Aflac, Inc. Uses Deception for Zero-False-Positives Threat Detection

Company	Situation	Solution
Aflac, Inc. a Fortune 500 insurance provider.	With an ever-changing threat landscape, Aflac needed a solution that provided early and accurate threat detection of cyber attackers.	The team deployed the ThreatDefend™ Deception and Response Platform to detect in-network threats with zero false positives and to identify any misconfigurations in their network.

Overview

The organization has a very mature security posture and has implemented high-end cyber security technology into their network. But their main concern was that with the rate that threats were changing, becoming stronger, and more invasive, there was a gap in their ability to early and accurately detect threats that were inside their network. Even with high-end prevention devices and practices, they knew that they could not quickly detect new and emerging threats as they penetrated their network.

Challenge

The infosec team saw the ever-changing landscape of threats as the biggest challenge that faced their organization. The threats were everywhere. And with a gap in their ability to detect new strains of attacks, the organization needed a device that was able to catch zero-day and signatureless threats. Additionally, the team found devices that generated a lot of alarms and whistles to be very distracting because of the rate of false positives that were produced – so much so that they were determined to find a solution that generated zero false positives. They didn't need more alerts, they needed quality alerts.

Solution

The infosec team chose the ThreatDefend Deception and Response Platform because it allowed them the ability to detect threats inside their network that other technologies missed entirely. Moreover, the level of camouflage that deception technology employs as well as the ability to mimic the hygiene of the network provided complete authenticity – meaning an attacker would not be able to tell the difference between the deceptive assets and the organization's critical assets. Additionally, the team is using the ThreatDefend solution as a means for early detection of ransomware attacks.

The team deployed the ThreatDefend Deception Platform throughout their network and assigned ThreatStrike deceptive credentials to their endpoints in order to detect the threats that were inside their network as well as any misconfigurations that might be present.

To test the full detection capabilities of the ThreatDefend, they hired a white hat hacker to run a penetration test on their network. The hacker spent over two hours trying to hack the web services of a decoy system placed in the network. The infosec team caught him very early on and was able to quarantine him and study his attack methods throughout the entire penetration test. By diverting the hacker, the ThreatDefend Solution protected all of the organizations critical assets.

ROI

By deploying the ThreatDefend Deception Platform throughout their network, the team achieved their goal of no false positives and only high-integrity alerts. This greatly reduces the amount of "noise" their team needs to respond to given that they are not chasing dead ends that other devices generate.

Having Attivo brings a significant peace of mind that we would detect somebody in the environment.

Furthermore, the team can be fully confident that the threats that penetrate their network will not only be detected quickly, but also will be diverted away from their critical assets and be quarantined for detailed attack forensics.

Lastly, the ThreatDefend platform identifies any misconfigurations that are present in the organization's network. This allows them to patch any areas that are especially susceptible to attackers, greatly strengthening their ability to prevent attacks in the future.

Outcome

The ThreatDefend Platform is operationalized and fully integrated into their threat intelligence system. The ThreatDefend takes new information it gathers on threats and feeds it into their overall threat intelligence system, allowing the threat management team to use the information for their hunting efforts. The detailed information provided by the ThreatDefend is also used in conjunction with the organization's correlation engine and used for overall risk profiling.

Attivo Products

Attivo Networks ThreatDefend Deception and Response Platform.

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