Fidelis Deception: There’s no other better trap for Attackers!

The art of deceiving enemies on the battlefield dates back to early history and continues to be firmly embedded in military doctrine. To defeat increasingly sophisticated and increasingly aggressive nation-state-sponsored actors, cybercriminals, and hacktivists, Fidelis Security® has applied the “art of deception” to the cyber battlefield (cyberspace).

Fidelis’ deception capabilities enable you to deceive attackers and lure them into a trap, improve your ability to detect and track their tactics, techniques, and procedures (TTPs), and confuse and delay attackers by providing them with a constantly changing set of deception decoys. Deployment of Fidelis Deception solution across the DoD and Intel communities is enabling our Nation’s cyber warriors to identify and block sophisticated attackers before the attackers can damage critical infrastructures and exfiltrate sensitive data. One of several ways we work to modernize the cyber security posture of the federal government.

Why Deception Is a Game-Changer for Cyber Defense

Deception technology is a critical component to enhancing your cybersecurity arsenal. Despite our best efforts, all systems remain susceptible to attack and compromise, so your team must move from a reactive posture to a proactive one in order to outperform your enemy and stop sophisticated attackers before significant damage can be done to your mission operations. But how do deception technologies address key security concerns – ***especially as computer and network security controls and strategies increasingly become the foundation of new military warfighting strategies?***

Typically, sophisticated adversaries perform reconnaissance to gain detailed knowledge of the environment before exploiting a vulnerability and gaining entry to the system. Once they gain their initial foothold, they will move laterally through the environment, take full control of critical systems, and then mount their attack – whether it be corrupting systems, encrypting data (ransomware), exfiltrating data, and/or denying or degrading critical mission operations.

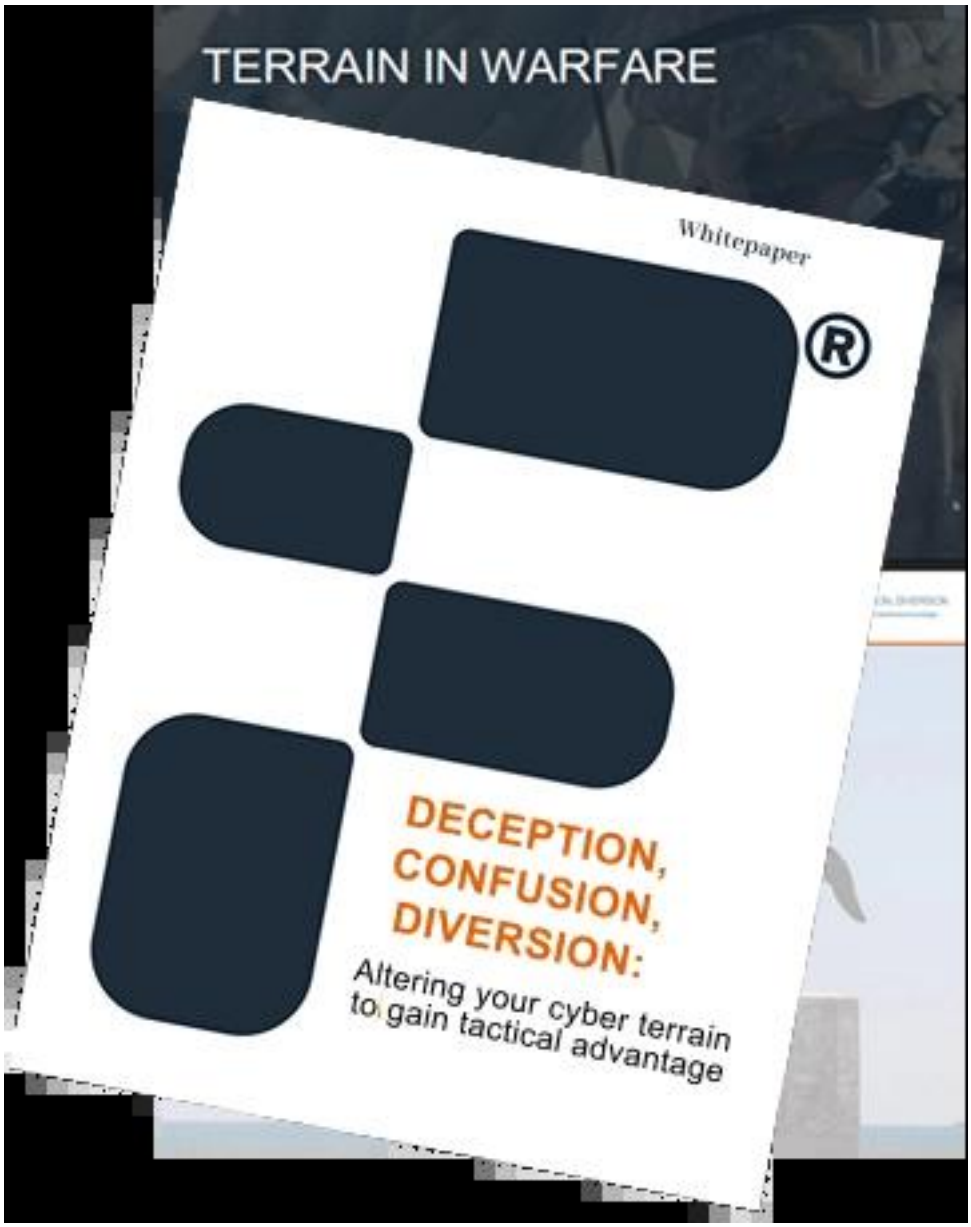
To combat this, it is critical to understand your environment as well as the attacker (know your cyber terrain), ensure that you understand the highest risk elements of your terrain and have put in place appropriate countermeasures to mitigate those risks, and have deployed an integrated set of detection and response capabilities that provide full coverage of your network environment.

Once this is in place, you are ready to deploy deception capabilities and enhance your ability to detect adversary Indicators of Compromise (IOCs) quickly and with higher confidence.

Altering your Cyber Terrain to Gain
Tactical Advantage

- Understanding your Cyber Terrain in Real-Time
- Identifying Blind Spots
- Computing the vulnerable Attack Surface

Download Now



Fidelis Decoys and Breadcrumbs: Leading Attackers Into the Trap

Fidelis makes this all easy for you with our Fidelis Elevate® platform that combines:

1. Fidelis Network®, our network detection and response (NDR) platform,

2. Fidelis Endpoint®, our endpoint detection and response (EDR) platform, and

3. Fidelis Deception®, advanced cyber deception technology for threat hunt.

One common security concern among DoD and Intel community teams is the fact that attackers can move undetected in your network. This is where Fidelis Deception's capabilities shine. With Deception, the first layer deployed is a set of decoys: decoys are emulated assets that are automatically created and deployed within your network to mimic the capabilities of real-world assets.

The decoys blend into your existing environment to intentionally make the devices in your network look vulnerable and open to a breach. To make each decoy authentic, it must mimic real assets in the network, which includes the domain it is registered to, the services it publishes, the ports it has opened, the file system it reveals, and the network traffic it exposes. The moment an attempt is made to communicate with these decoys, it sends off an alert to the analyst who becomes aware of an attacker on the network. Since there is no legitimate reason for users and systems to interact with decoys, alerts produced by decoys are almost certainly related to an ongoing attack and are treated as high-confidence alerts.

Fidelis Deception automates the process of creating, deploying, and managing decoys enabling you to spread many decoys around your networks to mimic the critical systems and services running within your network. Based on the government entity, hundreds or thousands of decoys can be deployed in the network, each with a different operating system and role.

To make decoys look real, Fidelis Deception assists your team in deploying breadcrumbs, which are pieces of information placed on real assets to lure attackers to the decoys. Breadcrumbs show usage of the decoy services by holding information and credentials for those services.

Examples of breadcrumbs include documents, configuration files, and credentials. Like decoys, breadcrumbs blend into the cyber environment and are created to be relevant to the asset and applications the breadcrumb is deployed to. Once again, Fidelis Deception automates much of the work to create, deploy, and manage breadcrumbs.

Another security concern is understanding an attacker's tactics, techniques and procedures (TTPs). Fidelis leverages the MITRE ATT&CK Framework®, which gives insight into cyber adversary behavior, to help guide your security teams in understanding an attacker's TTPs. With a deception tool, we can analyze the techniques used in real attacks and map these against attack techniques contained in the ATT&CK Framework. This provides security teams with important insights into the activities of their adversaries in the context of the MITRE ATT&CK Framework.

As a Cyber Warrior for the federal government, your mission is to detect and respond to cyber attackers before critical operations are degraded or denied. Our goal is to help you outperform, outmaneuver, and outfight your most advanced cyber adversaries to keep your critical mission operations safe.

Our award-winning Fidelis Deception technology gives you an opportunity to reduce cyber dwell time by altering the adversaries' perception of the attack surface. Doing so slows down the attacker's ability to move undetected, giving your cyber warriors the time to understand the tactics, techniques and protocols (TTPs) of the enemy and respond before damage to your mission operations is done.