merlin cyber mlabs

SOC Modernization for Federal Agencies

From Detection to Hunt and Response in Minutes – Automated, but Governed

A SOC director at a civilian agency has four monitors open: SentinelOne, Splunk, Armis, and ServiceNow. Several senior threat hunters left last quarter, and the short-staffed Operations Team is working through a backlog of critical vulnerabilities and POA&Ms. Then, a critical EDR alert is triggered, which may be linked to a recent CISA KEV advisory. The agency needs to answer a simple question: Do we have this vulnerability, where is it, and can we fix it without breaking a mission-critical system?

This is the operational and staffing reality federal SOCs operate in. The tools are already in place. What is missing is not another platform but rather a SOC-tuned workflow that allows those tools to operate as a coordinated system instead of separate security consoles.

The gap compounds across both response time and security compliance posture. Hours and sometimes days between detection and authorized response. Every manual correlation step introduces delay, and every delay increases vulnerability exposure. Additionally, every action still needs to be justified, documented, and defensible under audit.

Mandates such as KEV remediation timelines, NIST 800-53 controls, and Zero Trust requirements sit above this reality, but they do not solve it. They simply make the consequences of delayed or incorrect action more visible and costly.

THE CHALLENGE

Closing the Gap Between Detection and Response

Federal agencies are already invested in strong security platforms. The problem is not the tools but rather the workflow between them remains heavily manual and siloed.

Even mature SOC environments still struggle with:

- **MANUAL CORRELATION** across disparate security platforms.
- **DELAYED RESPONSE** to known threats such as CISA KEVs.
- **INCONSISTENT WORKFLOWS** that depend on analyst experience and competency.
- **LIMITED REPEATABILITY** and incomplete audit trails.
- **DIFFICULTY DEMONSTRATING ZERO TRUST MATURITY** and security compliance.

This creates exposure windows measured in hours or days, even with known threats.

THE SOLUTION

SOC Modernization as a Merlin Validated Solution

The AI SOC workflow is a Merlin Validated Solution (MVS) designed to close this gap by integrating existing security technologies into a unified, end-to-end detection-to-response workflow. Rather than replacing current investments, it operationalizes disconnected tools into a coordinated workflow that can identify threats, analyze security data, validate automated actions, and respond at machine speed and scale.

Merlin works with the agency to lab test and validate a four-vendor architecture: **Torq**, **Armis**, **SentinelOne**, and **ServiceNow** as a coordinated system for detection, enrichment, decision, and response. The solution combines AI-assisted analysis and orchestrated automation with a human-in-the-loop authorization model. The result is automated threat investigations, while response actions remain under analyst control until approved. Once authorized, remediation is executed immediately, with every step documented for audit and compliance purposes.

This changes the operating model of the SOC in a meaningful way. Instead of relying on analysts to manually move between systems, interpret data, and coordinate actions from scratch each time, agencies gain a repeatable and validated SOC workflow that strikes the right balance between governance and agentic automation.

How It Works

The AI SOC is designed around a continuous operational flow that compresses the distance between intelligence and action. It begins with the ingestion of threat intelligence, including IoCs, threat data, and KEVs from trusted sources. From there, the solution automatically executes threat hunts across endpoint and asset intelligence platforms, gathering the relevant context needed to understand impact and scope.

AI-driven enrichment then helps prioritize actions by combining threat intelligence with asset and exposure context. Instead of leaving analysts to piece together the full picture manually, the solution presents findings in a more actionable form. Before any remediation occurs, a human authorization gate ensures responsible oversight. Approved actions are then executed automatically, and the workflow is logged end-to-end to support compliance attestations and audit documentation.

Under testing in Merlin's federal lab environment, this workflow reduced response timelines from hours of manual correlation across disparate tools to under five minutes. In practice, this enables agencies to:

- Reduce detection-to-response timelines from hours or days to minutes
- Standardize and automate investigation and response workflows.
- Maintain human control over automated actions.
- Produce a complete, demonstrable audit trail of every decision and action.

Where It Delivers Value

Because the architecture is workflow-centric rather than tool-centric, the AI SOC effectively addresses use-cases and scenarios federal SOC teams manage daily:

VULNERABILITY DISCOVERY AND REMEDIATION
Identify and remediate KEVs within mandated timelines without manual cross-platform analysis.

MULTI-PLATFORM THREAT HUNTING AND RESPONSE
Execute coordinated investigations across heterogenous environments in minutes, not hours.

ZERO TRUST ENFORCEMENT
Continuously validate and remediate device and user security posture without disrupting operational systems.

PHISHING TRIAGE AND REMEDIATION
Automate high-volume workflows while maintaining consistency and control.

CRYPTOGRAPHIC DISCOVERY AND REMEDIATION
Identify and remediate emerging cryptographic risks, including post-quantum vulnerabilities.

Why This Architecture Is Different

Agencies evaluating SOC modernization find themselves choosing between three imperfect paths: continuing with manual and reactive operations, consolidating around a single-vendor platform, or attempting to stitch together automation through custom integrations.

The AI SOC solution offers a different path. It is an integrated architecture that is evaluated in partnership with Merlin against your agency's priority use cases before deployment:

Torq
provides workflow orchestration and AI SOC analyst.

Armis
delivers asset intelligence, visibility, and vulnerability exposure context.

SentinelOne
executes endpoint detection and remediation actions.

ServiceNow
is the system of record for approvals, case management, and audit trails.

Because each component contributes a distinct function, the solution avoids overlapping responsibilities while preserving vendor flexibility and reducing lock-in. This means swapping in and out vendors to fit an agency's deployed toolset is supported. This model also ensures fail-safe validation of actions across each component, reducing exposure and risk.

Validated Outcomes

Merlin's role is not to just assemble these tools but to validate that they work together in the agency's environment under defined constraints before commitment. Merlin's initial validation demonstrates these measurable improvements vs. current SOC workflows:

1 **THREAT INVESTIGATIONS REDUCED TO UNDER 5 MINUTES**
(from hours of manual correlation across multiple systems)

2 **60–80% REDUCTION IN ANALYST TRIAGE EFFORT**
(from hours of manual correlation across multiple systems)

3 **CONSISTENT, AUDITABLE RESPONSE WORKFLOWS**
(aligned to NIST 800-53 SI, IR, and AU controls)

4 **HUMAN-VALIDATED AUTOMATED RESPONSE ACTIONS**
(ensuring control is preserved while speed increases)

These outcomes enable agencies to reclaim analyst time, reduce operational and security gaps, and scale security outcomes without scaling headcount.

REQUEST A MERLIN LAB DEMO
merlincyber.com/contact

SCHEDULE AN ARCHITECTURE WORKSHOP
merlincyber.com/contact

merlin cyber mlabs

ABOUT MERLIN CYBER

Merlin Cyber is the go-to-market and Zero Trust Modernization affiliate of Merlin Group, a network of companies that invests in, enables, and scales technology companies with disruptive cyber solutions. Through Merlin Cyber, the U.S. Government can access innovative, public sector-ready cybersecurity solutions that are designed to meet government requirements and mission priorities. Merlin does this by selectively partnering with best-in-class cybersecurity brands, investing in visionary emerging technologies, and enabling the U.S. Government to successfully keep ahead of today's critical threats, accelerate Zero Trust modernization initiatives, and defend our nation.

254.371.3843
themerlingroup.com/**mlabs**

For more information, contact
info@merlincyber.com