MITRE ATT&CK vs NIST CSF

What is the MITRE ATT&CK Framework? How does it relate to NIST CSF? How can they be used together?

A key component in any cyber security program, whether enterprise (IT), operational (OT), or a converged version of the pair (IT/OT) is driven by the governance laid out by the organization to manage cyber-related risks.

A successful governance model communicates how an organization identifies threats, prioritizes and manages risks, determines how risks are transferred or budgeted, and lays out the procedures to respond. One such framework to guide this area of management is the National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF).

Why choose NIST CSF?

Verve uses NIST CSF as a common model when discussing cyber security because it is easily relatable for decision makers and IT security teams.

There is no shortage of competing cyber security frameworks, but the NIST CSF is easily mappable to other standards, and when combined with NIST SP-800-82r2, the industrial cyber security companion, the NIST CSF is perfectly suited for Operational Technology (OT) environments and critical infrastructure.

So, without further ado, let us introduce our two contestants in this framework discussion:

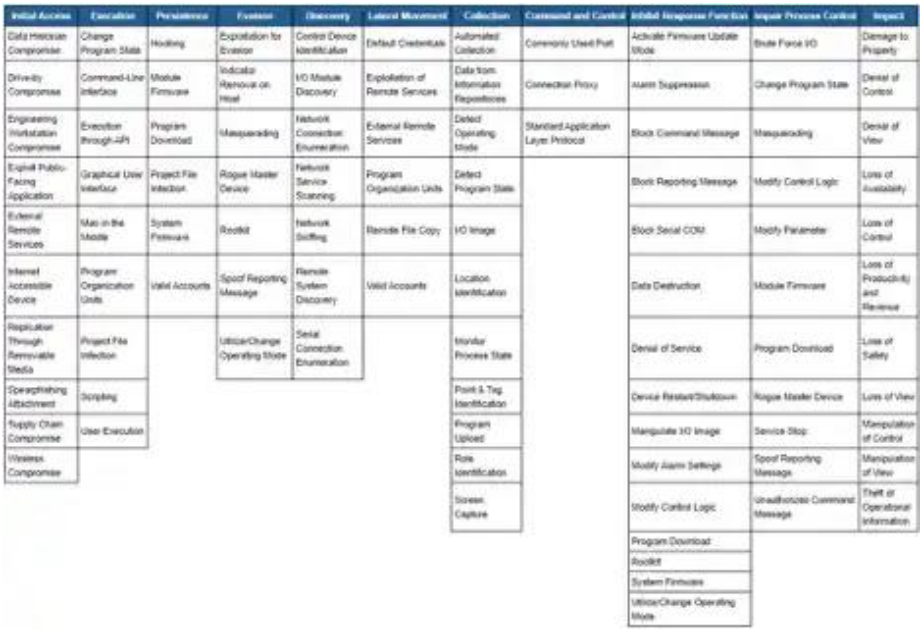
- **NIST Cybersecurity Framework** is a set of best practices, standards, and recommendations that help an organization improve its cybersecurity measures. Originally, it was targeted towards IT, but it was later expanded to include an ICS component.
- **MITRE ATT&CK ®** is a framework that describes the common tactics, techniques, and procedures that advanced persistent threats against Windows enterprise networks. This was later expanded to Industrial Control Systems (ICS).

Whether NIST CSF or a different standard is the best is beyond the point, an organization must start somewhere. When the MITRE ATT&CK framework was released, the cyber security industry was ablaze with articles touting its usage, so we waited and tried to see how it would take effect.

What is the MITRE ATT&CK framework?

In the creators own words: the MITRE ATT&CK framework is an expansive system that provides a common taxonomy of tactics, techniques, and procedures that is applicable to real-world environments, more useful than the cyber kill chain module, and represents how adversaries interact with systems.

It is a matrix of columns that look left to right for each of the phases of an attack, and vertically under each column header – tactics and techniques that befit the vertical. Each element can be picked and chosen as befits the technology, process, or expert. They can be drilled down and provide additional information with a page of reference.



In this way, the tactics represent “why” an attacker may use those techniques, and the techniques, represent that “how” they do so, which is very different in nature from the core concept of governance.

While governance is composed of structures, systems and practices that encompass decision making, strategic direction guidelines, implementations of policy, and reports on performance for improvement and corrective action, ATT&CK groups various techniques into piles for cyber security professionals and tools to communicate defensive coverage, cyber threat intelligence, detection capabilities and incident/red team results.

The relationship between NIST CSF & MITRE ATT&CK

Most organizations have a governance structure and process that includes how the organization protects itself from cyber threats or utilize technology.

The NIST CSF is made up of five governance areas that comprehensively describe: protect, identify, detect, respond, and recover. These five areas consist of different properties and capabilities, but they do not directly outline how to dissect a cyber security incident or provide analytical markers to test detection technologies for example.

It does, however, give an organization the scaffolding to govern itself, and at a minimum, determine which security capabilities and processes are necessary for a certain level of cyber security maturity.

Therefore, the MITRE ATT&CK matrices (Enterprise and ICS) are still relevant, but have far less value when appropriate cyber security governance is lacking. To bridge those gaps, the NIST CSF describes various components you should have in place, and the ATT&CK framework puts forward the necessary information or use cases that should be captured.

One without the other is not very effective, but when used together, they drive effective cyber security governance for both IT and OT environments.

Why should the NIST CSF and MITRE ATT&CK be used together?

Imagine the following scenario:

"It is a typical day at X organization, and a variety of alerts are generated from anti-virus and affected system's logs. A cybersecurity incident is clearly under way."

Using the above scenario, an analyst would be assigned to investigate the alerts or anomalous conditions, but how would they do so and in what manner? Surely governance is required!

At a minimum, if it were ad hoc and without a repeatable structure, it would be less than ideal, and so many events may not be properly evaluated, or even managed without appropriate frameworks and technology.

This is clearly not in the best interests of teams securing the organization, so a good approach in this scenario would be to:

- Set up sufficient technology and guidance/governance aligned with the five NIST CSF areas so the security teams have clear processes and tools at their disposal

- Ensure resources and staff are adequately trained on core security tools to identify and detect threats, protect systems, isolate, and remediate an attacker, and recover affected systems
- Use predefined playbooks that are fine-tuned and supported using ATT&CK tactics, techniques, and procedures
- Use the ATT&CK framework to outline, identify, and triage the cyber event as it occurs, but also as part of the post-mortem process
- Follow the organization's guidance from start to finish including communicating the impacts to management

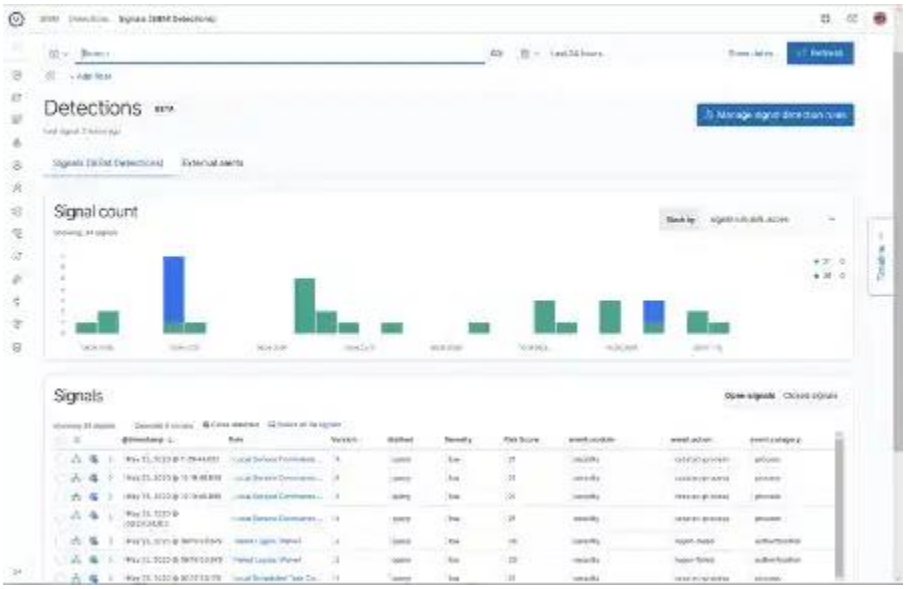
This is a high-level overview that requires customization for your organization, but it is important to note that you can use the frameworks together in ICS and OT.

Comprehensive OT Security using NIST CSF, MITRE ATT&CK, and Verve

On its own, the ATT&CK framework may not be particularly useful for a holistic OT cyber security program, but when combined with the NIST CSF wheel and technology, it becomes a force multiplier and makes your current ICS cyber security investments truly comprehensive when used correctly.

Neither framework fulfills its absolute potential without being executed alongside adequate technology and resources. But when operationalized as part of an organization focused on structured action, Verve becomes an invaluable OT cyber security solution to secure critical infrastructure.

The Verve Security Center goes beyond asset inventory management and vulnerability management to apply a robust OT Systems Management (OTSM) approach.



ATT&CK works best when using a SIEM, which is significant as SIEM functionality for logging and alerts (Signals) is a new feature to the Verve Security Platform. Even more, we support a variety of ATT&CK detection use cases and provide additional resources to enable the use of both frameworks to enhance your organization's security posture. This includes:

- Identifying risks, and areas where gaps exist in an organization's NIST CSF wheel coverage
- Enumerating vulnerabilities and tracking remediation
- Creating custom policies to secure endpoints against specific techniques
- Layering compensating controls to deny an attacker initial compromise vectors
- Fine-tuning logs, alerts, and SIEM functionality
- Creating custom detection "signals" that are grouped or use specific ATT&CK TTPs
- Dissecting timelines into a series of events that contributed to an incident

Given the unique ability for Verve to install on commodity systems to communicate natively to a wide catalog of devices, patch, and ingest logs from applicable OT systems, you get a powerful cyber security tool to aids security teams.

Retrieved from https://verveindustrial.com/resources/blog/mitre-attck-vs-nist-csf/ 03 Oct 2022.