Fidelis™ Cybersecurity

DATASHEET

Fidelis Deception Module

Change the Playing Field to Lure, Detect, and Defend

The Opportunity

Cybercriminals seek passwords and credentials to enter networks and applications in order to monitor and steal data. Capture the flag exercises highlight how human attackers analyze email, files, documents, and unstructured data for credentials, while automated malware mainly focuses on structured data in web browsers and apps. Passwords are a top priority for attackers to successfully enter and move within networks. Each successful step helps an attacker stay quiet, preventing digital "noise" that might otherwise give them away. *Knowing what attackers desire creates an opportunity for an active defense; to lure, detect, and defend.*

The Challenge

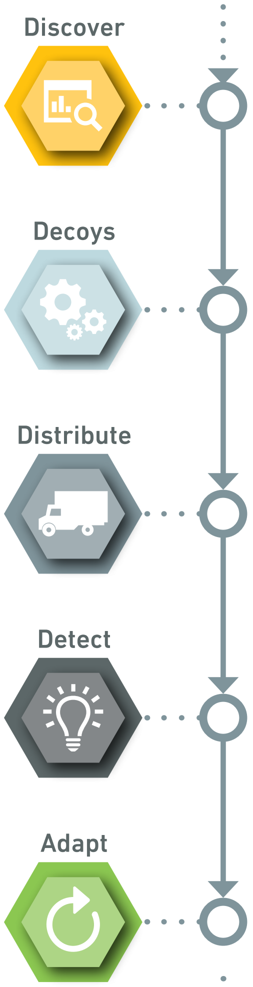
- Detect attackers and malware inside networks
- Deliver high fidelity alerts with few or no false positives
- Automate investigation and response
- Increase effectiveness and efficiency of security analysts
- Map kill chains to improve security defenses

The Solution

- Create a wide variety of realistic decoys and breadcrumbs
- Clone real assets, emulate services, OSs and automatically update them
- Decoys that run applications to engage attackers and consume time
- Detections created from decoy access, MITM (Man In the Middle), and traffic analysis
- Decoys hidden from actual users as unknown assets eliminating unintentional access

> "We found Fidelis deception to be very efficient. Its decoy aspect provided an excellent way to detect anomalies without having to sort through so much data as with other approaches."

Weston Nicolls, SVP, Information Security Manager, First Midwest Bank



Discover

- Perpetually maps network and assets
- Profiles created and updated for asset location, use, type, etc.
- **Result:** Unique foundation created for each decoy and deployment

Decoys

- Builds deception layer from discovery
- Automatically creates decoy network based on real assets, services, and processes
- **Result:** Realistic and persuasive decoy network

Distribute

- Automatically places decoys in networks
- Seeds breadcrumbs in real assets and Active Directory
- **Result:** Rapid deployment and immediate effectiveness

Detect

- Alerts from decoy access and engagement
- Analysis of poisoned data use (e.g. credentials)
- **Results:** Credible insider threat, credential spoofing, and lateral movement detection

Adapt

- Recognizes new assets and network topologies
- Automatic updates to discovery mapping and decoy network
- **Results:** Intelligent and adaptive deception defense

How Deception Works

Deception improves and becomes deterministic with breadcrumbs leading to decoys to lure attackers and automated malware known to scan hundreds of applications. Deception changes the playing field of security. Instead of searching in vain for the bad actor within an ocean of good data, deception delivers actionable alerts and events from decoys, MITM behavior, and traffic analysis. These have extremely high fidelity and few false positives. Fidelis Deception goes a step further and provides simulated access data including Active Directory entries and simulated enterprise resource access. This simulated access data creates a persuasive decoy network that includes devices, data, and behavior all designed to turn the tables on the attackers. They pursue the lures so you can detect, learn, and defend.

Decoy Profiles

- Hardware — laptops, servers, routers, switches, cameras, printers, enterprise IoT devices etc.
- Software — OS, apps, ports, services, applications, and similar data
- Decoys are unknown and obfuscated assets, no reason for employee access or use
- Consume attacker time and distract from real assets

Breadcrumb Profiles (Traps)

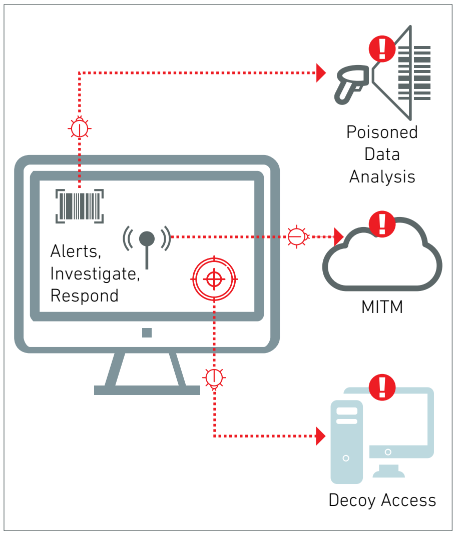
- Traps: file, application, network, or credential based
- Breadcrumbs: files, documents, email, or system resources, etc.
- Poisoned data, often credentials, profiles attacker use

Detection of Post-Breach Attacks

- Access of decoys as unknown assets (i.e. attackers, insiders)
- Data analysis showing the use of poisoned data (e.g. credentials)
- Monitoring attacker actions engaged with decoys and breadcrumbs
- Network analysis around decoys and data alerts

Intelligent Deception

- Automates and adapts deployment of decoys and breadcrumbs
- Detects lateral movement, C2 traffic, and data exfiltration
- Visibility and forensics to learn TTPs (tactics, techniques, and procedures) and desired assets
- One console with complete deception telemetry for analysis and hunting, and action
- No impact to operations or users, no risk to data or resources



High fidelity alerts with very few false positives

> "DDPs [Distributed Deception Platforms] give rise to a new type of detection capability, leveraging deception to rapidly enhance detection and response regardless of the evasiveness of an advanced attacker."

Gartner, Competitive Landscape: Distributed Deception Platforms, 2016, Lawrence Pingree, Refreshed: 26 December 2017 | Published: 04 August 2016, G00310123

Why Choose Fidelis?

Fidelis goes beyond honeypots and legacy decoys with intelligent deception that lures, confuses, and thwarts attackers and malware. Fidelis Deception helps security operations teams detect the hidden, learn new attacker techniques and defend critical data assets. The Fidelis Deception Module analyzes 'east-west' internal traffic while Fidelis Network provides unmatched analysis of 'north-south' egress traffic. Fidelis automates detection and response across networks and endpoints using our innovative set of purpose-built and integrated technologies. Fidelis empowers first level responders and helps advanced hunters to identify, investigate, validate, and respond to threats.

Contact Us Today to Learn More About Fidelis

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis is the industry's only completely integrated, automated network and endpoint detection and response platform. Fidelis improves the efficiency and effectiveness of security operations teams by condensing alert data into actionable threat summaries and then automating response and investigation actions instead of piling more alert data on already fatigued security staff. With automatic validation, investigation and prevention of attacks, Fidelis is engineered for visibility, designed for response and trusted by the most important brands in the world. See what you've been missing.