MAPPING THE ENGAGE MATRIX TO MITRE ATT&CK®

When an adversary engages in a specific behavior, they are vulnerable to exposing an unintended weakness. In MITRE Engage,™ we look at each ATT&CK technique to examine the weaknesses revealed and identify an engagement activity or activities to exploit this weakness. By mapping the various MITRE Engage Engagement Activities to ATT&CK, we can ensure that each activity in Engage is driven by observed adversary behavior.

ATT&CK MAPPINGS

In adversary engagement operations it can be tempting to try to anticipate the adversary's actions. However, this line of thinking can lead the defender to make incorrect or ineffective decisions due to cultural, experiential, or any of a host of other differences. By mapping to ATT&CK, we can ensure that our chosen engagement activities are driven by observed and reported adversary behavior, not our expectations.

When an adversary engages in a specific behavior, they are vulnerable to expose an unintended weakness. By looking at each ATT&CK activity, we can examine the weaknesses revealed and identify an engagement activity or activities to exploit this weakness. For example, when adversaries display the ATT&CK Technique of Remote System Discovery (T1018), they are vulnerable to collect, observe, or manipulate deceptive system artifacts or information. Therefore, as defenders we can use lures to cause them to reveal behaviors, use additional or more advanced capabilities against the target, and/or impact their dwell time.

For a given ATT&CK technique we offer the following mapping:

- **ATT&CK ID & Name**—The ATT&CK Technique ID and Name
- **Adversary Vulnerability**—The vulnerability that the adversary exposes when they engage in a specific behavior
- **Engagement Activity**—The action the defender can perform to take advantage of the vulnerability the adversary has exposed

These mappings are one to many (ie a single ATT&CK ID may have one or more unique vulnerability and Engagement Activity pairs).

ATT&CK Technique		Adversary Vulnerability	Engagement Activity
When adversaries perform specific actions,	▶	their actions reveal vulnerabilities	that the defender can take advantage of for defensive purposes

> "MITRE ATT&CK lays out detections and mitigations against adversary behaviors, but MITRE Engage opens up a new set of options that a defender can take with adversary engagement."
>
> Adam Pennington, MITRE ATT&CK Lead

For information about MITRE Engage™, contact engage@mitre.org, visit us at engage.mitre.org, or connect with us on LinkedIn @MITRE Engage

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2022 MITRE PR_21-01759-8 2-22-2022