scans from MicroFocus Fortify or SonarQube and SonarCloud for other vulnerability data. With our upload interface or API to post scan results or raw JSON data you can also ingest other container, log, or other vulnerability data that affects your system package as well. All linked to your POAM and all automatically tracked for scores, status, and impact to your system package and cyber compliance.

Open API for Automation, Integration, and Client Solutions

We did not create yet another data silo with OpenRMF® Professional. Through our open API you can upload vulnerability scan data automatically to keep your continuous monitoring processes flowing. You can also query data to show dashboard information for your team, agency, security operations center (SOC) or other use. You also can use OpenRMF® Professional as a data source for your business intelligence and reporting application.

Developers and integrators also can use the open API to have OpenRMF® Professional be the compliance engine and repository for all this data in a larger solution for government or commercial customers. Combine OpenRMF® Professional with a DevSecOps process to track vulnerabilities and allow gated delivery or deployment based on rules around vulnerabilities. Automate remediation of vulnerabilities from SCAP and audit compliance scans, rescan, and then upload results to show cyber compliance improvements over time. And allow OpenRMF® Professional to automate the POAM, data calls, and require documentation for submission to your approving authority or authorizing official.

About OpenRMF® Professional

OpenRMF® Professional is a web-based single source-of-truth for your cyber compliance data. Through ingesting benchmark scans, patch scans, and other vulnerability scans, OpenRMF® Professional gives you a comprehensive view of all your cyber compliance data. All data is managed in your system packages to track all vulnerabilities, checklists, devices, and compliance against your RMF, FedRAMP or tailored cyber compliance needs. A live plan of action and milestones (POAM) tracks all open issues and mitigations. Integration with project management software allows tracking the workload and tasks associated with your cyber compliance system package. And the open API allows you to automate upload of scans, integration with other applications, ties into software delivery mechanisms as well as create a data source for your reporting needs.

Automation in OpenRMF® Professional enables you to quickly perform the following:

- scan data and turn them into checklists
- tracks all vulnerability data changes and scores
- Notify team members of key data changes
- Update POAM entry status
- Tracks changes in compliance status due to inherited common control changes
- Track software, devices, ports, protocols and services running on your hardware devices automatically based on authorized scan results

The time to do this manually is now given back to your team to perform other value-added work around hardening and securing your infrastructure and applications.

About Soteria Software

Soteria Software develops cyber compliance automation software solutions for government agencies and commercial companies. Whether it is RMF or FedRAMP authorization automation, security operations center (SOC) data feeds, or integration into DevSecOps Software Factories our solutions are automating time-consuming manual processes for your compliance and continuous monitoring needs. Soteria Software can be reached at https://www.soteriasoft.com/, info@soteriasoft.com or by calling (855) RMF-0848.