NEOVERA

www.neovera.com

VULNERABILITY & REMEDIATION PROGRAM AN INTEGRAL COMPONENT TO IMPROVING THIS LARGE BANKING INSTITUTION'S SECURITY POSTURE

OPPORTUNITY

A LARGE BANKING INSTITUTION WITH OVER 50 BRANCHES ON THE EAST COAST, CONTACTED NEOVERA TO ASSESS THEIR CURRENT SECURITY ARCHITECTURE. THEY SOUGHT TO INCREASE THEIR SECURITY POSTURE BY OPTIMIZING VULNERABILITY SCANNING AND PATCH MANAGEMENT PROCESSES.

At a glance

KEY CHALLENGES

- BACKLOG OF VULNERABILITIES
- GAPS IN STAFFING & INADEQUATE TOOLS
- IMMATURE VULNERABILITY MANAGEMENT

IMMEDIATE NEEDS

- 24X7 CROSS-FUNCTIONAL TEAM
- CENTRALIZED TRACKING
- PRIORITIES FOR REMEDIATION

CHALLENGE

When the bank first approached Neovera, it was discovered that they were faced with staffing gaps coupled with immature internal and external vulnerability management processes and inadequate tools. This resulted in a significant backlog of risks.

The bank planned to address this accumulation and achieve a steady state of minimal to no outstanding vulnerabilities. The idea was adoption of a mature vulnerability management and patching program. Scheduling scanning and regular maintenance and integrated with the overarching IT enterprise architecture roadmap including IT service management tools, and ITIL process best practices.

To achieve this goal, Neovera was asked to collaborate with the Senior IT Leadership and Information Security Team to refine and prioritize scope, skillsets and level of effort, and to develop RACI diagrams supporting a Vulnerability and Remediation Management Program.

ASSESSMENT FINDINGS

Once it was determined who, on the bank's internal team, would be involved in the vulnerability program management, Neovera, in conjunction with their team, completed a thorough assessment. It was found that multiple contributing factors were identified across the people, process, and technology domains that were causing vulnerabilities throughout the architecture.

Neovera recommended addressing immediate needs including implementing a 24x7 cross-functional vulnerability and remediation team, a CMDB, centralized tracking of vulnerabilities and patching, developing a simplified IT ecosystem, and adding additional staffing across the bank's technology landscape.

NEOVERA'S RECOMMENDATIONS

To address the findings from the assessment, Neovera recommended establishing a multi-layered response that included three key components:

- **Cross-Discipline Technical Process & Design IT PMO & Architecture Team**
- **Create a Vulnerability & Remediation Program**
- **Implement a 24x7 Cross-Functional team to perform patch management**

NEOVERA

ABOUT

NEOVERA IS A TRUSTED PROVIDER OF MANAGED SERVICES INCLUDING CYBER SECURITY AND ENTERPRISE CLOUD SOLUTIONS, COMMITTED TO DELIVERING RESULTS THROUGH THE INNOVATIVE USE OF SCALABLE ENTERPRISE-GRADE TECHNOLOGIES THAT CAN BE QUICKLY DEPLOYED TO MEET ANY REQUIREMENT. OUR GOAL IS TO HELP YOU ACHIEVE THE HIGHEST RETURN ON YOUR IT INVESTMENT, ENSURING CONVENIENCE, SUPERIOR SUPPORT AND SECURITY OF YOUR MISSION-CRITICAL SYSTEMS.