Case Study:
Penetration & Vulnerability Testing

Client Profile

Business: Market Research

Size: 35 Employees

Industry: Services

Compliance: NIST 800 171, HIPAA

Key Metrics

Data speaks louder than words, so we selected a few points of interest to help tell the story:

7
Critical security findings identified and remediated

125
End user devices, servers, and network components scanned and tested

CHALLENGES

A small market research firm that handles sensitive customer data through survey collection and direct inquiry needed immediate assistance to complete several security measures to satisfy compliance requirements. This included a vulnerability scan and subsequent penetration test to ensure that malicious actors could not access their network.

SOLUTIONS

Our security team escalated the service delivery, considering the tight timeframe, and initiated the process by installing a specialized computing device on the client network to perform the tests. Vulnerability scanning was conducted to scan for open ports, unpatched network equipment, and outdated operating systems. Positive findings were quickly remediated so that a penetration test could be completed at a stronger security posture. Penetration testing was executed at the client's desired time of day to minimize any potential impacts on business operations. The results of both the vulnerability and penetration testing were delivered in a report that included an executive summary and detailed findings.

RESULTS

1

Accelerated Compliance Achievement

Due to our fast-tracked service delivery, the client met their compliance requirements within the tight deadline, avoiding potential penalties.

2

Security Posture Strengthening

By assessing the environment using our staged approach, we identified vulnerabilities, implemented enhancements, and tested the improvements to validate their effectiveness, improving overall security.

3

Security Visibility & C-Level Engagement

The client gained critical insight into their security risks, transforming uncertainty into confidence in their network's protection. Reported findings prompted C-level staff to enhance internal communication and their security strategy.