Synack

CASE STUDY

Global retailer uses testing to learn the truth about their own vulnerabilities

CISO of a top 100 global retailer suspected inaccurate data about its security posture and sought the truth

Situation

The first task the new CISO of a top 100 global retailer had was to establish the security posture of the company's host infrastructure and web applications, as well as securing a rapidly growing set of cloud assets. A good litmus test was counting how many security vulnerabilities were found, but not patched. So she asked her team for an inventory of all unpatched security vulnerabilities.

First, the report was 200. The next day, it was 2. Something was wrong.

Problem

It quickly became clear that the security team did not have access to a reliable vulnerability count. The new CISO needed help to establish the company's security posture. She called in Synack to assist.

Synack Resolution

In the first year, Synack found 50 vulnerabilities which established a baseline for further testing. Using Certify Tests — a test to discover novel vulnerabilities plus checking a list for known ones, the CISO was able to better understand the company's security status. And she finally had vulnerability data she could trust.

Synack provided two powerful data types: 1) an Attacker Resistance Score and 2) a contextualized list of vulnerabilities. The Attacker Resistance Score provides a single security number from 1 to 100 that determines a realistic assessment of assets' actual hardness against attack based on penetration test performance data. Vulnerabilities were measured and categorized, so critical or high severity findings could receive special attention. Testing and results went through the Synack Portal to capture intelligence for tracking trends.

Certify Tests provided an evaluation of the general hardness of tested targets, and to keep them protected, the CISO opted to move to continuous testing with Synack365. Trust had been built between Synack and the security team. When a Synack-sourced critical vulnerability came in, meetings would stop and action would be taken immediately for remediation.

By the third year, security processes around testing were efficient and flowed easily. With additional special projects on the horizon, such as mergers and acquisitions and cloud platform retesting, efficiency kept the team from being overwhelmed and shortstaffed during a global talent shortage. With Synack, the team had greater confidence in managing their security posture no matter the issues thrown their way.

Results

- More than 1,000 valid vulnerabilities discovered in three years
- Number of vulnerabilities discovered increased 20x over the first year's efforts.
- 16% improvement in Attacker Resistance Score, a measure of how easy or hard it is to find new vulnerabilities.
- Implemented process to test all new apps before they see a single user
- Development teams know if an app is "synacked," it is tested, protected, and ready