CROWDSTRIKE

REQUEST FOR INPUT ON NIST CYBERSECURITY FRAMEWORK 2.0 CORE DISCUSSION DRAFT

May 31, 2023

I. INTRODUCTION

In response to the National Institute of Standards and Technology's ("NIST") discussion draft on the Cybersecurity Framework 2.0 ("CSF 2.0") Core, 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

We appreciate NIST's efforts to provide tools to organizations which in turn will better protect the nation from cybersecurity threats. The original NIST CSF has a legacy of being a useful tool and this update is timely.

CrowdStrike previously commented on NIST's CSF 2.0 Concept Paper, and we've reemphasized certain points in this response.[1] We do not have feedback on every aspect of the proposed changes presented in the discussion draft, but we do want to offer several points.

A. Suggestions for New Categories and Subcategories

In the Protect Function, the discussion draft proposes a new Category titled "Platform Security" ("PR.PS"). The revised PR.PS-04 Subcategory which reads: "log

[1] *https://www.crowdstrike.com/wp-content/uploads/2023/04/NIST-CSF-2.0-Comments.pdf.*

records are generated for cybersecurity events and made available for continuous monitoring," is an important addition to the CSF 2.0. We recommend the following language for PR.PS-04 in the CSF 2.0 draft: "*Log records are generated for cybersecurity events to find potential adverse cybersecurity effects and made available for real-time continuous monitoring*." The addition of "real-time" is an important distinction to take the action of monitoring from passive to actively prevent threats.

The discussion draft also updates the description of the Continuous Monitoring ("DE.CM") to read: "Assets are monitored to find potential adverse cybersecurity events, including indicators of attacks and compromise, unauthorized and inappropriate activity, protection deficiencies and failures and other activity with a potentially negative impact on cybersecurity." We recommend the description of DE.CM be updated to state: "*Assets, accounts, and resources are monitored to find potential adverse cybersecurity events, including indicators of attack and compromise, unauthorized and inappropriate activity, protection deficiencies and failures and other activity with a potentially negative impact on cybersecurity*." In the context of modern cybersecurity practices, monitoring must extend beyond assets themselves.

DE.CM-09 is created in the discussion draft. The Subcategory calls for: "Computing hardware and software and their data are monitored to find adverse cybersecurity events." We recommend DE.CM-09 be amended to include holistic endpoint monitoring: "*Endpoints and their data are monitored using Endpoint Detection and Response (EDR) to find adverse cybersecurity events*." Endpoints can include servers, desktops, laptops, all-in-ones, tablets, mobile or cellular telephones, thin clients, computing peripherals, virtual containers, and cloud workloads. We recommend NIST use "endpoints" in this Subcategory instead of "computing hardware and software."[2] This update to DE.CM-09 will encourage organizations to defend each individual element of its network, and will present that practice more clearly given increased prevalence across the industry of ephemeral endpoints (e.g., virtual machines and containers).

B. Include Zero Trust Architecture Subcategory

[2] We suggest this edit align with the current draft's configuration. However, we propose a more robust solution for integrating detection and response in Section C. Unify Detect and Respond Functions, below.

In the concept paper, NIST explained that the CSF 2.0 will expand the outcomes in the Respond and Recover Functions to emphasize the importance of incident response and recovery and consider additional response and recovery planning outcomes. In the discussion draft, NIST made changes to the Identity Management, Authentication, and Access Control Category and changed its abbreviation to "PR.AA."

We support NIST revising this important Category; however, there are additional measures that the CSF 2.0 can suggest. The current framework includes credential management, principles of least privilege, network integrity, and user/device authentication. These cybersecurity practices do not represent the current best practices of identity management, authentication nor access control. NIST has undertaken many projects that focus on Zero Trust Architecture (ZTA) that would be helpful to implement into the CSF 2.0 PR.AA.

CrowdStrike recommends that the CSF 2.0 include a Subcategory titled "Implement a Zero Trust Architecture" – within PR.AA – that includes best practices like the use of cloud-based EDR, comprehensive logging, identity protection and use of multi-factor authentication. Due to fundamental problems with today's widely-used authentication architectures, use of these practices and technologies constitute best practices. While these measures alone do not provide users with full ZTA, we highlight them for their efficacy in real-world defense.

Last year, 80% of cyberattacks leveraged identity-based techniques to compromise legitimate credentials and evade detection; this year, adversaries are doubling down on advertising stolen credentials and access-broker services in the criminal underground.[3] Identity attacks will only continue to increase. Revising the Protect Function to include ZTA will further align CSF 2.0 with existing NIST work, increase ease of adoption for users, and raise organizations' security against these attacks.

C. Unify Detect and Respond Functions

Given developments in the practice of cybersecurity in recent years, NIST should consider unifying the "Detect" and "Respond" Functions. Once conceptually separate, cybersecurity tools, practices, and controls across these Functions have

[3] *CrowdStrike Global Threat Report*, 2023. *https://www.crowdstrike.com/global-threat-report/.*

evolved and merged over time. Today, security operations concepts employ detection in response in concert. With respect to specific tools and technologies, EDR helped define and continues to embody this concept. Emerging Extended Detection and Response (XDR) concepts bring this approach elsewhere in the security stack. In addition to unified tooling, the same teams and personnel are engaged in detection and response activities in modern enterprise security teams.

In previous security models, an organization first detected an attack and then engaged in separate steps or processes to respond and remediate. This approach failed. *Breakout time* - the time it takes an adversary to move laterally from an initially compromised host - of adversaries is getting faster each year. Based on CrowdStrike data, breakout time decreased from 98 minutes in 2021 to 84 minutes in 2022.[4] CrowdStrike advises users that when responding to a security incident or event, every second counts. The more an organization can do to detect and stop adversaries at the outset of an attack, the better chance of preventing them from achieving their objectives. By combining the "Detect" and "Respond" categories, NIST can signal a change in thinking and cause organizations to create cybersecurity plans and strategies that reflect adversaries' capabilities.

D. Create Intelligence Category

CrowdStrike also recommends that NIST consider creating a new "Intelligence" Category under the Identify Function. Given the current threat landscape, it is necessary for organizations to be familiar with the adversaries that could target their systems. Cybersecurity threats are evolving and increasing. Illustrative of this, in CrowdStrike's 2023 *Global Threat Report*, we observed a notable surge in identity-based threats and cloud exploitations. To name a few, we found a 112% year-over-year increase in advertisements on the dark web for identity and access credentials, a 95% increase in cloud exploitation by threat actors, over 30 new adversaries and numerous new ways that eCrime actors weaponize and exploit vulnerabilities.[5] As the adversaries continue to evolve and find new ways to target victims, organizations need to increase their emphasis on cybersecurity practices that leverage the most effective technologies.

[4] *CrowdStrike Global Threat Report*, 2023. *https://www.crowdstrike.com/global-threat-report/*.
[5] *CrowdStrike Global Threat Report*, 2023. *https://www.crowdstrike.com/global-threat-report/*.

Integrated threat intelligence makes it easier to detect and respond to an attack due to the real time visibility to indicators and what threat actor deploys similar tactics. An organization's ability to effectively incorporate cyber threat intelligence processes within cybersecurity activities is an increasingly necessary step to ensure the accuracy and completeness of security capabilities and controls. Integrated threat intelligence should be referenced as a best practice or example in CSF 2.0. Currently, the CSF has one direct reference to "threat intelligence" (ID.RA-2) and two references to threat (ID.RA-3, ID.RA-5). In addition to integrating these elements within a new Intelligence Category, additional Subcategories could include "conduct an assessment of the threat landscape" and "develop and maintain an understanding of relevant threat actors, evolutions their targeting practices, and changes in their in tactics, techniques, and procedures (TTPs)."

III. CONCLUSION

We commend NIST for strengthening cybersecurity by amplifying attention given to this issue and defining expectations. There are many key steps organizations should take to strengthen their security posture already included in the CSF, and continuing to add the current best cybersecurity practices will benefit organizations along with the cyber ecosystem as a whole. As NIST moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any framework updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

CONTACT

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

Robert Sheldon
Director, Public Policy & Strategy

Elizabeth Guillot
Manager, Public Policy

Email: policy@crowdstrike.com

***