An Introduction to MITRE Shield

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release. Distribution unlimited 20-00398-1.

©2020 The MITRE Corporation. All rights reserved.

MITRE ATT&CK and ATT&CK are registered trademarks of the MITRE Corporation.

Authors:
Christina Fowler
Mike Goffin
Bill Hill
Richard Lamourine
Andrew Sovern

August 2020

Abstract

MITRE Shield[1] is a publicly accessible knowledge base of active defense tactics and techniques based on real-world observations. Active defense can be useful to counter an adversary and ultimately help change the game in favor of the defender. The Shield knowledge base describes some foundational activities in active defense, cyber deception, and adversary engagement operations. We believe these activities can be employed for defensive benefit in the private sector, in government, and in the cybersecurity product and service community. Our work to codify our experience into Shield continues, and we expect a next version to have an improved structure and additional content. Although there are too many possible activities in the active defense space to fully enumerate, we believe Shield will be an important resource for organizations seeking to understand or implement defenses using active defense.

[1] http://shield.mitre.org

This page intentionally left blank.

Executive Summary

This paper presents an overview of the structure, contents, and potential uses of the MITRE Shield knowledge base. It also discusses the connection to MITRE ATT&CK® and how both projects can be used together for defensive purposes.

Table of Contents

List of Figures

This page intentionally left blank.

Introduction

MITRE Shield is a knowledge base designed to give defenders tools that can be used to counter cyber adversaries. Shield includes a database of techniques a defender can use to mount an active defense. The knowledge base also describes a number of tactics common to defensive plans. It then maps the tactics to the activities that may help achieve them. The knowledge base includes a mapping between MITRE ATT&CK and Shield techniques, to illustrate the defensive possibilities introduced by adversary tactics, techniques, and procedures (TTPs).

MITRE's corporate defenses have included adversary engagement operations for more than ten years, and those engagements and our operational experience inform Shield. The Shield active defense knowledge base was created by our engagement team in 2019 to improve operational planning. When we were documenting our inventory of engagement techniques, we wanted to organize them, and an obvious choice was to do that in relation to the move/countermove we experienced with our adversaries. This led us to formalizing the linking concept; adversary actions found in MITRE ATT&CK frequently present opportunities for defender counteractions. So, we mapped our Shield techniques to MITRE ATT&CK, enabling us to develop plans to exploit those opportunities to the defender's advantage.

This first version of the knowledge base focuses on foundational security techniques, because those are the cornerstones upon which good deception and adversary engagement are built. We believe there are too many possible activities in the active defense space to fully enumerate, so Shield is admittedly incomplete. Even so, we believe Shield is a good resource for organizations seeking to understand or implement defenses based on active defense and can serve to stimulate discussion and technique exchange throughout the defensive community.

Using Shield

The U.S. Department of Defense defines active defense as "The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[2] Active defense ranges from basic cyber defensive capabilities to cyber deception and adversary engagement operations. The combination of these defenses allows an organization to not only counter current attacks but also to learn more about that adversary and better prepare for new attacks in the future.

General Cyber Defense

Shield includes foundational defensive techniques we believe are applicable to all defensive plans; we consider these general cyber defense techniques. Particularly when informed and prioritized by an assessment of the threats an organization faces, many Shield techniques can be applied within an enterprise network, especially to detect and deter the adversary.

Cyber Deception

There is a growing collection of ideas, tools, and products that use a "tripwire" approach to cyber defense that is broadly being labeled "Deception."[3] More active than the hardening and

[2] https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727

[3] https://securitytoday.com/articles/2019/08/12/how-deception-technology-can-help-you-detect-threats-early.aspx

instrumentation activities found with general cyber defense, deception finds defenders intentionally introducing targets and “breadcrumbs” (clues to the location of targets). Carefully constructed deception systems are often indistinguishable from production systems and can serve as high-fidelity detection systems. Shield techniques can include deceptions for detection, deterrence, or other desired effect.

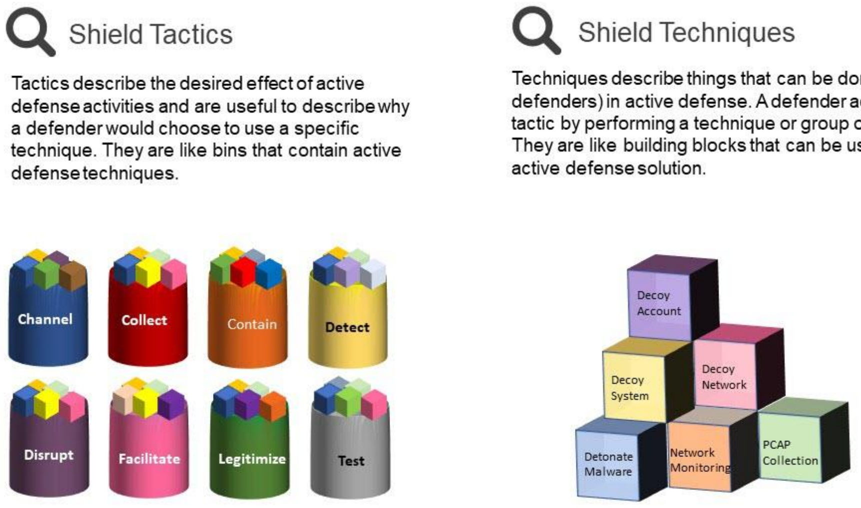
Adversary Engagement

Many techniques in Shield are designed for defenders that want to observe, collect, and understand adversary activities against the defender’s system. Deployable in either production or synthetic environments, Shield adversary engagement techniques promote effective, productive engagements. The Shield knowledge base can be useful in analyzing what is already known about an adversary (with the help of ATT&CK), planning defenses, and capturing what is learned for future consideration.

The Shield Model

The foundation of Shield is the set of techniques that defenders can use in their active defense operations. Shield also has a set of tactics: abstract, high-level descriptions of what defenders may (in whole or in part) be trying to achieve through the operation. We have found that tactics can be useful as shorthand for high-level planning. They classify groups of techniques and can be referenced when the details of the techniques are not salient to the discussion, (i.e., when the why is more important than the how).

As a metaphor to explain Shield techniques and tactics, imagine multiple containers each filled with building blocks. Each block in those containers has specific characteristics, such as size, color, and shape, but all the blocks in a container can have something in common, like general shape or material. The builder can choose to pull blocks from the container of his choosing (say from the one with large cement blocks) and build whatever model he desires. A defender can use Shield in much the same way. The defender can survey the tactics (the containers) offered within the knowledge base and choose the one that best fits the active defense need (for example collection). Then the defender can examine the techniques (the blocks) grouped within that tactical objective and select the one that allows them to build the best active defense solution.



Tactics describe the desired effect of active defense activities and are useful to describe why a defender would choose to use a specific technique. They are like bins that contain active defense techniques.

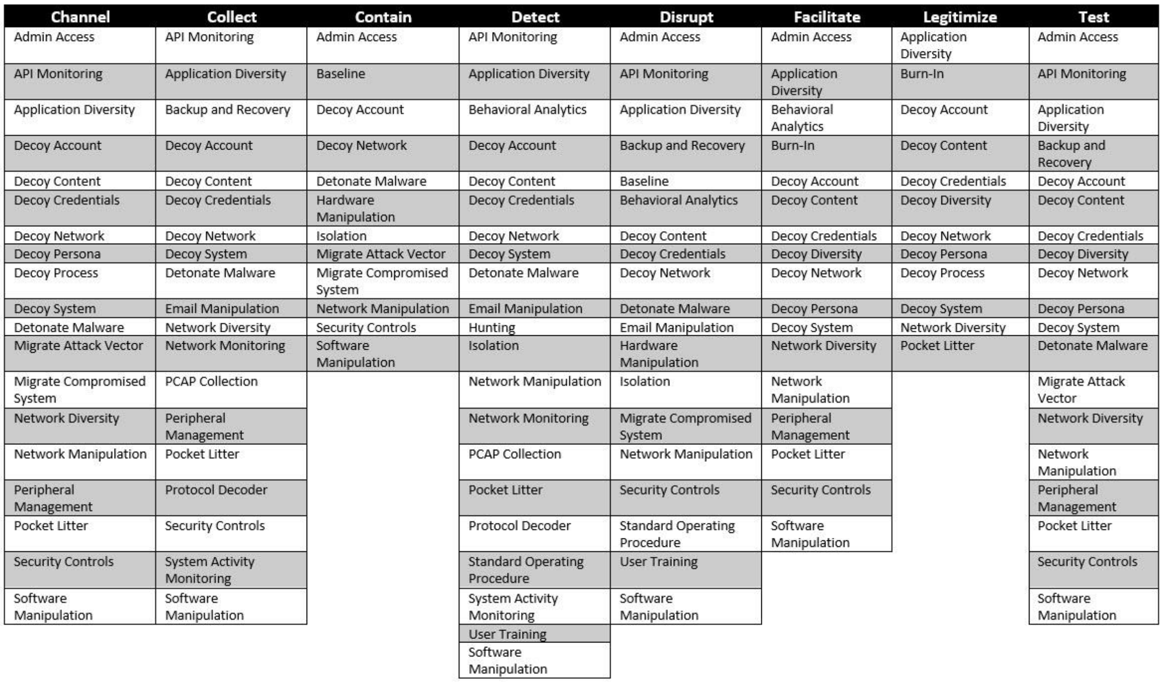
Techniques describe things that can be done (by defenders) in active defense. A defender achieves a tactic by performing a technique or group of techniques. They are like building blocks that can be used to build an active defense solution.

Figure 1. The Shield Model

The Shield Matrix

The relationship between tactics and techniques can be illustrated in a matrix. The matrix consists of:

- Tactics, denoting what the defender is trying to accomplish (the columns)
- Techniques, describing how the defense achieves the tactic(s) (the individual cells)



Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Admin Access
API Monitoring	Application Diversity	Baseline	Application Diversity	API Monitoring	Application Diversity	Burn-In	API Monitoring
Application Diversity	Backup and Recovery	Decoy Account	Behavioral Analytics	Application Diversity	Behavioral Analytics	Decoy Account	Application Diversity
Decoy Account	Decoy Account	Decoy Network	Decoy Account	Backup and Recovery	Burn-In	Decoy Content	Backup and Recovery
Decoy Content	Decoy Content	Detonate Malware	Decoy Content	Baseline	Decoy Account	Decoy Credentials	Decoy Account
Decoy Credentials	Decoy Credentials	Hardware Manipulation	Decoy Credentials	Behavioral Analytics	Decoy Content	Decoy Diversity	Decoy Content
Decoy Network	Decoy Network	Isolation	Decoy Network	Decoy Content	Decoy Credentials	Decoy Network	Decoy Credentials
Decoy Persona	Decoy System	Migrate Attack Vector	Decoy System	Decoy Credentials	Decoy Diversity	Decoy Persona	Decoy Diversity
Decoy Process	Detonate Malware	Migrate Compromised System	Detonate Malware	Decoy Network	Decoy Network	Decoy Process	Decoy Network
Decoy System	Email Manipulation	Network Manipulation	Email Manipulation	Detonate Malware	Decoy Persona	Decoy System	Decoy Persona
Detonate Malware	Network Diversity	Security Controls	Hunting	Email Manipulation	Decoy System	Network Diversity	Decoy System
Migrate Attack Vector	Network Monitoring	Software Manipulation	Isolation	Hardware Manipulation	Network Diversity	Pocket Litter	Detonate Malware
Migrate Compromised System	PCAP Collection		Network Manipulation	Isolation	Network Manipulation		Migrate Attack Vector
Network Diversity	Peripheral Management		Network Monitoring	Migrate Compromised System	Peripheral Management		Network Diversity
Network Manipulation	Pocket Litter		PCAP Collection	Network Manipulation	Pocket Litter		Network Manipulation
Peripheral Management	Protocol Decoder		Pocket Litter	Security Controls	Security Controls		Peripheral Management
Pocket Litter	Security Controls		Protocol Decoder	Standard Operating Procedure	Software Manipulation		Pocket Litter
Security Controls	System Activity Monitoring		Standard Operating Procedure	User Training			Security Controls
Software Manipulation	Software Manipulation		System Activity Monitoring	Software Manipulation			Software Manipulation
			User Training				
			Software Manipulation				

Figure 2. The Shield Matrix

Techniques

Techniques describe things that can be done (by defenders) in active defense. A defender achieves a tactical objective by performing one or more actions. For example, a defender can seed *decoy credentials* on an adversary engagement system to see if an adversary dumps the credentials and uses them to gain access to other systems within the engagement network.

Shield techniques range from basic to advanced. There are foundational techniques, such as *backup and recovery*, *network monitoring*, and *system activity monitoring*, which can be applied widely across many organizations. These techniques are useful when layering on other techniques that come into play as deception and adversary engagement are introduced as part of an organization’s active defense portfolio. Advanced techniques that manipulate network and software may only be useful to deception vendors and organizations that seek to study or engage with adversaries at a deeper level.

Procedures

Procedures are another important component of the TTP concept, and one cannot talk about tactics and techniques without also including procedures. Within this initial version of Shield, procedures are high-level descriptions of the implementations of a technique.

Linking Tactics and Techniques

As previously mentioned, we have found it useful to associate active defense tactics and techniques. Factoring in tactics should be part of every well planned or complex active defense operation. As the plan develops, techniques are necessary to build out the actual systems and controls in an operational environment.

We find the relationship between tactics and techniques can be many to many; a single technique may be able to support several different tactics, and for any tactic there are multiple techniques that may be used. For example, *security controls* can be tightened to *disrupt* an adversary's activity or loosened to *facilitate* further engagement.

It is also true that in an actual operation, a single action or technique may contribute to more than one tactic at the same time and accomplishing a tactic may require multiple techniques.

Shield and ATT&CK

As our team progressed in adopting active defenses, we saw a natural opportunity to organize what we were learning in a way that can relate to the adversary techniques found in MITRE ATT&CK. For this reason, a section in our knowledge base is devoted to ATT&CK tactics and techniques. The ATT&CK mapping section of Shield contains a list of the adversary tactics found in the ATT&CK framework. Each ATT&CK tactic has a dedicated page that lists (from ATT&CK) the adversary techniques associated with that tactic, and (from Shield) active defense information applicable, including the opportunity space presented, active defense technique to be implemented, and use case for that implementation.

The information displayed on the detail page is designed to illuminate the possibilities for active defenses to the ATT&CK technique. The high-level possibilities resulting from the adversary technique are described in the Opportunity Space column of the ATT&CK mapping table. Many adversary techniques present more than one opportunity; when we have captured multiple ideas, they each get a line in the table. The Use Case is a moderately detailed description of how a defender can use the listed Active Defense Technique to take advantage of the opportunity presented. Many of the listed opportunities allow for use of basic active defense techniques to detect and disrupt adversaries within an enterprise network. Other listed opportunities suggest a more involved active defense, and these may invite management conversations about adding active defense and adversary engagement techniques to an organization's cyber defense portfolio.

We think using ATT&CK and Shield together can help defenders deepen their understanding of adversary behavior and engagements and suggest ways the defender can mount a more active defense.

Future Work

The team envisions an evolution of the current data model to accommodate more sophisticated active defense solutions. This will allow us to combine multiple techniques and procedures to create complex playbooks. Leveraging ATT&CK's group information provides the potential to create active defense playbooks that apply to specific adversaries.

Summary

MITRE Shield is a knowledge base giving defenders tools that can be used against cyber adversaries. It is our goal that defenders can leverage the tactics and techniques contained in Shield to better create, instrument, and operate their active defense solutions. We also hope that by showing how the defensive side of Shield can be aligned to MITRE ATT&CK, we can help organizations leverage both solutions to maximize their defensive efforts.