WHAT IS ADVERSARY ENGAGEMENT?

Adversary engagement is the combination of denial and deception to increase the cost and decrease the value of your adversary's cyber operations. Adversary engagement goals can be any combination of the following: to detect adversaries on the network, to elicit intelligence to learn about adversaries, or to affect adversaries by raising the cost and lowering the value of their cyber operations.

OVERVIEW

Cyber defense has traditionally focused on the use of defense-in-depth technologies to deny an adversary access to an organization's networks or cyber assets. In this paradigm, any time the adversary can exploit a network vulnerability to access a new system or exfiltrate a piece of data from the network, they win. However, when a defender introduces deceptive artifacts and systems, they increase the ambiguity for the adversary. Is the system they just accessed legitimate? Is the piece of data they just stole real? These questions drive up the cost and drive down the value of the adversary's cyber operations.

Adversary Engagement is a combination of cyber denial and deception activities to interact with cyber adversaries to achieve the defender's goals. When paired with defense-in-depth technologies, adversary engagement allows defenders to proactively interact with cyber adversaries to achieve the defender's strategic goals.

Cyber Denial is the ability to prevent or otherwise impair the adversary's ability to conduct their operations. This disruption may limit the adversary's movements or collection efforts, or otherwise diminish the effectiveness of their capabilities.

Cyber Deception intentionally reveals deceptive facts and fictions to mislead the adversary, while concealing critical facts and fictions to prevent the adversary from forming correct estimations or taking appropriate actions. When used in unison, and within the context of strategic planning and analysis, cyber denial and deception provide the pillars of adversary engagement.

Denial, deception, and adversary engagement technologies augment, rather than replace your current SOC operations. Think of these technologies as a dam. You build walls with your current defensive strategies to stop what you can and incorporate adversary engagement technologies to channel and move adversaries in ways that benefit you, the defender.

> Adversary Engagement operations provide opportunities for defenders to demonstrate tools, test hypotheses, and improve their threat models, all with the added benefit of negatively impacting the adversary.
>
> Gabby Raymond, Adversary Engagement Capability Area Lead, MITRE

engage@mitre.org

engage.mitre.org

@ 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®