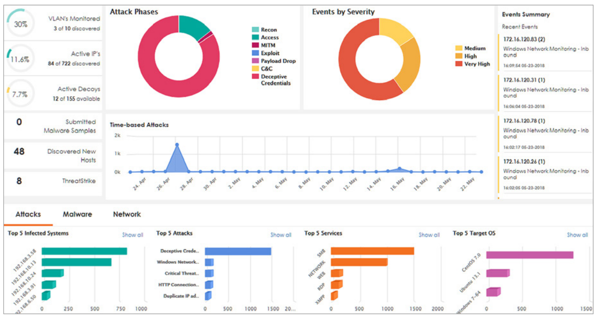

Attivo Networks

ThreatDefend

Attivo's ThreatDefend approaches deception at the platform level, a comprehensive collection of dynamic traps and lures that attract intruders to imitation networks, offsite connections, IoT-related endpoints, cloud applications and point of sale networks. The portfolio also includes endpoint deceptions that provide credential and file deceptions, along with visibility tools for identifying likely attack paths.

A new name to our roster this year, Attivo has operated within the space since 2015 and demonstrates exceptional vendor growth. Security professionals are clearly recognizing the promise offered by this additional layer of detection, with many new industry segments adapting the deception model to their discrete infrastructure landscapes. Savvy attackers will expect to interact within specific surfaces and endpoints. This could mean IoT-connected medical devices within a healthcare system or logic controllers in a manufacturing setting. Therefore, it is crucial to the deception to meet these expectations, as to draw in intruders ever deeper within the deceptive net.

The ThreatDefend platform sits on a trunk port and is scalable with up to 100 VLANs per box and an unlimited number of IPs that can be assigned dynamically. We are especially keen on the superbly thought-out Shuffle button, a practical utility that changes hosts names, MAC addresses, IP addresses and adjusts the number of endpoint decoys with the click of a button. The endpoint deceptions are agentless and provide extensive deployment options including group policy objects, SCCM, WMI, and endpoint vendor integrations. There's no need to build everything from scratch or manually change decoys or endpoint deceptions. The same ease of use applies when adding new components to your existing system. ThreatDefend can set alerts for any new real VLANs and endpoints for analysts to coordinate and build new parameters into the deception strategy.

However capable the detection-oriented functions of the platform, we should not ignore the requirements of gathering forensic information. Based on engagement with an adversary, ThreatDefend safely collects attacker TTPs, IOCs, and counterintelligence for insight into attacker capabilities, goals, and the information they are seeking to exfiltrate. This analysis is accomplished after detection when ThreatDefend is poised to grab malicious URLS and analyze pertinent details about the intruder's goals. Similar efforts involve extracting a payload and performing an initial analysis in order to capture the full attack's TCP scheme.

Concerns about identifying interactions with traps can be addressed by a convenient interface display which "plays out" actions on a timeline to better understand the interactions that have taken place. And when the decision is made to respond and handle an active intrusion, ThreatDefend is Incident Response capable and makes use of Attivo's C2 Engagement, Malware analysis, and repeatable playbooks known as ThreatOps. These responses involve initiating the forensic memory analysis and quarantining IP's in real-time, followed by IOC identification to accelerate remediation.

We find noteworthy the extensive third-party integrations through which the ThreatDefend platform shares indicators of compromise. Integrations with Playbook, cloud (i.e. Google Drive, Box) monitoring, and connectors to SIEM products speed up incident response times and opens up new avenues of strategies for how to remediate threats. Attivo partners with many leading platforms such as McAfee, Cisco, Check Point.

Pricing starts at an introductory $50K with add-on subscriptions for the platform's many added features.

– Dan Cure

reviewed by: Michael Diehl & Matthew Hreben

DETAILS

Product ThreatDefend Detection and Response Platform

Vendor Attivo Networks

Contact attivonetworks.com

Price $50,000

What we liked Well-polished platform; one of the more mature solutions we've seen in this space.

46601 Fremont Blvd.,
Fremont, CA, 94538
(510) 623-1000
https://attivonetworks.com