CASE STUDY

MANUFACTURER PROTECTS INTELLECTUAL PROPERTY WITH THREATDEFEND PLATFORM

COMPANY

A global semiconductor manufacturer.

SITUATION

Protection of chip design intellectual property and lab environments.

SOLUTION

The ThreatDefend® Platform gave visibility into in-network threats, stolen credential attacks, and replaced false positives with substantiated alerts.

OVERVIEW

The organization has a significant investment in its intellectual property, specifically chip design in highly sensitive labs. The Infosec team was concerned that advanced threats could penetrate their prevention systems and extract valuable information such as chip designs and other critical intellectual property. The organization was particularly worried about targeted stolen credential attacks against its employees. If attackers were to swipe valid credentials, they could move laterally through the network, escalate privileges, and exfiltrate critical data undetected.

An undetected, targeted attack would result in significant consequences if the attacker exfiltrated critical intellectual property. The exposed data would not only reveal the organization's technological advancements but would also diminish its competitive edge in the market place. Losing any competitive advantage would have a severe impact on the organization's bottom line.

The organization had multiple locations across different continents, which created additional complexity and increased the potentially exploitable endpoints for cyberattacks. Moreover, given the ability for attackers to move between locations undetected, these remote sites added an extra layer of concern for the Infosec team.

CHALLENGE

The organization faced a significant problem with its cybersecurity infrastructure lacking visibility into the subnets that contained its most critical data. If attackers breached these subnets, the team would have considerable difficulties detecting the threat inside.

The organization also confronted high volumes of alerts that its other security solutions generated. Not only did these alerts negatively impacted the efficiency of the SOC, but the high incidence of false positives or unsubstantiated alerts increased analyst fatigue. The team had to research these alerts with enough evidence to determine confidently between actual incidents and false positives, wasting time and effort before they could escalate the event to the Incident Response team to remediate.

These challenges reduced the organization's confidence in its security controls to protect its critical intellectual property effectively.

SOLUTION

The Infosec team deployed the ThreatDefend Detection and Response Platform across multiple locations in their critical subnets to increase awareness of in-network threats. As the team operationalized the deception solution, they immediately

saw an improvement in their network visibility and alert fidelity. Within 30 minutes, they gained awareness of and notifications on activity across their critical subnets. With immediate visibility, the team now receives alerts only on suspicious or malicious activity inside of their network without extensive investigations to determine if it is a false positive. However, the team needed a solution that added more than high fidelity detection.

The team decided to take advantage of the ThreatDefend solution's malware analysis sandbox by configuring their network to redirect URLs the firewall blocked to the platform for analysis. By letting the attack execute to its conclusion, the platform captures all of the activity and creates exportable forensic data and reports for analysis. The detailed forensics allows the Infosec team to have more visibility into not only what an attack is doing but how to better prevent it in the future. The team also gains threat intelligence specific to the attacks and attackers currently targeting the organization to improve its overall defensive posture.

> 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

The team has seen a significant return on their investment due to their time savings and efficiency gains. The ThreatDefend platform provides early detection and accurate detection, saving time by generating only high-fidelity, actionable alerts. The organization sees efficiency gains by reducing investigation times confirming and investigating false positive alerts generated by security controls that incorrectly or incompletely identified threats. The organization saw its highest return on investment in the visibility that it has into its critical subnets containing highly sensitive information. These gains allow the team to focus its resources on remediating threats instead of investigating and chasing down false alerts.

OUTCOME

The organization has implemented and fully operationalized multiple ThreatDefend platform units in several networks. The results, in their words, have been "magnificent." The ThreatDefend platform alerted the team to malicious activity inside their subnet, and they quickly acted on the detailed alert. The team could then use the forensics gathered from the platform to drastically decrease their incident response time. They remediated the threat before the attacker could breach any critical data. Without visibility into the threat that the ThreatDefend provided, likely, the team would not have detected the attack before it had exported critical assets. As an added benefit, the Infosec team gained justification for talking essential devices off-line. With the substantiated attack details, the team could show that they needed to take the infected systems offline for remediation, saving much frustration and accelerating their incident response.

ATTIVO PRODUCTS

ThreatDefend Detection and Response Platform, BOTsink engagement servers, and ThreatStrike deceptive credentials.

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com.