[redacted]
Subject: EXT :FW: The NIST Cybersecurity Framework
Date: Thursday, March 9, 2023 1:55:46 PM

CAUTION: This email originated from **outside** your organization Exercise caution when opening attachments or clicking links, especially from unknown senders

[redacted]

Sent: Saturday, January 21, 2023 12:23 PM
To: cyberframework <cyberframework@nist gov>
Subject: Fwd: The NIST Cybersecurity Framework

Good afternoon,

Per NIST s request for feedback on the CSF, please see my recent article on the topic

Regards,

Walter Haydock

Begin forwarded message:

Date: August 5, 2022 at 8:17:03 AM [redacted]
Subject: The NIST Cybersecurity Framework
Reply-To: Deploying securely <reply+12uy5g&rr5uj&&eac3e188d6aae62403947c5c01cf895622e4596222e302d34f21596a25e6718f@mg1 substack com>

Open in browser [gcc02 safelinks protection outlook com]

The NIST Cybersecurity Framework [gcc02.safelinks.protection.outlook.com]

What Uncle Sam says about vulnerability management: Part I.

[gcc02 safelinks protection outlook com]

[redacted]

[gcc02 safelinks protection outlook com]

Aug 5 [gcc02 safelinks protection outlook com] [gcc02 safelinks protection outlook com] [gcc02 safelinks protection outlook com]

[gcc02 safelinks protection outlook com]

As you know, I have spent some time in the federal government but yet am often quite critical about its approach to cybersecurity

That's not to say there is nothing to learn

Thanks for reading Deploying Securely! Subscribe to receive new posts.

Subscribe now [gcc02.safelinks.protection.outlook.com]

Thus, in this article, I will examine the National Institute of Standards and Technologies (NIST) Cybersecurity Framework (CSF [gcc02 safelinks protection outlook com]) The CSF is important because Executive Order 13800 [gcc02 safelinks protection outlook com] made its use mandatory by federal departments and agencies Due to NIST's role in standard

setting, it also has become part of the laundry list of frameworks on which many companies [gcc02 safelinks protection outlook com] claim [gcc02 safelinks protection outlook com] to base their security programs

In order to avoid boiling the ocean, I will look at only the aspects specifically related to vulnerability management (my speciality), possibly leaving the rest for a later time

In its own (vague) words, the CSF is

> "voluntary [for the private sector] guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders "

At a high level, the CSF breaks down cybersecurity into five functions:

- Identify (ID)
- Protect (PR)
- Detect (DE)
- Respond (RS)
- Recover (RC)

Each requirement is annotated by its function as well as a unique (and arbitrary) identifier I'll examine the relevant ones below:

ID.RA-1: Asset vulnerabilities are identified and documented

The only way to consistently manage the risk from vulnerabilities in a system is to identify them first Having an overlapping series of processes, procedures, and tools to do so should thus form a key strategy of an organization's security plan This can (and should) start at the design phase, where threat modeling [gcc02 safelinks protection outlook com] and other assessment techniques [gcc02 safelinks protection outlook com] can find and close potential security gaps before development of a system even beings It can also include manual and automated peer code reviews once work has begun to build the system Finally, when the system is in production, penetration testing and additional scanning tools can continue to identify flaws for remediation

Ensuring that you have complete and redundant coverage throughout your product's lifecycle is important for minimizing the risk of hackers exploiting gaps Also important, although generally underemphasized, is *how* you document these findings I would strongly recommend using the engineering team's tool of record (Jira, etc) to record all security findings Creating a separate system for compartmentation purposes makes it extremely difficult to slot security issues into sprints and releases, and I have seen this practice cause great confusion Use the permissions/access control functionality built into such engineering tools to control dissemination without impacting productivity (and thus reducing the speed of vulnerability remediation)

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

Vulnerabilities are but one aspect of the organization's total risk picture If there is no threat actor capable of or interested in exploiting an issue, then there is likely no risk involved Furthermore, the impact to the organization's data of such exploitations will vary exponentially rather than linearly between situations The Common Vulnerability Scoring System (CVSS [gcc02 safelinks protection outlook com]), unfortunately, depicts such impacts in the latter fashion and thus is likely to result in a highly unrealistic view of the impact of a vulnerability Furthermore, even though CVSS - when including the temporal and environmental aspects of the score - does encompass all of the relevant risk factors described above Finally the specification itself explicitly says "CVSS Measures Severity, not Risk " Thus, I would advise not using it for the latter (or any) purpose

The Factor Analysis of Information Risk (FAIR) technique [gcc02 safelinks protection outlook com], conversely, is an excellent philosophical tool for going about such an analysis, but is difficult to automate when evaluating individual vulnerabilities Thus, I would recommend using the Deploy Securely Risk Assessment Model (DSRAM [gcc02 safelinks protection outlook com]) or similar tool to incorporate all of these considerations

PR.IP-12: A vulnerability management plan is developed and implemented

Dwight Eisenhower once said [gcc02 safelinks protection outlook com] "plans are worthless, but planning is everything " When faced with a newly identified security flaw, having an easily implementable standard operating procedure will save you huge amounts of time that would be otherwise lost orienting on the problem and deciding how to proceed While a formal policy is a bedrock document for explaining organizational responsibilities and risk tolerances, a more actionable flow chart are similar procedure can help ensure that every participant knows what to do at every given juncture (check out this template [gcc02 safelinks protection outlook com] if you need a ready-built one) Make sure you practice this drill and that your procedures are not just vague boilerplate

DE.CM-8: Vulnerability scans are performed

This is a subset of requirement ID RA-1 and, in my opinion, is duplicative because scanning is merely one of several ways to identify vulnerabilities in assets With that said, I'll take a deeper look at the topic, because the devil is in the details There is a massive difference between running a single scan using one open-source tool once per year and deploying an overlapping and continuously-running set of SAST, DAST, IAST, and SCA tools [gcc02 safelinks protection outlook com] Such a suite is certain to produce a steady stream of vulnerability readings (many of which will be duplicates, if you have multiple of the same types of tools running) The former is likely to generate a single spreadsheet of thousands of findings from a single point in time There is certainly a point of diminishing returns here, but getting rapid updates regarding known vulnerabilities [gcc02 safelinks protection outlook com] in your code is critical in determining how to manage the risk from them Thus, I would lean toward comprehensiveness when deploying scanners

Furthermore, your remediation speed can mean very different things based on how much scanning you do If you do very little but successfully meet aggressive timelines for identified issues, you probably shouldn't be too confident in your security posture, as many unknown [gcc02 safelinks protection outlook com] (to you, at least) issues probably lurk in your network Conversely, if you have a massive backlog but are able to burn through it in a consistent and risk-driven manner, you should worry too much about the total number of issues [gcc02 safelinks protection outlook com]

RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

This is really critical Although its somewhat duplicative of PR IP-12, it's probably worth discussing twice Many organizations that deploy a bevy of scanning tools actually have very

little in terms of documented processes for handling the findings Whether or not the process is documented, step one is usually implicitly "panic," which is not a good place to start When you compound this with a high volume of issues detected, it becomes very difficult to manage and prioritize them effectively If you expect reports from security researchers (which you don't really have a say in any way), having a well-developed coordinated vulnerability disclosure (CVD [gcc02 safelinks protection outlook com]) program is vital to avoiding chaos as well as the potential for a PR black eye

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

Although this sounds simple, it is really important I would probably expand "are mitigated" to "have the associated risk mitigated, transferred, or avoided," but the dichotomy is basically between reducing the risk to the organization or accepting it There really are no other options [gcc02 safelinks protection outlook com] for dealing with risk, but yet I still see organizations unable to understand this harsh truth Making sure your vulnerability management policy has clear deadlines for making such decisions [gcc02 safelinks protection outlook com] will help to prevent you from enduring endless and aimless discussions about what to do

Conclusion

As a foundational cybersecurity planning document, the CSF is a good start Although there are some logical overlaps that make the document not MECE [gcc02 safelinks protection outlook com] and it reeks of passive voice government-speak, it isn't a bad place to start your vulnerability management or broader cybersecurity program I hope that version 2 0 [gcc02 safelinks protection outlook com], which is under development, will fix some of the gaps Additionally, and as with all things, specific implementations of the concepts will make or break an organization's security posture, and I have targeted my recommendations at how to avoid common pitfalls in this regard