# Major Entertainment Organization Deploys Deception for Insider Threat Visibility

| Company | Situation | Solution |
| --- | --- | --- |
| Major entertainment organization. | The organization is extremely concerned about targeted and stolen credential attacks on their intellectual property from both insiders and external threat actors. Their current solutions were not effective and generated a high volume of false positives. | Deployment of ThreatDefend™ Platform on multiple subnets and wide distribution of ThreatStrike deceptive credentials to close visibility gaps and minimize risk. |

## Overview

This organization conducts major product launches and is a leader in an extremely competitive entertainment market that is a prime target for cyberattacks. Their intellectual property is very valuable and a leak of data or projects would significantly diminish their competitive advantage in the landscape and, as a nature of the industry, have tremendous impact on their revenue stream. For this organization, a breach is unacceptable and avoiding one is top priority.

The primary concern for this organization is stolen credential attacks. With the right credentials, a malicious actor could easily infiltrate critical assets to steal intellectual property for financial gain. Given the high value of their intellectual property, visibility into malicious activity from insiders in their organization was also of critical importance. They needed a discrete detection tool that would give them real-time visibility into threats within the network and misconfigurations that could lead to an attack. The solution also required that it not be easily detected by insiders within their organization. The company has gone to great lengths to set traps for attackers and limit the number of people within their organization who know of the Attivo solution deployment.

## Challenge

The organization's greatest challenges were driven by their large network and that they had multiple high-traffic locations with little to no visibility into activity that could be indicative of a stolen credential attack. Essentially, there was no way to distinguish between an employee using their credentials to access a project and a malicious actor using stolen credentials to steal intellectual property. This proved extremely troublesome for the organization because it forced the infosec team to patch their visibility gaps with multiple different products that generated a high volume of alerts with the majority being false positives. Moreover, the team had to spend their resources monitoring the devices and, given there was not enough bandwidth to research every alert that was generated, they were forced to escalate false positives because they did not have enough actionable information to decipher a real threat buried within the noise. The time burden of false positives had a palpable impact on the team's ability to successfully protect their intellectual property and their bottom line.

The infosec team needed a solution that would not only be able to monitor and thwart stolen credential attacks, but also be able to cut through the noise of their network with substantiated, actionable alerts.

## Solution

The organization implemented the ThreatDefend Deception and Response Platform throughout their network with multiple devices. The team operationalized the devices both inside of the data center to protect and monitor their critical intellectual property as well as on their user networks to monitor for stolen credential attacks and additional visibility into attacker lateral movement. They are able to do this by their use of ThreatStrike deceptive credentials that they have placed throughout their network on end-user devices. These deceptive credentials act as alarm bells for attackers stealing usernames and passwords and using them to gain admin privileges. If a login attempt is made with the deceptive credentials, the team is alerted that there is an attack in process, which credentials are being used, and which system the infection is coming from – enabling the team to act quickly to remediate the situation.

## ROI

The return on investment the information security team has achieved by installing ThreatDefend for continuous threat management is that they now have visibility into the type of attacks they were most worried about: stolen credentials. By having the ThreatStrike deceptive credentials, they not only have visibility, but they will also be better protected against any potential threats. Visibility and protection against attacks plus a no false positive alert solution provides the biggest return on investment that the team could have asked for: they protect their bottom line and do so with efficiency. The visibility and protection provided by ThreatStrike means that the infosec team will catch malicious activity in their network long before the attack can have a chance to exfiltrate critical assets. Achieving early detection into insider and external threats with the ability to detect stolen credential attacks has significantly reduced the risk of a successful attack and has simplified their incident response with actionable alerts and a means to reduce their time to remediation.

## Outcome

The outcome for the organization is that they have operationalized the ThreatDefend platform within multiple segments of their network and have implemented a wide distribution of the ThreatStrike deceptive credentials. Combined, these products allow the organization to drastically increase their visibility into the attacks they were most worried about, focus their resources on remediating threats rather than trying to identify them, and significantly reduce the risk to their revenue stream by protecting their IP.

*...the team is alerted that there is an attack in process, which credentials are being used, and which system the infection is coming from...*

## Attivo Products

ThreatDefend Deception and Response Platform and ThreatStrike deceptive credentials.

## 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