[redacted]
Sent: Thursday, May 4, 2023 6:03 AM
[redacted]
Subject: Re[2]: NIST CSF 2.0 Feedback

I would like to add another feedback related to patch management which is currently in Identify.

In many ways, patch management can and should be be broken into two pieces:

- Identifying vulnerable software on the network
- Remediating the vulnerable software also called patching

Since the software is already part of the asset management in Identify, this part should remain in Identify.

The key strategic issue is that there is a gap in time between when the vulnerability is known and the patch is available. This must be reflected in the framework. In the event of a nation state attack, by design, there will be no patch, but there still should be a method for the nation to react. Solutions will rise once NIST makes this distinction.

Currently, patch management is scan and remediate and they are very time consuming and focuses on known vulnerabilities. By separating vulnerabilities into identify the vulnerability then the protect function with access control can block the vulnerable software in real time in the event there is no patch.

Of course, this is contingent of expanding the role of Access Control to include software and hardware. The protect function gives more real time and proactive response.

I want to thank NIST and the efforts of the dedicated cyber security professionals for building these frameworks for the betterment of all.

Rob Cheng
[redacted]

[redacted]
Sent: 5/2/2023 6:00:50 PM
Subject: RE: NIST CSF 2.0 Feedback

[redacted]
Sent: Tuesday, May 2, 2023 4:05 PM
To: cyberframework <cyberframework@nist.gov>
[redacted]
Subject: NIST CSF 2.0 Feedback

Feedback on NIST CSF 2.0 from Rob Cheng:

I would like to thank NIST for creating the NIST Cybersecurity Framework, perhaps one of the greatest advancements in cybersecurity since the ascent of ransomware. The framework emphatically states the importance of the Identify function to the foundation of any cybersecurity stack. The framework effectively summarizes the complexities of cybersecurity and makes cybersecurity accessible to millions more cybersecurity professionals.

This framework has greatly influenced my thinking and my company's direction. The framework shows clearly that the American cybersecurity stack is oversubscribed on the Detect and Respond functions, and undersubscribed on Identify and Protect. In this way, the NIST CSF is visionary. My company is working to build and create Identify and Protect solutions that solidify any existing framework. Keeping this in mind, we would like to suggest changes and provide feedback to the draft NIST CSF 2.0.

The two most important cybersecurity components of the Asset Management category in the Identify function are software and hardware. Software Asset Management not only specifies what software is on the network but also which are authorized. Hardware Asset Management is equally

important since a foreign device can enter a network when user credentials have been compromised. In the NIST CSF 1.1 states that the Identify function is foundational, it is really the HWAM and SWAM that are the most foundational for the effective use of the framework.

HWAM and SWAM in of itself is insufficient to create a foundation We recommend that Identify include attribution of hardware and software as a new category or function. There are two types of attribution. First is attribution of the publisher of the software. Can the publisher of the software be accurately known including the name, location and country of origin of the product? This is where digital signing certificates and the concepts of SBOM begin to enter the equation. This will increase use of digital signing certificates since the lack of digital signing certificates for legitimate software is indeed a security hole. The Log4J vulnerability is an example of the proper use of attribution. When a library vulnerability is found, the vulnerability can be immediately be identified through proper attribution.

The second level of attribution is a stated purpose for the existence of the software on the network. Is this custom software that is being developed internally for human resources? Or perhaps a new accounting software?

By building a framework with publisher and business reason attribution, then the protect function can be expanded beyond user authentication to include software and hardware authentication. For example, if a software has no valid publisher and no valid business reason, then it is blocked by default, and perhaps a business reason can be established and later the software is allowed on the network. It is this simple speed bump that prevents ransomware while allowing simple IT governance. Similar to software, hardware should be authorized on the network as well. Although there is not a VIN yet for devices and MAC addresses can be spoofed, making device authorization part of the framework will force innovation in device identification and authentication.

Similar to software, a business purpose can be stated for a device and an alternate method to allow a device on a network when it can not be adequately identified and attributed.

A key and necessary distinction that must be made in the framework is which can be automated rather than accomplish by humans. Hybrid models should be entertained. For example, much of the detect function is currently accomplished by humans, but perhaps through AI some of it can be automated. The Governance function should be accomplished by humans and not by ChatGPT. Similarly, in the newly created Attribute category in the Identify function, the verification of vendor should be automated and the business purpose must be done by humans.

If the Protect category can be expanded to hardware and software, more granularity would help usability and access. A software can be authorized on the network with inadequate attribution if that software has no ability to communicate outside of that device.

The most important topic is to understand how the framework can deal with Zero Day Vulnerabilities. As written in the book “This Is How They Tell Me The World Ends”, zero day vulnerabilities are being stockpiled by America’s enemies including China Russia, Iran and North Korea.

In the event of a zero day by a nation state, reaction time is critical to mitigating risk and damage. Vulnerability scanners are slow to react to zero days. In fact, with the recent infections due to the Goanywhere vulnerability, these scanners are not particularly effective when the patch is known. Once a previously known good software becomes vulnerable, its attribution is changed from good to vulnerable. It can then be caught in the protect function since it is not longer authorized. Not all vulnerabilities are the same, so for example, low and medium vulnerabilities can be allowed and logged, where as high vulnerabilities are blocked. In the case of a high vulnerability without a patch, also known as a zero day, the process would be blocked and buys time for the patch to become available and damage is minimized.

I want to thank NIST for its dedication to building better cybersecurity for our country and the world.

Thank you.

Best Regards,

Zack Austin
Vice President,
Business Development