CASE STUDY

MAJOR ENERGY PROVIDER CHOOSES DECEPTION TECHNOLOGY TO BETTER PROTECT CRITICAL ASSETS

Company Profile

A Large Public Energy Utility Company

Situation

Information Security management believed existing defenses provided inadequate detection and reporting capability in the event of a compromise.

Attivo Deployment

The ThreatDefend™ Deception Platform provides visibility into misconfigurations, early detection of threats, and actionable alerts for efficient incident response.

OVERVIEW

The Director of Cybersecurity for a large public energy utility organization had confidence in their perimeter security, but realized they needed better visibility into their internal network in the event of a compromise or when facing an insider threat. They chose to take a proactive approach with a full Defense in Depth posture. After extensive research, the Director decided to implement a layer of deception to detect and slow attackers that made it past the perimeter.

CHALLENGE

Existing perimeter defenses were not providing adequate visibility into the organization's complex network environment. Their environment was diverse, with systems and topologies unique to their business, such as SCADA systems and the typical user and datacenter spaces. Any solution needed to scale and be able to detect intruders in this diverse environment without adding excessive workload to the Information Security team.

SOLUTION

The organization chose to implement the Attivo Networks® ThreatDefend™ platform, including BOTsink, and Attivo Central Manager systems, to gain deeper and more comprehensive visibility into their network environment. The ability to clearly detect a breach and thwart an attacker early in the attack cycle were major driving forces behind their adoption of the Attivo solution. They are planning to add ThreatStrike and other ThreatDefend™ components in the future to further expand their active defense capabilities.

ROI

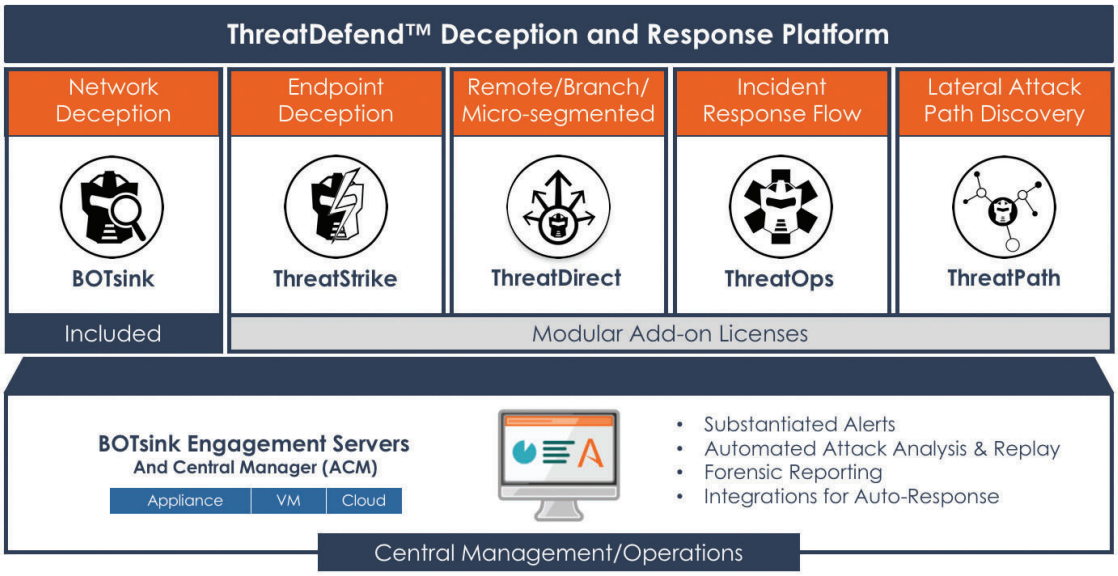
The Director had done extensive research and determined that implementing deception technology would be the most efficient and cost-effective way to add the detection capabilities they required. Once deployed they very quickly discovered some misconfigurations and other issues in their environment, giving an almost immediate return on investment. Further, the Attivo Networks® solution required no additional staffing. The organization found that their existing security team could easily deploy and maintain the solution without impacting their normal responsibilities, and integration with their existing security infrastructure gave improved visibility with minimal overhead.

OUTCOME

The organization added deception proactively to improve visibility and threat response capabilities, rather than in response to a security incident, putting them ahead of the curve. The Attivo Networks® ThreatDefend™ platform includes native integrations with 3rd party security applications, enabling the organization to seamlessly mesh deception into their existing security infrastructure, feeding their SIEM and ticketing systems directly, improving efficiency and effectiveness. The system has quickly identified existing misconfigurations and proven to be very effective in testing, leaving the organization confident they will be able to detect, and respond to, a sophisticated attack or insider threat.

ATTIVO NETWORKS PRODUCTS

The organization selected the full range of Attivo Networks® ThreatDefend™ products including BOTsink, and Attivo Central Manager, allowing the company centralized control and management in a single system.



ABOUT ATTIVO NETWORKS

Attivo Networks® is the leader in dynamic deception technology for the real-time detection, analysis and forensics of cyber-attacks. The Attivo Deception Platform provides inside-the-network threat detection for user networks, data centers, clouds, and ICS-SCADA environments. Not reliant on known signatures or attack patterns, Attivo uses high-interaction deception techniques based on Attivo BOTsink® engagement servers to lure attackers into revealing themselves. Combined with the Attivo Endpoint Deception Suite, advanced luring technology is deployed to detect the use of stolen credentials, ransomware, and targeted attacks. Comprehensive attack analysis and forensics provide actionable alerts and can be set to automatically block and quarantine attacks for accelerated incident response. For more information, visit www.attivonetworks.com.