CASE STUDY

STATE UNIVERSITY SYSTEM CHOOSES DECEPTION FOR ENHANCED DETECTION AND INCIDENT RESPONSE

ORGANIZATION

A multi-campus state university environment.

SITUATION

Like many educational institutions, the university had to protect a diverse and dynamic environment from a broad range of threats. Compounding the challenge was the variety of specific infrastructures, information, and regulatory requirements governing each section of their network and the data contained therein. Academic research environments, student-accessible networks, and university administration networks each presented different challenges they needed to address without adding an undue burden to the information security team.

SOLUTION

The Attivo Networks® ThreatDefend™ platform delivered the versatility and efficiency the university needed to address their varied security challenges without straining their available resources. Deception technology proved an ideal fit into the university's multiple environments.

OVERVIEW

The University had a moderately sophisticated cybersecurity infrastructure, but the director of Information Security recognized some gaps in their defenses and that their limited resources were getting overtaxed in their ability to respond to all alerts. For example, the size and breadth of their various environments made it difficult to gain visibility throughout the entire network across multiple campuses. With the vast and dynamic user base typical of a state university system, the threat of misused and stolen credentials was a significant concern, as was the potential loss of both intellectual property and personal records. Ransomware and related malware that could spread rapidly through the environment could potentially cause significant damage. Additionally, having the ability to automate incident response would enable a small information security team to respond quickly and efficiently, acting as a force multiplier, while improved forensic analysis tools would give them the data needed to mitigate future attacks.

© 2019 Attivo Networks. All rights reserved.

CHALLENGE

Accurate and easy to manage detection in an exceptionally diverse infrastructure, with assets distributed across multiple campuses state-wide, presented several distinct problems. The organization needed a solution that was effective against a broad range of threats, could quickly adapt to a changing threat landscape and evolving attack techniques, would be easy to deploy and manage even in remote locations, and would not unduly increase their information security team's workload.

SOLUTION

The university selected the Attivo Networks® ThreatDefend™ platform for high-fidelity detection and to enable a more active approach to defending their environment. The platform offered many components that addressed their current needs and that could scale to cover additional use cases. The BOTsink® server deploys decoys and hosts the analysis capabilities, while the ThreatDirect™ solution projects decoys into remote sites across the state's university system for scalability. The ThreatStrike® solution places deception credentials and other assets on the endpoints, and the ThreatPath solution identifies orphaned or misconfigured credentials an attacker could leverage to traverse the Active Directory environments. In total, the ThreatDefend platform was able to deliver a comprehensive solution that met all the university's detection and visibility requirements.

While a multi-campus multi-environment deployment at this scale is a substantial undertaking, the university was able to leverage the ThreatDefend platform's machine learning capabilities to make the installation fast, efficient, and painless. They deployed in under a week and minimal resources for ongoing management. The included automation features simplified preparation, deployment, and ongoing operations while maintaining environmental authenticity that made deception a successful tool to divert attackers away from production assets.

ROI

The Director of Information Security selected the ThreatDefend platform from several options after determining that it would provide the most efficient and effective platform for meeting their needs. The scalability and ease of deployment, use, and maintenance made the ThreatDefend platform an excellent fit for the university's environment. Additionally, the reliable, accurate, and actionable alerts and forensic capabilities served as a force multiplier to improve the information security team's efficiency and effectiveness.

OUTCOME

The university successfully implemented deception technology to address a range of use cases including enhanced threat visibility, protecting research assets and intellectual property, interrupting attacker lateral movement, identifying and thwarting credential theft and misuse, automated incident response, and improved threat analysis.

© 2019 Attivo Networks. All rights reserved.

The university demonstrated that the ThreatDefend platform is easy to deploy and maintain at scale, requiring less than 1/20 FTE (Full Time Employee equivalent) in their environment. Additionally, the solution provided insight into activity at the network and endpoints with high-fidelity, accurate alerts, including identifying attacks against laboratory equipment. Deception technology has given them "eyes inside the network" visibility they had not received from other solutions. The ability to gather adversary threat intelligence was also a powerful tool that enabled them to fortify their defenses.

> "Before we had Attivo we would be spending 4-6 hours dealing with one event, but now with Attivo its about 5-10 minutes for us to understand what is going on."
>
> – Director of Cybersecurity at multi-campus state university

ATTIVO NETWORKS PRODUCTS

The university had a broad range of requirements starting with visibility and thwarting lateral movement, but also needed to add forensics capabilities and prevent credential theft. The installation started with BOTsink® servers to provide decoys, ThreatDirect™ to allow them to project decoys seamlessly into remote locations, ThreatStrike™ to place deception credentials and other deceptive assets on endpoints throughout the organization, and ThreatPath to identify and help remediate misconfigured or orphaned credentials that an attacker could use to traverse the 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 85 awards for its technology innovation and leadership.

www.attivonetworks.com

© 2019 Attivo Networks. All rights reserved.