SentinelOne™

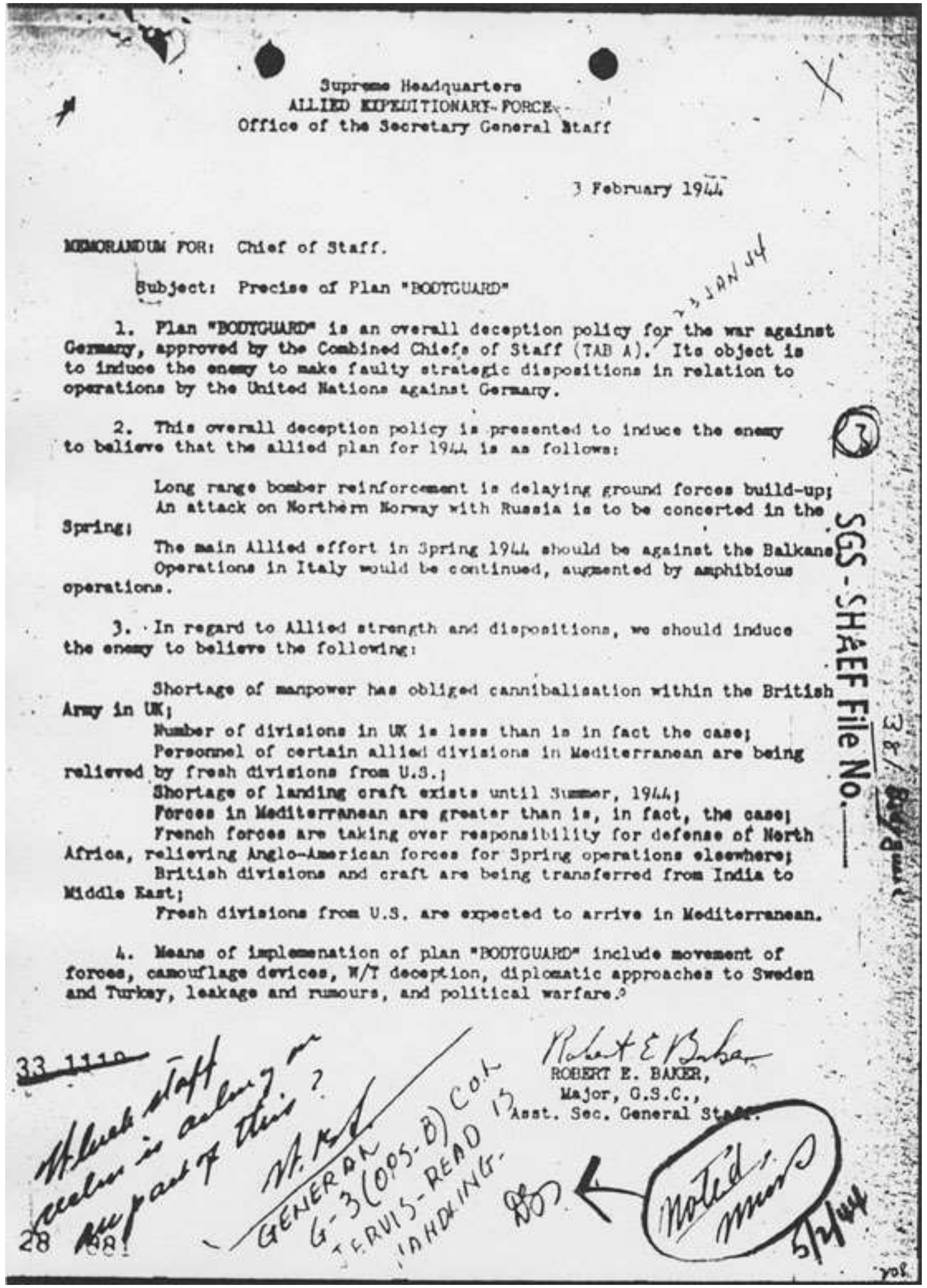
Understanding MiTRE ENGAGE *– Deception for Adversary Engagement, Early Breach Detection, and Improved Incident Response.*

- Mark Howell
- VP Deception / Identity
- mark.howell@sentinelone.com
- +447919057244

- Wouter Marien
- Account Director – BENELUX
- wouter.marien@sentinelone.com
- +32476503202

Deception – The Oldest Doctrine in Warfare

Operation Bodyguard / Mincemeat



Supreme Headquarters
ALLIED EXPEDITIONARY FORCE
Office of the Secretary General Staff

3 February 1944

MEMORANDUM FOR: Chief of Staff.

Subject: Precise of Plan "BODYGUARD"

22 JAN 44

1. Plan "BODYGUARD" is an overall deception policy for the war against Germany, approved by the Combined Chiefs of Staff (TAB A). Its object is to induce the enemy to make faulty strategic dispositions in relation to operations by the United Nations against Germany.

2. This overall deception policy is presented to induce the enemy to believe that the allied plan for 1944 is as follows:

Long range bomber reinforcement is delaying ground forces build-up;
An attack on Northern Norway with Russia is to be concerted in the Spring;
The main Allied effort in Spring 1944 should be against the Balkans;
Operations in Italy would be continued, augmented by amphibious operations.

3. In regard to Allied strength and dispositions, we should induce the enemy to believe the following:

Shortage of manpower has obliged cannibalisation within the British Army in UK;
Number of divisions in UK is less than is in fact the case;
Personnel of certain allied divisions in Mediterranean are being relieved by fresh divisions from U.S.;
Shortage of landing craft exists until Summer, 1944;
Forces in Mediterranean are greater than is, in fact, the case;
French forces are taking over responsibility for defense of North Africa, relieving Anglo-American forces for Spring operations elsewhere;
British divisions and craft are being transferred from India to Middle East;
Fresh divisions from U.S. are expected to arrive in Mediterranean.

4. Means of implemenation of plan "BODYGUARD" include movement of forces, camouflage devices, W/T deception, diplomatic approaches to Sweden and Turkey, leakage and rumours, and political warfare.

Robert E Baker
ROBERT E. BAKER,
Major, G.S.C.,
Asst. Sec. General Staff.

SGS - SHAEF File No. 381/Bodyguard

~~33 1110~~

What staff section is acting on our part of this?

GENERAL
G-3 (OPS-B) COL
JERVIS-READ 13
HANDLING.

Noted

5/2/44

28 88

The deception strategy, now named *Bodyguard*, was approved on Christmas Day 1943. The new name had been chosen based on a comment by Winston Churchill to Joseph Stalin at the Tehran conference: ***"In wartime, truth is so precious that she should always be attended by a bodyguard of lies."***[10][11]

Inflatable tanks were used during Operation Fortitude, one of the three major operations making up *Bodyguard*

The corpse of Glyndwr Michael, dressed as Martin, just prior to placement in the canister

Converging Analyst Opinion on CyberDeception

Gartner

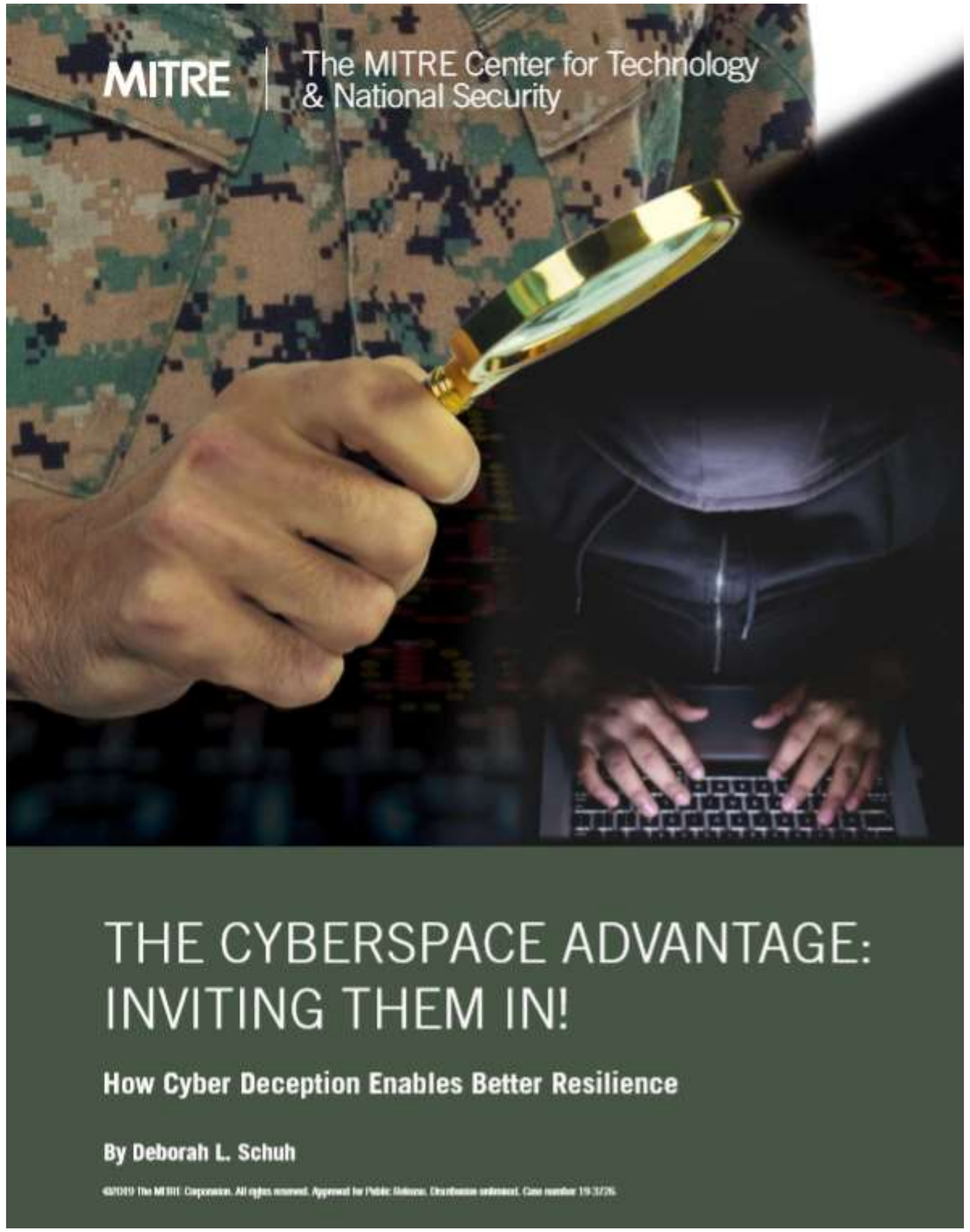
National Cyber
Security Centre
a part of GCHQ

W | R
Wellington Research

MITRE

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

MITRE – Center for Technology & National Security



MITRE | The MITRE Center for Technology & National Security

THE CYBERSPACE ADVANTAGE: INVITING THEM IN!

How Cyber Deception Enables Better Resilience

By Deborah L. Schuh

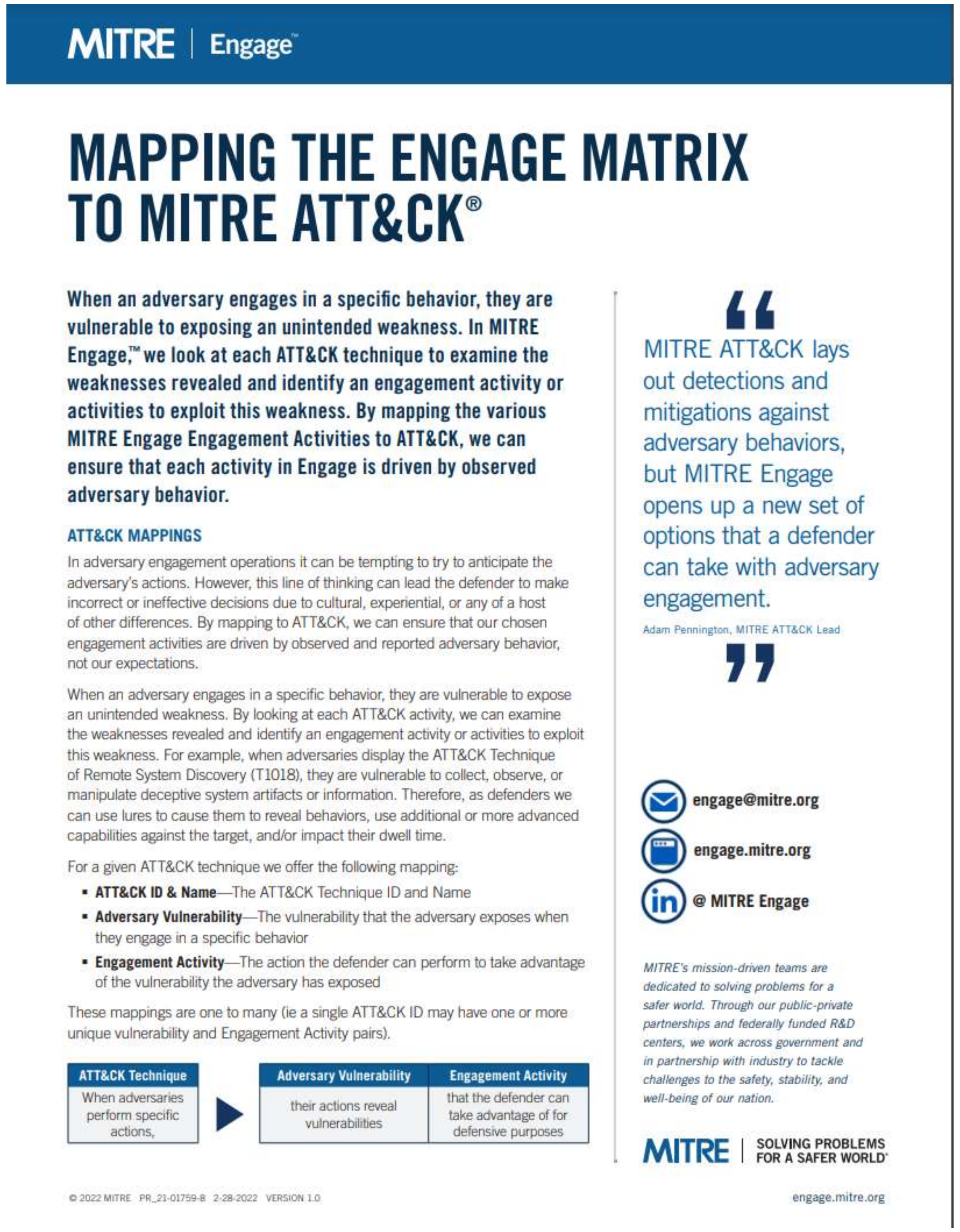
The Value of Cyber Deception

1. Finding and managing adversaries.
2. Learning adversary techniques to better inform defense
3. Finding insider threats
4. Better incident response
5. Deceiving the adversary

“Judicious use of networks, pocket litter, and honeytokens can waste the adversary’s time and resources, expose their pedigree, and create false knowledge on their part. Deception can also add randomness and unpredictability to an architecture, network traffic, service, or mission activity, making an adversary’s understanding of the environment more challenging and at best inaccurate”

MITRE Engage

- Active Defense Capabilities
- MITRE Corp. released a publicly available guide called Shield(now Engage) cataloging measures that organizations should take to actively engage with and counter intruders on their networks
- Adversary engagement is learning about how our adversaries attack us, what tools they use, what they will do after they establish a beachhead on our systems, insights into what they are seeking



MITRE | Engage™

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

✉ engage@mitre.org

engage.mitre.org

in @ 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®

engage.mitre.org

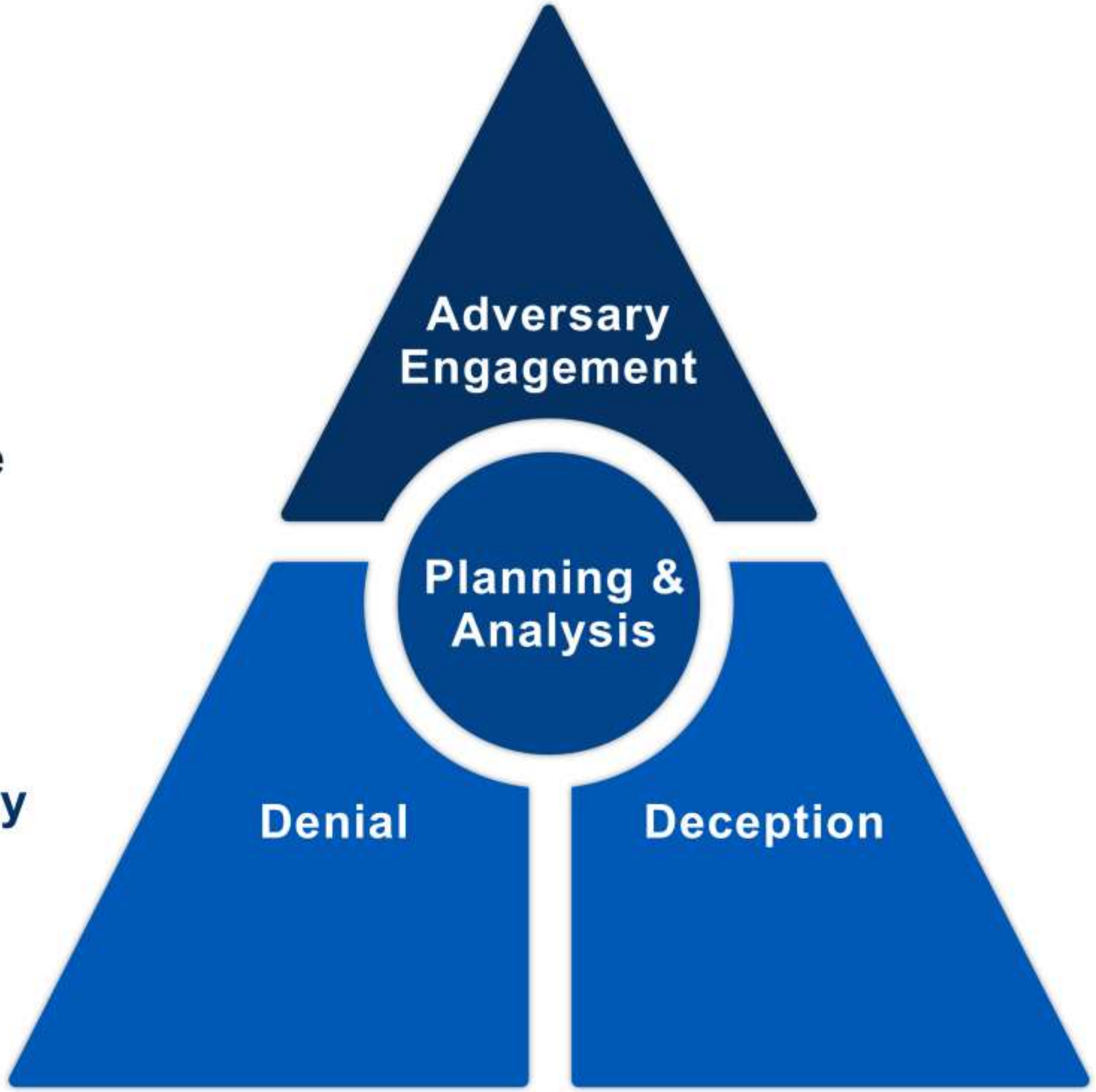
Engage was put together to start a conversation about the benefits of active defense.

What is Adversary Engagement?

Cyber Denial prevents or impairs the adversary's operations.

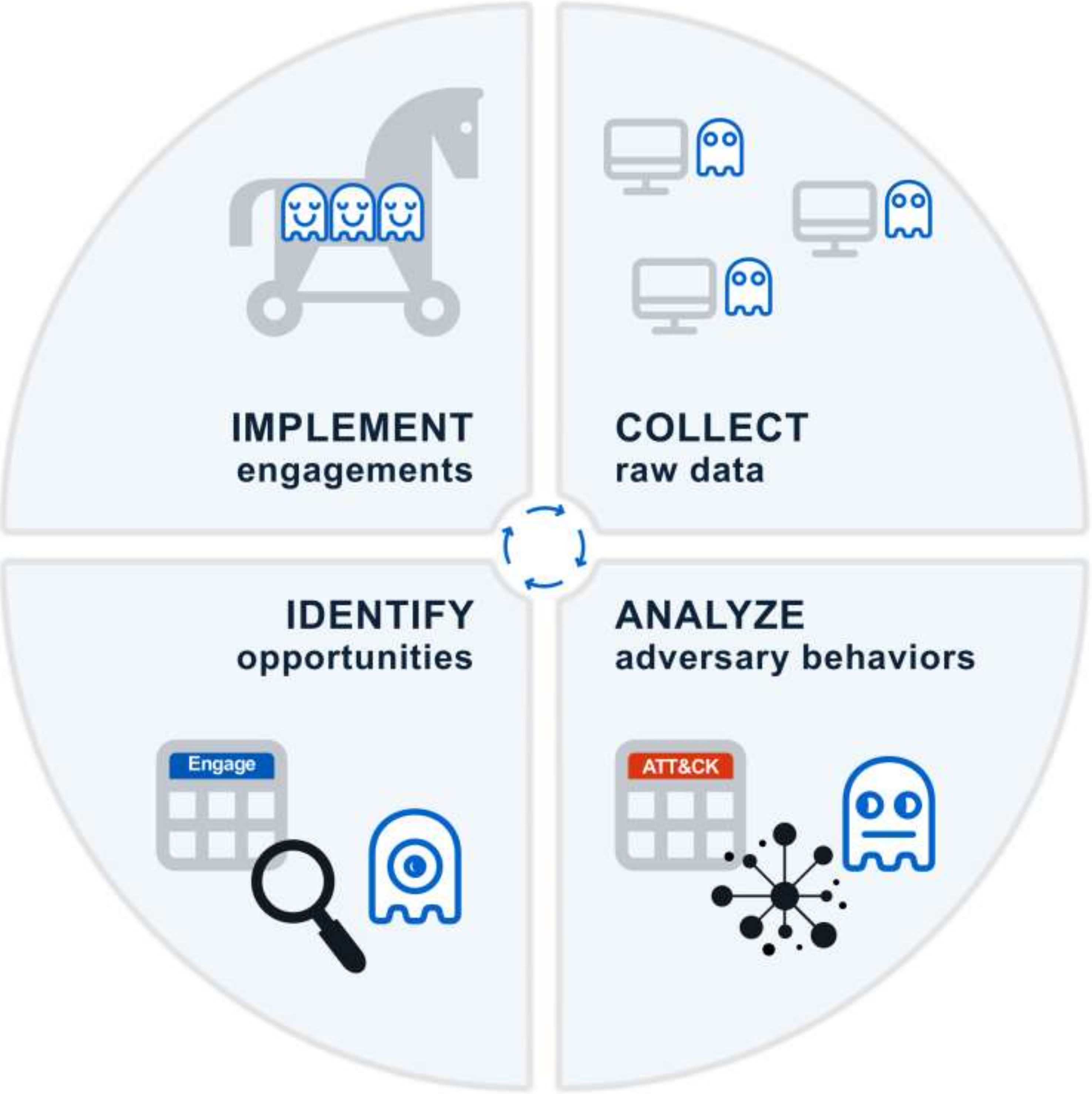
Cyber Deception reveals and conceals deceptive facts and fictions to mislead and confuse the adversary.

When used together with strategic **Planning & Analysis**, they provide a foundation for **Adversary Engagement**.



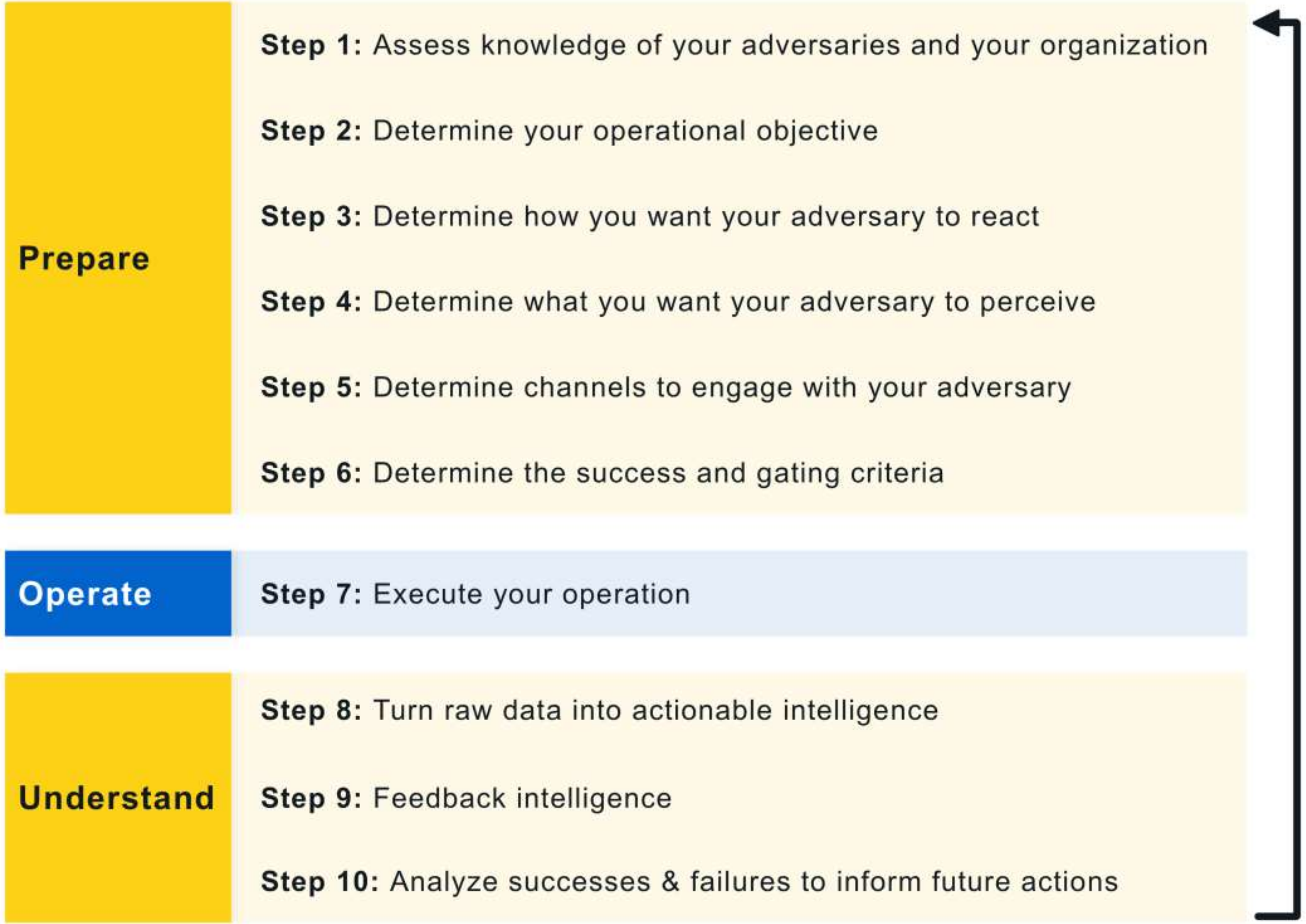
MITRE | Engage ™

Operationalizing the MITRE Engage Matrix



PR_21-01759-22 Last updated: 2/28/2022 Version: 1.0

The Engage 10-Step Process



Prepare	**Step 1:** Assess knowledge of your adversaries and your organization
	Step 2: Determine your operational objective
	Step 3: Determine how you want your adversary to react
	Step 4: Determine what you want your adversary to perceive
	Step 5: Determine channels to engage with your adversary
	Step 6: Determine the success and gating criteria
Operate	**Step 7:** Execute your operation
Understand	**Step 8:** Turn raw data into actionable intelligence
	Step 9: Feedback intelligence
	Step 10: Analyze successes & failures to inform future actions

The MITRE Engage Matrix

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				

MITRE | Engage ™

PR_21-01759-20 Last updated: 2/28/2022 Version: 1.0

engage.mitre.org

SentinelOne™