CASE STUDY

CASE STUDY: LEADING MULTI-COUNTRY BANK CHOOSES ATTIVO NETWORKS DECEPTION TECHNOLOGY

ORGANIZATION

A leading financial institution in the META region.

SITUATION

As a well-recognized financial institution with branches in several countries in the META region, this organization had to meet a range of regulatory requirements imposed by the countries they operated in. The Information Security manager worked with the Attivo Networks® ThreatDefend™ Platform at another financial institution in the region and, upon starting this new position, spoke of the value deception brought to their past security team and suggested this organization look into it.

Detecting lateral movement was a primary concern as was protecting their SWIFT system from attacks. On the recommendation of their InfoSec manager, the organization invited Attivo Networks to perform a Proof of Concept in their environment to show the efficacy of the ThreatDefend solution.

The local representatives performed a highly successful Proof of Concept which included attack simulations against the environment. The POC effectively demonstrated the value the Attivo Networks ThreatDefend platform has to offer and elevated the solution from a “nice to have” option to a “must have” component in their security stack.

SOLUTION

The Attivo Networks® ThreatDefend™ platform delivered a high-powered solution that the bank needed to defend their assets across an environment spread through several countries. Deception technology turned the environment into a virtual minefield of lures and traps that is effective against both live threat actors and their automated tools, delivering high fidelity alerts based on verified activity. Additionally, integration with the rest of their security stack gave the cybersecurity team a force multiplier to make them more effective and efficient without increasing their workload.

ATTIVO NETWORKS PRODUCTS

The installation started with an Attivo BOTsink server deployed as a physical appliance. The BOTsink server acts as the hub and central control for Attivo's deception technology. Visibility into remote offices was a primary concern, so this organization deployed multiple instances of the ThreatDirect solution to securely project deception from their BOTsink server into those sites across the region. For endpoint defense, the bank deployed the ThreatStrike® solution to place deceptive credentials and other assets on each of over twenty-five hundred workstations and servers across their organization. Additionally, the ThreatPath® solution gave them the tools to identify orphaned and misconfigured credentials and display potential paths an attacker could use to traverse the network, augmenting their endpoint defense with tools they did not get from other solutions.

IMMEDIATE VALUE

The bank conducted active testing during the Proof of Concept (POC) phase demonstrating the ThreatDefend platform's effectiveness in a real-world deployment. The Attivo solution was able to close the gaps they had in their existing security stack and the demonstration gave them the confidence to fund a full deployment covering their entire production 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 offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 90 awards for its technology innovation and leadership.

www.attivonetworks.com