CASE STUDY

REGIONAL BANK SELECTS ATTIVO NETWORKS® DECEPTION TECHNOLOGY TO CLOSE DETECTION GAPS

COMPANY PROFILE: REGIONAL COMMERCIAL FINANCIAL INSTITUTION SPANNING FIVE US STATES.

Situation

The organization uncovered gaps in their detection capabilities during a penetration test and wanted to close the gaps without straining their information security resources.

Attivo Deployment

Working with an Attivo Networks® partner, this regional bank chose to deploy the full range of the ThreatDefend™ platform's threat deception capabilities. This gave them the visibility they needed and allowed them to provide deception capabilities efficiently into their branch locations.

Working with an Attivo Networks® partner, this regional bank chose to deploy the full range of the ThreatDefend™ platform's threat deception capabilities. This gave them the visibility they needed and allowed them to provide deception capabilities efficiently into their branch locations.

OVERVIEW

Penetration testing conducted by a 3rd party red team revealed security gaps in several areas of detection and visibility. The financial institution wanted to improve their detection and response capabilities against insider threats, Man in the Middle (MitM) attacks, and adversary internal reconnaissance. The organization decided to pilot the ThreatDefend platform in their production environment and planned to roll deception out to their entire infrastructure pending the results of the pilot program. Following a successful pilot, the Information Security team saw immense value in the solution and chose to move forward with a full, enterprise-wide deployment the following fiscal year.

CHALLENGE

The organization had a small Information Security team with limited resources, which required tools that met their needs without adding to their workload. Ideally, they wanted to reduce the time it took to detect an attacker, leverage automation to improve their efficiency, gather improved forensic information, and streamline incident response. Any new solution was also required to efficiently scale to meet the security and limited staffing needs of their remote branch offices.

SOLUTION

The Attivo Networks ThreatDefend platform satisfied all of their requirements to provide visibility and insight into threats that had bypassed their perimeter defenses. Additionally, by leveraging the platform's automated attack correlation features and native integrations, they were able to generate high-fidelity alerts, concise reporting, and automated incident response actions to drastically improve their capabilities with minimal impact on their resources . The organization started with a staged rollout that included a production-scale pilot and then moved into an enterprise-wide deployment.

ROI

The organization saw immediate improvements in asset visibility, including exposed credential vulnerabilities with the ThreatPath® visualization tool. The security team also found the deployment to be so intuitive and easy to use that they were able to successfully deploy decoys before the scheduled Attivo Networks Customer Care Team arrived to assist.

OUTCOME

After a successful deployment, the Information Security team saw major improvements in visibility and detection and were able to easily fit the ThreatDefend solution into their existing security architecture. After this initial success, the organization chose to move forward and budget for a full enterprise-wide deployment in the following fiscal year. In full production, they expect the system's accurate alerts to reduce their mean time-to-detection, and forensic information from the deception environment to provide valuable information for remediation.

ATTIVO NETWORKS PRODUCTS

The organization chose the ThreatDefend platform in its entirety, including BOTsink® as the foundation, ThreatStrike® to provide endpoints deception with deceptive credentials and other lures, ThreatDirect™, allowing them to efficiently extend decoys into branch offices, and ThreatPath to identify potential attack path routes of compromise in their environment.

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 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 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 for accelerated incident response. Attivo has won over 65 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com

[1] Attivo Networks customers have reported needing as little as 1/20th of an FTE to manage an Attivo deployment.