cybereason

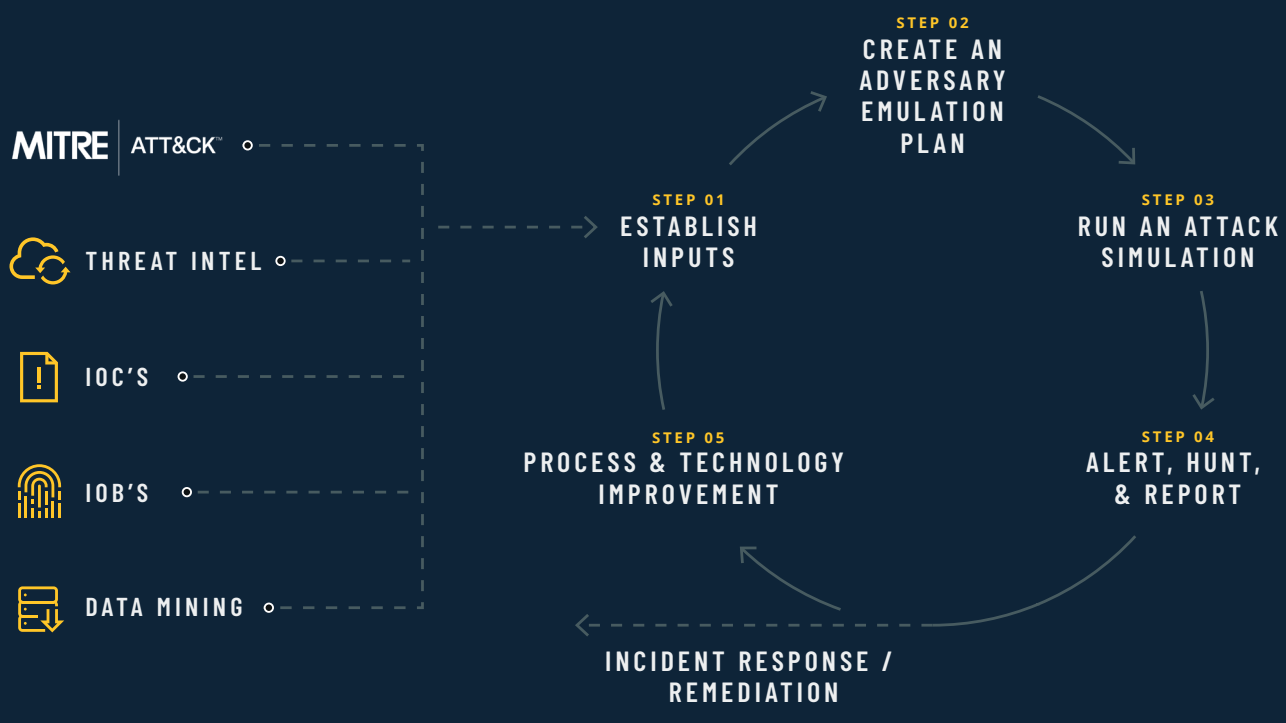
FIVE CLEAR STEPS TO IMPLEMENT MITRE ATT&CK

Mitigate threats before they become breaches

Though MITRE ATT&CK gives a good basis of knowledge and input, it's important to expand your inputs to other areas to give you a more complete and timely perspective. Be sure to incorporate threat intel, IOCs, IOBs, and data mining efforts wherever possible.

Create an Adversary Emulation Plan

AEPs are made up 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. A detailed and complete AEP is a good resource that newer L1 analysts can use to learn about specific attacks and the security tools they will be working with.



Run an Attack Simulation

Ensure red team 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.

Alert, Hunt, & Report

At a minimum, your red team should use adversary emulation plans and 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. Document any successful detections and alerts for evaluation at the end of the attack simulation.

Process & Technology Improvement

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.