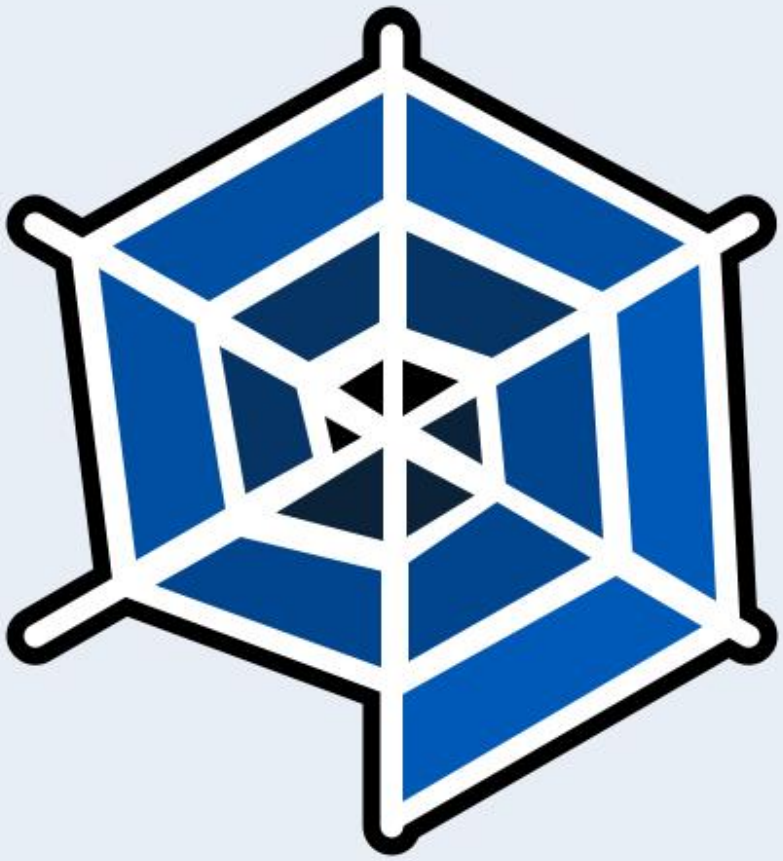


A STARTER KIT IN ADVERSARY ENGAGEMENT

MITRE | Engage™

This page intentionally left blank

Table of Contents

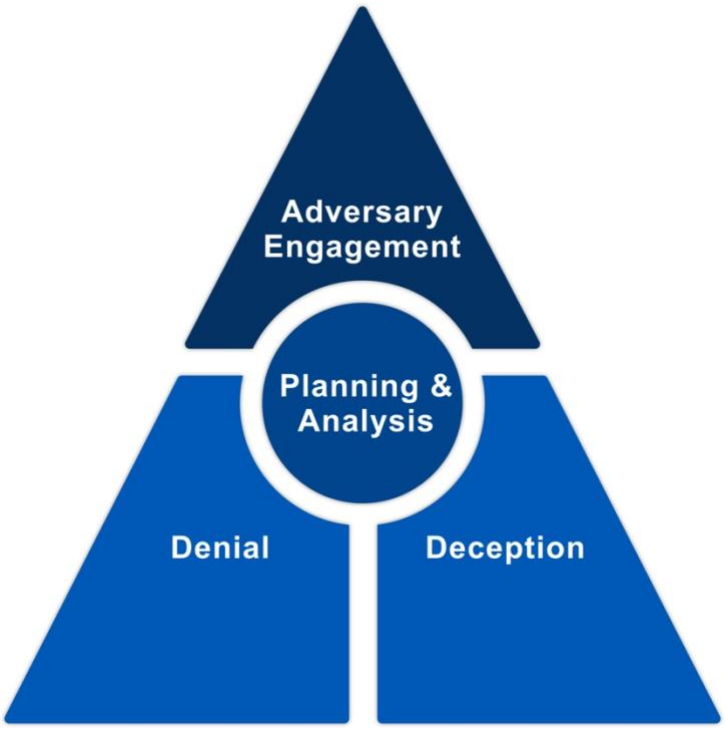
This page intentionally left blank

1 Start with the Basics

Get started with the basics of adversary engagement

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

Cyber Denial is the ability to prevent or otherwise impair the adversary's ability to conduct their operations. This disruption may limit their movements, collection efforts, or effectiveness of their capabilities. **Cyber Deception** intentionally reveals deceptive facts and fictions to mislead the adversary. In addition, it conceals critical facts and fictions to prevent the adversary from forming correct estimations or taking appropriate actions. When cyber denial and deception are used together, within the context of strategic planning and analysis, they provide the foundation of **Adversary Engagement**.

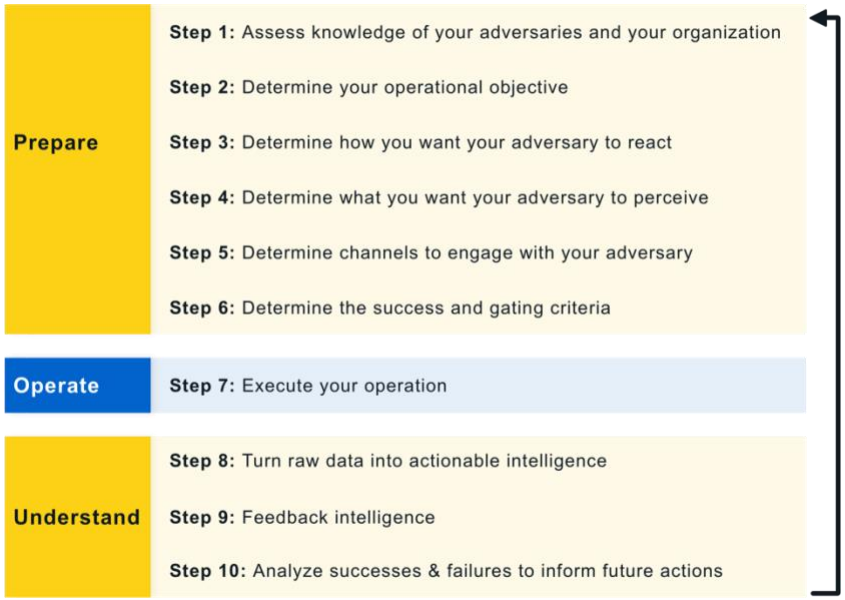


Want to share these definitions with your organization? Check out the whitepaper and poster below entitled *What is Adversary Engagement*.

Successful adversary engagement operations can be broken down into four components: **narrative**, **environment**, **monitoring**, and **analysis**. The narrative is the deception story you intend to portray to your adversary. The engagement environment is the set of carefully tailored, highly instrumented systems, designed on an engagement-by-engagement basis, as the backdrop to the engagement narrative. These systems may be completely isolated or integrated into your production network. Monitoring refers to the collection system used to observe the adversary as they move through the environment. Monitoring is essential for maintaining operational safety throughout an operation. Finally, analysis refers to the actions you take to turn the outputs of your operation into actionable intelligence. The connective tissue joining all four of these elements is your operational objective, the ultimate goal of your engagement. This objective can be derived from any combination of the following: to **expose** adversaries on the network, to **affect** the adversary by impacting their ability to operate, and/or to **elicit** intelligence to learn about adversaries Tactics, Techniques, and Procedures (TTPs). Adversary engagement operations provide opportunities for the defender to demonstrate tools, test hypotheses, and improve their threat models, all with the added benefit of negatively impacting the adversary.

Let’s explore how each of these components come together in adversary engagement operations.

Adversary engagement is an iterative, goal driven process, not merely the deployment of a technology stack. It is not enough to deploy a decoy and declare success. Rather, you must think critically about what your defensive goals are and how denial, deception, and adversary engagement can be used to drive progress towards these goals. Unlike other defensive technologies, such as antivirus (AV), adversary engagement technologies cannot be considered “fire and forget” solutions. Adversary engagement is a thinking game; it is as much about your mindset, as it is about what tools you use. The Engage 10-Step Process helps you consider engagement activities within the scope of this mindset.



This process is not unique to cyber deception. In *The Art and Science of Military Deception*, Barton Whaley wrote a chapter entitled, "The Process of Deception." There, Whaley laid out a ten-step process for creating military deceptions. We refined and repurposed Whaley's work for the cyber domain.

Want to share the 10-Step Process with your organization? Check out the whitepaper and poster below to dive in.

As seen in the graphic above, the 10-Step Process is divided into three categories: **Prepare**, **Operate**, and **Understand**. In the *Prepare* phase, you define your operational objective. You then construct an engagement narrative that supports this objective. This narrative informs the design of the engagement **environment** and all operational activities. Additionally, the Prepare steps invite you to gather any relevant stakeholders to define the acceptable level of operational risk. By setting this level of risk up front, you can construct clear Rules of Engagement (RoE) to serve as guardrails for operational activities. Your **monitoring** and **analysis** capabilities should be sufficient to ensure that your activity remains within these bounds. In the *Operate* phase, you implement and deploy your designed activities. We explore these activities more in the *Operationalize the Methodologies* section below. Finally, the *Understand* phase guides you in turning operational outputs into actionable intelligence to assess, whether or not you met your operational objective. Additionally, this evaluation gives you opportunities to capture lessons learned and refine future engagements.

Now that we understand the basic principles behind adversary engagement you are ready to start learning some of the terminology.

2 Learn the Language

Build on the basics by learning the terminology to enable sharing and collaboration

As with any technology area, language matters. In this section we provide you with the Engage Glossary of Key Terms. Currently, the adversary engagement community lacks a cohesive set of shared terms. This document serves as our attempt at capturing the most used terms and definitions. However, this should be considered a living document as we continue to ask the community for help building and standardizing these terms. Take a moment to read through this glossary and familiarize yourself with some of the basic terminology.

Now that you have explored some of the standard terms, begin to identify the key stakeholders and users in your organization who will need to be part of the conversation as we move to operationalize these methodologies. These stakeholders may include executive leadership, legal, and InfoSec, among others. These voices and perspectives will be important as you begin to integrate these technologies into your defensive strategy.

3 Operationalize the Methodologies

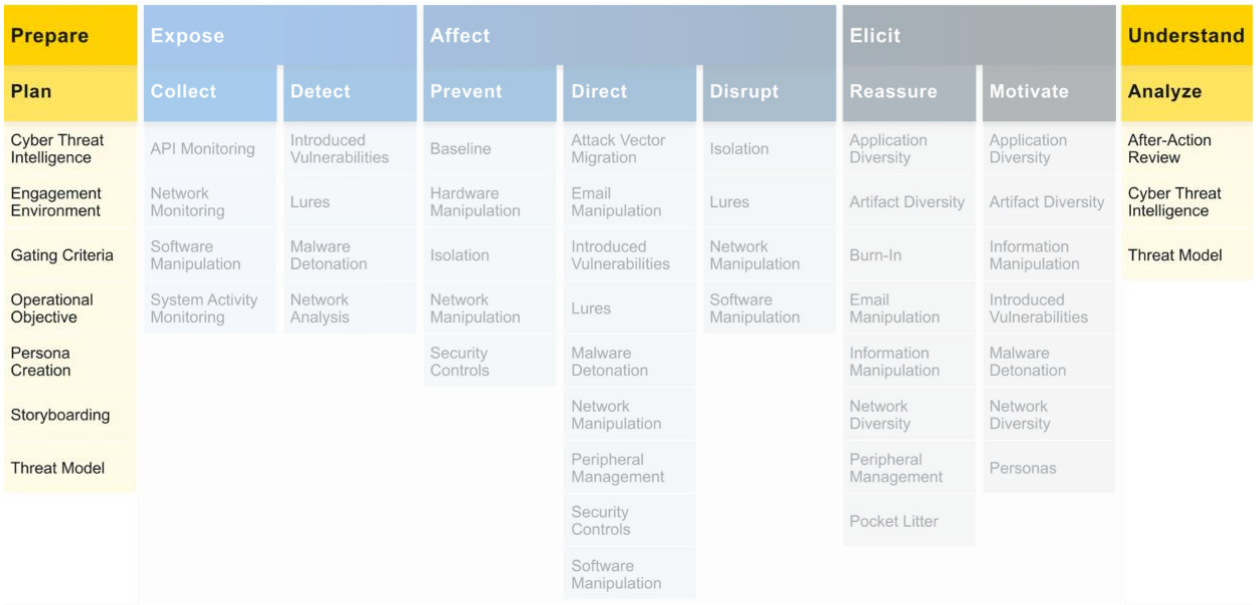
Now that you are talking about adversary engagement with the necessary stakeholders in your organization, let's dive into creating a template to operationalize these methodologies for your organization

Let's start by exploring the Engage Matrix, the foundation to your adversary engagement strategy. The Engage Matrix is a shared reference that bridges the gap between defenders and decision makers when discussing and planning denial, deception, and adversary engagement activities. The Matrix allows us to apply the theoretical 10-Step Process to an actual operation. At its core, the Matrix empowers you to identify your adversary engagement goals, and then use those goals to shape operational activities. Building on this foundation, we will create an operational template that you can adapt to fit your own organization.

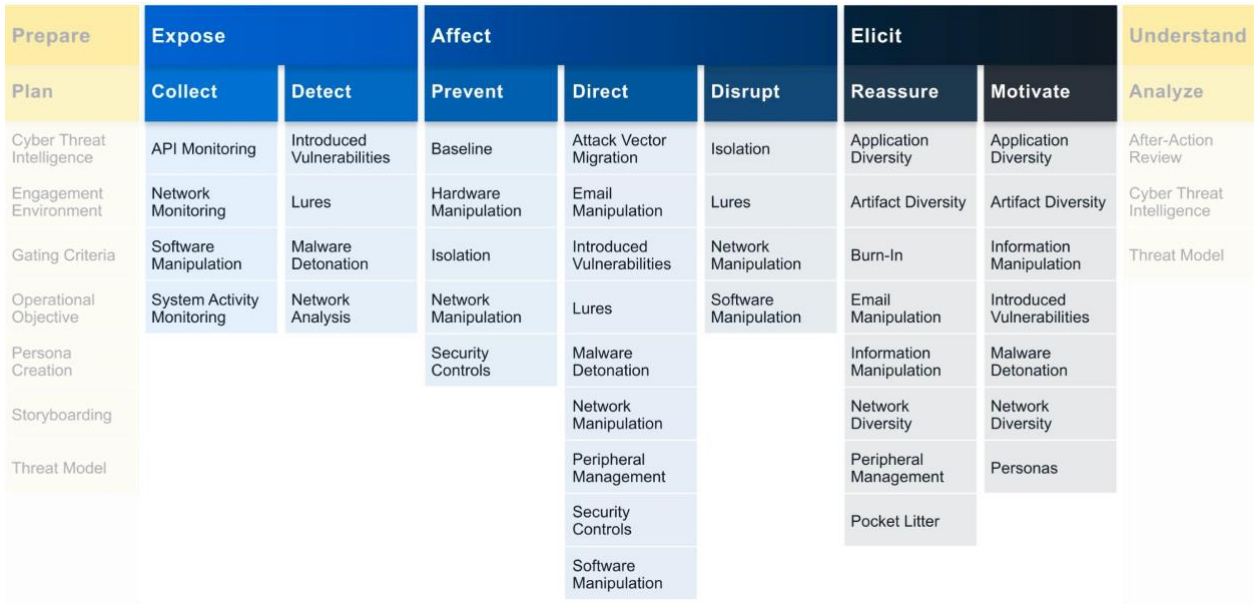
The Engage Matrix is broken into several components, mirroring the 10-Step Process.

The Engage Matrix is divided vertically into two categories of actions. Strategic actions bookend the Matrix and ensure that defenders appropriately drive operations with

strategic planning and analysis. These actions map to the Prepare and Understand phases of the 10-Step Process.



Engagement actions are the traditional cyber denial and deception activities that are used to drive progress towards your objectives. These actions map to the Operate phase of the 10-Step Process.



The Engage Matrix is further subdivided horizontally into Goals, Approaches, and Activities. Across the top of the Matrix are the Engage *Goals*. Goals are the high-level outcomes you would like your operation to accomplish.

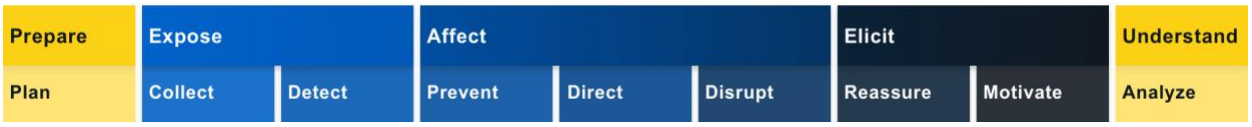
The Prepare and Understand Goals focus on the inputs and outputs of an operation. While the Matrix is linear, just like the 10-Step Process, it should be viewed as cyclical. As the operation proceeds, you are constantly aligning and realigning your actions to drive progress towards your Engagement Goals. The Engagement Goals are Expose, Affect, and Elicit. These Goals focus on actions taken against your adversary. Let's explore each of these Goals in more detail.

We can *Expose* adversaries on the network by using deceptive activities to provide high fidelity alerts when adversaries are active in the engagement environment.

We can *Affect* adversaries by having a negative impact on their operations. Affect activities are ultimately about changing the cost-value proposition in cyber operations for the adversary. You may want to increase the adversary's cost to operate or drive down the value they derive from their operations. It is important to note that we limit all Affect activities to the defender's network. We are NOT talking about hack back or any activities in the adversary's space. This distinction is important to ensure that our defense activities are legal!

We can *Elicit* information about the adversary to learn about their TTPs. By creating an engagement environment that is uniquely tailored to engage with specific adversaries, the defenders can encourage the adversary to reveal additional or more advanced capabilities. Observing an adversary as they operate can provide actionable cyber threat intelligence (CTI) data to inform the defender's other defenses.

The next row contains the Engage *Approaches*. Approaches let you make progress towards your selected goal.



Strategic Approaches help you to focus on the steps you must complete before, during, and after an operation to ensure that your activities are aligned with your overall strategy. Engagement Approaches help you to identify what actions you would like to take against your adversary and help you to drive progress towards that impact.

The remainder of the Matrix is composed of the Engage *Activities*. These are the concrete techniques you use in your approach.

Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

You will notice that the same activities often appear under one or more Approach or Goal. Activities can be adapted to fit a spectrum of use cases and objectives based on implementation. Additionally, activities are driven by real adversary behavior. When an adversary engages in a specific behavior, they are vulnerable to expose an unintended weakness. In Engage, we look at each MITRE ATT&CK® technique to examine the weaknesses revealed and identify engagement activities to exploit this weakness.

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

ATT&CK Technique	Adversary Vulnerability	Engagement Activity
Remote System Discovery (ATT&CK ID: T1018)	When adversaries interact with the environment or personas, they are vulnerable to collect, observe, or manipulate system artifacts that may cause them to reveal behaviors, use additional or more advanced capabilities against the target, and/or impact their dwell time	Decoy Artifacts and Systems

By mapping the engagement activities to ATT&CK, we can better plan which activities will enable us to reach our strategic objectives. If you are unfamiliar with MITRE ATT&CK, spend some time exploring their website, attack.mitre.org.

Spend some time exploring the Matrix. By clicking on various components, you can learn more about each action. Think of these actions as building blocks as you create the outline of your engagements.

4 Integrate Adversary Engagement

Let's put it all together and see how you can grow from running a single operation to integrating adversary engagement into your cyber strategy

The MITRE Engage Cycle illustrates how the Engage Matrix can be operationalized over the course of a single operation.

This cycle has no defined beginning or end, but for the sake of walking through the model, we will start with *collecting raw data from sensors.* This collection is tool agnostic—it simply refers to your collection methods regardless of how that collection happens. These collection tools can range from low-cost solutions such as collection Windows System Monitor (Sysmon)/Auditd/etc., to vendor Endpoint Detection and Response (EDR) solutions. The next step in the cycle is *analyzing raw data in the context of existing CTI data.* Here you can use tools such as MITRE ATT&CK to contextualize this new data. By analyzing adversary actions and comparing this data to past behavior, the defender can identify patterns that offer indications about the adversary's current, and possibly future, activities. Armed with this knowledge, the defender can use the Engage Matrix to *identify opportunities for engagement* to meet defensive goals. It should be noted that as you begin your deception program, you may rely heavily on intelligence feeds, open-source reporting, and/or information sharing

groups to learn about the behavior of your target adversary. As you build your deception capabilities, you can complement this CTI data with insights gained by watching adversaries in your own environment. After you have found opportunities, it is time to *implement your engagements*. At this stage, the deceptive assets are deployed and the engagement begins.

Adversary behavior should drive the engagement. Each time the adversary interacts with the engagement environment, the expert defender refines operational activities to manage the operation most effectively. Did the adversary ignore or overlook a deployed lure? The operator may move or change the lure to better encourage engagement. Did the adversary display a new behavior? There may be new opportunities for deception given this new activity. At the conclusion of each operation, lessons learned, distilled intelligence, and other operational outcomes should drive future operations.

Driven by the defender's goals, we designed Engage to complement a traditional cyber defense strategy. The Engagement Goals are not inherently deceptive. Therefore, it is easy to imagine how these goals may already be guiding an organization's security practices. Are you worried about insider threats? Look at the Expose activities to start adding deceptive artifacts around your critical assets. Do you have legacy systems that are no longer able to be updated? Look at the Affect activities to understand how you place decoys to direct adversaries away from these vulnerable systems. Do you feel exhausted by the endless game of CVE whack-a-mole? Look at the Elicit activities to begin to generate your own CTI feed to drive your defense by the adversary's TTPs and not the CVE of the day. Whatever your defensive goals, the Engage Matrix can help you find complementary engagement activities to ensure that if a defense-in-depth approach fails, you remain in control.

While we often consider adversary engagement as a distinct security practice, the most effective and mature implementations are seamlessly integrated into the very culture of an organization. Just as we train our workforce in good cyber hygiene habits, we must train the security community to consider deception as a best practice. In the United States, we have pathologized deception; we consider deception as inherently negative, sneaky, and dishonest. However, Engage enables defenders to normalize denial and deception activities as routine, essential, and responsible security practices.

Now, you are ready to employ adversary engagement as an integral part of your organization's security culture. This starter guide was adapted from the Engage handbook. Dive into the full handbook below to learn more.

5 Join the Community

There are ways for everyone to learn and grow with the Engage community – even if you choose to stay anonymous.

It is important to consider Operational Security (OPSEC) concerns when incorporating adversary engagement into your organization's cyber strategy. First and foremost, you must consider who should be aware of your adversary engagement program. At MITRE, we spent many years keeping a close hold on our use of adversary engagement as part of our InfoSec strategy. It was only after years of successful operations that we decided to be more open about our use of adversary engagement as a means of maturing and growing the community.

There is a continuum of options between the two extremes of never speaking about adversary engagement and openly presenting at conferences and releasing tools. For example, some organizations may find middle ground by sharing operations with a closed group of trusted partners. No matter where your organization falls on this spectrum, there are pros and cons to consider. By keeping a closed program, you may have more opportunities to engage unsuspecting adversaries. When adversaries enter an environment without expecting deceptive assets, their natural biases may increase their tolerance for imperfections in the environment and improve the overall believability of the ruse. With an externally known program, you may have the opportunity to deter adversaries through increased ambiguity; if they know deception is in play, they must question everything on your network. Additionally, participating in adversary engagement communities of interest or sharing groups, such as the Engage community, may expose you to new technologies and research. It could also enable you to compare operational data to complement and enhance your own findings. Whatever you chose, it is important to gather stakeholders and consider your options carefully at the onset of developing your program.

We now invite you to explore the *Engage with Us* tab at the top of the page. Here you will find a link to our Medium blog and our Community Spotlight. Additionally, we invite you to check out our *Tools* tab to explore the All Tools section.

Even if you chose to keep your program internal, the MITRE Engage resources are intended to help lower the barrier to entry while raising the ceiling of expertise in adversary engagement.

If you do choose to join the Engage community, connect with us by filling out the form below, sending us an email to engage@mitre.org, or connecting with us on LinkedIn.