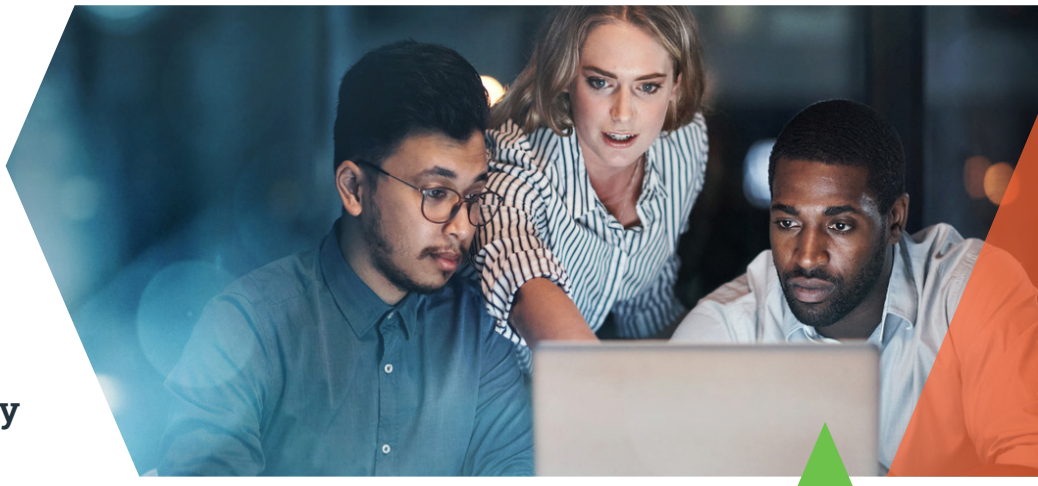
TEVORA™

Case Study



Tevora's Adversary Simulation Defends Large Semiconductor Firm Against Sophisticated Attacks

With environments constantly under threat from attackers using the latest advanced social engineering, physical penetration, and cyberattack techniques, it's more important than ever to fortify defenses to ensure your organization's valuable resources are secure.

In this case study, we'll explain how Tevora's Adversary Simulation Services helped a global semiconductor company identify and remediate vulnerabilities in their environment that were open to sophisticated attacks.

To protect our client's confidentiality, we'll refer to them by a fictitious name, Global Semiconductor Incorporated (GSI).

GSI Identifies a Significant Problem

A little over a year ago, one of GSI's executives read about another leading semiconductor company that had suffered a devastating attack in which attackers used a combination of sophisticated hacks to gain access to their environment and steal proprietary intellectual property related to their chip designs.

After reading about the attack against his competitor, the GSI executive met with his security team. By the time the meeting was over, GSI realized they would likely be vulnerable to similar attacks.

Tevora Engaged

After considering several security consultancies, GSI contacted Tevora to use their Adversary Simulation services. This suite of simulated attack services is designed to identify and exploit vulnerabilities in corporate environments.

Tevora held an initial kickoff with GSI to meet key staff members and learn about their objectives, business operations, and overall environment. Tevora then constructed a multi-faceted adversary simulation approach tailored to GSI's environment.

Our agreement with GSI management was that the simulated attacks would be performed without advanced notice to their team regarding the timing and methods used. This makes attack simulations more realistic. If we had telegraphed to GSI staff that a specific simulated attack was coming, they would have been on high alert, which would not be the case during a real attack.

Passive Reconnaissance

Tevora's adversary simulation testers started by looking for ingress points to access GSI's facilities. Reconnaissance efforts showed that GSI's building had an anti-tailgate system with badged access at the entrance. GSI had also posted armed security guards to monitor the entry area.

Active Reconnaissance

On the first day of attempted entry, our tester—wearing business casual attire to blend in—approached the anti-tailgate entrance. When they attempted to tailgate into the building, an alarm went off and the guard manning the station looked over at our tester. The tester de-escalated the situation by laughing it off, saying that it was a long day and that he must have left his badge in his car. He exited the building to regroup and try another tactic.

Initial Access

After further reconnaissance, Tevora observed that there was no badge required to access the GSI cafeteria. Posing as a GSI employee, our tester casually entered the cafeteria. He noticed a GSI employee standing in line to get lunch and observed the clip-on badge hanging from his belt. Our tester was able to swipe the badge by "accidentally" bumping into the employee, after which he sat down to eat with the badge hidden under his lunch tray.

Lateral Movement

After eating lunch, our tester entered the elevator and used the stolen badge to gain access to an upper floor, where he found an unattended Apple workstation that was not password protected. He executed commands on the computer that caused it to overheat and activate the fan, which was quite noisy. Using the workstation as an entry point, the tester began searching for vulnerabilities on the GSI network.

Persistence

After gaining entry to the third floor, the tester noticed that the stolen badge had been deactived which limited access. The tester knew he would need another badge to maintain access to the environment .

Our tester approached a GSI employee to ask if the fan running was normal. The employee was immediately concerned and asked if he should take the computer to IT. Our tester said there was no need to take it to IT because he had identified and fixed the problem. He then ran a command which shut down the fan. During this exchange, Tevora pocketed this employee's badge to obtain lateral movement and access to the elevator.

In this second attempt, the tester identified several vulnerabilities that could allow real attackers to gain access to GSI's building, where they would have a much easier time compromising personal information about GSI employees and confidential GSI information such as chip designs, marketing plans, and competitive assessments:

No badge was required to access the cafeteria.

Clip-on badge holders are used, which are relatively easy to steal.

The Apple workstation had no password protection.

Network Access and Post Exploitation

After compromising a second badge, the tester took the elevator to another floor, where he found an empty conference room with an ethernet port. After plugging his laptop into the port, he was able to execute penetration tests to identify network vulnerabilities that allowed him to compromise a GSI Admin ID. Using this ID, he was able to fully compromise GSI's network and obtain access to a wide range of sensitive GSI information including sensitive employee information and chip design documentation.

In this phase of the simulated attack, we identified these additional vulnerabilities:

The conference room did not require a badge to enter, which gave the tester access to an ethernet port

Ethernet ports in the conference room allowed full access to the network

Administrator IDs were poorly secured

Egress

By the time our tester had compromised the network, the second badge had been reported missing, and was deactivated. Fortunately, reconnaissance had uncovered the fact that GSI did not have anti-tailgating systems for exiting the building. Using this intel, our tester was able to exit the building undetected through a badge-required exit by tailgating a GSI employee.

During the exit phase of the simulated attack, we identified this additional vulnerability:

There was no anti-tailgating system at the exit.

Alternative Attack Vector Identified

Having successfully compromised the GSI network without being detected, we decided to try once more. Our tester returned the same night and told the cleaning crew that he had lost his badge. Upon hearing this, the cleaners granted him access to the building, which allowed him to compromise GSI's network again.

During the follow-on phase of the simulated attack, we identified this vulnerbility:

The cleaning crew was not adequately trained in security.

Comprehensive Reporting

Having successfully compromised GSI's network twice, we concluded our adversary simulation efforts and developed comprehensive documentation of our results, including the physical penetration methods used, exploit code examples, and detailed remediation recommendations. We also presented a summary of our findings and recommendations to GSI management.

Completed Client Objective

While GSI management was concerned about the vulnerabilities found in their environment, they were extremely pleased and impressed with the work Tevora had done. After the report was delivered, they implemented all our recommendations.

GSI remains a valued Tevora customer, and we are asked back to perform periodic adversary simulation engagements to continually probe their environment for vulnerabilities.

Tevora's Adversary Simulation Services go above and beyond what you would expect in a conventional penetration test by using a mix of social engineering, physical penetration, and cyberattack techniques that are highly customized for your environment.

More Than Just a Conventional Penetration Test

In this case study, we've demonstrated how Tevora's Adversary Simulation Services go above and beyond what you would expect in a conventional penetration test by using a mix of social engineering, physical penetration, and cyberattack techniques that are highly customized for your environment. Our team of adversary simulation experts draw on their deep experience to think and act like a sophisticated real-world hacker, adapting and shifting strategies in real time as they encounter roadblocks and changes in your environment.

With a conventional penetration test, you would typically find a less customized approach that is cannot rapidly adapt to roadblocks and environmental changes. In the scenario described in this case study, it's likely that a conventional approach would not have identified any vulnerabilities in the client environment.

Let Tevora be Your Trusted Partner

If you'd like to learn more about Tevora's Adversary Simulation Services or engage us to help identify and remediate vulnerabilities in your environment, just give us a call at (833) 292-1609 or email us at sales@tevora.com.

Go Forward. We've got your back.