March 17, 2023

NIST Cybersecurity Framework 2.0 Concept Paper:

Feedback from Industry

Submitted To: Cherilyn Pascoe

Senior Technology Policy Advisor
National institute of Standards and Technology

Submitted By: BedRock Systems Inc

[redacted]

[redacted]

POC: John Walsh, SVP Strategy & BD

[redacted]

[redacted]

000

1.0 Summary

BedRock Systems appreciates the opportunity to provide feedback to the Cybersecurity Framework. BedRock is comprised of former senior government officials, cybersecurity experts, and business professionals. We believe in the advancement of cybersecurity for the protection of American infrastructure and regularly contribute to the NIST National Cybersecurity Excellence Partnership (NCEP) and the National Cybersecurity Center of Excellence (NCCOE). We are providing strategic and tactical feedback to the formation of CSF 2.0. Thank you for this opportunity.

2.0 Changes- Section 2.6 Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices

Since the issuance of the original Cybersecurity Framework (CSF), technology increased pervasiveness in our lives, where now corporations and people maintain completely online presence in the orchestration of their operations or lives. Additionally, adversaries increased competence, familiarity, and digital presence, targeting individual targets in online and offline methods to achieve their ultimate objective. In order to incorporate these technological changes, we ask that NIST modernize CSF 2.0 with the following guidance.

2.1 Move beyond an Incident Response Focus

The current cybersecurity market is heavily focused on reaction based security products in network security, endpoint security, and cloud application security. [1] The methods used by the market providers is a detect and response, incident focused process, where the security product identifies malware, illicit activity, or adversarial actions based on past performance of the systems, adversary, or network. The new Cybersecurity Framework should advance beyond a reaction based focus to a framework focused on PREVENTING cyber attacks, rather than reacting to them. Prevention based activities center around asset management, identity and asset isolation at the network, memory, and compute layers. Utilizing these activities, systems can function even while being contested.

2.2 Include the concepts of Least Privilege and Least Functionality as Security Controls

The Current Cyber Security Landscape is changing with the abilities of current generation of ARMv8 and x86 based CPUs. These CPUs support revolutionary advancements in virtualization technology implementations, enabling the ability to substantially increase the ability to Prevent the successful execution of numerous exploitation techniques. Requiring virtualization technologies to implement strict least privilege and least functionality definitions and configurations for each Virtual Machine Manager/Monitor used enables compliance with additional SP 800-53 Rev 4 controls.

Recommend the addition of the following controls to:

Function – Protect /Category – Protective Technology (PR.PT) / Subcategory – PR.PT-3 – Least Functionality
CM-11(2) User Installed Software :
Multiple exploits exist that enable elevation of privileges and installation of software by un-authorized users or applications. Preventing these exploits by monitoring guest kernel actions and Preventing the attempts that are not detected by existing Anti-Virus, Logging, and End-Point Detection and Response systems is part of a comprehensive Least Functionality configuration.

[1] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

SI-3(8) Malicious Code Protection – Prevent execution of Malicious Code in/on guest kernels, thereby mitigating entire series of 0 and N-day attack successes.

SI-16 Memory Protection – Tight definition of memory allocated to VMMs and then preventing lateral movement via memory exploitation techniques.

2.3 Identify Zero Trust needs and separation between security and operations.

In a Zero Trust Network the system owner must build isolation and containment mechanisms that are themselves immune to being exploited and bypassed even if the attacker has gained root or administrative privileges on a compromised system. These containment mechanisms must provide "vertical isolation", namely deny the ability to gain more privileges (e.g. OS kernel privilege escalation attacks), and also "horizontal isolation". By "horizontal isolation" is to deny the ability to access resources in other trusted zones on the same system, or access resources laterally on connected systems.

Software exploits depend on vulnerabilities in code therefore isolation and containment mechanisms must be immune to bypass by vulnerability exploit-based attacks – a high barrier for any policy enforcement mechanism – thereby making the security controls un-bypassable and unbreakable. Adversaries are adept at implementing practices to disguise malicious malware as legitimate traffic or lying in wait in a network that is already compromised.

Since general purpose software is used by a trustworthy hypervisor kernel, the notion of "Trust Zones" could be a CSF activity incorporated at a very fundamental layer of a CSF segmented Compute Base, to provide freedom from software defects, and resistance to side-channel timing attacks. This is done with intelligent allocation of CPU microarchitecture resources by the security aware hypervisor, such that different trust zones don't share exploitable resources even at the CPU microarchitecture level, thereby defeating timing side-channel attacks. Such enclaves can be used in a wide variety of computing tasks, where neither the cloud service provider, nor untrustworthy software running on the same server, can extract code or data from these computing enclaves. Examples include microservices and containers that are perfectly isolated from other computing tasks running on the same server.

To meet ZT Target and Advanced requirements, ZT capabilities must support fine-grain micro-segmentation and continuous monitoring and feedback control loops for dynamic policy enforcement to **PREVENT attacks from execution**. The components of the ZT model architecture and its enclaves relied on for providing trust must be "trustworthy" and protected in this manner.

2.4 Incorporating Intelligence Operations to Risk Management in the Cybersecurity Framework

The measurement of cybersecurity risk includes intelligence, which is defined as the knowledge and foreknowledge of the world around us that allows leaders to consider alternative options and outcomes in making decisions.[2] In the course of cybersecurity intelligence, this involves methodology for characterizing adversary actors, adversary activities, intent, and capability. It is only based on threat actor activity, intent, and capability to act where you can properly assess severity of exploting a vulnerability and consequence to a system or system of systems if unprotected. Measuring intelligence characterizations also provides an opportunity to continuously measure and manage implementation and capacity of the CSF to provide a best practice for government and industry in the cyberspace domain.

[2] George, Roger Z. and Bruce, James B. Analyzing Intelligence: National Security Practicioners' Perspectives, 2nd Edition 2014.