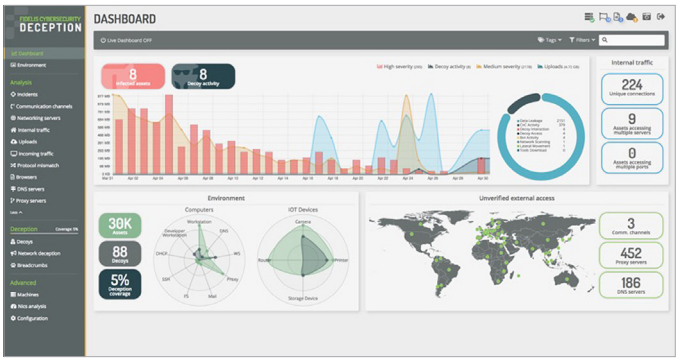
SC MEDIA
EMERGING PRODUCTS



Fidelis Cybersecurity

Fidelis Deception

Fidelis is a fresh player in this group, having recently integrated TopSpin's deception solution into its own security platform. Since this strategic acquisition in October 2017, the re-badged Fidelis Deception has seen a flurry of development activity and is already into its third product release phase. Automation has been the key development focus as the solution's network visibility utilities were previously established. These include the ability to analyze an organization's own network activity and conduct an asset inventory and profiling of all services.

The solution's deception process can be broken down into several phases. The first stage compiles an inventory of everything in the current environment including assets, OS, ports, services and data. Sometimes running this discovery scan can also shed light on other assets that were unknown previously, such as legacy systems or shadow IT. Profiles are created and updated accordingly. If an asset changes location post discovery, its location will update in the system since network discovery is running constantly.

Decoys are then automatically created from the discovery profiles, based on real assets, services and processes that currently exist in the scanned environment, and seated on a trunk port much like a VLAN, or automatically placed within targeted networks. Testing of decoys and advertising to the network confirms they are accessible and performing as their real counterparts would.

We were curious why other vendors use real OS decoys in the cloud while Fidelis Deception relies on emulation. The obvious answer is low risk and never exposing the operating system to prevent compromise. According to Fidelis there is no impact to operations when implementing the decoys via emulation, no high-level credentials are needed as opposed to non-emulation.

After testing, static breadcrumbs – structured and unstructured data – are rolled out and sit on real assets such as endpoints, servers, and desktops. Unstructured data is used by end users in a varied manner such as project files, emails, and office documents. Structured data is machine based. Once the attacker follows the breadcrumbs to the decoys, Fidelis sends out alerts. Because the environment is being continuously analyzed, automatic adaption occurs and reacts to network or machine changes, which in turn updates the discovery mapping, profiles, and the deception layer without any human intervention.

Once a deception alert initiates, the next step is to use an EDR which involves investigating the compromised decoy system thanks to the breadcrumbs. Fidelis points out that a deception net without a detection response is almost useless, as it is impossible to carry out an investigation and establish a forensic record. Fidelis is not just a deception vendor; they carry a few other products such as Fidelis Network, which is a breach detection and data loss prevention tool. They also offer Fidelis Endpoint, which features automated Endpoint Detection Response.

Fidelis Deception can run as software, on a VM, on a hardware appliance, or can be operated for the customer as a Managed Service option hosted by Fidelis Cybersecurity.

Licensing is handled as incremental VLANs, if there is an odd number Fidelis will discount appropriately. The basic price starts at $35,000 for decoys across 32 VLANs.

– Dan Cure

reviewed by: Michael Diehl & Matthew Hreben

DETAILS

Product Fidelis Deception

Vendor Fidelis Cybersecurity

Contact fidelissecurity.com

Price $35,000 for decoys across 32 VLANs.

What we liked Excellent EDR capabilities paired with a serious contender in the deception space.

Fidelis Cybersecurity

Contact Us:

1.800.652.4020

info@fidelissecurity.com

www.fidelissecurity.com