SC MEDIA First Look

AT A GLANCE

Product ThreatDefend™ Detection and Response Platform

Company Attivo Networks
attivonetworks.com

Price Starts at $35K

What it does Deception grid-enable incident response platform.

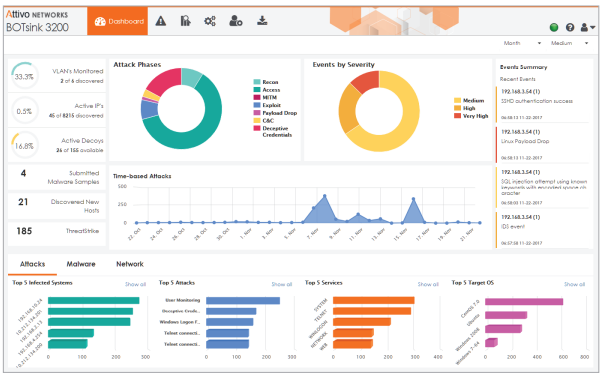
What we liked We really like the combination of deception and incident response – this is a lot of product for the money.

The bottom line For medium and large organizations, some form of incident response is a must. However, incident response is, by definition, reactive. ThreatDefend takes a lot of reactive elements out of the game because it is constantly misdirecting the attacker to harmless lures and decoys.

Attivo NETWORKS®

46601 Fremont Blvd.,
Fremont, CA 94538
https://attivonetworks.com
Phone: (510) 623-1000
Request a demo:
https://attivonetworks.com/request-demo/
Contact Us:
https://attivonetworks.com/contact/

Attivo Networks ThreatDefend™



We had intended to include Attivo Networks' ThreatDefend™ Detection and Response Platform in our deception networks group but after looking pretty closely at it we decided that it is quite a bit more than a deception grid. It is true, of course, that this system includes BOTsink, a deception tool that is both effective and well-known. But BOTsink is just part of the story. This is a full-featured incident response system.

The system is built around the Attivo deception and response platform, ThreatDefend. This consists of four pieces: BOTsink is the detection and analysis portion of the tool. It comprises the deception grid. The endpoint part of the deception is ThreatStrike. It provides honeycredentials and other deception bait at the endpoint. ThreatPath looks for vulnerabilities that would permit an attacker to succeed and provides this information in the form of work order tickets.

Finally, ThreatOps provides the incident response flow. It includes correlation and playbooks for managing an incident. It also generates work order tickets.

Deceptions are a big part of the system as one would expect. ThreatDefend provides operating system, network services, endpoint lures, and data and document deceptions. These are provided from the BOTsink Deception Server. The assumption is that any user on the enterprise who touches a deception lure likely is an intruder. The system then takes steps to contain the attempt and collect detailed forensics.

Decoys are the same, as far as the attacker knows, as the real enterprise assets. In part that is because lures are crafted from the organization's actual golden images. The tool is effective with typical enterprise systems and specialized systems such as SWIFT financial systems, and SCADA.

Attivo camouflage serves the same purpose as physical camouflage does. It makes the presence of the detection system invisible to the attacker. It uses the system's own golden images, learns the behavior of the network and acts accordingly, and builds new, believable, deceptions on the fly. That includes refreshing honeycredentials, evolves deception decoys and redeploying the deception grid after an event to keep the attacker from figuring out the deception grid.

One of the more important functions is to engage and prevent ransomware from getting a foothold on the enterprise. It starts by detecting the first stages of a ransomware attack. It immediately slows down the encryption, redirects it to the deception grid, engages with the ransomware by feeding it endless data – all of it bait – while it quarantines, collects forensics and starts alerting and rolling out quarantine measures. Using high interaction, ThreatDefend slows down the infection/encryption process by up to 25 times.

Administration is straightforward and you can use playbooks out of the box and, additionally, create your own. The administrator has full visibility of the network, the attacks and the deception grid. Lateral movement paths are identified rapidly and the tool alerts on new paths as they are created. Threat intelligence, kill chain analysis TTPs and reporting are just a few of the capabilities that the analyst has at his or her disposal. Forensics is equally strong and includes attacker memory. Reporting is strong and includes STIX, IoCs, Yara, C&C addresses and all of the action is captured in a pcap for further analysis.

ThreatDirect is a virtual machine forwarder that can be used for remote locations. It deploys deception locally It communicates directly with BOTsink.

The tool is priced attractively and is well-supported. Support, however, is an extra-cost item. The web site has a lot of useful information including white papers and webinars.

– Peter Stephenson, technology editor