

D3B3sh>5l>>o



Acalvio Deception and the MITRE ATT&CK Framework



Table of Contents

1.	Background: The Challenge of Post-Compromise Security	2
2.	The ATT&CK Framework: Details and Application.....	2
3.	Acalvio Support for ATT&CK	3

1. Background: The Challenge of Post-Compromise Security

The Cyber Attack Lifecycle (also known as the Cyber Kill Chain) has long been used to describe the stages of an attack commonly used to compromise sensitive assets. Unfortunately, too much emphasis has been placed on the initial exploitation stages, and not enough on the later stages, after initial penetration. As a result, organizations are ill-prepared to establish and operationalize detection and mitigation strategies. Given that “assume breach” is the new mantra, this is a serious shortcoming.

To overcome this problem, MITRE has developed ATT&CK. ATT&CK is a framework that describes the actions an adversary uses after it has penetrated the target organization. The 11 tactic categories within ATT&CK for Enterprise were derived from the later stages (exploit, control, maintain, and execute) of the Kill Chain. This provides a deeper level of granularity in describing what can occur during an intrusion.

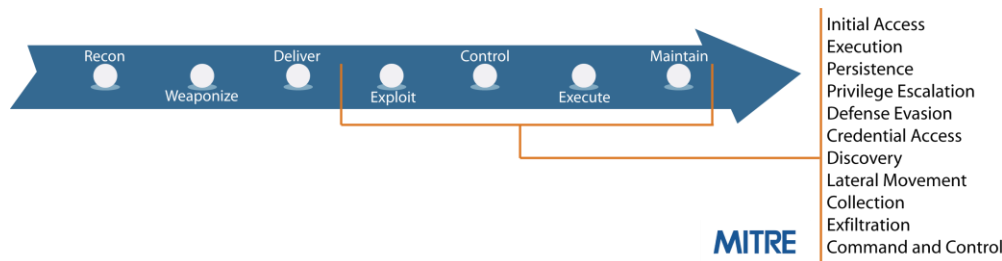


Figure 1. ATT&CK Focuses on Post-Compromise Adversary Tactics

2. The ATT&CK Framework: Details and Application

ATT&CK was born from research into APT detection research and methodology creation. It consists of three core components:

- **Tactics:** Short-term, tactical adversary goals during an attack. With limited exceptions, they are executed serially, with the ultimate goals being persistence and data exfiltration.
- **Techniques:** Means by which adversaries achieve tactical goals during an attack. Each tactic has a number of techniques attacks can choose from to meet the goal, and there are 219 techniques in total across the 11 tactics.

Highlights

- The MITRE ATT&CK Framework provides a model for understanding adversary post-compromise tactics and techniques.
- ATT&CK is based on the adversary’s perspective and is based on real-world malicious activity
- Acalvio ShadowPlex was designed specifically to detect and defeat the tactics documented in ATT&CK.
- ShadowPlex supports defensive strategies for 7 of the 11 adversarial tactics in ATT&CK.
- ShadowPlex operates with minimal false positives and support high-scale enterprise deployment

- **Documented adversary usage of techniques.** These are examples of how actual attacks string together specific techniques to complete the tactics successfully.

A key advantage of ATT&CK is that it is based on “in the wild” research, that is, documented attacker behavior. Another advantage is that it enumerates techniques for Windows, Linux, and MacOS hosts, making it easier to apply based on operating systems in use.

The full Technique Matrix can be found at: https://attack.mitre.org/wiki/Technique_Matrix

MITRE recommends that ATT&CK be used to architect computer network defenses (CND), using the following methodology:

- Prioritize development and/or acquisition efforts for CND capabilities
- Conduct analyses of alternatives between CND capabilities
- Determine “coverage” of a set of CND capabilities

MITRE also suggests that an organization can continuously evaluate the attack methods it is most susceptible to using threat intelligence, map that to specific techniques, and then implement adequate defenses. Unfortunately, such a nimble approach is beyond the capabilities of most organizations. What is more realistic is to consider deploying technologies and processes proactively to detect and mitigate the most common techniques, narrowing the effort based on the environment. For example, if the initial compromise is almost certainly going to be on network full of Windows hosts, implement detection capabilities for the “Initial Access” and “Exploitation” techniques relevant to Windows only.

3. Acalvio Support for ATT&CK

Acalvio solutions were designed to meet the challenge of post-compromise detection and response. When evaluated against ATT&CK, Acalvio ShadowPlex provides capabilities relevant to 7 of the 11 tactics in the framework. At a high level, Acalvio delivers

- Fast and accurate incident detection
- Adversary engagement and forensics
- Threat response to retard attack propagation

Like MITRE ATT&CK, Acalvio starts with the premise that attacks will be successful in penetrating the network. ShadowPlex is designed to find these compromises quickly, so that response measures can be executed before persistence and data exfiltration is achieved. It is well understood that most attacks go undetected for weeks or months, allowing the adversary to do significant damage before there is any response or mitigation. It is also well documented that most attacks do leave some form of forensic trail behind – the problem is that these clues are not obvious, and are drowned out in a sea of uncorrelated events and data. Acalvio solves this problem: events detected by ShadowPlex are

very likely related to actual attacks, because the platform assets serve no legitimate purpose. This enables the rapid response essential to execute effective response and mitigation. Implementing Acalvio protects key assets by containing and controlling the attacker early in the exploitation stages of the kill chain.

Acalvio deception-based detection is superior to alternative approaches such as behavioral analytics because it is both more accurate (few false positives) and more efficient and easier to deploy. Furthermore, what separates Acalvio from all other detection solutions is operational efficiency at scale. Legacy “Deception 1.0” honeypot solutions simply cannot be scaled or operated easily. Organizations do not have unlimited budgets for implementing cyber security, and the more efficiently they can deploy funds, the more effectively they can build a robust defensive architecture across their network.

The table below summarizes Acalvio’s support for the MITRE ATT&CK framework.

MITRE ATT&CK Tactic	Tactic Description	Acalvio Support
Persistence	Any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.	ShadowPlex Decoys get triggered at the slightest attempt by the adversary in their reconnaissance and discovery efforts. Thereby ShadowPlex detects their attempts to place assets required to persist in the enterprise environment. Lures attract attackers to deception assets, making it easier to detect attempts to establish persistence.
Privilege Escalation	The result of actions that allows an adversary to obtain a higher level of permissions on a system or network. Includes both highly privileged accounts, as well as any account needed for specific objectives during an attack.	ShadowPlex deploys fake privileged accounts in Active Directory as bait (honey tokens) to attract attackers seeking to escalate account privilege.
Defense Evasion	Techniques an adversary may use to evade detection or avoid other defenses. These may be applied at any phase of the overall attack.	ShadowPlex has an AI-based recommendation engine that ensures that the decoys are dynamic and refreshed. Consequently the decoys cannot be fingerprinted and thereby minimizes the possibility of Defenses being evaded.
Credential access	Techniques that result in access to or control over legitimate credentials, typically those with elevated privileges.	Acalvio Distributed Deception deploys decoys and honey tokens that attract attackers. When these assets are accessed using legitimate credentials, the solution identifies those credentials as compromised.
Discovery	Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network.	Discovery includes remote, network-based system discovery. ShadowPlex decoys obscure legitimate targets, and detect attempts by adversaries to discover assets to be compromised. Unlike alternative approaches, Acalvio achieves

		exceptionally low false positive rates.
Lateral Movement	Techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems.	ShadowPlex Fluid Deception deploys advanced decoys across the network, support by breadcrumbs to guide the attacker towards them. Attempts to access these assets provide clear indications of lateral movement activity, while Adversary Behavior Analytics models and records such techniques so that effective response can be quickly achieved.
Collection	Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.	Acalvio baits, or honeytokens, are deployed at scale by ShadowPlex as targets for collection. Attempts to access or copy such baits immediately identifies collection attempts, and the assets being used in the attempt

“ATT&CK can be used as a common behavior-focused adversary model to assess tools, monitoring, and mitigations of existing defenses within an organization’s enterprise”

MITRE ATT&CK™: Design and Philosophy, July 2018

“There are three conceptual ideas that are core to the philosophy behind ATT&CK:

- It maintains the adversary’s perspective;
- It follows real-world use of activity through empirical use examples;
- The level of abstraction is appropriate to bridge offensive action with possible defensive countermeasures.”

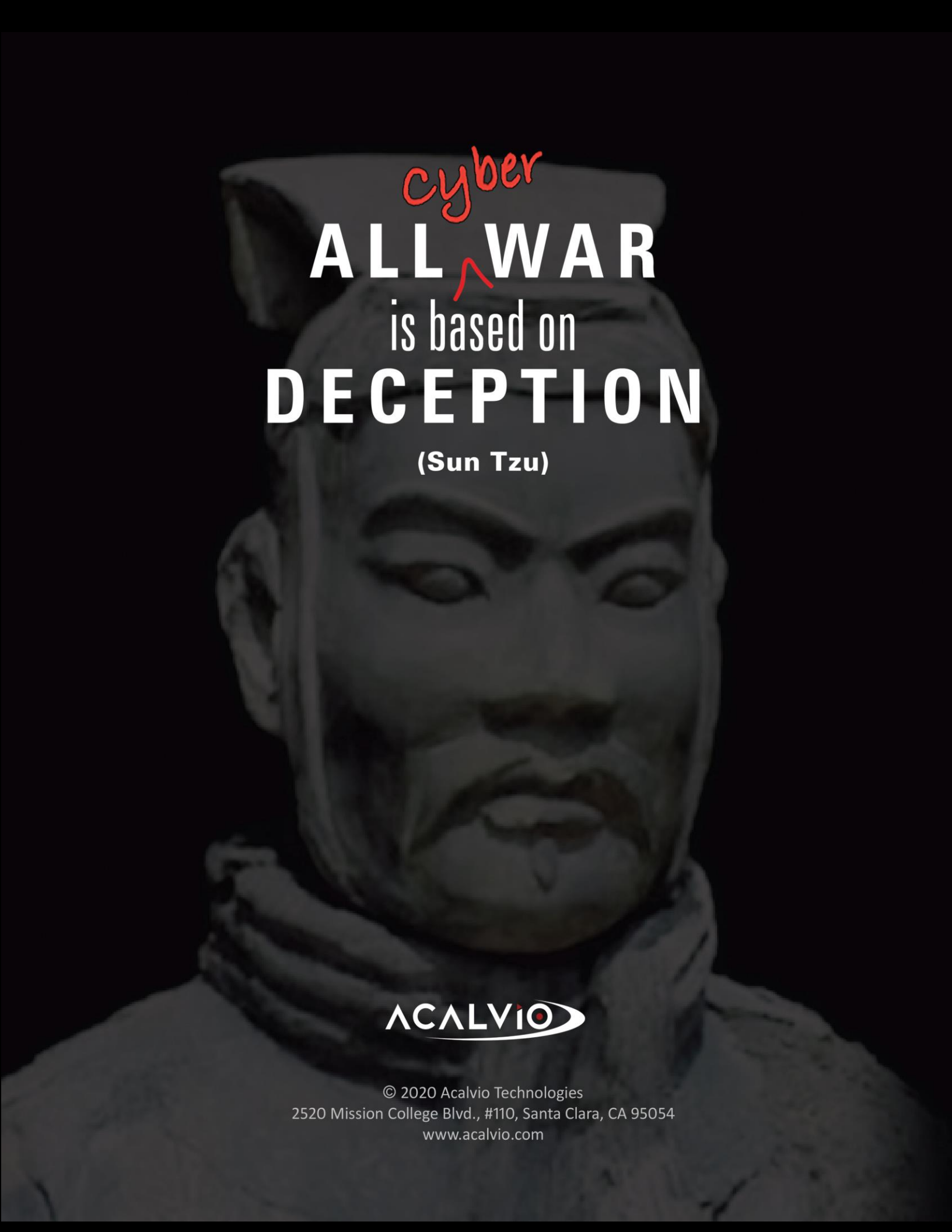
MITRE ATT&CK™: Design and Philosophy, July 2018

“ATT&CK’s use of an adversary’s perspective makes it easier to understand actions and potential countermeasures in context than it would from a purely defense perspective.”

MITRE ATT&CK™: Design and Philosophy, July 2018

“The activity described by ATT&CK is largely drawn from publicly reported incidents on suspected advanced persistent threat group behavior, which provides a grounding for the knowledge base so that it accurately portrays activity happening or likely to happen in the wild.”

MITRE ATT&CK™: Design and Philosophy, July 2018



cyber
ALL WAR
is based on
DECEPTION
(Sun Tzu)

ACALVIO

© 2020 Acalvio Technologies
2520 Mission College Blvd., #110, Santa Clara, CA 95054
www.acalvio.com