NEOVERA

CASE STUDY

RAPID SECURITY ASSESSMENT to improve Bank's Infrastructure and Optimize Vulnerability 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
- SIMPLIFIED IT ECOSYSTEM

Client:
EAST-COAST BANK WITH OVER 50 LOCATIONS

Sector:
FINANCIAL

Project:
SECURITY ASSESSMENT & IMPLEMENTATION PLAN

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 AND PATCH MANAGEMENT PROCESSES.

CHALLENGE

When the bank first approached Neovera, it was discovered that they were faced with staffing gaps coupled with immature vulnerability management processes and inadequate tools. This resulted in a significant backlog of vulnerabilities. The bank planned to address this backlog and achieve a steady state of minimal to no outstanding vulnerabilities. The idea was via refinement and adoption of a mature vulnerability management and patching program integrated with the overarching IT enterprise architecture roadmap including IT service management tools (e.g., ServiceNow), and ITIL process best practices.

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

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.

NEOVERA

LEARN MORE
WWW.NEOVERA.COM

ASSESSMENT FINDINGS

Once Neovera completed a thorough assessment in conjunction with the bank's internal team, it was determined that multiple contributing factors were identified across the people, process, and technology domains.

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**
- **Vulnerability & Patch Management Program**
- **24x7 Cross-Functional Vulnerability & Remediation Team**