FEATURE HIGHLIGHT

Attivo NETWORKS®

THREATDEFEND PLATFORM: AUTHENTIC DECEPTION

OVERVIEW

At its core, deception technology relies on presenting an attacker with decoys and lures that are indistinguishable from real assets. The Attivo Networks® ThreatDefend® solution places a comprehensive range of high-fidelity decoy systems, services, credentials, and other assets, that cover both the endpoint and network aspects of an environment. This obfuscates the attack surface and confuses intruders, shifting the advantage from the attacker to the defender.

Highly authentic decoys are vital for any organization looking to add deception technology for in-network threat detection. This feature highlight addresses the importance of authenticity in deception and the ways in which Attivo Networks has made authenticity a core feature of the ThreatDefend platform.

AUTHENTIC DECEPTION

Deceiving an opponent into making a mistake and handing over the advantage is an ancient tactic, and authenticity is at the heart of any deception effort. Deception, for the purpose of misdirecting an opponent, is strategically used in military, hunting, gaming, and cybersecurity operations.

To effectively fool an attacker in the context of cybersecurity, deceptive assets must closely match the production asset configurations of both systems and endpoints. For example, decoy servers running the same live operating systems (Microsoft, Mac, Linux) and services found in the production environment are considerably more effective than simple emulation. They look real because they effectively are real.

On the endpoints, credentials, file shares, decoy documentation, and other deceptive assets must follow the same form and format as their live counterparts. By integrating with Active Directory, deceptive credentials become indistinguishable from live ones while leading an attacker into the deception environment rather than to a production asset. Hidden file shares mapped to decoy servers also lead into the deception environment, deflecting an attacker's actions away from production and wasting his resources.

The only way an attacker will be able to tell the difference between a real asset and a decoy is to engage with it, by which time it is too late. Once the attacker engages, the system immediately flags the event and the information security team can respond to a high-fidelity alert.

PRACTICAL USE

Attivo Networks® ThreatDefend® platform is a comprehensive deception system that creates a "hall of mirrors" effect throughout the environment both on endpoints and across the network. An attacker inside the environment will not be able to tell the difference between live production assets and the deceptive ones, making their task considerably more difficult, causing them to make mistakes, and shifting the advantage to the defender.

For example, user credentials, especially administrator credentials, are a high value target for most attackers. Deceptive credentials, integrated with the environment's Active Directory service, look and feel real on the endpoint and even authenticate with AD, but are in fact carefully crafted breadcrumbs that leads an attacker into the controlled deception environment. This level of authenticity is maintained across the rest of the lures and breadcrumbs that appear on the endpoint, including remote access credentials, file-server credentials, mapped shares, application credentials, cloud credentials, and cloud access keys.

Across the network, decoy systems appear and respond identically to production assets. The ThreatDefend platform incorporates a machine learning capability that analyzes the environment, automatically creating decoys that match the operating systems and services seen on the production servers and workstations. The decoys can be further customized to meet the organization's needs, including creating decoys based on gold disk images that exactly match production systems. By utilizing the same operating systems and services the decoys appear authentic – because they are authentic. Beyond the perimeter, deception extends to the cloud with such things as decoy S3 buckets and serverless lambda functions.

A common misconception is that there is a trade-off for achieving optimal believability in deception. This is actually not true since machine-learning completely automates the process and because the ThreatDefend technology is designed to project the deceptions, negating the need to manage separate operating systems and applications on each decoy device. It is truly no more difficult, and some may argue, easier to maintain an attractive and authentic environment as it is an emulated environment.

With deception in place, even simple reconnaissance will trigger alerts while the attacker is unable to determine which systems and services are real and which are decoys. By accurately matching the production environment it becomes extremely difficult for an attacker to choose a target and engage without risking early discovery.

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide variety of specialized attack surfaces. The portfolio includes expansive network, endpoint, application, and data deceptions designed to efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 65 awards for its technology innovation and leadership.