From: Troy L Townsend
Sent: Monday, April 25, 2022 7:01 PM
To: CSF-SCRM-RFI <CSF-SCRM-RFI@nist.gov>
Cc: Brian Abe
Subject: RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Attached response details how the MITRE ATT&CK Framework and NIST CSF are complimentary, and how ATT&CK is being used to operationalize concepts from the CSF. Please consider for question 8 of your RFI. Thank you!

Troy Townsend

Better Together: NIST CSF and ATT&CK™

MITRE ATT&CK™ was originally developed to provide a framework to categorize and describe the techniques used by cyber adversaries to achieve their goals on a compromised system. The MITRE ATT&CK framework has evolved to become an industry standard with many commercial companies and government agencies adopting ATT&CK. The MITRE ATT&CK framework is a "curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target." ATT&CK builds out its knowledge through adversary emulation, red teaming, behavioral analytics development, defensive gap assessment, and cyber threat intelligence enrichment. Below are examples of how ATT&CK aligns to the CSF and how organizations can use ATT&CK to operationalize CSF concepts.

IDENTIFY:

The IDENTIFY Function of the CSF is tightly coupled with NIST Special Publication 800-53 guidance on implementing security controls (mitigations) to help characterize and drive down risk. Within MITRE we consider risk to be represented as the functional equation:

$$f(risk) = \frac{(vulnerability\ x\ impact)\ x\ threat}{mitigations}$$

In combination with MITRE CVE, NIST guidance can describe and characterize the severity of risk, but organizations traditionally have had difficulty representing the threat component of the equation. MITRE ATT&CK provides an opportunity to characterize a threat actor's methods to inform a risk scenario, making it particularly relevant for the CSF functional categories of **Risk Assessment (ID.RA)** and **Risk Management Strategy (ID.RM)**. The most natural relationship between ATT&CK and the CSF is in the application of the ATT&CK framework to characterize adversary tactics and techniques, addressing the Subcategories of **ID.RA-2**, **ID.RA-3**, and **ID-RA-5**.

In January 2022, MITRE Engenuity's Center for Threat Informed Defense demonstrated a relationship between NIST 800-53 and ATT&CK by mapping security controls to ATT&CK techniques. The mappings provide a critically important resource for organizations to assess their security control coverage against real-world threats as described in the ATT&CK knowledge base and provides a foundation for integrating ATT&CK-based threat information into the risk management process. With over 6,300 individual mappings between NIST 800-53 and ATT&CK, this resource greatly reduces the burden on the community to do their own baseline mappings– allowing organizations to focus their limited time and resources on understanding how controls map to threats in their specific environment. For example, NIST 800-53 security control *CA-3* is mapped to **ID.AM-3**, which is then mapped to ATT&CK (Sub)-Techniques *T1020.001*, *T1041*, *T1048*, *T1048.002*, *T1048.003*, *T1567*.

This project demonstrated how the mappings can determine if there are threats relevant to a system/organization, where gaps exist, and inform risk decisions that could be made (e.g., tailor in a control). This project also showed that such decisions align with senior leadership risk guidance and mission/business needs. These mappings can also help provide insight that could come from CSF Profiles which include Informative References that highlight specific controls to support specific cybersecurity activities and outcomes, priorities of what to implement given limited resources, and how often to monitor. As this is a part of the **Asset Management (ID.AM)** Category, the ATT&CK Techniques' descriptions can lend a hand in what assets to monitor.

PROTECT:

ATT&CK Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed. Mitigations outlines the appropriate safeguards to limit or contain the impact of a potential cybersecurity event. ATT&CK Mitigations has been used to inform development of personnel training, organizational response plans, or system resiliency requirements which align to the subcategories of **PR.AT-5**, **PR.IP-9**, **PR.IP-12**, and **PR.PT-5**. Moreover, ATT&CK Mitigations focus on security concepts that emphasize strong access controls, data security measures, and processes to protect both enterprise information and systems or assets. ATT&CK Mitigations can help advise implementation of baseline subcategories such as: **PR.AC-**1, **PR.AC-4**, **PR.AC-5**, **PR.DS-1**, **PR.DS-2**, **PR.IP-1**, **PR.IP-4**, **PR.IP-6**, **PR.PT-1**, and **PR.PT-4**. For example, NIST 800-53 security control *SC-6* is mapped to **PR.PT-5**, which is then mapped to ATT&CK (Sub)-Technique *T1564.009*. In this example, the ATT&CK Tactic leads to Defense Evasion on Hidden Artifacts: Resource Forking and through ATT&CK Mitigations you learn how to protect your systems with application developer guidance.

DETECT:

ATT&CK Detections & Data Sources define the appropriate activities needed to find the malicious activity. A high-level analytic process, sensors, data, or strategies that can be useful to identify a technique that has been used by an actor and how to collect that data. ATT&CK Detections and Data Sources is intended to inform those responsible for detecting malicious activity so that they can take action to remedy the impact done to an organization. ATT&CK Data Sources align with the data collection necessary in CSF Subcategory **DE.AE-3**. Data sources listed can improve monitoring for cybersecurity events and detection of a given ATT&CK technique, addressing Subcategories **DE.CM-1**, **DE.CM-7**, and **DE.DP-5**. Per **DE.AE-2**, information collected from data sources can be used to understand adversarial behavior and methods.

The NIST 800-53 Mappings specifically calls out **DE.CM, DE.AE, DE.DP** Categories. These mappings are closely tied to 389 ATT&CK Techniques and Sub-Techniques. For example, NIST 800-53 security control *SA-9* is mapped to **DE.CM-6**, which is then mapped to ATT&CK (Sub)-Techniques *T1041, T1048, T1048.002, T1048.003, T1567*. In this example, the ATT&CK Tactic leads to Exfiltration over Command and Control, Alternative Protocols, and Web Services. With ATT&CK Detections and Data Sources you will learn how to monitor for external service providers and cybersecurity events through network traffic, file access, and command-line execution.

RESPOND/RECOVER:

The ATT&CK framework includes a tactic on Impact, which can be mapped back to the CSF, specifically for Categories **RS.AN, RS.MI, RS.IM, RS.RP, RS.CO, RC.RP, RC.IM, RC.CO**. These Categoires are closely tied to 343 ATT&CK Techniques and Sub-Techniques. For example, the NIST 800-53 security control *CP-10* is mapped to **RC.RP-1**, which is then mapped to ATT&CK (Sub)-Techniques *T1485, T1486, T1490, T1491, T1491.001, T1491.002, T1561, T1561.001, T1561.002, T1565, T1565.001*. In this example, the ATT&CK Tactic leads to Impact and what the adversary is trying to manipulate, interrupt, or destroy on your system and data. This information alone can give you knowledge on what data and systems you need to plan for within the recovery process in hindsight of a cybersecurity incident. Though ATT&CK gives insight on what systems and data to monitor for, what ATT&CK doesn't give is actual recovery processes and procedures which is an instance where the CSF excels as a complimentary framework to ATT&CK.