10 Ways to Take **MITRE ATT&CK From Plan to Action**

A guide to creating a threat-informed defense for your organization

splunk> turn data into doing™

10 Ways to Take MITRE ATT&CK **From Plan to Action**

The MITRE ATT&CK framework has been around for years but now we are seeing organizations adopting it more as they realize they need a strong IT security team and more funding is becoming available to increase the maturity of information security programs.

Companies are investing in more than just prevention technologies. They are establishing early detection capabilities, as well as building incident response capabilities, while moving away from a vendor-led approach to an analytics-driven security approach.

For both security practitioners and organizations trying to add maturity to their security programs, it's key to understand what tactics and specific techniques are used in cyberattacks from different threat groups.

> **"In a digitized world, data has become a mandate for a security team's strategic planning for threat detection and incident response to protect the organization's business, customers and employees."**
>
> – Matthias Maier, CISSP & CEH, Security Evangelist, Splunk

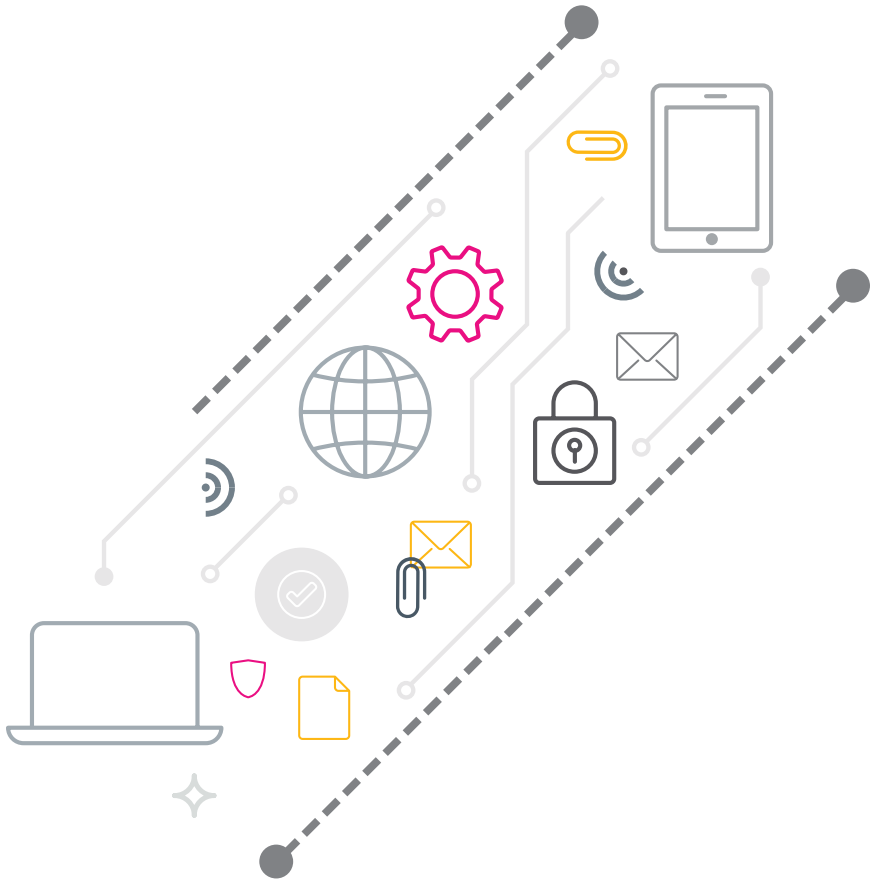
This approach helps organizations manage cyber risk better, plan what data they need to have available in case they want to investigate a security incident and establish early detection points where traditional prevention-based technology fails or would be too strict for an organization's workforce culture.

The MITRE ATT&CK framework does not stop with the security practitioner, there are many other ways how the MITRE ATT&CK framework can be used to increase visibility and communicate how effective the security efforts across an organization are — it doesn't even matter how large the security team is. Still looking for an example of what the MITRE ATT&CK framework looks like? Check this blog out.

Learn How the MITRE ATT&CK Framework **Empowers Different Teams**

In this e-book, we will explore how the MITRE ATT&CK framework helps different parts of the organization, including the:

1. Head of security operations establish a prevent, detect, respond and improve strategy
2. Security content developer/blue team respond with a short analytics turnaround
3. SIEM architects validate coverage
4. SOC engineer justify his or her data needs to the IT Ops teams
5. IT security managers to make and document risk decisions based on the coverage of logs and components
6. CISOs to justify investments and differentiate based on asset-criticality monitoring efforts and to develop a roadmap
7. SOC analysts develop a risk-based alerting (RBA) model
8. SIEM admins to ensure the quality of data onboarding and coverage needs
9. Penetration tester/red teams to document and communicate improvements efforts
10. The purchasing department and IT leaders to define tactical IT security baselines and needs for incident response and monitoring, and visibility with third party suppliers



1

Empower Head of Security Operations to establish a strategy built on prevention, detection and response.

With the techniques documented in the MITRE ATT&CK framework, organizations can start to build a roadmap to go beyond prevention and focus on detection, response and improving processes.

The SIEMENS EAGLE Datacenter security team is following this approach and it built a quality assurance and continuous improvement process. Their first priority is to prevent every threat it possibly can. What the team can't prevent, it wants to be able to detect the threat early and get alerted on it. From that point, the team responds by executing an investigation, learning about the case and either adjusting the detection or configuring a prevention measure, if possible, for improvement.

A similar concept is documented in the NIST Cybersecurity Framework with identify the risk, protect, detect, respond and recover.

> **"We want to lean forward as (much) as possible with prevention so we do not have to deal with it daily. (When) we can't lean forward, we aim to detect adequately and respond to it (the threat) in an appropriate manner. The knowledge (we win) from the daily business goes into improvement so we have it covered (tomorrow)."**
>
> – Oliver Kollenberg, EAGLE DataCenter, Siemens AG

NIST CyberSecurity Framework Core Functions to organize basic cybersecurity activities at their highest level

The basis of both examples is built on a security team with a threat-informed defense mindset and the availability of the right data on which they can ask their questions about what is happening in their environment.

2

Empower Security Content Developer/Blue team to respond with a short analytics turnaround.

The MITRE ATT&CK framework allows blue teams and security content developers to quickly map new cyberattacks seen in the news to techniques used, identify data needs and build analytics to cover detection across the different stages of tactics used by adversaries.

"Think about detecting the operation, not the attack. You might be familiar with the kill chain or MITRE ATT&CK framework. If you just try to detect the delivery of an attack you probably get unlucky one time. If you do some analytics at the delivery stage, some at the exploration stage and some of the C2 stage you can detect the operation.

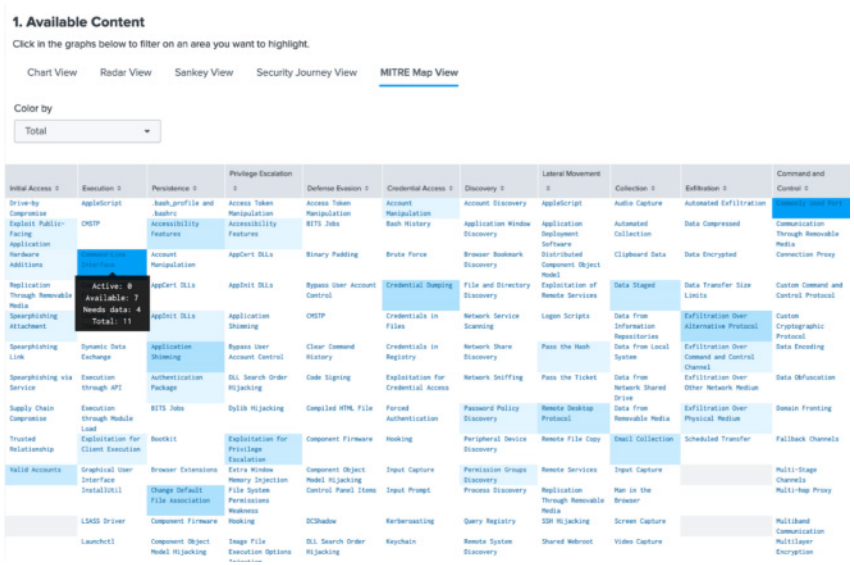
Our quickest turnaround was two hours in developing a new way of detecting attacks when we learn about a new behavior — there is no way to turn around to a vendor asking this new thing is happening can you built it into the product and then waiting 3 months for it."

– Jonathan Pagett, Head of Security Defense Center, Bank of England

3

Empower SIEM Architects to validate coverage and measure adoption.

It's challenging for SIEM architects to find an answer to how much is actually covered by their SIEM, especially when coverage needs to be defined by more than which systems or system components are delivering log data. It needs to be defined if the right actions are resulting in a logged event by the source device. The second part is to identify if the SIEM content, which is active, is looking for the right things. For these reasons, the MITRE ATT&CK framework is ideal for SIEM architects as a map for their SIEM coverage.



Tabular listing of all of the tactics and techniques in ATT&CK while highlighting the analytics available in Splunk. You can highlight content that is Active, Available but not active or content that Needs data. The darker the color the more content exists. Source: Analytics Advisor in the Splunk Security Essentials App (Version 2.4)

4

Empower SOC Engineers to justify data needs to the IT operations teams.

Usually the SOC engineer is not the owner of systems or applications that need to be protected. Ensuring that the SOC team has the visibility they need can be a daunting task, especially communicating that the right types of actions are audited and stored might demand time from the IT operations team to review logging levels and configurations.

The MITRE ATT&CK framework allows SOC engineers to document and communicate why they need events from certain activities such as when a scheduled task is created on a Windows machine or PowerShell logging. It also allows IT operations teams to decide which way to collect data based on what technology is the best architectural fit — such as collecting endpoint activity native with a sysmon configuration from SwiftOnSecurity or through a deployed endpoint protection solution.

5

Empower IT Security Managers to make and document risk decisions on coverage of logs and components.

The MITRE ATT&CK framework allows IT security managers to further specify audit and logging guidance within an organization's security controls. This allows a SOC engineer, for example, to better understand the accepted risk level by an organization.

For example, ISO/IEC 27002 defines in the guidelines of the control section Event Logging: "Event logs should include, when relevant: … system activities; …

The MITRE ATT&CK framework allows an IT security manager to define a control such as: [10%] of techniques in the [initial access] tactic need to be covered from event collection to event correlation.

6

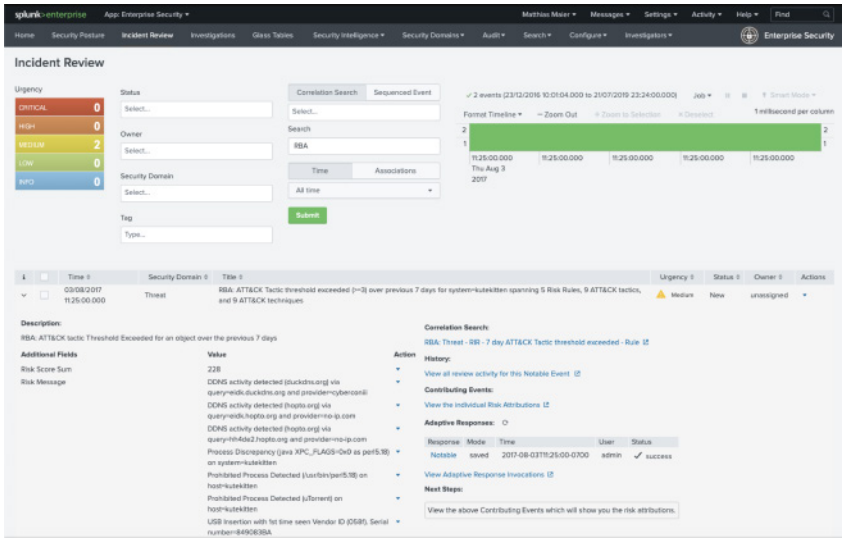
Empower CISOs to strengthen security posture, expand monitoring efforts and justify new investments.

Rather than having a one-size-fits-all policy, the ATT&CK framework enables a CISO to build a security posture based on the needs and risk profile of the organization. By mapping back to specific risks, experienced attacks, threat groups and documented APT threat reports, security management can identify gaps in their strategy and develop a roadmap for strengthening the organization's security apparatus, whether that means increased staffing, greater visibility or new security tools. The ATT&CK framework allows CISOs to focus security efforts based on abstraction layer, application criticality or logging levels. For example, the vulnerabilities of essential assets might be covered by a specific set of MITRE techniques, while other techniques are less relevant to the organization's needs — a CISO might position the SOC to invest more resources in those techniques that protect the more valuable assets, ensuring that the right data is gathered more frequently and made centrally available in case of a major security incident.

7

Empower SOC Analysts to develop a risk-based alerting (RBA) model.

As SIEM content developers are building and establishing detections for MITRE ATT&CK techniques, SOC analysts might be overwhelmed by the amount of alerts generated. To prioritize MITRE ATT&CK techniques, alerts can be converted into signals that can attribute risk value to an asset. Based on the type of technique and behavior seen, the risk value can be higher, or based on the asset or user involved, a multiplier could be added for the calculation. This allows an abstraction layer for the SOC analysts to not be overwhelmed by alert fatigue and focus on the assets or users who have the highest risk score and investigate those first.



Alert Title: RBA: ATT&CK Tactic threshold exceeded (>=3) over previous 7 days for system=kutekitten spanning 5 Risk Rules, 9 ATT&CK tactics, and 9 ATT&CK techniques. Risk Score Sum: 228. Source: Splunk Enterprise Security

8

Empower SIEM Admins to ensure data onboarding quality and coverage needs.

The SIEM administrator's job is made easier when the security operations team and the organization as a whole can identify what data, logs and events they need for threat hunting, security monitoring or incident investigation. Using the MITRE ATT&CK framework, the SIEM admin can check the data during the onboarding process to ensure that the needs of the SOC are met or if additional tooling is required. Simulating threat activities and anomalies is an additional mechanism for ensuring data quality and coverage.

> **"Simulate adversaries and create data to validate if your detection mechanisms works end-to-end."**
>
> – Dave Herrald, staff security strategist, Splunk

9

Penetration Testers/Red Teams to document and communicate improvements efforts.

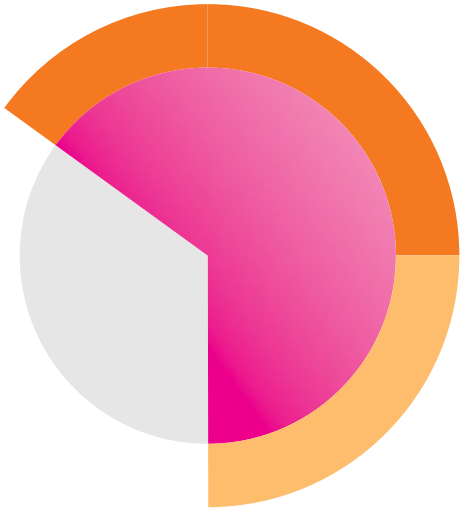
Penetration testers and Red Teams are tasked with finding weak points in an information network. The first question most of these teams ask is where key vulnerabilities are. But an equally important investigation — that is often overlooked — examines the activities that lead to the exploitation and were not detected by the SOC. In short, whether you're working with a third-party penetration testing team or your internal SOC, the MITRE ATT&CK framework is a great way to standardize communication. Once everyone is working with the same framework, it is easier and more effective to examine the tactics and techniques used in the investigation and determine the locations of holes in the security system.

10

Empower Purchasing and IT Leaders
to define tactical security baselines and needs for incident monitoring and response.

Purchasing tools and services from third parties is standard operating procedure for IT and business leaders. For these vendors, ensuring their products are secure and meet compliance requirements is top-of-mind, and they are regularly audited by their customers and regulatory agencies to validate their security practices. The MITRE ATT&CK framework is a good layer to define requirements in detail and go beyond IT governance frameworks, such as ISO27001 or NIST-800-53 certificates. Especially in a shared responsibility model where the information security team of an organization remains accountable for some parts of the service, it is key that the service provider allows the automated collection of audit trails, as well as ensuring the right event data is within the audit trails. Defining the "right event data" on an abstraction layer independent of the providers architecture, threat evolution or new operating systems with new features that attackers might use will make it.

> **"In a digitized world, data has become a mandate for a security team's strategic planning for threat detection and incident response to protect the organization's business, customers and employees."**
>
> – Matthias Maier, CISSP & CEH, security evangelist, Splunk



Getting Started.

Do you have the right data? Are you asking the right questions?

Explore what is possible with Splunk and the power of Search Processing Language (SPL) and try Splunk Security Essentials App on Splunkbase.

20-47401-10-Ways-to-Take-Your-MITRE-ATT_CK-From-Plan-to-Action-103-11x8.5-EB

splunk> turn data into doing™