Tuesday, January 28, 2025

3:40 PM – 4:00 PM

Automation, AI, and Scalability: A New Era in DoD Cyber Risk Management

Brian Recore

Cybersecurity Solutions Engineer

Merlin Cyber

Abstract:

The U.S. Department of Defense (DoD) is at the forefront of defending a vast and increasingly complex digital infrastructure. As threats evolve, so must its approach to cybersecurity. Modernizing its cyber risk management strategy is crucial to protecting cloud systems, hybrid environments, containers, and IoT devices in an era of ever-expanding attack surfaces. To meet these challenges, the program needs enhancements such as real-time scanning, seamless integration of new technologies like DevSecOps pipelines, and scalable solutions that ensure all assets are covered. These advancements will not only strengthen defenses but also position the DoD to anticipate and neutralize future threats effectively.

Automation and smarter integration can revolutionize how vulnerabilities are managed, reducing the time from detection to resolution from weeks or months to mere hours. By adopting automated remediation and integrating with tools like SIEMs and IT Service management (ITSM) platforms, the DoD can transform its workflows for greater efficiency and precision. Advanced threat intelligence, intuitive reporting, and AI-driven insights will enable proactive responses to complex threats such as zero-day vulnerabilities and advanced persistent threats (APTs). Furthermore, ensuring alignment with frameworks like RMF and STIGs, while leveraging AI and machine learning to predict and counter emerging vulnerabilities, will keep the DoD ahead of its adversaries.

The Qualys TruRisk Platform embodies this vision, delivering a comprehensive solution to enhance DoD cybersecurity capabilities. It combines real-time vulnerability detection with automated remediation, streamlining processes and reducing response times. With built-in scalability and coverage for cloud, hybrid, and OT environments, the cloud-native TruRisk Platform adapts to the DoD's dynamic needs. Its AI-powered risk assessments and

actionable insights empower the DoD to prioritize and address critical vulnerabilities, ensuring a secure and resilient infrastructure in the face of evolving threats.

Summary Points

Scalability and Real-Time Scanning: Manage increasing data volumes and diverse environments.

Automation and Integration: Reduce detection-to-resolution time from weeks to hours with ITSM platform integration.

AI-Driven Threat Response: Leverage dynamic updates and predictive analytics for proactive cybersecurity.

Qualys TruRisk Benefits: Enhance cyber risk management with scalable and intelligent solutions tailored for evolving threats.