Tuesday, May 6, 2025
3:20 pm – 3:40 pm
*MSM Technology: DevSecOps Transformation*

**James Matney**
Senior Vice President of Technology
MSM Technology, LLC

Abstract:
MSM presents a strategic roadmap for DISA's DevSecOps transformation, engineered to deliver rapid capability deployment and fortified security through the seamless integration of immutable infrastructure and Continuous Authority to Operate (cATO) within a Zero Trust framework. Our methodology employs a structured, five-phase approach, beginning with foundational alignment and a focused pilot initiative, and advancing through collaborative design, automated security integration, rigorous validation, and continuous optimization. We emphasize the development of a resilient DevSecOps pipeline, leveraging industry-leading tools for comprehensive code analysis, infrastructure vulnerability assessments, and automated security testing. Recognizing the complexities of legacy systems, MSM provides tailored strategies for risk-prioritized transitions and the implementation of alternative Zero Trust controls where full DevSecOps adoption is initially constrained. Our approach is designed to empower DISA to achieve accelerated delivery, enhanced security posture, and a culture of sustained improvement, ensuring mission success in an evolving threat landscape.

MSM Technology Response:
DISA's initiative to adopt DevSecOps and Agile practices is crucial for accelerating capability delivery and enhancing security. MSM understands that this transformation extends beyond technical implementation; it requires a fundamental shift in organizational mindset, particularly focusing on immutable workloads and Continuous ATO (cATO).

1. How Should an Organization Start? MSM's Approach: Strategic Foundation & Pilot Team with Emphasis on Immutability and cATO

To initiate DISA's DevSecOps transformation, we recommend a foundational phase centered on strategic alignment, security, and the establishment of immutable workloads. This entails conducting comprehensive workshops with stakeholders to establish a clear understanding of DISA's strategic goals and security requirements, with a specific focus on transitioning to serverless/container architectures and implementing Infrastructure as Code (IaC). From the outset, we prioritize aligning to DISA’s Zero Trust architecture, ensuring security is embedded throughout the development lifecycle, and integrating cATO by tracking security concerns, POA&Ms, and bug fixes through Agile sprints and release pipelines.

Importantly, we advocate for starting with a pilot team, preferably a development team already familiar with Agile and DevSecOps principles and focusing on a project that can demonstrate the benefits of immutable workloads and cATO. This approach allows for controlled experimentation, rapid feedback, and demonstrable success. We use tools like Jira Align to ensure the DevSecOps transformation is aligned with strategic business goals, and integrate code scanning tools like Veracode, SonarQube, and Palo Alto Prisma Cloud into

the pipeline. The direct impact of this approach is minimized risk, built internal expertise, the establishment of a strong foundation for scaling DevSecOps across the organization, and a clear path towards achieving immutable workloads and cATO.

2. How Should the Transformation Process Be Structured? MSM's Approach: Phased Approach & Continuous Improvement with Detailed DevSecOps Pipeline Integration

MSM provides a strategic and effective approach for organizations to adopt DevSecOps through a phased and iterative methodology. This framework is firmly rooted in Zero Trust principles and is intrinsically linked with continuous improvement practices and a robust DevSecOps pipeline. The central goal is to achieve measurable security and operational results, with a specific focus on Continuous Authority to Operate (cATO) and the deployment of immutable workloads.

The transformation is structured into five distinct phases, offering a clear and progressive roadmap for implementation. This journey begins by establishing a secure foundation grounded in Zero Trust, followed by collaborative and secure design practices that embed security from the outset. The methodology then emphasizes automation-first security, leveraging advanced tools throughout the development lifecycle to ensure continuous security and cATO readiness. Subsequent phases prioritize rigorous validation and secure deployment, culminating in continuous optimization and governance to foster a culture of ongoing improvement.

Underpinning each phase is a comprehensive DevSecOps pipeline, integrating a suite of specialized tools for threat intelligence, security analysis, secure access, policy management, collaboration, code management, CI/CD, vulnerability management, and infrastructure automation. This holistic approach ensures that security is seamlessly integrated into every stage of the software development lifecycle. MSM's structured transformation process delivers a comprehensive and actionable strategy, ultimately driving successful DevSecOps adoption and the realization of tangible, measurable enhancements in both security and operational efficiency.

3. How Should Target Programs for Transition Be Identified? MSM Approach: Risk Assessment & Strategic Value with Consideration for Legacy Systems

To identify target programs for transition, MSM recommends a risk assessment and strategic value approach, with a particular focus on minimizing complexity and maximizing existing expertise for the initial pilot phase and addressing the challenges of legacy COTS/GOTS applications. We advocate for prioritizing programs with high potential impact, such as those involving critical operations or sensitive data, ensuring the most critical missions benefit first.

However, for the initial pilot, we strongly recommend selecting programs with the fewest number of dependencies and interface requirements, effectively choosing less-complex programs. We also recommend selecting programs where the development teams are already familiar with DevSecOps best practices and platforms. Additionally, we suggest selecting programs already aligned with Agile principles or modern development practices and are deemed secure, further facilitating smoother transitions.

For legacy COTS/GOTS applications, we recommend assessing their compatibility with DevSecOps and exploring options for achieving immutable workloads through scripted installations and automated deployments. If full DevSecOps is not feasible, we suggest enforcing other Zero Trust functionalities like micro-segmentation, ICAM, encryption, and API protections. We can conduct workshops with stakeholders to evaluate the strategic importance and feasibility of each program, ensuring alignment with DISA's overall objectives.

This targeted approach maximizes the return on investment, minimizes initial pilot complexity, leverages existing expertise, and ensures that the DevSecOps transformation delivers tangible benefits to DISA's most critical missions, while also addressing the complexities of legacy systems.