CASE STUDY

AFLAC, INC. ACHIEVES ZERO-FALSE-POSITIVES THREAT DETECTION

COMPANY

Aflac, Inc. a Fortune 500 insurance provider.

SITUATION

With an ever-changing threat landscape, Aflac needed a solution that provided early and accurate threat detection of cyber attackers.

SOLUTION

The team deployed the ThreatDefend® Platform to detect in-network threats with zero false positives and to identify any misconfigurations in their network.

BACKGROUND

The organization had established a very mature security posture, with high-end cyber security technology implemented in their network. But faced with rapidly changing, stronger and more invasive threats, the team was concerned about their ability to accurately detect threats inside their networks early enough in the process. 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 threat landscape as their biggest challenge. With a gap in their ability to detect new strains of attacks, the team needed a solution to catch zero-day and signatureless threats. Additionally, the team wanted to avoid devices that generated numerous alarms and whistles, as they were highly distracting due to the rate of false positives. This prompting the team to look for a solution that provided high quality alerts with zero false positives.

SOLUTION

The infosec team chose the ThreatDefend® Platform because it allowed them the ability to detect threats inside their network that other technologies missed entirely. Moreover, the solution's level of camouflage and ability to mimic the network hygiene provided complete authenticity – derailing an attacker's ability to distinguish between the deceptive assets and the organization's actual critical assets.

The team deployed the ThreatDefend® Platform throughout their network and assigned ThreatStrike® deceptive credentials to their endpoints 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® Platform, the team hired a white hat hacker to run a penetration test on their network. The hacker spent over two hours trying to infiltrate the web services of a decoy system placed in the network. The infosec team caught and quarantined the hacker very early in the process, and studied the attack methods throughout the entire penetration test. By diverting the hacker, the solution protected all the organization's critical assets.

© 2021 Attivo Networks. All rights reserved.

ROI

By deploying the ThreatDefend® Platform throughout their network, the team achieved their goal of only high-integrity alerts with no false positives. 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. Additionally, the team is now using the ThreatDefend® solution for early detection of ransomware attacks.

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.

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

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 solution 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® Platform is also used in conjunction with the organization's correlation engine and used for overall risk profiling.

ATTIVO PRODUCTS

Attivo Networks ThreatDefend® Platform.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Attivo has 150+ awards for technology innovation and leadership.

www.attivonetworks.com.

© 2021 Attivo Networks. All rights reserved.