Acalvio ShadowPlex for MITRE Shield

MITRE recently announced the first release of Shield (https://shield.mitre.org/), an active defense knowledgebase on how to defend and engage with adversaries. The knowledgebase is a significant endorsement to Cyber Deception as a dynamic dimension for detecting and engaging with threats inside the network. The uniqueness of deception stems from the ability to introduce new elements into the enterprise network, which actively attract attacks. Deception elements are not part of the production network, and hence any access to deception is suspect and provides a high-fidelity alert. Besides detection, deception can also engage with the attacks to gather the TTPs.

We at Acalvio have built ShadowPlex Autonomous Deception solution that provides the entire spectrum of defensive tactics and techniques listed in MITRE Shield covered by deception. However, covering the listed tactics and techniques is necessary, but not sufficient for deception to be an effective defense. Deception should also be easy to deploy and manage at enterprise-scale, across the distributed network. Deception should be configured and customized for each neighborhood and host. Finally, deception has to be managed as each network neighborhood evolves. ShadowPlex, based on 25+ issued patents, does all this and more autonomously to provide an effective solution.

The MITRE Shield lists 33 Defense Techniques against attacks (Figure 1). Techniques describe the active defense actions. Three of the techniques (*Email Manipulation, Hardware Manipulation, User Training*) are preventive measures, and three more (*Backup & Recovery, Baseline, Protocol Decoder*) are response actions. The remaining 27 techniques are based on deception. Acalvio ShadowPlex covers all these 27 techniques and provides multiple procedures for each of these techniques.

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

Figure 1: MITRE Shield Defense Techniques

Channel	Guide an adversary down a specific path or in a specific direction.
Collect	Gather adversary tools, observe tactics, and collect other raw intelligence about the adversary's activity.
Contain	Prevent an adversary from moving outside specific bounds or constraints.
Detect	Establish or maintain awareness into what an adversary is doing.
Disrupt	Prevent an adversary from conducting part or all of their mission.
Facilitate	Enable an adversary to conduct part or all of their mission.
Legitimize	Add authenticity to deceptive components to convince an adversary that something is real.
Test	Determine the interests, capabilities, or behaviors of an adversary.

Figure 2: MITRE Shield Defense Tactics

MITRE Shield describes 8 Defense Tactics (Figure 2), which are desired outcomes of active defense. Each tactic maps to a set of techniques. ShadowPlex covers all these active defense tactics.

How Exactly is Shield Useful?

MITRE ATT&CK is the comprehensive knowledge base of adversary tactics and techniques. The ATT&CK Framework consists of 12 ATT&CK Tactics used by adversaries. For each tactic, adversaries may use multiple ATT&CK techniques. MITRE Shield provides a formal framework of defense against the ATT&CK

tactics. Figure 3 shows the list of Shield Defense Techniques (from Figure 1) that can be used for each of the ATT&CK Tactics. The 27 Shield Deception Techniques that Acalvio ShadowPlex covers provide coverage for all the MITRE ATT&CK Tactics that an adversary may use.

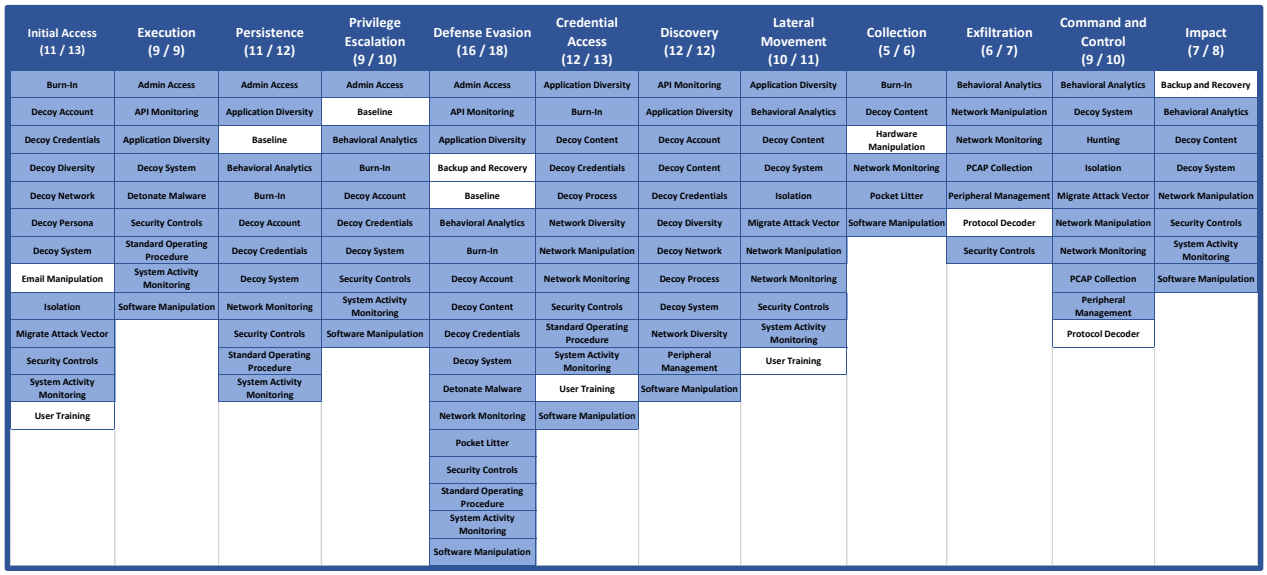

Figure 3: Shield Defense Techniques for ATT&CK Tactics

ShadowPlex Autonomous Deception

The coverage of all Shield Defense techniques does not guarantee effective defense. For example, consider the "Decoy System" technique. Creating a couple of static decoy systems in a network of thousands of hosts provides very little defense. Decoy systems that match the network scale, customized to blend into the network, provide depth of interaction, and change as the network changes are significantly more effective. ShadowPlex achieves this over hundreds and thousands of subnets across the distributed enterprise, using AI-driven automation.

ShadowPlex provides autonomous deception using unique "Deception Playbooks" concept. Playbooks encapsulate the design of the deception and separate it from the deployment of deception. Acalvio provides deception playbooks to address all of the MITRE ATT&CK Tactics. The playbooks embody the Shield Defense techniques associated with the tactics. Deploying Shield Defense in a subnet is as simple as assigning the corresponding playbook to the subnet. ShadowPlex Autonomous Deception completely automates the deployment and management of the Shield Defense Tactic.

MITRE Shield is a great affirmation of the power of deception in active defense. The framework will help cyber defenders formulate an effective defense against various ATT&CK tactics and techniques. Acalvio ShadowPlex provides the state-of-the-art platform to deploy an effective defense based on the MITRE Shield framework at enterprise-scale.