Financial Institution Thwarts Penetration Test with Deception

Company	Situation	Solution
A hedge fund institution.	The team needed to prove that their network was secure and that they could reliably detect threats by passing a Red Team penetration test that they had previously failed multiple times.	The Attivo ThreatDefend™ Deception and Response Platform was installed, providing 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 operates under the "assumed breach posture", meaning that the infosec team positioned their security infrastructure with the assumption that threats are within the network and that they need to proactively seek out infections and prevent full on breaches from ever occuring. With detection added to their prevention security posture, the team needed a solution that would provide an early warning system that would generate high-fidelity alerts for suspicious network activity. With time as the most critical resource during a cyberattack, the team knew an effective warning system would grant the visibility 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 devices was not only overwhelming, but almost guaranteed that something malicious would slip through unnoticed. The impact to the team was that they were spending the majority of their time analyzing alerts rather than remediating threats in their system and thus were forced into being reactive to attacks once they were well underway. They recognized that they needed an accurate and efficient solution to detect attacks from all vectors and the ability to cut through the noise and generate only high-integrity alerts with zero false positives.

Solution

The team implemented the ThreatDefend Deception and Response Platform throughout their network and installed the ThreatStrike deceptive credentials on their endpoints. The solution was able to provide high quality alerts so that the team could focus their resources on proactively addressing threats, rather than reactively. They were also able to use the ThreatDefend platform to demonstrate the security of their network and ability to detect and shut down attacks.

ROI

To understand the full return on investment of the Deception Platform, the organization initiated a Red Team penetration assessment. They had failed these tests multiple times and it was critical for the security operations team to demonstrate improvement in their security infrastructure and results.

The red team started by stealing what they thought were authentic credentials off of an endpoint solution and used those credentials to move laterally throughout their system until they were able to access what they believed to be critical assets. What the red team didn't know was that the credentials that they used were the ThreatStrike deceptive credentials and the critical assets they found were deceptive assets. The team also was unaware that the ThreatDefend Platform captured all of their tactics and movements through the entire process. In the end, none of the information that the red team gained access to was real and the deceptive credentials effectively diverted the attack.

By having the ThreatDefend Deception Platform installed in their network, the organization was able to thwart the red team and pass the penetration test with flying colors. The results of the penetration test highlight deception as an invisible and unexpected layer of security for cyber criminals looking to exploit organizations.

With their investment, the infosec team now not only has visibility into their network that was previously unachievable, they also can operate with the confidence that they can detect and deceive advanced threats inside of their network before their critical assets are compromised.

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

The ThreatDefend platform empowers the infosec team with the visibility to monitor their network on a continuous basis to see what types of activity are normal. Once installed, they were able to pinpoint misconfigurations in their network and, more importantly, better identify unusual activity that could indicate a threat. This significantly reduces the time it takes for the team to identify and remediate threats in their network, better protecting their critical assets.

Outcome

After passing the penetration test, the financial institution continues to maintain the ThreatDefend Platform throughout their entire network in order to gain visibility into in-network threats and protect themselves from stolen credential and phishing attacks.

Attivo Products

ThreatDefend Deception and Response Platform and ThreatStrike deceptive credentials.

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com