From: Farid Abdelkader
To: cyberframework
Subject: NIST CSF 2.0 Recommendation
Date: Monday, August 14, 2023 11:54:59 AM
Attachments: Outlook-h1mtvqyo.png
Outlook-33wdofo1.png
Outlook-frtwxd3c.png

Good Morning,

In reviewing the NIST CSF 2.0, I wanted to make a recommendation:

The Framework holds itself short of controls around Software/Applications. I have held numerous discussions with CISOs and Heads of IT Risk. Many are torn on the focus of prioritizing Infrastructure and applications for SOC onboarding. If the framework highlights the importance of Software/application logging and monitoring, it would put an end to the debate here. I know the framework highlights a risk assessment of "assets," but even consulting firms are weighing in and throwing this up for debate.

There are quite a few arguments made on relying heavily on infrastructure vs. Application monitoring:

1. **Limited Visibility into Application Behavior**: Infrastructure monitoring, while essential, only scratches the surface. It fails to provide a deep understanding of how applications are interacting with users, other applications, and even potential attackers. This lack of visibility can lead to undetected vulnerabilities within the application layer, allowing for potential breaches that could go unnoticed until it's too late.
2. **Inadequate Response to Application-Specific Threats**: Application-specific threats require specialized monitoring and response strategies. Without dedicated application logging and monitoring, the organization may be unable to detect sophisticated application-level attacks, such as advanced persistent threats (APTs) targeting specific business functions.
3. **Potential Misalignment with Business Objectives**: Applications are the lifeblood of modern business operations. Ignoring application monitoring can lead to a disconnect between IT and business strategy, resulting in inefficiencies, customer dissatisfaction, and potential revenue loss.
4. **Compliance Challenges**: Regulatory bodies are increasingly focusing on application-level controls. Solely focusing on infrastructure might not only lead to compliance challenges but also hefty fines and reputational damage.
5. **Overemphasis on Inherent Risk Approach**: The rapidly changing threat landscape requires a dynamic approach. By not considering residual risk and solely relying on inherent risk, the organization may become complacent, failing to adapt to new threats targeting applications.
6. **Potential False Sense of Security**: A high percentage of infrastructure onboarding might create a false sense of security. Without a comprehensive view that includes application monitoring, hidden risks within the application layer may remain undetected, leading to catastrophic failures.
7. **Ignoring the Interconnected Nature of Risks**: The symbiotic relationship between applications and infrastructure means that a vulnerability in one can affect the other. A holistic view that considers both layers is essential to understanding the complete risk profile.

8. **Impact on Innovation and Agility**: By not prioritizing application monitoring, organizations may stifle innovation and agility. Understanding application behavior is key to continuous improvement, enhancing user experience, and staying competitive in the market.

Very happy to see all of the other updates, and new subdomains entering the framework. However, I strongly urge a reconsideration of the approach towards application monitoring, recognizing its critical role in a comprehensive cybersecurity strategy.

Stay Safe,

Farid Abdelkader *CBE, CEH, CISA, CISM, CISSP, CMMC-RP, CRMA, CRISC, CSX-P, MCSE, PCI-QSA*

ISACA New York Metropolitan Chapter

Immediate Past President and Cyber Security Education Leader

[redacted]