SOLUTION BRIEF

Proactive Threat Hunting & Automated Incident Response: Strengthening Federal Cyber Resilience

The Federal Cybersecurity Challenge: A Reactive and Overwhelmed Defense

Federal agencies operate in one of the most highly targeted cyber environments globally. Nation-state actors, ransomware groups, and advanced persistent threats continuously evolve their tactics, often outpacing traditional security measures. The challenge is not just detecting threats but responding swiftly and effectively preventing operational disruption, data breaches, and risks to national security.

Despite significant investments in cybersecurity, federal security teams often find themselves in a reactive posture, overwhelmed by a plethora of security alerts and unable to prioritize their most critical threats. Manual investigation and incident response processes slow time to remediation, increasing the risk of successful cyberattacks. Without an automated and orchestrated approach, agencies struggle with:

- **Alert Fatigue & Lack of Prioritization**: Security teams must manually sift through thousands of alerts daily, leading to overlooked critical threats.
- **Slow Incident Response & Containment**: Manual processes delay response times, allowing threats to spread and increasing operational downtime.
- **Disjointed Security Tools & Lack of Integration**: Siloed security tools prevent teams from gaining comprehensive visibility of their threat landscape, resulting in disparate and inefficient security operations.
- **High Risk of Human Error**: The complexity and volume of security incidents create room for errors, increasing vulnerability to advanced cyber threats.

To secure mission-critical systems and data, federal agencies must transition from a reactive security approach to a proactive, automated, and efficient cybersecurity strategy.

Transforming Government Cybersecurity Practices with Automation

A proactive cybersecurity approach demands integrating real-time threat detection, automated incident response, and centralized security operations. This approach enables federal agencies to move beyond basic detection toward a fully integrated and automated response framework. Employing automated and optimized security solutions to augment EDR, XDR, NDR, and SIEM processes plays a critical role in responding and recovering from cybersecurity incidents and modernizing federal cybersecurity operations.

1. Centralized Alert Management, Correlation, and Analysis

Without a unified approach to threat intelligence, security teams must manually analyze alerts across disparate security tools, leading to security inefficiencies and overlooked critical threats. Palo Alto XSOAR centralizes alerts from multiple sources, including CrowdStrike, Veeam, and CyberArk, providing a single source of truth for security teams. To ensure accurate threat assessment and prioritization, XSOAR integrates with your entire security tool stack to provide one platform for threat hunting, enrichment, and rapid remediation:

- **Qualys:** Scans impacted assets for vulnerabilities, assigns real risk scores, and prioritizes threats based on exposure level and contextual risk.

Automating security alert analytics ensures that security teams focus on the agency’s most critical threats, rather than sorting through a queue of low priority alerts.

2. Automated Incident Response and Rapid Remediation

Speed and efficiency are critical when responding to cyber threats. Automated containment, remediation, and reporting workflows help federal agencies secure mission-critical systems while minimizing disruption.

- **Host Isolation with EDR such as CrowdStrike**: Upon detecting an active threat, CrowdStrike’s automation capabilities isolate infected hosts, preventing lateral movement, ransomware spread, and data exfiltration.
- **Automated Scanning and Patching with Qualys VMDR**: Once vulnerabilities are identified, Qualys automates patching workflows, ensuring rapid remediation across hybrid and multi-cloud environments.
- **AI-Generated Incident Reports with ChatGPT**: Security teams can quickly generate detailed, executive-ready reports, ensuring timely communication with stakeholders.

By automating these processes, agencies significantly reduce human error, streamline response efforts, and improve operational efficiency.

3. Continuous Monitoring and Adaptive Security

To ensure mission continuity and national security, federal agencies must maintain continuous, real-time visibility across their IT environment. The integration of detection, protection, and response tools within XSOAR enables real-time validation of remediation efforts. Revisiting initial malware and other threat detections, security teams can confirm that threats have been remediated, and no further infections exist.

This seamless, end-to-end security orchestration not only strengthens cyber resilience but also ensures compliance with federal security frameworks and mandates, including:

- FISMA
- NIST 800-53 & Zero Trust Architectures
- FOCAL Plan Objectives
- CISA BOD 22-01 and BOD 23-01
- CISA CDM Program

Enhancing Federal Cyber Resilience

By integrating Palo Alto Networks XSOAR, and Qualys VMDR, federal agencies achieve a layered, automated, and adaptive security framework that transforms their cybersecurity posture:

✓ **Proactive Threat Hunting & Continuous Testing**
Defensive security automation identifies vulnerabilities before adversaries can exploit them.

✓ **Centralized Alert Correlation & Prioritization**
XSOAR aggregates and enriches alerts, reducing noise and enabling faster decision-making.

✓ **Automated Response & Remediation**
Workflow automation expedites containment, patching, and threat response.

✓ **Improved Operational Efficiency & Reduced Human Error**
Automation eliminates manual redundancies and enhances the accuracy of incident response.

✓ **Scalability & Future-Proofing**
Adaptive security orchestration evolves with emerging threats and shifting regulatory requirements, ensuring long-term mission success and operational resilience.

Securing the Mission with Cybersecurity Automation

The cybersecurity threats facing federal agencies demand a shift from reactive to proactive defense strategies. Automation, orchestration, and AI-enriched threat intelligence are the key enablers of modern, mission-ready security operations. By implementing Palo Alto XSOAR CrowdStrike FIM, and Qualys VMDR, federal security teams can eliminate noise, prioritize critical threats, and respond at machine speed, ensuring the security of mission-critical systems and national security assets.

Ready to Strengthen Your Agency's Cyber Resilience?

Contact Merlin Cyber today to learn how automation-driven cybersecurity solutions can help secure the mission and protect against evolving threats.

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.

Learn more at:
merlincyber.com

Contact:
info@merlincyber.com