CASE STUDY

FINANCIAL INSTITUTION THWARTS PENETRATION TEST WITH DECEPTION

COMPANY

A hedge fund institution.

SITUATION

The team needed to prove that their network was secure and that they could reliably detect threats by succeeding in a Red Team test that they had previously failed multiple times.

SOLUTION

They installed the Attivo ThreatDefend® Deception and Response Platform, gaining visibility into threats and their lateral movement within the network. The platform successfully detected the Red Team and deceived them into engaging.

OVERVIEW

This organization operated under an "assumed breach posture," meaning that the Infosec team positioned their security infrastructure assuming that threats are within the network and that they must proactively seek out infections to prevent full breaches from occurring. With a security strategy of overlapping detection and prevention security controls, the team needed a solution that would provide an early warning system to generate high-fidelity alerts for suspicious network activity. With time as the most critical resource during a cyberattack, the team knew that an effective warning system would grant the visibility and early awareness to react to a threat as soon as possible and to derail its success.

CHALLENGE

The challenge facing the Infosec team was that, like many security professionals, the volume of alerts generated by their current solutions was not only overwhelming but significantly increased the chances of something malicious slipping through unnoticed. The team was spending most of their time analyzing alerts rather than responding to and remediating threats in their network and thus could only react to attacks once they were well underway. The team recognized that they needed an accurate and efficient solution that could detect attacks from all vectors and cut through the noise to reduce false positives and generate only high-fidelity alerts.

SOLUTION

The organization implemented the ThreatDefend Deception and Response Platform throughout its network and installed the ThreatStrike endpoint deception suite's deceptive credentials on its endpoints. The solution provided high-quality alerts so that the team could focus their resources on proactively addressing threats, rather than reactively. They also used the ThreatDefend platform to demonstrate the security of their network with its ability to detect and shut down attacks.

ROI

To validate the effectiveness and show the benefits of the ThreatDefend platform, the organization initiated a Red Team assessment. They had failed these tests multiple times and the security operations team needed to demonstrate improvement in their security infrastructure through positive results from the evaluation.

The Red Team started by stealing what they thought were authentic credentials from an endpoint and used those credentials to move laterally throughout the network until they accessed what they believed to be critical assets. What the Red Team didn't know was that the credentials they stole were the ThreatStrike suite deceptive credentials and the assets they accessed were decoys.

The Red Team also was unaware that the ThreatDefend Platform captured all of its activities and movements throughout the entire process. In the end, none of the information that the Red Team accessed was real and the deceptive credentials effectively diverted the attack.

By having the ThreatDefend deception platform installed in its network, the organization thwarted the Red Team and passed the penetration test with flying colors.

The results of the penetration test highlighted deception as an invisible and unexpected layer of security for criminals looking to exploit organizations.

> The solution was able to provide high quality alerts so that the team could focus their resources on proactively addressing threats, rather than reactively.

With their deception deployment, the Infosec team gained not only visibility into their network that they did not have prior, but they can now operate with the confidence that they can detect and deceive advanced threats inside their network before it can compromise their critical assets.

The ThreatDefend platform empowers the organization with the visibility to monitor its network continuously for abnormal activity. Once they installed the solution, they could pinpoint misconfigurations in the network and, more importantly, better identify unusual activity that could indicate a threat. This capability significantly reduces the time it takes for the team to identify and remediate threats, better protecting their critical assets.

OUTCOME

After passing the Red Team assessment, the financial institution continues to maintain the ThreatDefend platform throughout its entire network to gain visibility into in-network threats and protect ifself from stolen credential and phishing attacks.

ATTIVO PRODUCTS

The Attivo ThreatDefend Deception and Response Platform with multiple BOTsink deception servers.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 130+ awards for its technology innovation and leadership.
Learn more: www.attivonetworks.com