Manufacturer Protects Intellectual Property With ThreatDefend Platform

Company	Situation	Solution
A global semiconductor manufacturer.	Protection of chip design intellectual property and lab environments.	ThreatDefend™ Platform gave visibility into in-network threats, stolen credential attacks, and replaced false positives with substantiated alerts.

Overview

The organization has a large investment in their intellectual property, specifically chip design in highly sensitive labs. The designs and other critical intellectual property were of concern to the infosec team because of advanced threats that could penetrate their prevention systems and extract valuable information. In particular, this organization was most worried about targeted stolen credential attacks against their employees. If an attacker were to swipe the credentials off a worker, they could move laterally through their network stealing more credentials leading to an attacker being able to exfiltrate their critical data undetected.

An undetected, targeted attack would render significant consequences if critical intellectual property was stolen and exfiltrated. The exposed data would not only reveal the technological advancements the organization made, but it would also diminish their competitive edge in the market place. Losing any competitive edge would have a serious impact on the organization's bottom line.

Additionally, the organization had multiple locations across different continents, which created additional complexity and increased the potentially exploitable endpoints for the cyberattacks. Additionally, the different locations added an extra layer of concern to the infosec team given the ability for attackers to move from one location to the other undetected.

Challenge

A major problem the organization had with their cyber security infrastructure was that they had extremely limited visibility into the subnets that contained their most critical data. If these subnets were breached, the team would have significant difficulties detecting the threat inside.

Another challenge the organization was facing was the number of alerts that were generated by their other security devices. The alerts generated were not only high in volume, but many times were false positives or unsubstantiated. The impact that the alerts had on the team was that they were unable to conduct the research necessary on these alerts to decipher between substantiated alerts and false positives. Therefore, they could not be confident that if they escalated an alert it would not be a false positive and a waste of resources to investigate. A situation such as this is extremely problematic for any infosec team because it forces them to choose between wasting resources investigating false positives or hoping that their incident response tools will be good enough to remediate an advanced threat that had penetrated their system.

Facing this choice, the team was not confident in their security controls to protect their critical intellectual property.

Solution

The infosec team deployed the ThreatDefend Deception and Response Platform across multiple locations in their critical subnets to increase the visibility of in-network threats. As the team operationalized ThreatDefend deception, the visibility gap that had widened in their network immediately closed and their alerts were now substantiated so that threats could be quickly addressed. Within 30 minutes, they had complete visibility across their entire network and saw high-fidelity alerts that were previously unattainable. With immediate visibility, the team is now alerted to only the malicious activity inside of their network. They now had the visibility they were looking for to catch in-network threats with zero false positives. But the team needed a solution that could do more than just detect.

The detailed forensics allow the infosec team to have more visibility into not only what an attack is doing, but how to better prevent it in the future.

Taking advantage of the power of the ThreatDefend™ solution to analyze threats and produce detailed attack forensics, the team has configured their network so that blocked URLs from their firewall are automatically redirected to the ThreatDefend platform for analysis. Letting the entire attack play out, the ThreatDefend captures all of the activity and relays the information in a variety of formats. The detailed forensics allow the infosec team to have more visibility into not only what an attack is doing, but how to better prevent it in the future.

ROI

Time being the most critical element in detecting cyber threats, the team has seen significant return on their investment due to the fact that the ThreatDefend Platform provides early detection and saves time by generating only high-fidelity, actionable alerts. By having actionable alerts, the organization saves money by no longer chasing false postives generated by devices that were incorrectly or incompletely identifying threats. Additionally, the biggest return on investment for the company is the visibility that they have into their subnets containing highly sensitive information. High visibility into their subnets coupled with the confidence of zero false positives allows the team to focus their resources on remediating threats.

Outcome

The organization has implemented multiple units in several networks and has fully operationalized the ThreatDefend platform. The results, in their words, have been magnificent. The ThreatDefend alerted the team to malicious activity inside of their subnet and quickly acted on the detailed alert. The team was then able to use the forensics gathered from the ThreatDefend platform to drastically increase their incident response time. The team was able to remediate the threat before any critical data was breached. Without the visibility into the threat that the ThreatDefend provided, it is likely that the team would not have detected the threat before it had exported critical assets. Another added benefit to the team was the ability to remove the debate about taking critical devices off-line. With the substantiated attack detail, the team was able to take the Attivo alerts and show irrefutably that the systems were infected and that they needed to be remediated. This also saved them a great deal of frustration and eliminated the need to do additional research to justify their actions.

Attivo Products

ThreatDefend Deception and Response Platform, BOTsink engagement servers, 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