SWIMLANE

Optimizing the MITRE ATT&CK Framework with SOAR

How Swimlane can help your organization leverage the MITRE ATT&CK framework and strengthen your SOC

What is the MITRE ATT&CK Framework?

The MITRE ATT&CK framework is the defacto standard for security operations center (SOC) teams to measure and view malicious actors' tactics and techniques. When SOC teams can view each of these tactics—or attack phases—quickly, they are provided with specific details about different techniques used by the bad actor to accomplish each attack phase.

MITRE ATT&CK is a strong framework and knowledge base for threat models and methodologies, but it should not be considered absolute defensive coverage. Rather, it is a starting point. As an organization's security posture matures, it will contribute to the MITRE ATT&CK knowledge base with additional forms of attack tactics and techniques used within its industry or vertical.

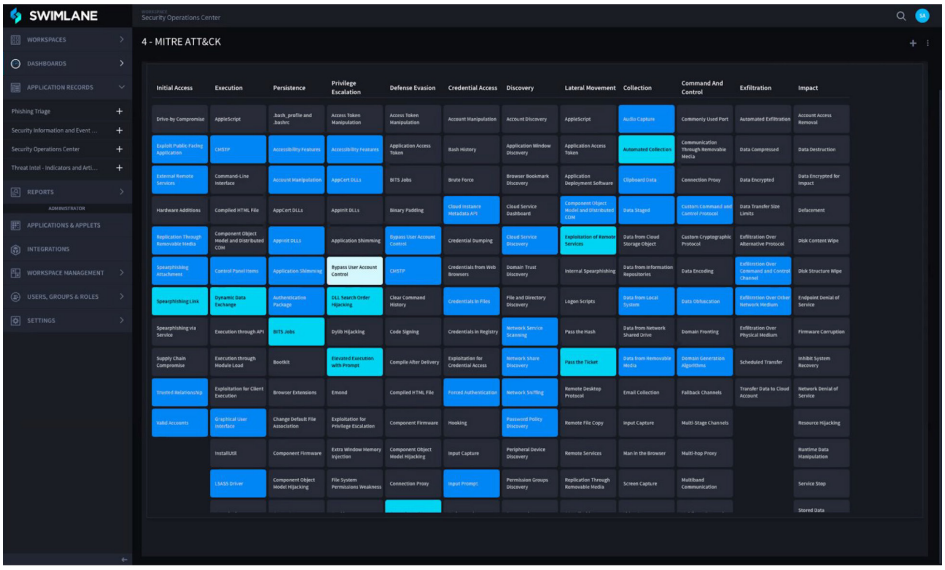
Challenges with MITRE ATT&CK Framework

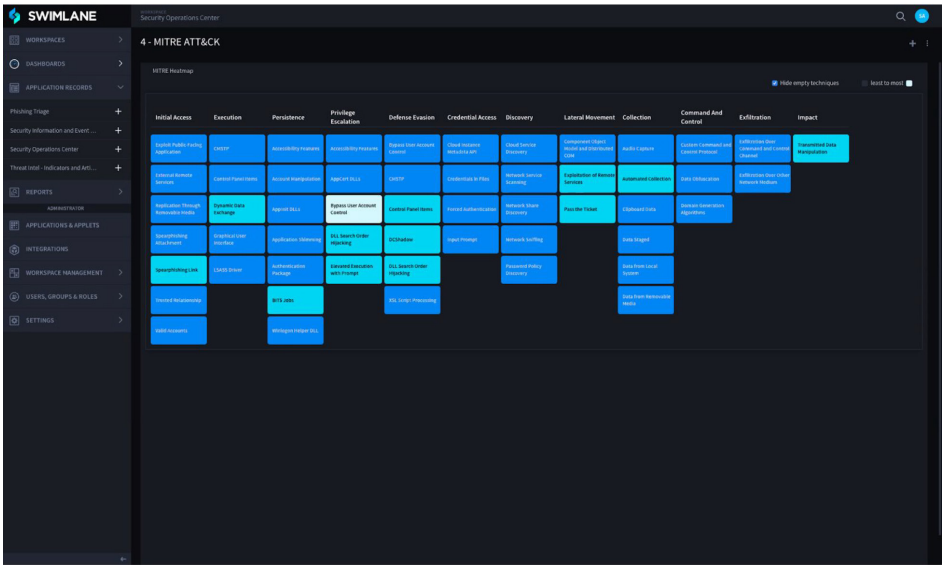
MITRE ATT&CK can provide organizations visibility into their defensive capabilities while enabling them to track attack vectors used by bad actors at scale. Getting defensive visibility can be difficult for organizations as it requires manual creation of detection rules and alerts. Since the MITRE ATT&CK framework provides guidance in the form of text-based data, it can be difficult to interpret or generate absolute defensive coverage for a given technique.

MITRE ATT&CK Framework & Swimlane

By leveraging a security orchestration, automation and response (SOAR) solution, such as Swimlane, SOC teams can associate different alerts with specific tactics and techniques within the MITRE ATT&CK framework. As an organization's security posture matures, it will add tactics, techniques, malicious actors, tools, malware and mitigations identified during its operations to the MITRE ATT&CK knowledge base. This then increases the organization's management and tracking of its defensive measures, strengthening its overall security posture.

By utilizing data attributed to specific MITRE ATT&CK tactics and techniques, Swimlane can provide your security team with the ability to track and measure alerts visually, giving your SOC insight into your defensive coverage with a clearer understanding of different attack vectors used against your organization.





About Swimlane

Swimlane is a leader in security orchestration, automation and response (SOAR). Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations by automating time-intensive, manual tasks and delivering powerful, consolidated integrations, analytics, real-time dashboards and reporting across your entire security infrastructure.

Swimlane's flexible and scalable SOAR solution offers a broad array of features aimed at helping organizations address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire organization.