Using the MITRE ATT&CK framework in Splunk Enterprise Security

Many security teams want to find the right context in which to view security detection coverage. The MITRE ATT&CK Framework and its application to existing SIEM deployments, particularly Splunk Enterprise Security, helps security teams understand where they have threats covered and where they do not. It's important for businesses and security professionals alike to take advantage of the benefits this framework has to offer and to explore how MITRE ATT&CK implemented on Splunk Enterprise Security can help you grow your security maturity.

This article is part of Splunk's Use Case Explorer for Security, which is designed to help you identify and implement prescriptive use cases that drive incremental business value. In the Security maturity journey described in the Use Case Explorer, this article is part of Threat hunting.

What is MITRE ATT&CK?

From the official website, "MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations."

ATT&CK stands for Adversarial Tactics, Techniques and Common Knowledge. The framework documents common tactics, techniques, and procedures (TTPs) that cyber criminals employ when attacking networks, and outlines adversarial behaviors specific to Windows, Linux, Mac, cloud-based and mobile environments.

Organizations rely on the MITRE ATT&CK knowledge base to implement offensive and defensive measures to strengthen their overall security posture. The ATT&CK framework can help threat hunters and other cyber defenders better classify attacks, understand adversary behavior, and assess an organization's risk. Security teams can also use the framework to gain insight into how adversaries might operate in various scenarios so they can create informed strategies on how to detect and prevent those behaviors from affecting the security of their organization. The ATT&CK framework's unique ability to provide insights into adversaries' behaviors, as well as its ability to provide a standardized, easily accessible global threat language, has led to its growing popularity for organizations looking to share threat intelligence and bolster their security posture.

The MITRE ATT&CK framework provides guidance on how to approach cyber security related issues based on four use-cases:

1. Threat intelligence
2. Detection and analytics
3. Adversary emulation and red teaming
4. Assessment and engineering

Why use MITRE ATT&CK with Splunk Enterprise Security?

The MITRE ATT&CK framework evolves as new threats emerge. Security operations teams must continue to update their methodologies as fast as adversaries adapt to detect new threats and prevent breaches. Splunk Enterprise Security, along with the Splunk Security Essentials application, provides a set of use cases that teams can use to assess their security program coverage and gaps, so they can prepare for future threats that leverage similar exploits. Integrating MITRE ATT&CK into your Splunk Enterprise Security environment can provide the following benefits:

- Helps you identify your top risks, control gaps, and risk appetite.
- Helps you map threats to identify the controls and processes you need to mitigate top risks, while providing a framework for security governance and maturity.
- Helps you identify, recommend, and choose new data sources based on quantifiable risk reduction aligned with your ATT&CK coverage.
- Sharpens your view of attack paths, improving your team's knowledge and skills.
- Informs your SOC on how to prioritize alerts and detections for their quickest impact and remediation.

How is the MITRE ATT&CK framework used?

The ATT&CK framework is used by security teams in everyday defense activities, particularly those that look to address threat actors and their attack methods. ATT&CK is used in a variety of activities by both red (offensive) and blue (defensive) teams, providing both types of security professionals a common language and frame of reference around adversarial behaviors based on real attacks.

- Red teams (pen testers and offensive security professionals who regularly test and break into cyber defenses) can follow MITRE's ATT&CK framework to test network security defenses by modeling ATT&CK's documented adversary behavior. Using ATT&CK as an enhancement to existing methodology for predictive campaigns can make it easier for red teams to anticipate threats, detect patterns, and assess the effectiveness of defensive controls in their environment.
- Blue teams (defensive security professionals who oversee internal network security protections and defend against cyber threats) can use the ATT&CK framework to better understand what adversaries are doing, as well as prioritize the most severe threats and ensure the appropriate security controls are in place and working effectively.

Below are various ways in which ATT&CK's taxonomy can be applied in Splunk:

- **Mapping defense controls.** Security teams can have a clear understanding of defense tools, systems, and strategies when they're referenced against the ATT&CK tactics and techniques and their associated threats. MITRE ATT&CK tags are easily applied to Splunk Enterprise Security correlation searches to annotate and provide deeper understanding of the events.
- **Threat hunting.** Security teams can map defenses to ATT&CK to identify critical gaps in security infrastructure, which can help them detect previously overlooked threat activity. Using Splunk Security Essentials and the MITRE ATT&CK map, threat hunters can identify gaps in coverage and can then drive further development for detections or generate ideas about new searches or use cases that might fill the gaps.
- **Investigating.** Incident response and blue teams can refer to ATT&CK techniques and tactics to understand the strengths and weaknesses in their security infrastructure, validating effective measures while also giving them the ability to detect misconfigurations and other operational flaws.

- **Identifying actors and groups.** Security teams can align specific malicious actors and groups with associated documented behaviors.
- **Integrating solutions.** Organizations that have a wide range of disparate tools and solutions can categorize and standardize their solutions according to the ATT&CK framework, hardening their overall defense strategy.

How do I get started using the MITRE ATT&CK framework?

ATT&CK can be useful for any organization that wants to elevate threat knowledge and build a more informed defensive posture, regardless of how big or sophisticated the security team. While MITRE provides its materials at no cost for use, organizations can employ a myriad of MITRE integrations in Splunk Enterprise Security and Splunk Security Essentials to apply the framework to meet the specific needs of the organization.

- **Small or beginner teams.** If you're an organization with a small security team and want to expand your threat intelligence capabilities, you can focus on a relevant threat actor and their sets of intrusion activity, and look at the related attack behaviors as defined in ATT&CK matrix relevant to your organization. If you have Splunk Enterprise Security in your environment, Splunk Security Essentials can push MITRE ATT&CK and Cyber Kill Chain attributions to the Incident Review dashboard, along with raw searches of `index=risk` or `index=notable`. Just configure the Splunk Enterprise Security integration in the system configuration menu.
- **Mid-level teams.** If you're an organization that has a team of dedicated security professionals that regularly analyze threat information, you can get started by mapping intelligence to the ATT&CK framework yourself, as opposed to relying on what others have previously mapped. The Analytics Advisor dashboards are designed to help you understand what content you might want to deploy inside of Splunk based on the content you already have and the data that's present in your environment. The MITRE ATT&CK Overview dashboard also includes a customized MITRE ATT&CK Matrix that shows your level of coverage on MITRE ATT&CK while letting you filter for the data you have in the environment, or the threat groups that target you.
- **Large or advanced teams.** If your team is more advanced, you can map more information to ATT&CK, using it to guide how you build out your cyber defenses. You can map both internal and external information to ATT&CK, including incident response, real-time alerts and your company's historic data. After this data is mapped, you can

compare groups, prioritize commonly used techniques, and more. With an understanding of what data you have, you can specify the types of security concerns you're facing and then use MITRE ATT&CK to filter for the Splunk Enterprise Security content related to MITRE Techniques that are associated with many different threat groups.

The end goal of using MITRE ATT&CK in your Splunk Enterprise Security environment is to provide further insight and value to your existing deployment against the backdrop of the MITRE ATT&CK framework. Building this framework helps in the constantly changing world of security needs and detections by basing current and future work on relevant, real-world applications.

Next steps

Now you're doing more with Splunk Enterprise Security, get even more value through implementing use cases, or for additional information see some of these resources:

- .Conf Talk: ATT&CK™ Yourself Before Someone Else Does
- .Conf Talk: Building Behavioral Detections: Cross-Correlating Suspicious Activity with the MITRE ATT&CK Framework
- Blog: Answered: Your Most Burning Questions About Planning and Operationalizing MITRE ATT&CK
- Docs: Operationalize MITRE ATT&CK

Still having trouble? Splunk has many resources available to help get you back on track. We recommend the following:

- Splunk OnDemand Services: Credit-based services that allow direct access to Splunk technical consultants for a variety of technical services from a pre-defined catalog. Most customers have OnDemand Services per their license support plan. Engage the ODS team at OnDemand-Inquires@splunk.com if you require assistance.
- Splunk Answers**:** Ask your question to the Splunk Community, which has provided over 50,000 user solutions to date.
- Splunk Customer Support: Contact Splunk to discuss your environment and receive customer support