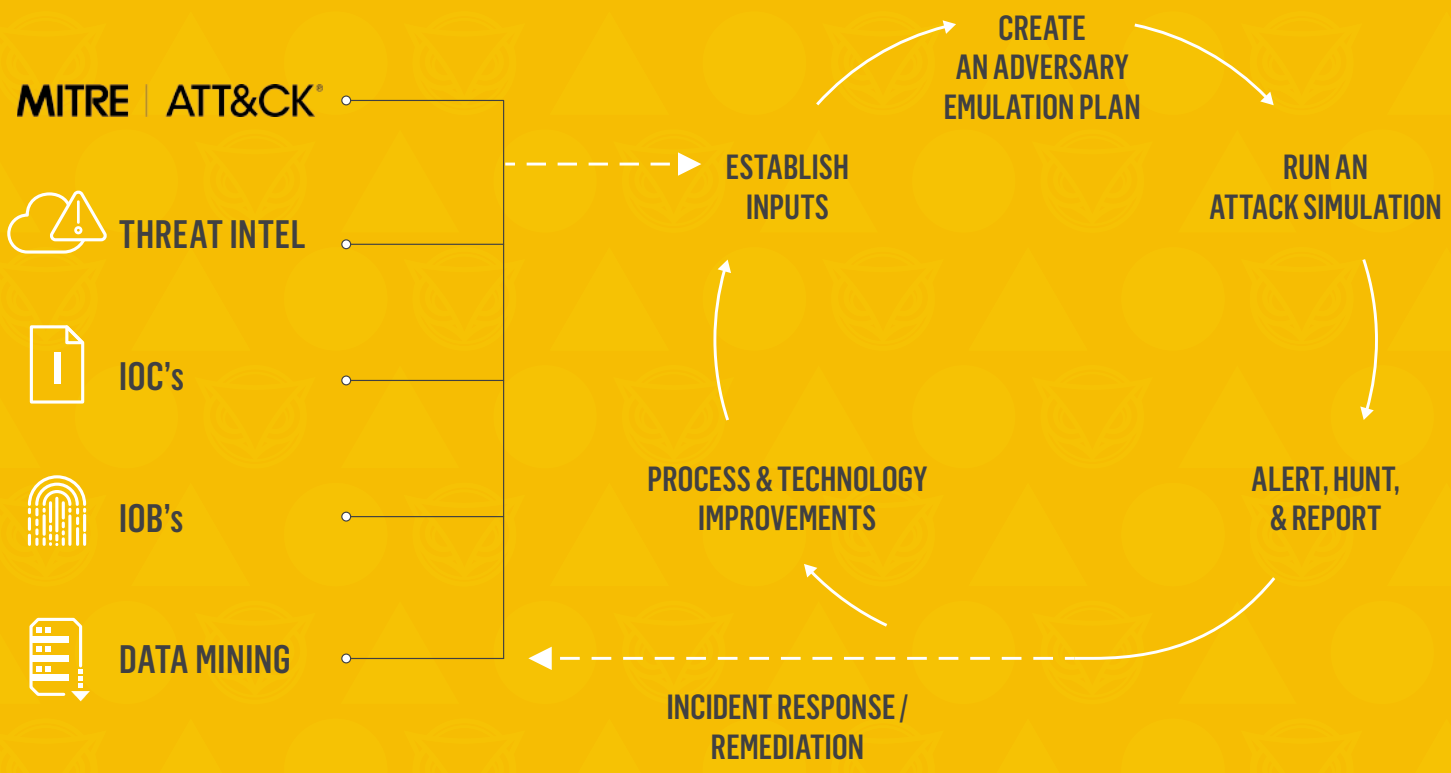
cybereason

5 Steps to Improve Defenses with MITRE | ATT&CK®

HOW TO LEVERAGE THE MITRE ATT&CK FRAMEWORK TO IMPROVE SECURITY



1 ESTABLISH INPUTS

Identify what inputs are available to you. Consider incorporating threat intelligence into your security processes, consider indicators of compromise, look at indicators of behavior, and leverage data mining from your own resources like Splunk and Hadoop to power your security process improvement.

2 CREATE AN ADVERSARY EMULATION PLAN

Take the time to create an Adversary Emulation Plan (AEP). When implemented, the AEP will guide your security team in safely testing itself against the latest threats while also identifying opportunities for security improvements. AEPs are composed of several sections, including an overview of the plan, an overview of the adversary group, a detailed listing of the emulation phases, and a biography of sources.

3 RUN AN ATTACK SIMULATION

When running the attack simulation, your red team must ensure their exercises simulate the actual attack resources the adversary uses. This includes resources and activities like an external command and control server, the proper infiltration and exploitation techniques, and the completion of data exfiltration. If your team skips or fails to execute certain steps, you will inevitably miss important activities that take place in an actual attack.

4 ALERT, HUNT, & REPORT

At a minimum, your red team should use adversary emulation plans and tactics, techniques, and procedures (TTPs) for execution and should actively report on the success of their activities. Be sure to document all resources your red team uses and maintain constant communication with them throughout the simulation. If your existing tooling is unable to detect parts of the attack simulation, your team should conduct threat hunting to uncover more aspects of the attack.

5 PLAN FOR PROCESS & TECHNOLOGY IMPROVEMENTS

Develop a process and technology improvement plan based on the results of the attack simulation and the final report. Incorporate the results of several different adversary group simulations, as changes per simulation can significantly influence technology decisions.

WHY ORGANIZATIONS SHOULD MAP TO THE MITRE ATT&CK FRAMEWORK

- MITRE ATT&CK helps defenders understand security from the eyes of the adversary. It provides a unique perspective to design better security programs, tools, and processes.
- The framework serves as a common language and shared repository for security professionals to provide feedback and inputs to continuously improve security.
- MITRE ATT&CK can improve efficiency by empowering analysts of all levels to understand what is happening during an attack, and what will happen next.
- Finally, MITRE enables security organizations around the word to make buying decisions that most effectively advance their security posture. Through the testing of vendors that build technologies like NGAV, EDR, and XDR, MITRE evaluates the ability of these solutions to systematically leverage the knowledge of the ATT&CK framework in real world scenarios.

Additional Resources

Whitepaper:
MITRE ATT&CK Emulation Results Explained

Fundamentals:
MITRE ATT&CK 101

Blog:
Cybereason Posts Best Results in History of MITRE ATT&CK Evaluations