Synack

January 19, 2017

The National Institute of Standards and Technology
Ms. Donna F. Dodson
Mr. Matthew Scholl
100 Bureau Drive
Stop 1070
Gaithersburg, Maryland 20899-1070

Sent via Electronic Mail

Dear Ms. Dodson and Mr. Scholl:

Synack thanks The National Institute of Standards and Technology ("NIST") for welcoming public comment on the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2. The Framework is a necessary document for securing the nation's infrastructure from increasing threats.

We look forward to continuing our work with the NIST and other stakeholders to better secure our nation's infrastructure. Synack's commitment to strengthening cybersecurity is rooted in our training at the NSA and our experience with challenges facing our network of public and private sector clients.

Our recent work for government agencies, including the Department of Defense (Hack the Pentagon program) and the Internal Revenue Service, has reinforced our belief in the need to elevate and emphasize the importance of penetration testing, especially crowdsourced penetration testing and vulnerability discovery. Please find our comments below.

The Framework should include penetration testing as a method for detecting cybersecurity vulnerability issues

As government systems move to online and cloud-based solutions, a proactive and dynamic approach to finding and fixing vulnerabilities before adversaries can exploit them is the best way to secure these systems against attackers. The Framework correctly identifies the need for security continuous monitoring (DE.CM) - a regular cadence of penetration testing should be a critical component of this defensive measure. The Framework also correctly identifies that vulnerability scans are a way to achieve this goal (DE.CM-8). However, vulnerability scans alone will fail to find security weaknesses in our systems. The adversary is creative and often attacks via vulnerabilities undetected by scanners - a human, hacker-powered perspective is a necessary complement to machine technology and a critical component of security testing. The best way to achieve a secure environment is through regularly testing digital environments from an adversarial perspective, and the best way to scale penetration testing is through a crowdsourced approach. This should be included in the Framework. For example, the NIST could add a subcategory to Security Continuous Monitoring (DE.CM) such as "DE.CM-9: Ongoing penetration testing methods, including crowdsourced penetration testing and vulnerability discovery, are established and performed." The Framework should cite NIST Special Publication 800-53 Revision 4 CA-8 as an informative reference. Penetration testing is one of the most powerful ways to proactively identify weaknesses and deficiencies within a system and this addition would strengthen the Framework.

Responsible vulnerability disclosure continues to evolve

Responsible Disclosure is a method for organizations to receive security vulnerabilities from the outside world in the hopes of closing security holes faster. We welcome the addition that NIST made regarding the coordinated vulnerability disclosure lifecycle. Responsible disclosure, when executed correctly, makes information systems as a whole safer. As NIST considers policies around responsible disclosure, we believe the following should be tenants of that policy:

1. Vulnerability disclosure needs to be voluntary and independent

RS.CO-5 correctly identifies the voluntary nature of responsible disclosure. However, the Framework should allow for varying degrees of disclosure. Vulnerabilities vary in sensitivity and organizations need the flexibility to intelligently respond in a way that would not jeopardize the security of others.

2. Responsible Disclosure Programs should allow for varied levels of responsiveness to submitters

Organizations have widely varying levels of readiness to handle reported security vulnerabilities. Some are able to respond quickly and consistently to reporters; others are not. Responsible disclosure programs should respect that reality and allow for responses ranging anywhere from best-effort to a fixed, known response time.

3. Trust and privacy must be prioritized

Organizations will have different privacy policies. For example, an organization may wish to start by reviewing the vulnerability report information before they engage with the submitter. Others may only be comfortable receiving vulnerability report information after the reporter is under a non-disclosure agreement, to have a more open and valuable conversation to help close the vulnerability. Still others may wish that all research activity be conducted via a secure gateway. However, all organizations should understand the risks associated with engaging third party ethical hackers, and Synack encourages organizations to establish clear rules of engagement that prioritizes ethical engagement and discourages submitters from holding vulnerability findings “for ransom.”

Responsible Disclosure Programs should allow for organizations to request confidential and secure communications agreements with submitters.

4. Responsible disclosure should allow for organizations to compensate submitters differently

Security vulnerability reporters may wish to be compensated for their time, via bug bounty payments. Organizations may wish to offer thanks, compensation, or promotional items. Given the wide differences in organizational maturity in security, any or no compensation should be deemed acceptable.

In many cases, open submissions may come from individuals who are difficult to pay or illegal to pay under other US laws. Other organizations may wish to use thanks or gifts (swag) instead of cash payments to best reward submitters.

About Synack

Synack, the leader of crowdsourced security testing, provides real security to the modern enterprise. We leverage the world's most-trusted ethical hackers and an industry-leading machine learning platform to find critical security issues before criminals can exploit them. Companies no longer have to choose between working with the best security talent and a lack of time, resources or trust. Headquartered in Silicon Valley with regional offices around the world, Synack has protected over 100 global brands by reducing companies' security risk and increasing their resistance to cyber-attacks. Synack was founded in 2013 by former NSA operators Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO.

We look forward to follow up conversations and participating in future Framework workshops. Please contact me if you have any questions. Thank you for welcoming these public comments.

___
Anne-Marie Chun
Senior Product Marketing Manager
Synack
achun@synack.com
855.796.2251 x 749