stackArmor

A TYTO ATHENE COMPANY

Challenges with AI in Today's Cybersecurity & Compliance Landscape

Modernizing Cybersecurity Operations for the Army and Enhancing RMF Compliance with Agentic AI

About stackArmor

stackArmor is the leading provider of FedRAMP, FISMA and CMMC compliance and security solutions

ATO Acceleration Experts

Headquartered in Washington, DC, stackArmor is an Advanced ATO partner with strong security and compliance experience in the education, DoD & Federal, commercial, public sector and non-profit markets.

Uniquely Positioned in the Ecosystem

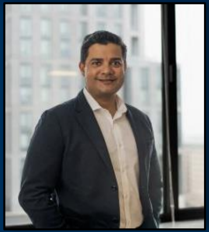
Acquired by Tyto Athene, an Arlington Capital Partner company, to accelerate innovation in delivery of secure cloud solutions for DOD and National Security customers. Actively engaged in continuous innovation around SBOMs, OSCAL, FR20X, DOD SWFT and DOD RMF Reimagined.

Thought Leadership and Awards

- Supported first Cloud ATO in 2009 for Recovery.gov
- Led first Cabinet Agency migration to cloud in 2010
- Supported over 200 system migrations & ATOs

THE FEDERAL 100 | RISINGSTAR AWARDS | CYBER DEFENDERS AWARDS 2024

Johann Detweiller
***CISO,* stackArmor**



Fawad Siraj
***CTO,* stackArmor**

Accomplishments

40%
Reduction in ATO Costs
Proven Track Record

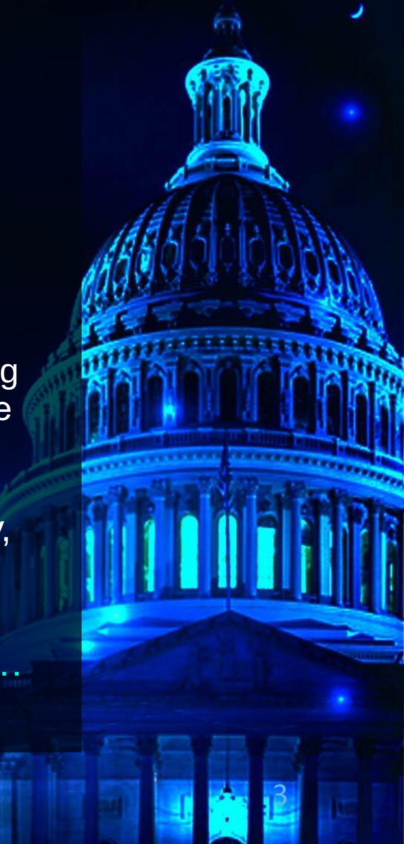
50+
ATOs
FedRAMP, DOD, FISMA

20+
Agencies
FedCiv, DOD Sponsors

The U.S. Government: A Critical Juncture

- Despite the recent significant personnel and budget cuts, the demand to enhance mission capabilities has never been greater.
- At the same time technology – fueled by rapidly evolving **AI capabilities** – is changing at lightning speed – with massive amounts of innovative (and potential risk) being infused into IT systems faster than most IT and cybersecurity teams can keep up.
- Finally, adversaries are wielding AI for their own malicious purposes, adding even more complexity to the risk management conundrum.
- Together, these facts have made it clear that the DoD's traditional Risk Management Framework (**RMF**) is too slow, too expensive, and no longer sufficient for safely adopting new technologies and ensuring mission success in today's IT environment. In fact, Katie Arrington, the acting DoD CIO, publicly stated her desire to "blow up the RMF."

This critical juncture is forcing industry leaders to re-evaluate the state of technology, the approach to risk management, and the role of AI in today's IT ecosystem to ensure these vectors can be leveraged to effectively meet critical mission objectives while keeping adversaries and associated risk at bay in today's **Threat Landscape**…



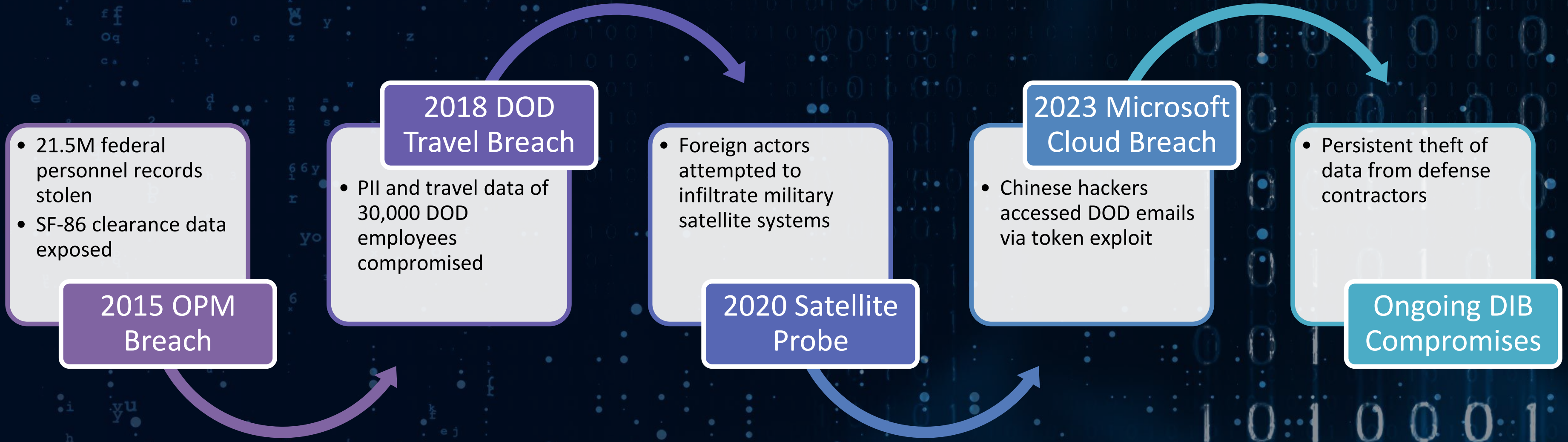
Today's Threat Landscape

- Adversaries are evolving their use of AI in their kill chain at warp speed
- The scale and frequency of attacks continues to rise exponentially
- 600 million cyber attacks are detected daily
- 12k cyber incidents have been recorded by DOD
- DOD's cyber workload remains intense with thousands of incidents requiring response and a budget to match
- Teams must cover more cyber activities with lower budgets

The RMF of yesterday must be re-imagined and modernized – leveraging the power of machine automation and Agentic AI to stay a step ahead of the adversaries in protecting our mission critical systems and the data it processes!

Timeline of Major Cybersecurity Breaches

Despite the Government's investment in cybersecurity and risk management, history shows we must continue improving and building on lessons learned…



2015 OPM Breach

- 21.5M federal personnel records stolen
- SF-86 clearance data exposed

2018 DOD Travel Breach

- PII and travel data of 30,000 DOD employees compromised

2020 Satellite Probe

- Foreign actors attempted to infiltrate military satellite systems

2023 Microsoft Cloud Breach

- Chinese hackers accessed DOD emails via token exploit

Ongoing DIB Compromises

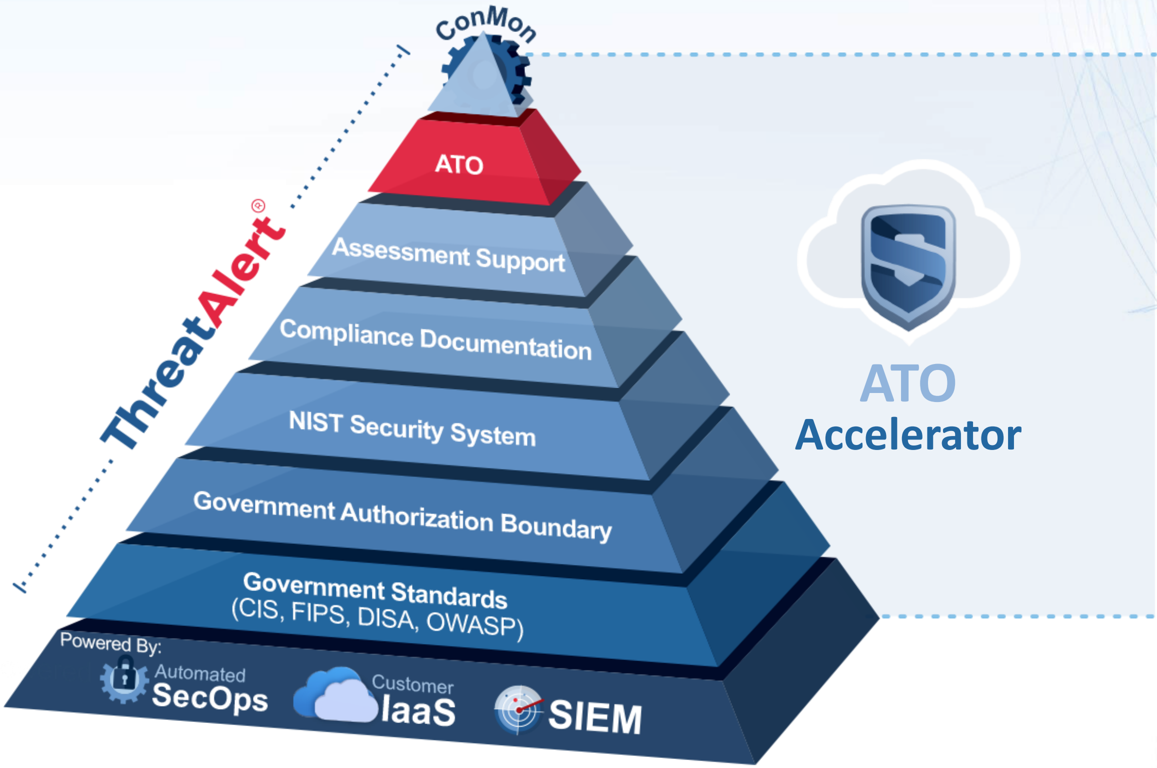
- Persistent theft of data from defense contractors

Breaches Reflect Weaknesses in RMF Control Gaps

	Example Incident	Breach Cause	RMF Control Gaps
2015 OPM Breach	OPM Breach (2015) – Chinese APT stole clearance data via spear-phishing and stolen creds	**Nation-State Attacks & Spear-Phishing**	SI-4 (System Monitoring), IA-2 (Identification & Authentication)
2018 DOD Travel Breach	DoD Travel Records Breach (2018) – Vendor compromise exposed PII of 30,000+ employees	**Third-Party & Supply Chain Vulnerabilities**	SR-3 (Supply Chain Controls), SA-9 (External System Services), CA-3 (System Interconnections)
2020 Satellite Probe	Multiple DIB Contractor Breaches – Poor patching, weak monitoring in contractor networks	**Insufficient Oversight of Contractor Systems**	CA-2 (Security Assessments), RA-3 (Risk Assessment), PM-30 (Supply Chain Risk Management)
2023 Microsoft Cloud Breach	DoD Legacy Systems – Unpatched servers & misconfigurations exploited for lateral movement	**Legacy Systems & Misconfigurations**	CM-2 (Baseline Configuration), SI-2 (Flaw Remediation), SC-7 (Boundary Protection)
Ongoing DIB Compromises	Cloud & On-Prem DoD Systems – Attackers moved laterally due to flat networks	**Poor Segmentation & Access Control**	AC-4 (Information Flow Enforcement), AC-6 (Least Privilege), IA-5 (Authenticator Management)

stackArmor’s ThreatAlert ATO Accelerator

- stackArmor’s ThreatAlert offering is an end-to-end ATO acceleration solution that today can reduce the time to ATO by as much as 40%
- The stackArmor team has 50+ ATOs to our name, and years of hands-on experience informing our offering and capabilities roadmap
- With each release of our core proprietary tools stack, we incorporate more automation and machine-driven SecOps (and risk management) capabilities
- In keeping with the tradition of being a leader in this area, stackArmor is **strategically incorporating Agentic AI** into our solution, bringing the power of machine-driven SecOps to our teams as the ultimate force multiplier - ushering our customers into an AI-driven future



stackArmor’s vision of the Future: Agentic AI Plus a Modernized RMF

Thinking beyond “Shift Left” to Re-imagining What’s Possible.

- **Agentic AI –** used to address well-defined use cases and implemented with appropriately trained models and guard rails, AI is an *increasingly invaluable force multiplier* for Cybersecurity Teams. AI is already in the hands of adversaries and permeates the threat landscape - so making AI a part of the solution is no longer revolutionary, but necessary.
- **Agentic AI as a Part of A Modernized RMF -** Shifting from a traditional RMF implementation to a more modern and integrated “data and machine-driven” approach addresses the intent of the original RMF while adapting to today’s technologies. In today’s systems, continuous monitoring and risk-posture information, controls compliance, and system-state documentation should be *derived from* zero-trust, well-architected systems – *not created outside of* those systems.

Challenges of Integrating AI into Today’s Systems

- Defining the Role(s) AI can and should Play in Modern Systems
  - Agentic vs Generative
- Trusting AI - Ensuring Integrity in AI Outputs and Actions
  - Addressing Risk and Security Issues Introduced by AI
  - Managing the Quality and Integrity of Data used to Inform AI Models
- Integrating of AI with Legacy Systems
- Governance and Oversight

Making Agentic AI Trustworthy

Traceability by Design

- Unlike generative AI use cases, agents are tailored to execute precise, specific actions.
- Hallucination risks can be further mitigated by carefully binding the AI's reasoning with real system scans - not allowing it to make IDS decisions or implement controls unless they exist in a predefined reference list.
- AI agent actions are additionally to be treated like privileged user actions and agents treated like the ultimate insider threat.
- Immutable logging of prompts, model decisions, and downstream effects.
- AI agent activity is aligned with RMF workflow artifacts (e.g., audit trails, ATO evidence).

Assurance through Alignment

- MCP servers are secured as high-value/critical assets.
- Policy-as-code is used to govern AI inputs/outputs.
- NIST AI RMF is incorporated into system design to build provable trust.

Transparency for Defenders

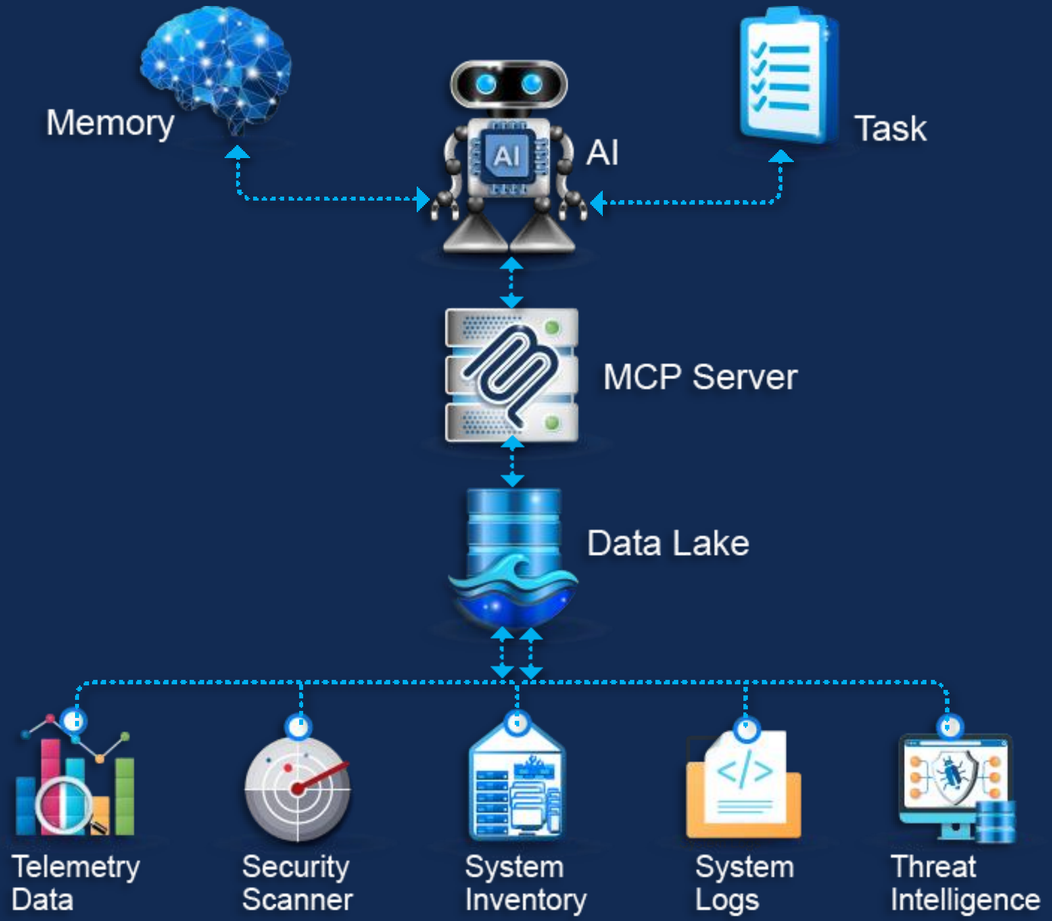
- AI behavior is interpretable for cyber teams.
- Maintained visibility into model updates, data lineage, and system logic.
- AI-driven actions impacting security posture have explainable outcomes.

Agentic AI Driven Process

Incorporating Agentic AI into today’s systems helps automate and orchestrate complex system and cybersecurity operations in ways humans alone cannot.

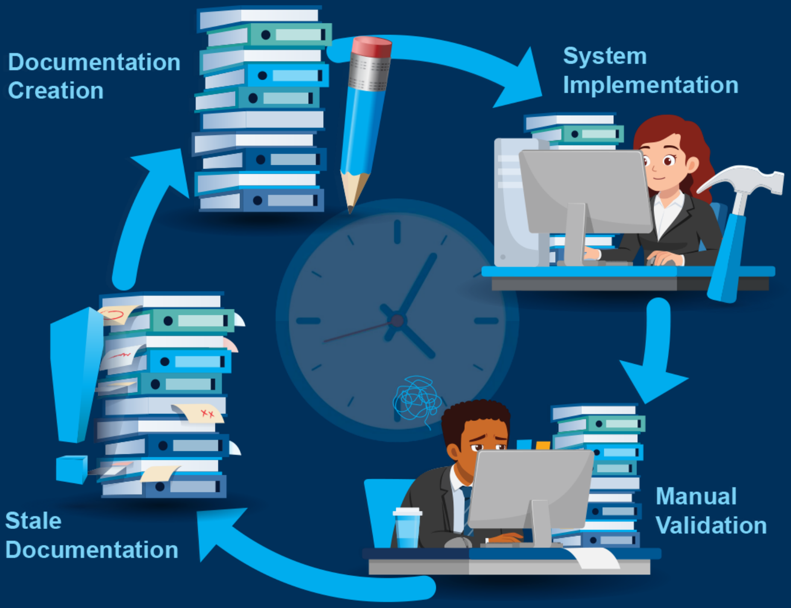
- **Utilize Model Context Protocol (MCP) server directed at telemetry/orchestration layer to:**
  - Poll system states continuously and orchestrate AI agent actions based on operational triggers.
- **Agentic approach deployed to autonomously support various aspects of SecOps and compliance.**
  - Validate system changes in real-time.
  - Perform automated risk assessments.
  - Generate audit-ready evidence with minimal human input.
  - Create and update Component Definitions based on current, validated system state.

Cyber AI Agent

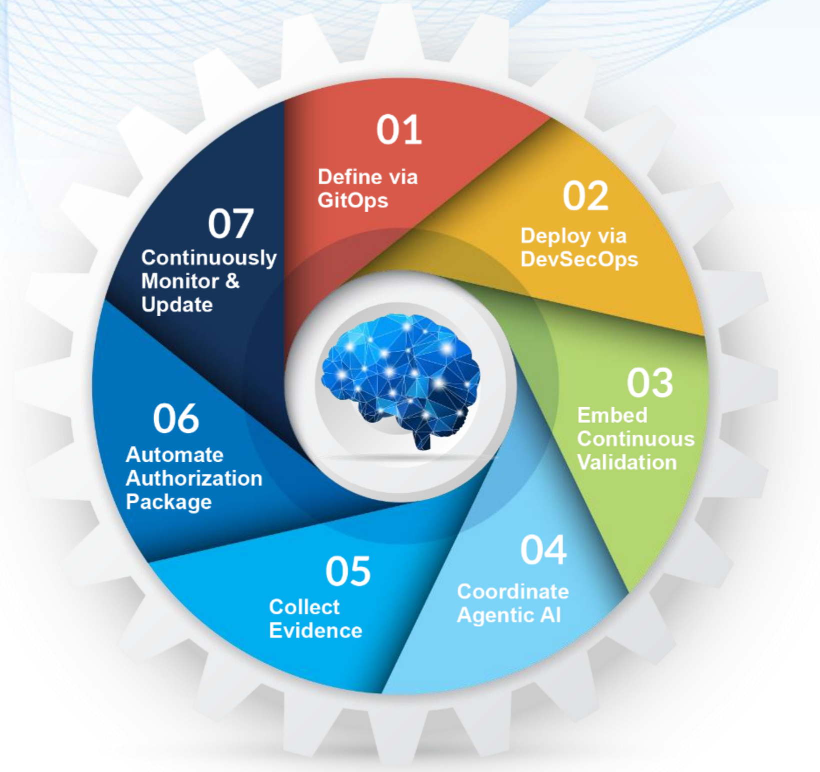


The RMF Challenge

- The current process is slow, labor intensive, and not aligned to today's fast-paced, machine-driven system environments.
- Manual documentation under NIST SP 800-37 Rev. 2 is resource-intensive and error-prone.
  - Often the wrong resources with the wrong data are charged with documenting system state.
- Limited cybersecurity workforce capacity to support ongoing compliance.
  - Continuous control validation strains limited cyber resources.
- Compliance often lags behind system changes, creating audit and operational risk.
  - Instead of managing risk, RMF has become a source of risk.

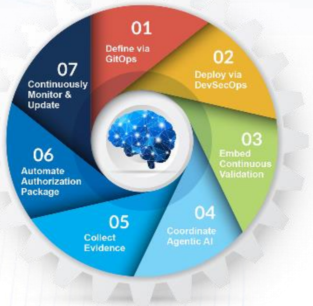


Vision: A Modernized RMF Workflow



1. **Define via GitOps** the desired system state using Policy-as-Code and Infrastructure-as-Code
   - *Git repositories used to manage infrastructure and application configurations declaratively, where Git is the source of truth, and changes are automatically applied to environments through automation.*
2. **Deploy via DevSecOps** pipelines and GitOps principles.
3. **Embed Continuous Validation** directly into infrastructure deployment workflows.
4. **Coordinate Agentic AI** with MCP (Model Context Protocol) for intelligent, continuous monitoring and validation of assertions of system state.
5. **Collect Evidence** by creating a “Data Lake” based on gathered assertions and gathered automated evidence.
6. **Automate Authorization Package** generation and maintenance which is informed of the actual system state by content in the data lake.
7. **Continuously Monitor and update** based on running system state via automation.

Define Policy and Controls Up Front

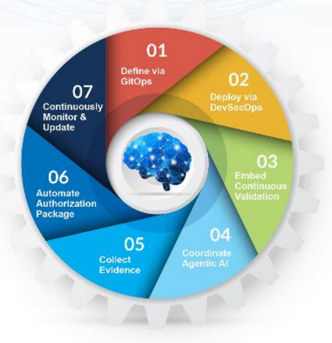


01 | Define

02 | Deploy via DevSecOps

- Policies drive system behavior and automation, not paperwork.
- Use Infrastructure as Code + Policy as Code to:
  - Define expected system state.
  - Establish control baselines.
  - Enforce approvals and traceability via GitOps.
- Leverage Continuous Integration/Continuous Deployment (CI/CD) pipelines to deploy code and policy.
  - Introduce stage gates and approvals.
  - Run automated checks and validation prior to deployment.
  - Ensure consistency and accuracy of updates.

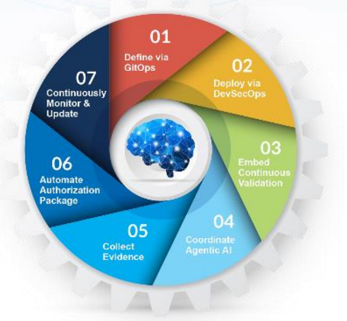
Telemetry/Orchestration Layer for Real-Time System State Validation



03 | Embed Continuous Validation

- Implement lightweight, plugin-based telemetry and query orchestration layer that polls live system configurations and security states using SQL-like queries across cloud and on-premises environments, providing real-time, structured data to drive automated compliance and security workflows.
- Derived Data Lake drives automation and orchestration.
- Stores:
  - Live system configurations.
  - Validation logs.
  - Control checks and outcomes.
- Generate real-time, audit-ready evidence.
- Enables transparency and continuous readiness.

Agentic AI for Automation and Orchestration

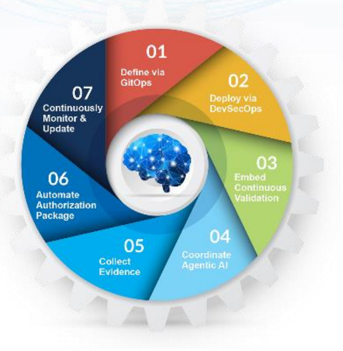


04 | Coordinate Agentic AI

Agentic AI drives automation and orchestration of complex system and security operations, taking actions and delivering information based on system data.

- Enables continuous validation of system configurations and assertions of system state
- Automates the creation of RMF documentation
- Reduces manual errors and reduces the burden on SecOps engineers and analysts
- Ensures that compliance is embedded directly into DevSecOps workflows

System Data Feeds Evidence Collection



05 | Collect Evidence

Audit-Ready Evidence - GitOps pipelines combined with carefully designed Data Lakes provide:

- A complete audit trail with zero manual paperwork.
- Full traceability (who, what, when, why).
- Evidence of approvals and control validation.

Evidence of Cybersecurity Posture and Compliance Status are Live-State Driven:

- System Security Plans (SSPs), Implementation Statements, and Policy Docs are generated automatically from live, validated system state.
    - Powered by Authpack Automator + Component Definitions.
    - Uses modular, reusable Component Definitions for each control and capability.
- Updates are derived from changes in the running environment.

Cybersecurity Hygiene and Compliance are Aligned with DevSecOps Pipelines:

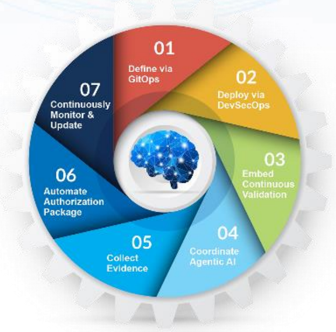
- Compliance keeps pace with mission system evolution, not something done after the fact.
- Documentation generation occurs during CI/CD deployment.

System Risk Posture and Status is Continuously Updated - As system configurations or controls change:

- Agentic AI and MCP validate new states.
- Updates are logged into the Data Lake.
- Documentation is generated continuously, ensuring alignment with system state.

System Data Powers Documentation

Using Component Definitions as Building Blocks of Control Implementation

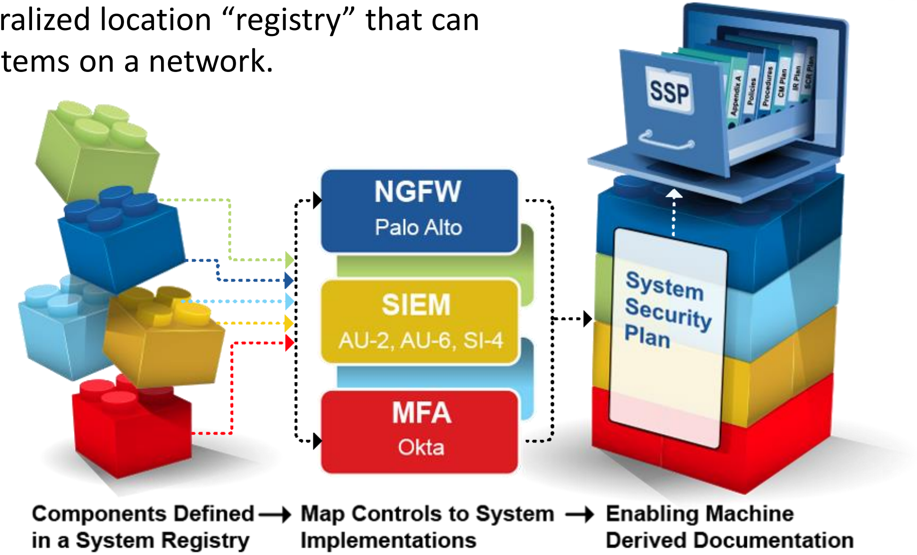


06 | Automate Authorization Package

Component Definitions:

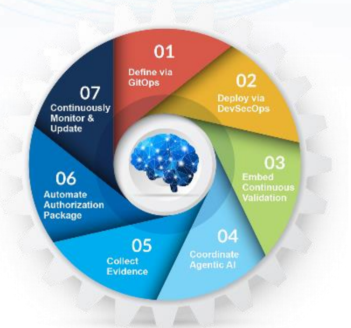
- Are machine-readable reusable components that create a system control mappings.
- Allow the generation of an SSP in hours instead of weeks.
- Utilize the concept of a centralized location “registry” that can be leveraged by multiple systems on a network.

As the registry of components grows, the creation and management of documentation becomes exponentially faster.



Components Defined in a System Registry → Map Controls to System Implementations → Enabling Machine Derived Documentation

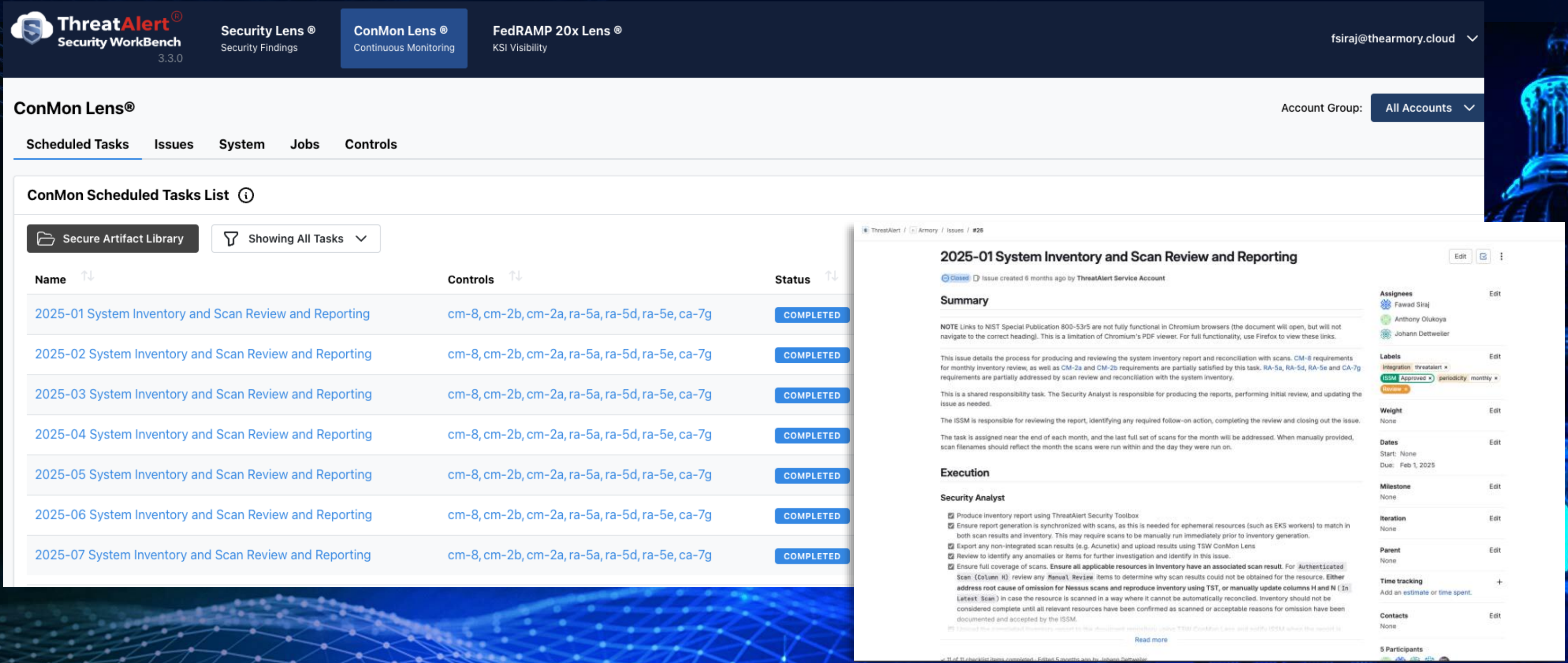
Modernized Systems Protect in Perpetuity



07 | Continuously Monitor and update

- Systems embracing a modern RMF model are architected to run via automation with machine-readable system state, compliance mappings, and continuous monitoring baked in.
- Agentic AI can be leveraged to deliver intelligent, continuous monitoring and validation of assertions of system state.
- SecOps teams are freed up to focus on exception handling and issues requiring human intuition and complex reasoning – with the automated system and AI capabilities serving as a significant force multiplier.
- Continuous monitoring is no longer an after thought, it’s a core behavior of the designed system.

Git Operations – An Automated Way Forward



ThreatAlert® Security WorkBench 3.3.0
Security Lens ® Security Findings
ConMon Lens ® Continuous Monitoring
FedRAMP 20x Lens ® KSI Visibility
fsiraj@thearmory.cloud

ConMon Lens®

Account Group: All Accounts
Scheduled Tasks
Issues
System
Jobs
Controls

ConMon Scheduled Tasks List

Secure Artifact Library
Showing All Tasks

Name	Controls	Status
2025-01 System Inventory and Scan Review and Reporting	cm-8, cm-2b, cm-2a, ra-5a, ra-5d, ra-5e, ca-7g	COMPLETED
2025-02 System Inventory and Scan Review and Reporting	cm-8, cm-2b, cm-2a, ra-5a, ra-5d, ra-5e, ca-7g	COMPLETED
2025-03 System Inventory and Scan Review and Reporting	cm-8, cm-2b, cm-2a, ra-5a, ra-5d, ra-5e, ca-7g	COMPLETED
2025-04 System Inventory and Scan Review and Reporting	cm-8, cm-2b, cm-2a, ra-5a, ra-5d, ra-5e, ca-7g	COMPLETED
2025-05 System Inventory and Scan Review and Reporting	cm-8, cm-2b, cm-2a, ra-5a, ra-5d, ra-5e, ca-7g	COMPLETED
2025-06 System Inventory and Scan Review and Reporting	cm-8, cm-2b, cm-2a, ra-5a, ra-5d, ra-5e, ca-7g	COMPLETED
2025-07 System Inventory and Scan Review and Reporting	cm-8, cm-2b, cm-2a, ra-5a, ra-5d, ra-5e, ca-7g	COMPLETED

ThreatAlert / Armory / Issues / #26

2025-01 System Inventory and Scan Review and Reporting

Closed · Issue created 6 months ago by **ThreatAlert Service Account**

Summary

NOTE Links to NIST Special Publication 800-53r5 are not fully functional in Chromium browsers (the document will open, but will not navigate to the correct heading). This is a limitation of Chromium's PDF viewer. For full functionality, use Firefox to view these links.

This issue details the process for producing and reviewing the system inventory report and reconciliation with scans. CM-8 requirements for monthly inventory review, as well as CM-2a and CM-2b requirements are partially satisfied by this task. RA-5a, RA-5d, RA-5e and CA-7g requirements are partially addressed by scan review and reconciliation with the system inventory.

This is a shared responsibility task. The Security Analyst is responsible for producing the reports, performing initial review, and updating the issue as needed.

The ISSM is responsible for reviewing the report, identifying any required follow-on action, completing the review and closing out the issue.

The task is assigned near the end of each month, and the last full set of scans for the month will be addressed. When manually provided, scan filenames should reflect the month the scans were run within and the day they were run on.

Execution

Security Analyst

- ☑ Produce inventory report using ThreatAlert Security Toolbox
- ☑ Ensure report generation is synchronized with scans, as this is needed for ephemeral resources (such as EKS workers) to match in both scan results and inventory. This may require scans to be manually run immediately prior to inventory generation.
- ☑ Export any non-integrated scan results (e.g. Acunetix) and upload results using TSW ConMon Lens
- ☑ Review to identify any anomalies or items for further investigation and identify in this issue.
- ☑ Ensure full coverage of scans. **Ensure all applicable resources in inventory have an associated scan result.** For `Authenticated Scan (Column H)` review any `Manual Review` items to determine why scan results could not be obtained for the resource. **Either address root cause of omission for Nessus scans and reproduce inventory using TST, or manually update columns H and N (** `In Latest Scan` **)** in case the resource is scanned in a way where it cannot be automatically reconciled. Inventory should not be considered complete until all relevant resources have been confirmed as scanned or acceptable reasons for omission have been documented and accepted by the ISSM.
- ☑ Upload the completed inventory report to this document repository using TSW ConMon Lens and notify ISSM when the report is

Read more

✓ 11 of 11 checklist items completed · Edited 5 months ago by Johann Dettweiler

Assignees
Fawad Siraj
Anthony Olukoya
Johann Dettweiler

Labels: Integration threatalert · ISSM Approved · periodicity monthly · Review

Weight: None

Dates
Start: None
Due: Feb 1, 2025

Milestone: None

Iteration: None

Parent: None

Time tracking: Add an estimate or time spent.

Contacts: None

5 Participants

Force Multiplier Through AI and Risk Management Automation

- Reduces need to expand workforce for routine compliance tasks.
- Frees up skilled personnel to focus on mission-critical cybersecurity operations.
- Maintains continuous compliance without dedicated manual oversight.
- Less “dedicated” compliance resources are required, but system authorization is still continuously maintained.

Outcomes for Cybersecurity Teams

- Accelerated risk mitigation and authorization timelines.
- Scalable compliance without expanding workforce.
- Continuous monitoring and compliance maintenance that is reflective of the running state of the system.
  - The state of the system remains transparent and fully auditable in near real-time.
- Enables teams to focus on mission-critical objectives.
- Stronger security posture aligned with DoD Zero Trust Strategy.

What’s Next?

stackArmor is fully invested in removing the friction inherent in the manual, inefficient processes and technologies of yesterday - and move our customers into the future of risk mitigation and ATO maintenance.

Let’s go even faster together!

Questions?

stackArmor

A TYTO ATHENE COMPANY

Thank You

Visit stackarmor.com to learn more.