CASE STUDY

Attivo NETWORKS®

PROFESSIONAL SPORTS ORGANIZATION PROTECTS CRITICAL INFRASTRUCTURE WITH DECEPTION TECHNOLOGY

COMPANY

A professional sports organization

SITUATION

The organization needed visibility into its ICS-SCADA network to ensure that there would be no network interference during major events.

SOLUTION

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

OVERVIEW

A professional sports organization had significant cybersecurity concerns about an upcoming large sporting event. They needed more visibility into their network and substantiated, actionable alerts when an attack bypassed their perimeter defenses. The Infosec team did not have the time (since the event televises live) nor resources for another security solution that generates a large volume of detections and sends them chasing after false-positive alerts.

CHALLENGE

The organization was mainly concerned about security threats to its ICS network. In particular, the Infosec team was most apprehensive about an attack that could work to shut down and lock their ICS systems – putting people in danger and potentially causing severe bodily harm. They did not have the resources (headcount, budget, infrastructure) to deploy and maintain a wide array of prevention tools to protect their network from outside threats. Additionally, ICS devices lack simple methods for patching or could run antivirus solutions. They needed to know exactly where the weaknesses in their network were so that they could focus their resources on fixing the specific areas that needed their attention. Furthermore, the Infosec team knew that there were many misconfigurations in their network, but had little idea as to where those misconfigurations were or what they needed to fix them.

SOLUTION

The team configured the Attivo ThreatDefend® Deception Platform within the network to gain unparalleled visibility into their environment. Once they deployed the Attivo solution, it alerted the team to several misconfigurations in the network that represented significant weaknesses. The Infosec team could see that there was much activity on their network that they did not have visibility into before they installed the ThreatDefend platform. At first, they were concerned that these were false-positive alerts, but further investigation revealed that not only were these alerts real, but the platform substantiated them with forensic evidence, making them actionable in ways that other security solutions could not provide. They also noted that the ThreatDefend platform's BOTsink server raised alerts on activity that had completely bypassed existing prevention controls.

ROI

Without the need to add resources, the team gained significantly more visibility into their network than they had before. The Infosec team no longer wastes time chasing false-positive alerts and unsubstantiated incidents. They can correlate the attack activity, cut through the noise, and use the ThreatDefend platform to detect early in-network threats. With high fidelity alerts, the team has greatly lowered the time-to-discovery and time-to-response to threats in their network, saving the team hours, if not days.

However, it is not just about saving time. By using the ThreatDefend platform to catch threats in their network that could not see before, they can better protect their network from attacks that could cause communications outages through to incidents that could cause serious bodily harm or death to the attendees of their events.

> Once the Attivo solution was deployed, it alerted the team to several misconfigurations in the network that represented large weaknesses.

OUTCOME

One early outcome was that the organization used the ThreatDefend platform to identify an unknown actor on their network within the initial stages of an attack. The Infosec team quickly quarantined the malicious actor and remediated the situation before the attack spread too far into their network and caused any harm. When comparing the alerts generated by the ThreatDefend platform to those from other security solutions, the team saw that the other solutions had flagged the attack as "suspicious" but not as "critical," meaning the attack could have caused extensive damage before the other solutions would have raised an alert. By using the ThreatDefend platform, the organization reduced the time-to-detect, gathered detailed attack forensics, and accelerated incident response more efficiently than with any combination of their other security controls.

The organization has now deployed the ThreatDefend platform across multiple stadiums across the United States. They have incorporated deception within the security infrastructure for every significant event that the organization hosts to monitor their network better for any new activity and for early detection to divert any attack.

ATTIVO PRODUCTS

ThreatDefend Deception and Response Platform

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence and automated attack analysis, forensics, native integrations streamline incident response. The company has won over 100 awards for its technology innovation and leadership.
Learn more: www.attivonetworks.com