
AVERTIUM
Whitepaper
THREAT-BASED SECURITY
at the Intersection of MITRE ATT&CK and NIST CSF

TABLE OF CONTENTS

Threat-Based Security Introduction

Managing alerts and responding to incidents are the most dramatic and visible aspects of cybersecurity. However, maintaining the tactical actions of a buzzing "alert factory" is not enough to protect a business on its own. In fact, the greater part of modern security ops functions at a deeper strategic level through industry frameworks and best practices for threat-based security.

This paper examines how to use the NIST CSF in conjunction with MITRE ATT&CK to help define and enact a threat-based approach to cyber protection. It provides an overview of the frameworks themselves and illustrates the value of using them together.

Reactive vs Proactive Cybersecurity Operations

Cybersecurity operations that focus on alerts, intrusions and malware are vital to protection, but they are fundamentally reactive. These measures also tend to handle issues at the micro level, rather than assessing and addressing the underlying threat patterns.

A threat-based defense strategy, by contrast, is based on systematically assessing an environment's strengths and vulnerabilities to foresee, analyze and mitigate specific potential threats. While tactical measures are critical to overall security posture and may employ sophisticated technologies such as machine learningbased analytics, the holistic and proactive nature of threat-based approaches makes them fundamental to security in depth.

A well-structured approach to threat-based security draws on established industry guidelines and frameworks to assess the environment as the basis for actions to advance its state of maturity.

- **NIST CSF.** The National Institute of Standards and Technology (NIST) developed its Cybersecurity Framework (CSF) to help practitioners manage cyber risk. The NIST CSF provides standards, guidelines and practices that organizations can use as the basis for assessing threats and the entity's state of readiness against them. This forms the basis for identifying priorities for advancing security measures.

- **MITRE ATT&CK.** The MITRE Corporation's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) framework is a public knowledgebase of adversary techniques, including a rubric and taxonomy for classifying them. The framework identifies tactics which correspond to objectives, suchas "initial access") and techniques (means toward those goals, such as "drive-by compromise"), organized into a series of matrices.

IT pros will see legacy tactics begin to become obsolete...

"In 2020, businesses will start to allocate more budget towards keeping their companies secure as IT pros will see legacy tactics begin to become obsolete, being forced to update their disconnected point tools, manual processes, and lack of staff."

Tiffany Bloomer, President,
Aventis Systems

Analyze & Map Compute Environments & Threats

The approach to threat-based security based on these frameworks begins with assaying the security maturity of the environment using the CSF and defining the environment's current state of security maturity against a target security state. Strengths and weaknesses in security posture revealed by that analysis are mapped back to ATT&CK to address the threats most likely to exploit known weaknesses in an organization's security posture.

Following this process allows IT shops to prioritize threats in terms of their likelihood and impact, then identify suitable tools, techniques and procedures to prevent, detect and respond to them.

Assessment and Maturity Modeling with NIST CSF

The CSF was developed as voluntary guidance to protect critical infrastructure in response to a Presidential Executive Order in 2013. The resulting framework applies to every organization, public or private, regardless of size and type. It draws together external standards, guidelines and practices to form a composite methodology.

The result is a prioritized, flexible, repeatable and cost-effective approach to identifying and managing cybersecurity risk**. The framework is made up of three main components:**

1. **Framework Core**
2. **Implementation Tiers**
3. **Profile**

1. Framework Core: A hierarchical set of functions, categories and subcategories that define desired cybersecurity activities and outcomes. The Core uses non-technical language and is outcome-driven rather than prescriptive, to facilitate working across groups with varying areas of expertise, within existing processes.

2. Implementation Tiers: The mechanism for characterizing the degree to which an organization's environment and practices adhere to the characteristics defined in the framework. In order from weaker to stronger alignment, the framework's four tiers bear the following labels: partial, risk-informed, repeatable and adaptive.

3. Profile: An organization's unique optimization of the framework to suit its individual needs, based on business objectives, requirements and controls in context of the threat environment. The profile identifies opportunities for cyber security improvements by juxtaposing the organization's current state with its target state.

Maturity modeling based on the CSF defines strengths and weaknesses in security posture. For example, mapping business objectives, practices and security requirements against the framework Core can produce a Profile that describes the current state in terms of the Tiers described above. Likewise, a Profile can be defined for the desired target state.

Maturity modeling is based on comparison of the current-state and target-state Profiles. Gap analysis reveals areas for potential improvement in the form of disparities between the Implementation Tiers reflected for specific functional areas between the two Profiles.

The framework provides taxonomy and mechanisms for creating roadmaps from the present to the desired state. Organizations begin by describing their current and target states for cybersecurity, based on how they identify and prioritize opportunities for improvement rooted in a structured, repeatable process. The framework also enables them to continually assess their progress and to iteratively redefine the roadmap.

This can provide high value to the CISO making investment decisions, as well as to the boardroom assessing the progress of the security program as it continues to mature towards its target state.

Investigating Potential Methods of Compromise with MITRE ATT&CK

The breakdown and classification of adversarial actions in the ATT&CK framework is designed explicitly to be independent of the underlying specific tools or malware attackers use. Focusing instead on the approaches they use to interact with systems during an operation makes the ATT&CK matrices a common frame of reference across organizations, attacker details and security tools and practices.

Providing tactics, techniques and procedures (TTPs) gives context for each aspect of an attack. Tactics describe an attacker's objective, and the framework nest the techniques and procedures attackers use to accomplish these objectives. The ATT&CK matrices visually depict relationships between specific techniques and tactics. This includes separate treatments for each of the following:

- **PRE-ATT&CK matrix** provides tactics and techniques related to preparation of security posture, including information gathering, planning, development and staging.

- **Enterprise matrix** includes platform-specific information for Windows, macOS, Linux and cloud (including specific popular public clouds and SaaS offerings).

- **Mobile matrix** contains information related to techniques with and without direct device access related to Android and iOS platforms.

- **ICS (Industrial Control Systems)** focuses on adversarial actions on control systems for resources such as utilities, transportation networks and manufacturing facilities.

Each matrix enables operators to drill down into specific techniques under each tactic. This allows access to a thorough examination that describes mechanisms of action by attackers as well as potential outcomes. MITRE provides known examples where techniques have been used in the past and by whom, as well as detection and mitigation guidelines. These materials enable security operations centers to identify, monitor and counter attacks as they progress through the kill chain.

Break the Intrusion Kill Chain

"The kill chain is a concept drawn from military science to describe the structure of an attack's lifecycle. In theory, attacks can be defeated by disrupting the sequence of events in the kill chain, which can be described in simplified form for this discussion as follows:

- **Initial foothold**. Attackers gain access by compromising credentials or installing malicious code by means that can vary from malware or social engineering to spear phishing or drive-by compromise.
- **Persistence and propagation.** To deepen and ensure lasting access, attacks may propagate laterally to other systems, compromise passwords and establish new accounts.
- **Action on objectives.** Once established, attacks execute on their eventual objectives, such as exfiltrating, destroying or (in the case of ransomware) encrypting data.

Considering the continuum of actions attackers take throughout the kill chain helps illuminate the nature of threats. Intersections of individual threat vectors with the kill chain represent points of interest, potential mitigation and detection strategies, underpinning the approach of threat-based security.

Enact and Operationalize Threat-Based Security

CSF standards, guidelines and practices enable security modeling that delineates areas of heightened exposure, weakness and risk. Characteristics specific to the organization must be considered with equal importance to define the desired target state. Target states must account for factors such as the following:

- Criticality of resources
- Regulatory environment and the organization's risk tolerance
- Objectives
- Budgetary constraints

Based on disparities between the current and target security states, organizations can formulate and act on priorities for advancing their levels of security maturity.

Threat Assessment and Mitigation Using Security Heat Maps

Disparities between current and target states can be translated into heat maps that use color gradients or similar means to visualize relationships between factors such as risk, reward and budgetary impact. This helps an organization to align security goals with other aspects of the business and technical environment. Based on the specific priorities revealed by heat maps, the organization can cross-reference weaknesses in security posture with tactics and techniques within the relevant ATT&CK matrices to identify relevant actors and mechanisms for detection and mitigation.

Threat assessment and delineation based on heat maps provides the basis for building targeted protections at the specific functional points of an organization's computing environment where they will do the most good. For example, an organization may identify relatively high risk from drive-by compromise based on malicious code injection that exploits vulnerable browser versions. Using the ATT&CK matrix could reveal that this threat can be partially mitigated with relatively low cost and effort by enforcing the use of modern browsers with security features turned on.

While this action doesn't represent the broadest possible mitigation for this risk, it represents a simple and cost-effective measure that the organization can take. Importantly, cross-referencing with the ATT&CK matrix helps delineate a broader range of possible mitigations, informing the ongoing security roadmap. At the same time, it also identifies detection measures that help indicate the activation of a given threat scenario.

Proactive Measures Based on Threat Hunting

In addition to the necessity of reacting to security threats as they arise, organizations must also proactively investigate the environment for threats that may be nascent or potential. Threat hunting is an open-ended, data-driven activity that extends both inside and outside company boundaries. It is based on an iterative process that includes the following phases:

- **Collect data** from security tools and technologies, including SIEMs, EDR systems, log files and threat intelligence feeds that potentially enable threat detection.
- **Establish hypotheses** by mapping specific threat conditions back to the ATT&CK framework and positing specific indicators of compromise (IOCs) associated with a given threat.
- **Perform hunt** using SIEMs, EDR systems and other security tools to identify specified IOCs and validate hypotheses about relationships between IOCs and threats, remediating threats as necessary.
- **Refine detection**, by improving on hypotheses as well as generalizing, operationalizing and automating validated measures for ongoing threat detection and response that is scalable and cost-effective.
- **Detect threats** on an ongoing basis based on IOCs established through the threat hunting process, by means of day-to-day monitoring by a security operations team or managed security service.
- **Triage and remediate threats** identified by means of the IOCs established during the threat hunting exercise, processing alerts and responding to incidents as needed.

The threats discovered through this process may be overt, such as phishing attempts by known actors, or they may be subtle cues based on partial information.

An example of the latter is suspicious patterns of user behavior or data movement. In either case, the focus and value of the threat-hunting exercise are based on patterns among data points that suggest threats that discrete data points alone would not reveal.

Build a Threat-Sensing Network with XDR

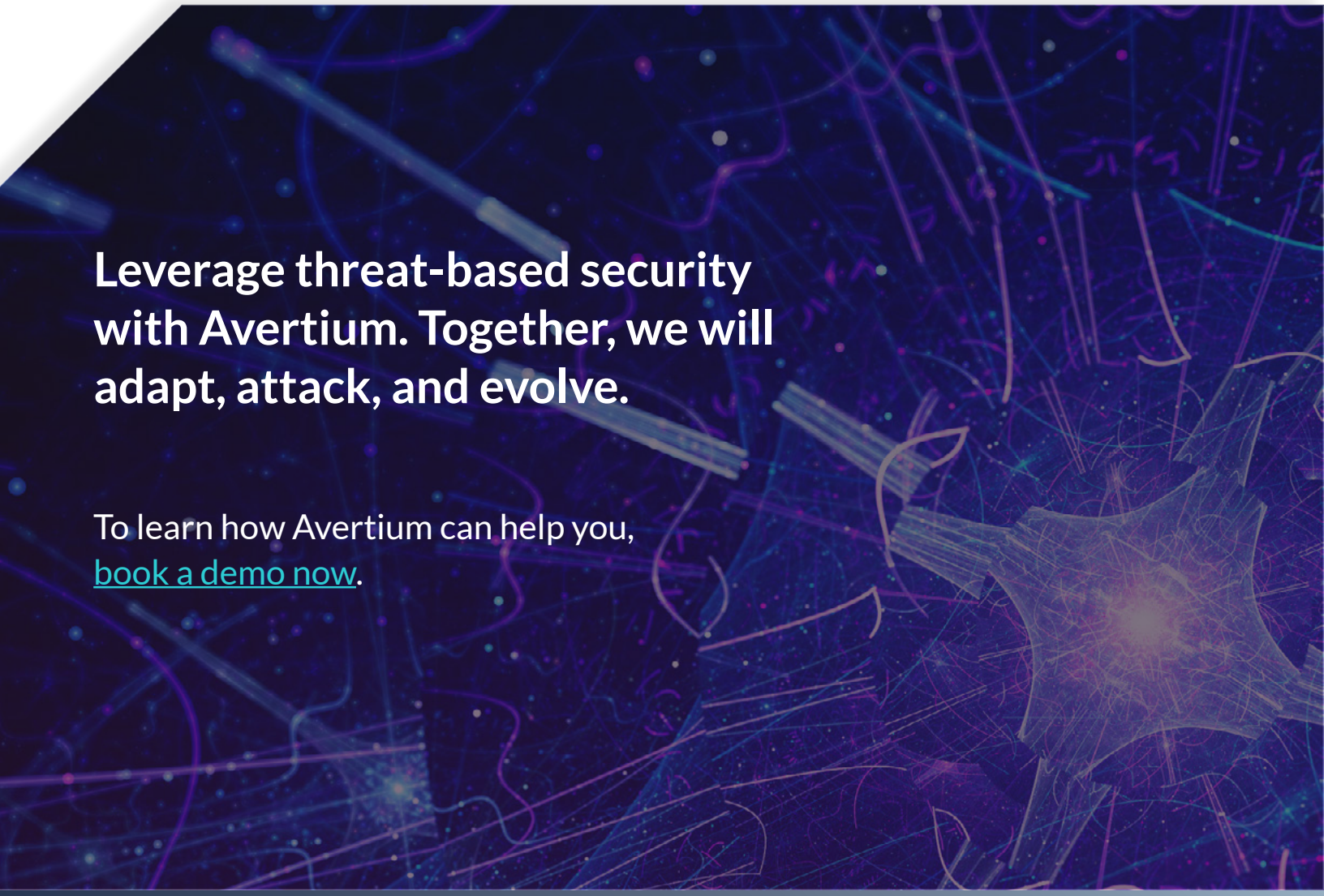
Extended Detection and Response (XDR) expands visibility and interrogates resources such as email, endpoints, servers and applications to detect and respond to threats. XDR platforms apply machine learning-driven analytics to data captured all over the environment, coupled with threat intelligence feeds.

This process identifies and adds context to threats so they can be prioritized and remediated, blunting their potential negative impacts to the organization.

Conclusion: How Avertium Can Help

Threat-based security is a strategic approach that is largely hidden from view and requires expertise. Teams trained in the use of specialized frameworks including NIST CSF and MITRE ATT&CK can enable this needed evolution beyond tactical, alert-driven approaches alone to create a more rigorous, relevant and responsive security landscape.

Avertium provides the resources and expertise needed to provide data-driven analysis of an environment and the specific threats against it, including maturity modeling and assessment of the necessary measures to improve security posture, together with operational approaches such as threat hunting to create, investigate and test hypotheses about threats, IOCs and countermeasures. With a rigorous strategy and analytics practice operating beneath the service, Avertium enables businesses to show no weakness by expanding their security beyond the alert factory, informing day-to-day tactical operations with richer context about specific vulnerabilities and potential attacks.



Leverage threat-based security with Avertium. Together, we will adapt, attack, and evolve.

To learn how Avertium can help you, book a demo now.

ABOUT AVERTIUM

Avertium is the security partner that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom.

That's why **over 1,200** mid-market and enterprise-level organizations **across 15 industries** turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**

CONNECT WITH US

AVERTIUM

Cyber Fusion Centers of Excellence
Arizona • Colorado • Tennessee

Contact Us | www.Avertium.com

SHOW NO WEAKNESS®