NIST Cybersecurity Framework 2.0 Concept Paper

Rebellion Defense, Inc.'s Comments regarding NIST Cybersecurity Framework 2.0 Concept Paper

RD Comment

In its concept paper, NIST lists several sections with potential significant changes to CSF 2.0. Further to section 6, "CSF 2.0 will advance understanding of cybersecurity measurement and assessment," NIST should encourage and describe the use of continuous automated tools, such as adversary emulation, to test the effectiveness of the "Protect" and "Detect" functions of the CSF.

One of the top challenges of cybersecurity is the evolving threat picture as our adversaries adapt to our countermeasures and develop ever more sophisticated techniques to penetrate our systems (GAO, 2021). Since NIST's 2021 report on systems security engineering noted the importance of red-teaming and automated incident response in developing a risk management strategy to counter evolving adversaries, federal guidance both from DoD as well as civilian oversight agencies have flagged the importance of advanced automation to emulate adversary tactics, techniques and procedures at scale across critical networks to deliver a contextualized understanding of how cyber defenses stand against a real-world attack scenario.

The DoD Software Modernization Strategy highlighted the importance of shifting from a cybersecurity "snapshot in time" compliance culture to "automation, real-time continuous risk monitoring" as the necessity for software development pipelines. The Department of Navy's Cyber Ready initiative includes the requirement for automated adversarial testing tools.

In November, 2022, the Defense Department released their Zero-Trust Strategy and Roadmap to accelerate "the shift from compliance-based to risk-based security approaches as the complexity of threats and vulnerabilities increases." Implementation of Zero Trust architectures is one thing but implementations will need to be tested; automated adversary emulation mechanizes manual security testing to allow for continued monitoring across the enterprise to inform a response to emerging threats. It validates the effectiveness of Zero Trust practices with speed and at scale.

Outside of Defense, the Cybersecurity and Infrastructure Security Administration (CISA)'s 2023 - 2025 Strategic Plan also highlights the importance of automating security controls to scale threat testing capability with the increasing workload and size of IT enterprises. GAO's recent 2022 report also recommended the Administrator of the National Nuclear Security Administration "develop and maintain cybersecurity continuous monitoring strategies" that address NIST guidance.

All federal government agencies and federal contractors (including subcontractors) must be compliant with a number of federal security standards, all of which align with the NIST framework. As such, and in the spirit of moving towards optimizing for true security versus compliance, it would be helpful for NIST to both encourage and describe use of continuous automated tools within the framework, as appropriate.