Vulnerability Scanning & Remediation

Business Case Study and Report

While certain project details have been adapted to protect confidentiality, they reflect the knowledge, challenges, and approach we bring to every collaboration.

grow

Service area:
Cybersecurity

Client type:
Professional Services Firm

Challenges and Objectives

Challenges

The client had grown in size and complexity, but its infrastructure had never undergone a formal vulnerability assessment. As external clients began requesting evidence of good security practices, they knew they needed visibility into risks — but lacked tools, time, and technical expertise to do so.

They needed support not just to run the scan, but to understand and act on the results.

Objectives

- Perform a comprehensive vulnerability scan across key systems
- Prioritize vulnerabilities by risk and likelihood of exploitation
- Guide remediation with actionable steps and low-disruption strategies
- Create clear documentation for internal compliance efforts
- Empower the client with the knowledge to repeat the scanning process

Our Approach

01

Discovery & Scanning

We used trusted tools (OpenVAS & Nessus Essentials) to perform a full network scan, identifying open ports, outdated software, default credentials, and misconfigurations.

02

Analysis & Prioritization

Vulnerabilities were triaged using CVSS scores, exploitability, and relevance to the environment.

03

Remediation & Documentation

We addressed critical findings, provided patching guidance, disabled insecure protocols, and documented repeatable steps for the client.

Solution Highlights

Updated software and systems flagged as end-of-life

Hardened firewall configurations and access rules

Disabled unused services and legacy protocols (e.g., SMBv1, Telnet)

Delivered a report with screenshots, severity tags, and next steps

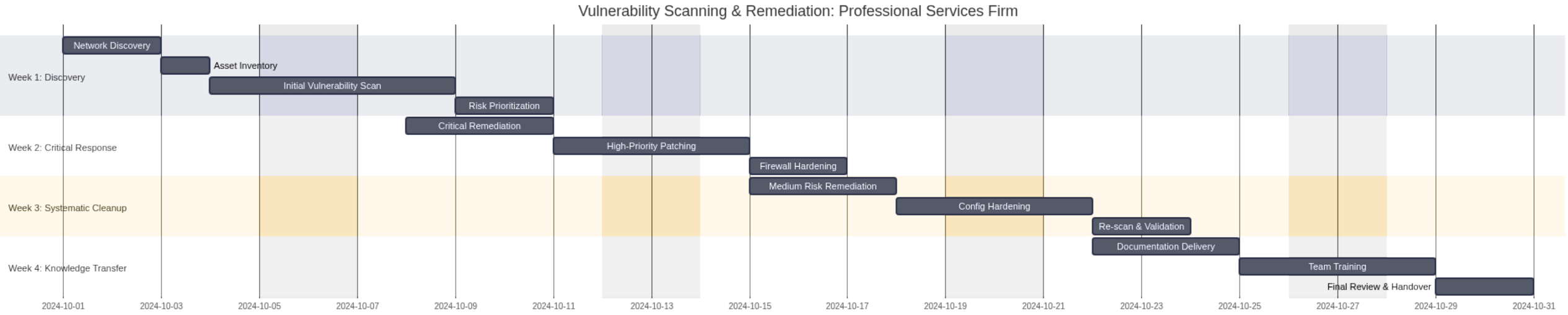
Results

- 100% of critical vulnerabilities resolved within 10 business days
- Gained visibility into 30+ systems with an average severity score drop of 3.2 points
- Documented processes contributed directly to the firm's compliance report
- Internal team trained to rerun scans quarterly

“The report made sense — for once, we understood exactly what needed to change. We feel much more in control now.”

— Operations Manager

Vulnerability Lifecycle: From Detection to Remediation



Get In Touch

Email

info@iniciativagrow.com

Social Media

@iniciativagrow

Call us

(+507) 6318-3683