TEVORA™ Case Study

Tevora Helps Leading Aerospace Company Prevent Compromise of Highly Sensitive Data

Cybercriminals are constantly evolving their strategies and tactics to find new ways to bypass the latest security controls and exploit vulnerabilities in targeted systems, software, and endpoints. Now, more than ever, it's important to identify partners that can help fortify your defenses against cyberattacks. This is especially true in the aerospace industry, where attacks have the potential to compromise highly sensitive data, which can damage a company's reputation and competitive advantage—or even impact national security.

This case study describes how Tevora's Red Team used penetration testing to helped an industry-leading aerospace company identify and fix a vulnerability that exposed massive amounts of highly sensitive and confidential product data, preventing a potentially devastating cyberattack.

To protect our client's confidentiality, we'll refer to them by the fictitious name of International Aerospace Products (IAP).

Going in Blind

IAP engaged Tevora's expert Red Team to conduct penetration testing to identify potential vulnerabilities in its environment. Our team was given no information regarding IAP's systems and network architecture or components.

This meant we were going in blind. We needed to view IAP's environment as a "black box," which is generally the view attackers will have.

Our expert Red Team used Tevora's Attack Simulation Process to simulate techniques and approaches that attackers would typically use to identify and exploit vulnerabilities in targeted systems and networks. Tevora has honed this process over time as we've performed penetration testing for some of the world's largest aerospace companies. Here's a summary of the process:

Tevora's Proven Attack Simulation Process

Reconnaissance

- Perform discovery efforts including:

  Data exfiltration
  Open source intelligence gathering
  Network enumeration
  Service footprinting
- Conduct stealthy exploitation of vulnerable systems
- Map and exploit externally-facing systems
- Run phishing (email) and vishing (phone) campaigns

Assessment

- Emulate known attack patterns and vectors
- Conduct thorough passive information gathering and public records analysis
- Identify known vulnerabilities
- Develop and execute exploits
- Pivot and exploit access
- Conduct social engineering campaigns against target employees

Report

- Conduct a collaborative debrief session
- Provide a detailed findings report with recommended remediation
- Retest with validation
- Present findings to executive team
- Create an executive summary of findings for management

Trade Secrets Exposed to Hackers

The Tevora Red Team followed the general Attack Simulation Process to conduct penetration testing at IAP, but as with every engagement, there were unique aspects of the IAP project. **Notably, in this case, we found that a massive amount of trade secret data was exposed to hackers.**

During the Reconnaissance phase of testing, our discovery efforts did not identify any known vulnerabilities in IAP's externally-facing attack surfaces. However, we were able to identify a substantial vulnerability in an application used by IAP staff and external contractors to store and transfer detailed plans and specifications on IAP's aerospace products and services.

To find this dangerous vulnerability, our Red Team used extensive trial and error techniques, probing every aspect of the file transfer application until we were able to identify user ID validation logic errors that allowed unauthorized users to access and download sensitive data.

We then developed and executed a zero-day exploit that leveraged this vulnerability to download massive amounts of highly sensitive IAP data, including highly confidential trade secrets and intellectual property. After successfully executing the exploit, we recommended a fix for the vulnerability, and IAP implemented it. Subsequent testing confirmed that the fix worked.

Dodged a Bullet

Fortunately, we were able to identify the vulnerability and recommend a fix before cybercriminals discovered it.

This allowed IAP to dodge what could have been a very large bullet. If attackers had discovered and exploited the vulnerability before we found it, they could have demanded a multi-million dollar ransom payment. If the information had fallen into the hands of competitors, it could have significantly eroded IAP's competitive advantage in many areas.

Let Tevora be Your Trusted Partner

Tevora's expert team of security specialists can partner with you to help build up your defenses against ransomware and other cyberattacks. This includes reviewing your environment for potential security weaknesses, implementing tools and techniques to protect your environment, and training your staff to be aware of emerging ransomware, phishing, spearphishing, and social engineering trends, so they are fully equipped to be the first line of defense against attack.

If you do suffer a ransomware or other type of cyberattack, Tevora's experienced incident response team can jump in at a moment's notice to help you get back up and running quickly, while minimizing financial, operational, and reputational damage.

If you'd like to learn more about how Tevora can be your trusted security partner, just give us a call at (833) 292-1609 or email us at sales@tevora.com.