MITRE

Getting Started with MITRE Shield

Authors:
Christina Fowler
Bill Hill
Andrew Sovern

August 2020

Approved for Public Release. Distribution unlimited 20-00398-3.

Table of Contents

Introduction

MITRE Shield is a knowledge base of active defense techniques and tactics designed with the practitioner in mind. Structured similarly to MITRE ATT&CK®, a widely used framework that catalogs adversary behavior, Shield organizes defense techniques in a framework of defensive tactics.

Shield is informed by over 10 years of MITRE's work observing and engaging adversaries in defense of our own network. It spans the range from strategic, chief information security officer-level opportunities and objectives to practitioner-friendly tactics, techniques, and procedures. We are sharing here ideas for how to start using the knowledge base as an aid for those thinking about adding some of these techniques to their defenses.

First, what is active defense? 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." 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 learn more about that adversary and better prepare for new attacks in the future.

For this introduction to using MITRE Shield, we will use the following terms:

- Level 1 for those new to active defense
- Level 2 for those with some active defense experience
- Level 3 for more advanced cybersecurity teams

The Building Blocks of Shield

As you start to consider implementing techniques found in the Shield knowledge base, it might be helpful to think in terms of building blocks. Each active defense technique is a building block that can be used alone or added to other building blocks to achieve something more elaborate. You can start small and add additional blocks when you are ready. For some purposes, a common, standard design will be effective and efficient, while in other cases specialized goals may require bespoke designs. Here we offer some "getting started" examples at each of our three levels.

Level 1 Examples

In the next two examples, we will also illustrate two different approaches. First, we'll begin by assuming the defender already has a sense of their problem and strategy and uses Shield to identify practical next steps. The second example is a bit more formal, starting with an adversary technique listed in MITRE ATT&CK and using the Shield mapping to consider the opportunities in that attack, and then moving to a course of action. Our goal in both these examples is adversary detection, as it is one of the most approachable active defense measures.

Example 1

A defender interested in addressing detection can consult the Shield Matrix and find a column of active defense techniques labeled "Detect." These techniques can also be found (by clicking on

the column title) summarized on the *Detect (DTA004)* tactic page. Both views link to individual technique pages with more detail.

Our defender in this case knows she'd like to improve her defenses against spearphishing and has heard (rightly!) that users can be turned into a defensive asset. Surveying the detection techniques, she sees the Shield technique *User Training (DTE0035)*.

Let's quickly examine the detail page for *User Training (DTE0035)*. After brief then detailed descriptions, it lists "Opportunities" and "Use Cases." These are part of the "glue" in the mapping between ATT&CK and Shield, which describe benefits that might be made possible by adversary actions, and general approaches to get those benefits. We also find "Procedures," which are about implementing the Shield technique, and finally a link to the relevant ATT&CK techniques.

In this case our defender likes the opportunity space (DOS018) "Users trained and encouraged to report phishing can detect attacks that other defenses do not," and the use case (DUC0018) "A program to train and exercise the anti-phishing skills of users can create 'Human Sensors' that help detect phishing attacks."

Our defender decides to train users to identify and report suspicious emails. If users can recognize things like spoofed senders, fake URL links, and other suspicious content, they can report the emails to the defender who can then review the messages and take other actions as needed.

Example 2

Let's look at how Shield can be used in conjunction with MITRE ATT&CK.

Our defender knows her adversaries use the ATT&CK technique OS Credential Dumping to obtain account login and credential information. Given this, she can use the Credential Access page of Shield's ATT&CK mapping to see what opportunities that presents for her defense, and finds: "There is an opportunity to deploy a tripwire that triggers an alert when an adversary touches a network resource or uses a specific technique."

How can our defender take advantage of this opportunity? The use case (DUC0005) begins to reveal that: "A defender can seed systems with decoy credentials in a variety of locations and establish alerting that will trigger if an adversary harvests the credentials and attempts to use them." Our defender now has the makings of a high-level plan. When she gets to planning the specifics, she will employ the listed Shield technique *Decoy Credentials (DTE0012)* hoping to detect the adversary. Decoy credentials are credentials that are not associated with an actual user, but rather are used for active defense purposes. Once the decoy credentials have been created, our defender can store these credentials on key systems within the network and monitor for any usage attempts. Information on how to implement monitoring be found in the Detections section for the ATT&CK technique OS Credential Dumping.

Level 2 Examples

At an intermediate level we move beyond describing how to navigate the knowledge base, and beyond individual techniques, toward considering the use of multiple techniques used together in what we call a "play." We see plays on both sides; adversaries employ a series of ATT&CK techniques (offensive plays) to accomplish their objectives, and defenders can likewise employ

defensive plays composed of techniques found in Shield. Somewhat obviously, the most effective defensive plays will be those more closely attuned to the expected offensive play.

Example 3

Building on our end user training example above (Example 1), we can add more Shield techniques for greater effect. After a suspicious email has been identified, a defender can *Migrate Attack Vector (DTE0024)* and move the email to an isolated *Decoy System (DTE0017)* for examination. The defender can then look at the email header and full contents without fear of activating any malicious content.

Example 4

Our defender recently read a report in which an adversary compromised an externally facing server and used credentials stolen from that victim to further attack a corporate network. Considering this adversary play, our defender wants to know if her corporation may also be the target of such an attack.

By examining the techniques used by the adversary, she decides to implement an external *Decoy System (DTE0017)* with *Decoy Credentials (DTE0012)*. She is cautious to avoid misconfigurations of this system that would allow an adversary to pivot into her network or attack other organizations. Our defender sets up alerting on other external hosts to detect for the usage of the *Decoy Credentials*.

Example 5

Our defender decides to layer her defenses, supplementing initial intrusion detections with detections for lateral movement "inside" her network. She has threat intelligence suggesting one of her adversaries uses malware with an automated capability to spread through an SMBv1 exploit commonly known as "EternalBlue." She decides to create a *Decoy System (DTE0017)* on her internal network with a specific set of patches installed to make it exploitable. Implementing *System Activity Monitoring (DTE0034)* and *Isolation (DTE0022)* for decoys is important so that an adversary cannot use them as a beachhead for additional compromise. Alerts based on activity from these systems will allow the defender to quickly find malicious activity in her environment, even if she did not detect the initial exploitation.

Level 3 Example

Moving beyond simple multi-technique plays, one can address more complex real-world scenarios such as more advanced threats, simultaneously defending against attackers with different styles, and adversaries that rapidly evolve their attacks. Defenders can also consider objectives beyond detection; for example, advanced defenders may wish to collect information and tools from adversaries in order to develop their own threat intelligence. The example in this section explores both more complicated plays and new objectives.

Example 6

Continuing to build on the user training example, our defender receives a tip that describes a malicious email campaign targeting organizations in her industry but provides few details about

the attack. Our defender decides that instead of merely blocking the mail (and hoping the attacker doesn't change it enough to avoid the block) she wants to learn more about what will happen if the mail gets through. Her high-level plan: divert the email to a safe, controlled "detonation chamber," and learn about the exploit that will be delivered. Using Shield, she works out some details:

- Use her email gateways for *Email Manipulation (DTE0019)*: Based on indicators described in the tip, implement an email redirection away from the intended victim into the control of the defender.
- Create a *Decoy System (DTE0017)* instrumented with *System Activity Monitoring (DTE0034)* along with *Network Monitoring (DTE0027)* and *Isolate (DTE0022)* it from all networks.
- Safely deliver the email to the decoy and *Detonate Malware (DTE0018)*.
- Collect Indicators of Compromise (IOCs) from the instrumented host.
- Use those IOCs for future detections.

Summary

Having seen over the past 10 years how helpful active defense has been to our corporate defense, we have been looking for ways to share these ideas with the defensive community. Thinking that nothing works with practitioners like details learned through experience, we developed Shield to get active defense more broadly discussed and, we hope, implemented. There certainly is no right way to begin adding active defense to your defensive tactics; we merely offer this getting started guide to help teams start considering their own defensive objectives and how they might be accomplished.