REQUEST FOR COMMENT ON SECURE SOFTWARE DEVELOPMENT, SECURITY, AND OPERATIONS (DEVSECOPS) PRACTICES

September, 12 2025

I. INTRODUCTION

In response to the National Institute of Standards and Technology's ("NIST") proposed guidance on Secure Software Development, Security, and Operations or "DevSecOps" Practices ("proposed guidance") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike appreciates the NIST's engagement with stakeholders and the opportunity to provide comments on the proposed guidance. We agree with NIST's goal of producing additional resources to guide DevSecOps best practices. As development teams continuously accelerate their software creation velocity, security becomes paramount. By tightly coupling security with the development process rather than treating it as an afterthought, teams can produce secure software efficiently and effectively.

We do not have feedback on every aspect of the proposed guidance, but we do want to offer several points that may be of value to NIST as they further develop this workstream.

A. DevSecOps Best Practices and Technologies

The proposed guidance encapsulates many of the best practices in the DevSecOps space today. NIST highlights Zero Trust Architecture (ZTA) implementation throughout the document and leveraging Artificial Intelligence (AI) technologies - both of which CrowdStrike views as best practices. While we support many of the practices outlined in the proposed guidance, there are several areas NIST could expand upon to represent the cutting edge, currently available technologies and practices that improve software security.

- *Application Security Posture Management* (ASPM). The proposed guidance references supply chain security and the visibility of third-party components as a challenge throughout the proposed guidance. To address those challenges, we recommend NIST include guidance on leveraging an Application Security Posture Management (ASPM) solution in the next draft of the guidance. An ASPM tool can provide runtime observability of third-party software libraries, offering visibility into code behavior after deployment, not just a static analysis,—a critical capability for managing the complex supply chain dependencies that characterize modern software development.

- *Zero Trust Architecture* (ZTA). As other NIST guidance reflects, ZTA concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. This constrains threat actors' ability to achieve actions on objective and provides additional opportunities for defenders to detect threats, making ZTA concepts core to the DevSecOps lifecycle. The proposed guidance generally references leveraging ZTA concepts throughout the software development lifecycle. CrowdStrike recommends in the final guidance NIST clarifies that ZTA practices should extend to developer endpoints to ensure that the development infrastructure itself maintains appropriate security posture, creating a foundation of trust that extends throughout the entire DevSecOps lifecycle. To be fully effective, ZTA concepts must be applied to developer's workstation and tools, not merely the software being developed.

- *Integration of Threat Intelligence*. The proposed guidance notes that there is a growing complexity and volume of cyber threats targeting software development environments. Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, skilled defenders can find them and thwart their goals. Leveraging real-time threat intelligence is a leading indicator of the strength of an enterprise cybersecurity program. CrowdStrike's approach to secure software development is informed by real-world threat intelligence to provide unparalleled visibility into how adversaries actually operate in modern development environments.

Leveraging this intelligence enables development teams to prioritize security efforts based on actual exploit likelihood rather than theoretical Common Vulnerability Scoring System (CVSS) scores alone. We recommend NIST include threat intelligence as a cybersecurity program best practice throughout the DevSecOps lifecycle.

- *Artificial Intelligence* (AI). CrowdStrike agrees with the proposed guidance approach to AI. Leveraging best-in-class cybersecurity technologies deploying AI is essential to meeting constantly-evolving threats. Defenders can leverage AI in several ways throughout the DevSecOps lifecycle such as generating security and compliance artifacts, providing contextual remediation guidance, and enabling continuous monitoring across the entire software development lifecycle—from code commit to production deployment. By embedding these capabilities directly into existing continuous integration/continuous delivery pipelines and development toolchains, organizations achieve the DevSecOps goal of shifting security left without sacrificing development velocity and ultimately creating more resilient software through enhanced collaboration between development, operations, and security teams. NIST should continue to encourage the use of AI and provide examples of the numerous use cases of AI throughout the DevSecOps lifecycle in the final guidance.

B. Security of Artificial Intelligence

As noted above, the proposed guidance notes many of the benefits AI will bring to the DevSecOps lifecycle. However, the paper also notes that there could be potential security concerns around leveraging AI. While AI is core to today's best cybersecurity practices, organizations must also consider AI system security. The use of AI has created a new attack surface for threat actors to target, so it is important that defenders have strong security practices in place to secure the data being used by AI, the identity or credentials interacting with the AI, and the systems hosting the AI. If an organization has strong security practices in place, likely, those can be applied to protecting AI systems as well.

Inherent trust can lead to inherent risk. Whether it's a human or an AI system, organizations must take steps to make sure access is appropriately defined and can't easily be abused.

III. CONCLUSION

NIST's proposed guidance represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. With an emphasis on adoption of practical security practices, these new requirements can raise the standard of cybersecurity across some of the most critical sectors. As NIST moves forward, we recommend continued engagement with stakeholders.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***