# Major Sports Organization Protects Critical Infrastructure With Deception Technology

| Company | Situation | Solution |
| --- | --- | --- |
| A major league sports organization | The organization needed visibility into their ICS-SCADA network to ensure that there would not be network interference during major events. | The ThreatDefend™ Deception Platform provided visibility into misconfigurations, early detection of threats, and actionable alerts for efficient incident response. |

## Overview

A sports organization had major cyber security concerns pertaining to an upcoming large sporting event. They needed more visibility into their network and substantiated, actionable alerts when an attack penetrated their perimeter devices. The infosec team didn't have the time (they are televised live) nor resources for another device that could generate a large volume of alerts and send them chasing with false positives.

## Challenge

The organization was mainly concerned about security threats to their SCADA network. In particular, the infosec team was most concerned about an attack that could work to shut down and lock their ICS systems – putting people in danger and potentially causing serious 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 are not always easily patched or enabled to 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 attention. Furthermore, the infosec team knew that there were multiple misconfigurations in their network, but had little idea as to where those misconfigurations were or what needed to be done to fix them.

## Solution

The team setup the Attivo ThreatDefend™ Deception Platform within their network in order to gain unique visibility into their environment. Once the Attivo solution was deployed, it alerted the team to several misconfigurations in the network that represented large weaknesses. The infosec team was able to see that there was a lot of activity on their network that they did not have visibility into before they installed the Attivo device. At first they were concerned that the alerts were false positives, but upon further investigation were able to see that not only were these alerts real, but they were substantiated and actionable in a way that was unobtainable by their other devices. They also noted that the ThreatDefend BOTsink engagement server raised alerts on activity that had completely bypassed their prevention devices.

## ROI

Without the need to add resources, the team has significantly more visibility into their network than they had before. The infosec team is no longer wasting time chasing false positives and unsubstantiated incidents; they are able to correlate all of the alerts, cut through the noise, and use the ThreatDefend Deception Platform to detect early inside-the-network threats. With high fidelity alerts, the team has greatly lowered the time-to-discovery and time to response on threats in their network, saving the team hours if not days.

But it is not just about saving time. By catching threats in their network with the ThreatDefend platform that were invisible before, they are able to better protect their network from attacks that could cause communications outages all the way 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 was able to identify an unknown actor on their network with the ThreatDefend engagement server in the initial stages of an attack. The infosec team was quickly able to quarantine the malicious actor and remediate the situation before the attack spread too far into their network and before the attacker was able to cause any harm. When comparing the alerts generated by the ThreatDefend Solution to the alerts generated by the other security devices, the team saw that the other devices had flagged the attack as "suspicious" but not as "critical", meaning the attack could have caused critical damage before the other security devices would have raised an alert. By using Attivo Networks, the organization is able to reduce the time-to-detect, get detailed attack forensics, and increase incident response faster and more efficiently than with any combination of their other devices.

The organization has now deployed the ThreatDefend Deception Platform into multiple stadiums across the United States. Deception is incorporated within the security infrastructure for every major event that the organization hosts in order to better monitor their network for any new activity and for early detection to divert any attack.

## Attivo Products

ThreatDefend Deception and Response Platform

## About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.
www.attivonetworks.com