REQUEST FOR INPUT ON NIST CYBERSECURITY FRAMEWORK 2.0 CONCEPT PAPER: POTENTIAL SIGNIFICANT UPDATES TO THE CYBERSECURITY FRAMEWORK

March 17, 2023

I. INTRODUCTION

In response to the National Institute of Standards and Technology's ("NIST") concept paper on the Cybersecurity Framework 2.0's ("CSF 2.0") significant changes 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 legal and regulatory environment surrounding cybersecurity is increasingly complex on account of (i) reliance on globally-distributed infrastructure, and (ii) compliance obligations for national and international standards and procedures. In order to ensure the most robust cybersecurity methods and disclosure, and compliance obligations remain feasible, regulators must endeavor to create clear and future-flexible expectations. Tools, like the NIST CSF, have been helpful for organizations to address multiple requirements and create basic standards for regulators.

While we do not have feedback on every aspect of the proposed changes, we do want to offer several points that may be of value to NIST as it continues to draft the CSF 2.0.

A. 2.6. Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices.

In the concept paper, NIST explains 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. The concept paper also expressed changes to the Identity Management, Authentication, and Access Control Category ("PR.AC").

The changes outlined in the concept paper are valuable additions to the CSF. However, there are additional measures, particularly in the Protect function, that can be suggested by the CSF 2.0. 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.AC.

Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. NIST states in the concept paper, "NIST believes no changes to CSF Subcategories are needed in order to accommodate ZTA principles. ZTA capabilities support the outcomes outlined in the CSF to secure environments, although the implementation differs based on the technology composition." We believe more explicit guidance on ZTA implementation would yield stronger cybersecurity outcomes. This is no longer a "next step" organizations can take to bolster their security posture, ZTA should be a security baseline.

CrowdStrike recommends that the CSF 2.0 include a subcategory titled "Implement a Zero Trust Architecture" – removing PR.AC-7 and creating a new subcategory in the Protect function – that includes best practices like the use of cloud-based Endpoint Detection and Response, comprehensive logging, identity protection and use of multi-factor authentication. Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication.

While these measures do not alone provide users with full ZTA, we highlight them for their efficacy in real-world defense. Specifically, Endpoint Detection and Response (EDR) is the cybersecurity approach to defending endpoints such as desktops, laptops, and mobile devices from malicious activity. Given that organizations have so many connected devices, EDR is critical to identifying and preventing threats and enabling threat hunting activities in case adversaries gain unauthorized access. Additionally, organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases. Logging is critical to support recovery actions for organizations.

While NIST already mentions multi-factor authentication (MFA) as a means to authenticate users and devices, it also says that single-factor could be an option - in today's threat environment that is not a strong enough security posture. Where adopting MFA is not possible, compensating control should be implemented appropriately with the risk level. Some adversaries have even been targeting traditional MFA methods, making it all the more important for organizations to embrace a ZTA.

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.[1] 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.

B. 4.1. Add a new Govern function.

CrowdStrike agrees with the addition of a Govern function in CSF 2.0. Privacy and cybersecurity cannot exist without each other and are more intertwined than ever before. Integrating the NIST Privacy Framework and the CSF through the addition of the Govern function will be useful to organizations looking to take a holistic approach to their cyber and data security strategies.

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

Today, many of the most innovative technologies for protecting personal data against breaches leverage endpoint telemetry data, cloud-native Software-as-a-Service (SaaS) delivery, 24/7 global threat hunting, and cross correlation of indicators of attack. As the Govern function is adopted for cybersecurity use, we recommend NIST include these innovative technologies as examples of ways to meet the subcategories of the new Govern function.

Additionally, modern IT infrastructure involves cross-border data transfers. This is important as the U.S. pursues international agreements. As NIST increases their international adoption of the profile (as described in "1.3 Increase international collaboration and engagement"), NIST should note to international partners that cross-border data transfers are both key to cybersecurity practices and implementation of a complete CSF.

C. 5.1 Expand coverage of supply chain.

CrowdStrike agrees with the concept paper's emphasis on the importance of cybersecurity supply chain risk management. Recent, wide-spread, cybersecurity supply chain attacks highlight the need for stronger supply chain protection. Whether through supply chain attacks, or otherwise, we know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organizations accept this premise – that cybersecurity involves not just a passive alarm, but a sentry actively looking for trouble – is the leading indicator of the strength of their cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give themselves to intervene as a breach attempt progresses through phases, commonly referred to as the *kill chain*. Multiple opportunities for detection help avert "silent failures" – where a failure of security technology results in security events going completely unnoticed.

With that in mind, as NIST expands the "Supply Chain Risk Management" category, we recommend threat hunting and use of AI/ML technologies be added to the examples for the appropriate subcategory.

D. Additional Recommendations

D.1. "Detect and Respond"

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 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.[2] 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.2. Threat Intelligence

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

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

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.[3] 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.

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). Subcategories of a new Intelligence Category could include conduct an assessment of the threat landscape and map known threat actors to existing assets through a risk assessment.

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

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

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

[redacted]

***