SOTERIA SOFTWARE

Continuous Authorization:

Bridging the Gap Between Operational Security and Regulatory Compliance with OpenRMF® Professional and Elastic

Executive Summary: The Evolution of Cyber Compliance

In modern, defense-grade environments, the strategic necessity has shifted from passing "point-in-time" audits to maintaining a state of Continuous Authorization (cATO). Traditional compliance models are failing to keep pace with dynamic threat landscapes and the rapid deployment cycles of cloud-native and hybrid architectures. To maintain a resilient security posture, organizations must move beyond the manual burden of documentation into a model of automated, telemetry-driven validation.

The "Better-Together" integration of OpenRMF Professional and Elastic represents a paradigm shift in how regulatory requirements interface with the Security Operations Center (SOC). By orchestrating a seamless data flow between Soteria Software's compliance automation and Elastic's analytics engine, this solution transforms compliance from a bureaucratic hurdle into an active defensive asset.

This integration reconciles raw telemetry into actionable NIST, CMMC, FedRAMP and other cyber compliance formatted data, providing a real-time view of risk that satisfies both the Authorizing Official (AO) and the SOC analyst. Ultimately, by instrumenting the right architecture, compliance becomes a competitive advantage that enables mission-critical systems to operate with higher assurance and lower administrative overhead.

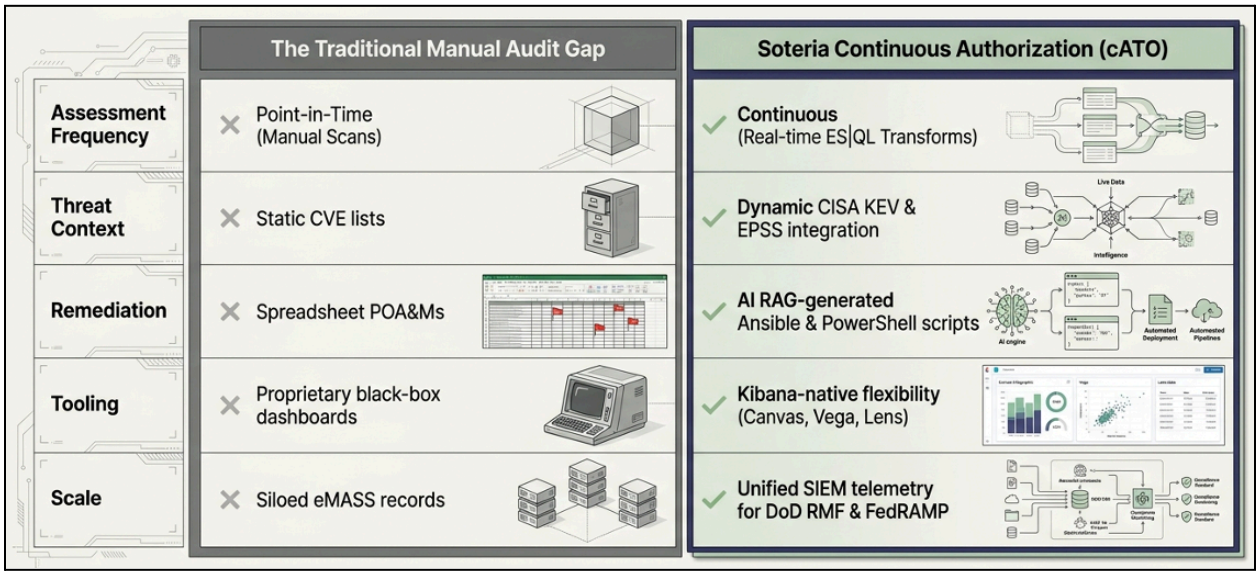
It also gives you verified compliance evidence that the blueprint offered by your cyber compliance scans and documentation is actually being carried out within your production networks and systems. Through a combination of compliance data mapped to active security and telemetry data, you show an actual view into how your cyber compliance is carried out in real-life production implementation.

The Compliance Gap: The Problem with Static GRC

A profound strategic disconnect exists between real-time security telemetry and the formal Authority to Operate (ATO) accreditation process. While security teams monitor live events, compliance officers are often buried in static spreadsheets and files, attempting to manually correlate SIEM alerts with hundreds of specific controls. For organizations facing C3PAO assessments or FedRAMP and RMF types of audits, this "massive manual gap" is more than an inefficiency—it is a critical risk.

Auditors now demand endpoint-level STIG compliance and verified host-bound evidence, which traditional GRC tools are ill-equipped to provide. And they need it real-time or near real-time, not from work done weeks or months earlier.

The failures of the traditional model include tracking static ATOs vs. using dynamic telemetry where authorization packages are often obsolete upon signature. SIEM logs reflect a constantly shifting environment with truthful up-to-date information. You also have evidence mapping hurdles, manually reconciling host-bound evidence to cyber compliance frameworks such as NIST 800-53/171 controls. This is very labor-intensive and prone to human error, often leading to audit failure.



And finally, you have the "Black Box" Problem, where most proprietary GRC platforms offer opaque dashboards that lack the granular detail required for defense-grade audits. This prevents analysts from drilling down into the raw data. And programs of record, including eMASS, require generating specific eMASS-formatted POA&Ms and documentation which remains a manual, time-consuming task that distracts engineers from remediation.

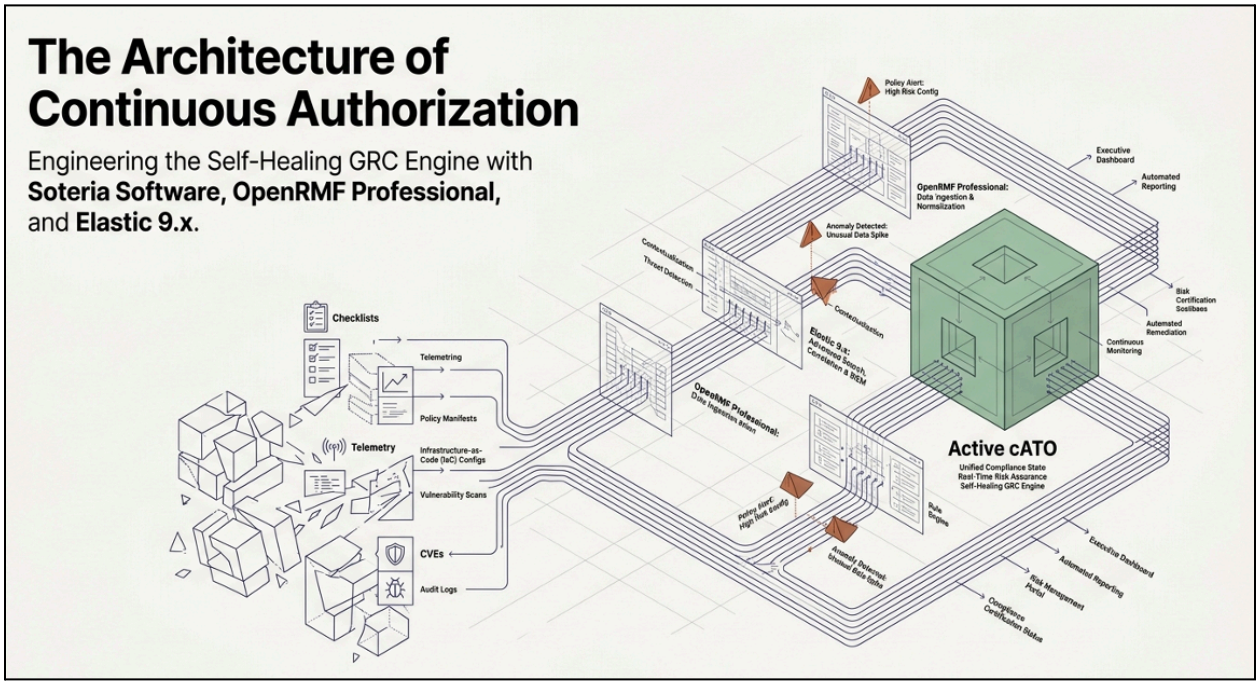
The integration of OpenRMF Professional and Elastic serves as the structural bridge for this gap, anchoring theoretical risk to operational reality.

The Power of Integrated Automation: OpenRMF Professional + Elastic

By leveraging a native Elastic environment, organizations can ingest and analyze compliance data with the same speed and rigor as security logs. The Soteria Software interface reflects a UI built for the high-pressure environment of a modern SOC.

The core of this synergy is Soteria Software's Elastic-based Service Provider Interfaces (SPI). These interfaces automate the push of compliance frameworks, CCIs, and vulnerability data (patches, checklists, and scan results) directly into Elasticsearch indexes. This "Open Index" philosophy is a strategic antidote to vendor lock-in.

Unlike closed-loop GRC systems, providing full access to underlying Kibana and Elasticsearch indexes allows organizations to run custom security analytics and manage cases using the same tools used for incident response. This architecture ensures that compliance data is not siloed but is instead part of the broader searchable data lake, facilitating deeper insights into the organization's security posture.



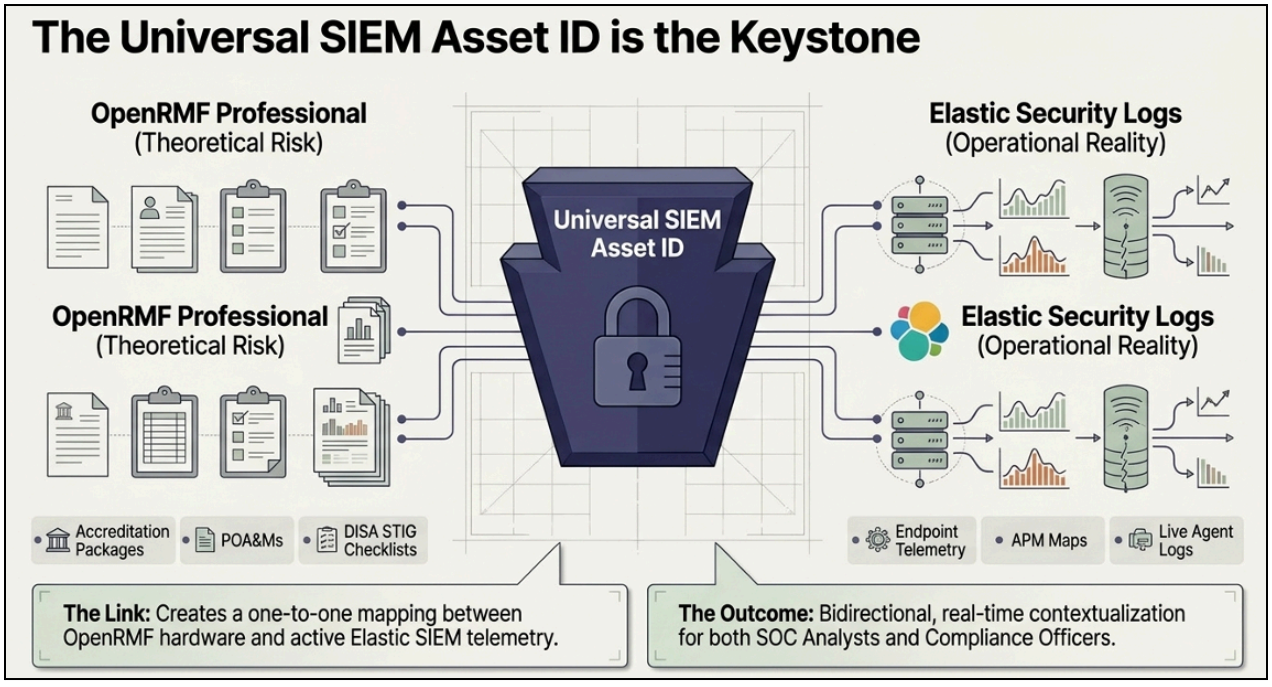
Technical Synergy: Universal Asset Mapping and Real-Time Telemetry

The foundational element of this integration is the creation of a 1-to-1 mapping between hardware assets and compliance records via the "Universal SIEM Asset ID." This identifier allows OpenRMF Professional to reconcile hardware assets against Elastic telemetry, ensuring every log and alert is associated with the correct accreditation package.

The integration utilizes dual interfaces to maintain this synchronization. The **Elastic AI Interface** automatically pushes compliance scores and POA&M items into Elastic while creating AI Tools and Agents to search and interact with the data.

In combination, the **Elastic Security (SIEM) Interface** ingests data from Elastic Machine Learning (ML) jobs to update compliance states in OpenRMF Professional. If Elastic Security detects a change in an asset's security posture, the corresponding cyber compliance controls are updated in real time.

This mapping allows for the visualization of actual baselines across hardware operating systems and software against the compliance data, ensuring that the intended state and the actual state are always in alignment.

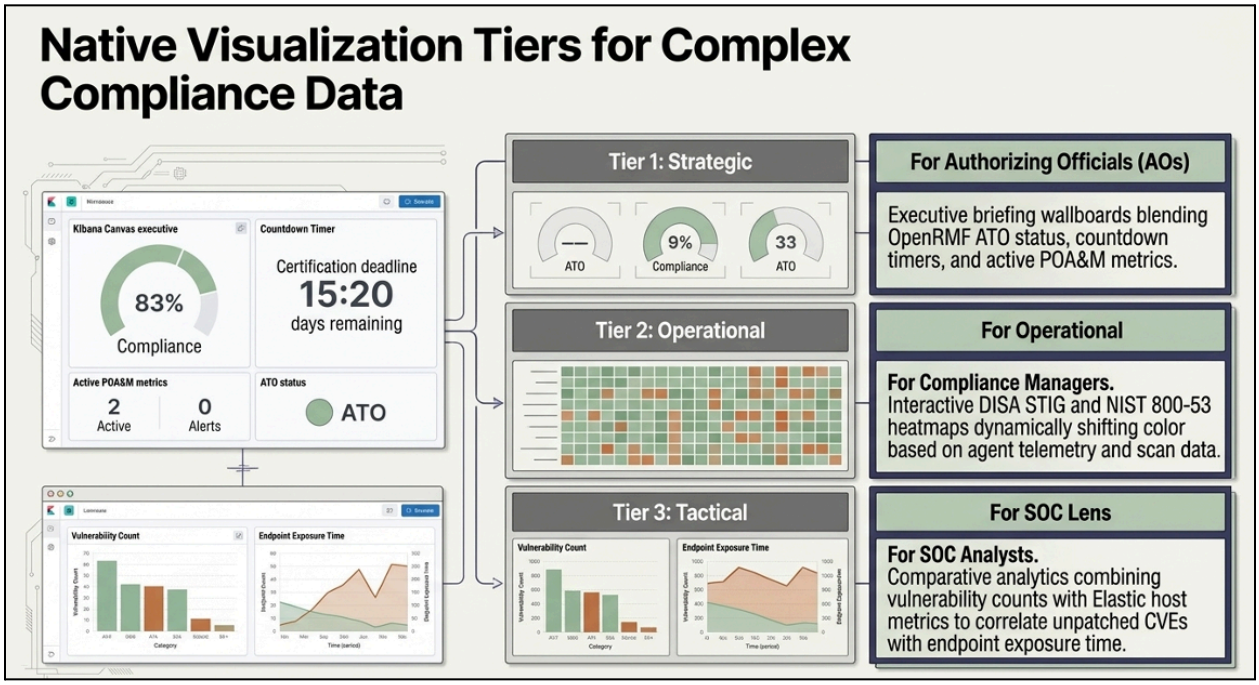


High-Value Visualizations: Transforming Data into Insight

The visual manifestation of this data link is critical for maintaining an ATO. By using automated compliance data from OpenRMF® Professional combined with Elastic's native visualization suite, the integration reduces "time-to-insight" for both executive leadership and technical staff.

There are several ways you use compliance data natively within Elastic. Kibana Dashboards (as Audit Wallboards) show real-time screens providing Authorizing Officials (AOs) with live ATO status, countdown timers for accreditation expirations, and active POA&M metrics. You also use Vega Custom Visualizations for interactive DISA STIG and NIST 800-53 heatmaps, allowing users to see compliance concentrations at a glance. Controls dynamically shift color based on Elastic agent telemetry, moving the focus from raw vulnerability counts to control-based health.

You also use Kibana Lens to enable comparative analytics, such as correlating unpatched CVE counts with endpoint exposure time, providing a clear picture of how long a system has been at risk. Or ES|QL Continuous Summaries to leverage the new Elastic Synthetic Query Language (ES|QL) to pivot raw telemetry and Universal Asset IDs into a consolidated ATO Health Summary index, updated in real time.



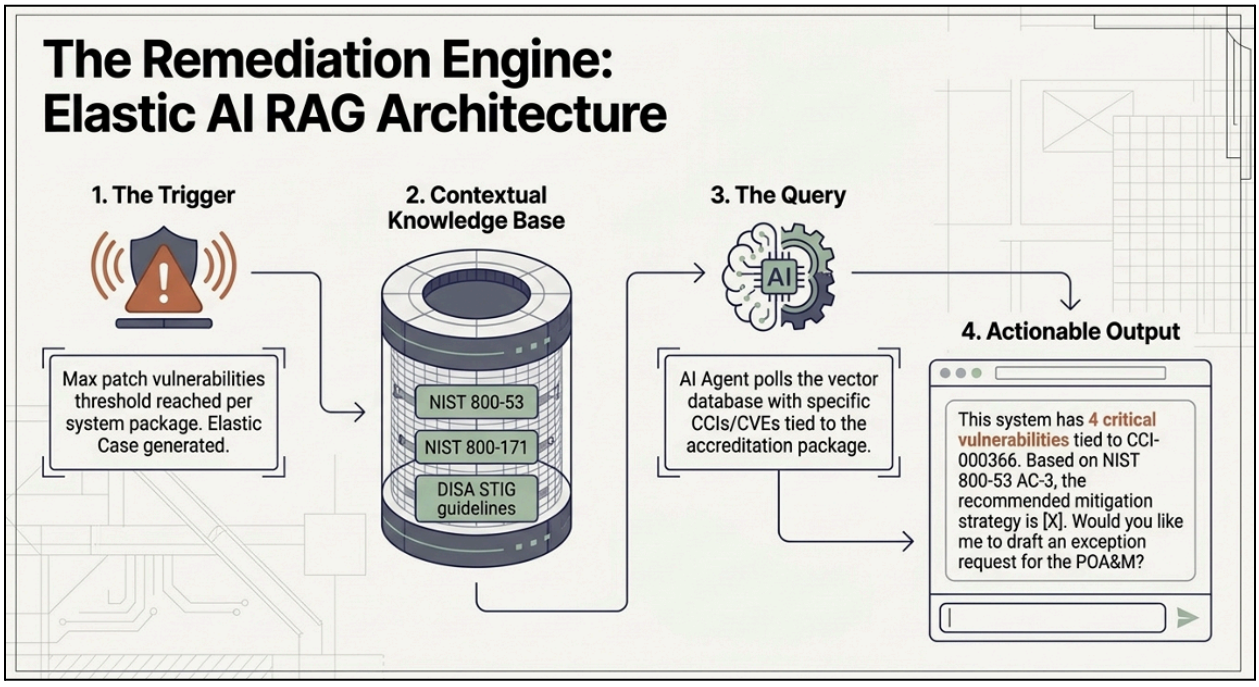
The Future of Cyber Defense: AI, ML, and Self-Healing GRC

The evolution of this platform points toward a "self-healing" GRC environment where predictive risk management replaces reactive reporting.

Elastic ML for Anomaly Detection: unsupervised ML to establish behavioral baselines for compliance trends. If a site's compliance score suddenly drifts—even if it hasn't hit a hard threshold—Elastic ML flags the anomaly as a proactive indicator of a degraded posture.

SBOM and APM Integration: instrument SBOM vulnerability inventories into Elastic APM service maps to allow the system to isolate vulnerable runtime application components, linking software components directly to the ATO's hardware hostname.

AI Assistant for Remediation (RAG): Using Retrieval-Augmented Generation (RAG) to read failed STIG requirements and auto-populate remediation scripts (PowerShell, Bash, or Ansible). The AI Assistant can even draft formal exception requests for POA&Ms based on NIST 800-53, 800-171 or any other cyber compliance guideline.

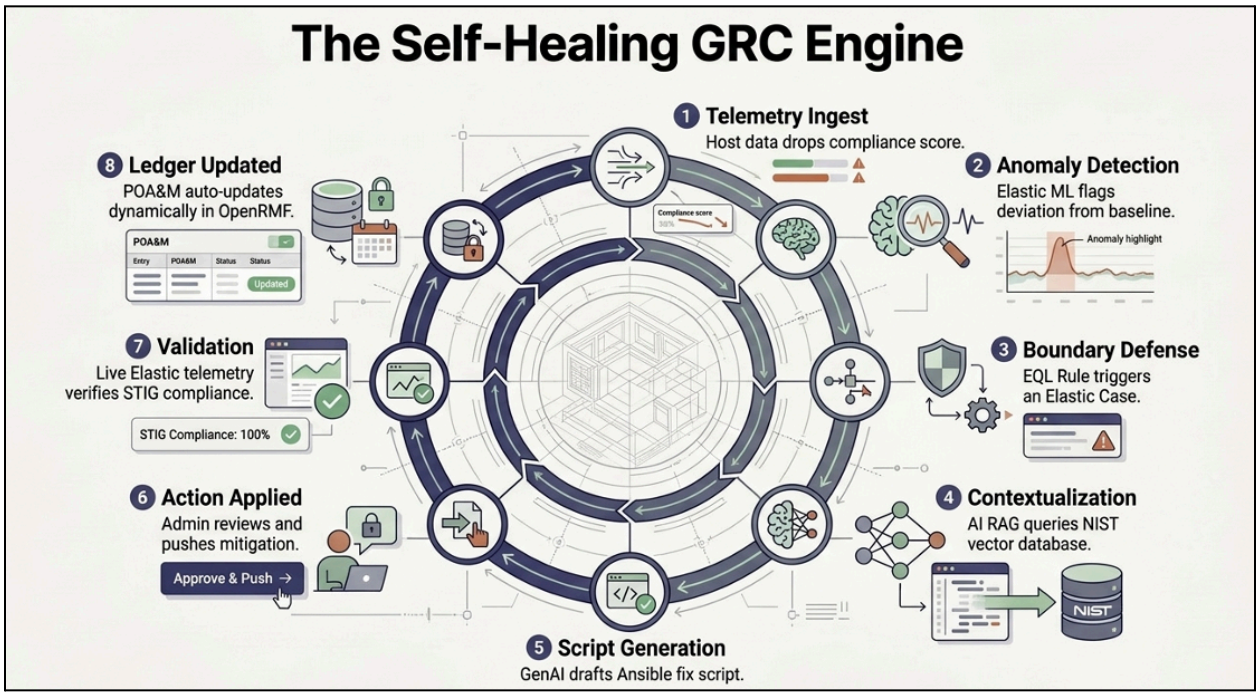


Searchable Snapshots: Enabling Searchable Snapshots for Multi-Year Audits allows archiving DISA STIG history into low-cost cold storage while maintaining instant query access for multi-year audits—a critical requirement for enterprise cost-efficiency.

Detection Engine Rules: EQL rules trigger SIEM alerts if local auditing services or Elastic Defend agents are disabled on hosts within an active ATO boundary, preventing "compliance tampering."

Osquery Live Evidence: Running targeted Osquery scripts directly from Kibana against hosts with failing checklists to auto-collect evidence files for auditors.

By completing the Threat Intel to POA&M loop, a Known Exploited Vulnerability (KEV) can automatically update the residual risk of a POA&M, creating a GRC platform that prioritizes remediation based on actual threat actor activity.



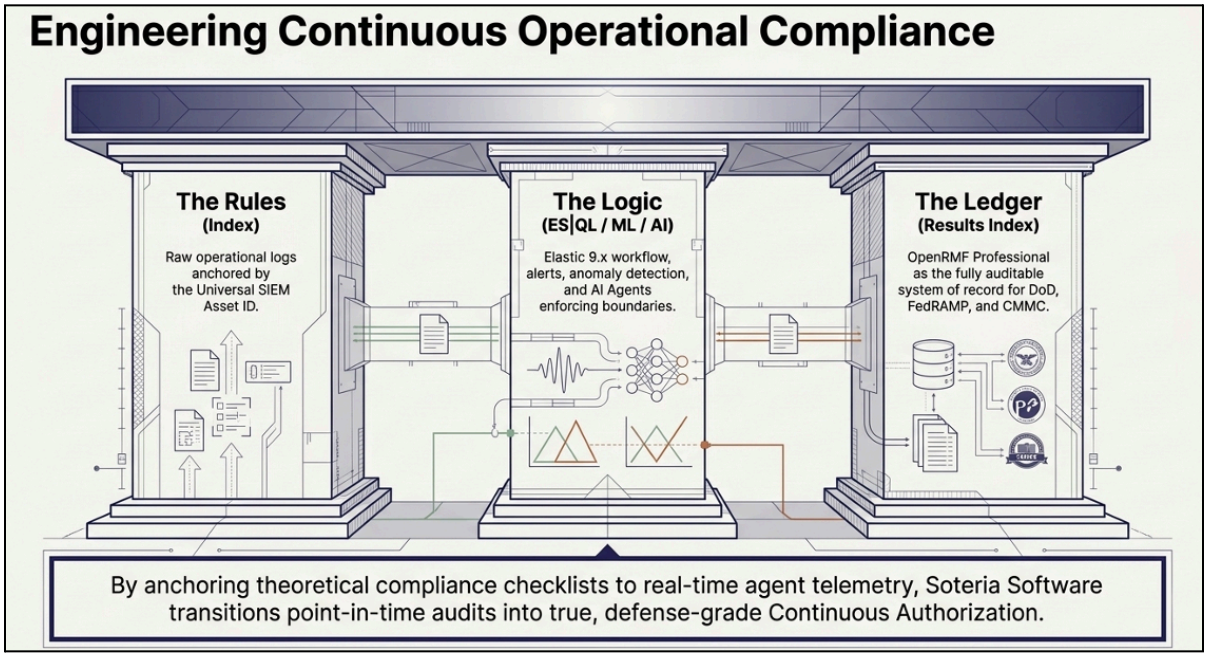
Conclusion: Operational Compliance as a Defensive Asset

OpenRMF Professional, powered by the Elastic 9.x ecosystem, represents more than a tool for passing audits; it is a platform for building a defense-grade operational posture. By bridging the gap between active threat detection and formal accreditation packages, organizations can save hundreds of engineering hours and eliminate the risks inherent in manual tracking.

The primary benefits are clear: real-time, asset-centric posture management that links SIEM telemetry directly to regulatory controls. Whether in the cloud, on-premises, or in fully air-gapped environments, this integration turns passive compliance into an active defensive asset. To explore how these features can transform your authorization process and help you achieve true Continuous Authorization, visit soteriasoft.com to learn more about our Service Provider Interfaces and automated cyber compliance solutions.

See more at https://www.soteriasoft.com/ by using our Live Demo site, our savings calculator, or any number of our videos and articles to see how we can help you and your team automate your cyber compliance.

As we say at Soteria Software: ***Do The Work. Automate The Paperwork!*** ®



About Soteria Software

Soteria Software creates cyber compliance automation software. Using the right technologies for the right purpose, we enable reduction of task-based work around accreditations and ATOs up to 90%.

Our passion is to change the expectation for the world around cyber compliance – to expect hyperautomation, giving you and your team the time, energy and resources for proper cyber hygiene and improved cyber security.

The amount of data to collect, track, analyze, and report is more and more overwhelming. Which means automation must come into play to allow confidence and trust to permeate the process. And de-stress the directors, managers, staff, assessors, and government officials at the same time.

This has been the conversation with us (the owners of Soteria Software) since 2004 when we met at the Navy EOD TechDiv in Indian Head, Maryland. For the next 14 years we kept doing the same thing over and over and saying "there has to be a better way"! And no one solved this growing problem. So in the summer of 2018 we started working on what has become OpenRMF® Professional! We started with a simple STIG checklist viewer and editing with OpenRMF® OSS. And innovated from there forward.

Now we have added functionality, APIs, an improved user interface, AuthN/AuthZ, additional scan imports, integration with task management software, updating STIG checklists, bulk editing and locking operations, and more. We were constantly asked for more and more features and saw a need for not just an open source OpenRMF® OSS. We saw a need for the larger organizations, agencies, and even commercial companies to track revisions, merge scans, track your POA&M, and perform continuous monitoring.

Our OpenRMF® Professional solution is designed to use your compliance, patch, and vulnerability scans from the ground up. Automate around the data you already need to have. And do so in an automated fashion to make a Live POAM, generate compliance snapshots, track history and configuration management of your data, run data calls, and hyperautomate with our API as part of your larger Cyber Security Mesh Architecture (CSMA).

This company, Soteria Software, was created to fill that need and innovate the cyber compliance landscape around OpenRMF® Professional and more.