

Case Study

A Leading Global Digital Trade Finance Platform on Blockchain Technology

Service(s) offered: **Cyber Resiliency (Virtual CISO Office)**

Sector/Industry: **BFSI**



Strengthening Cybersecurity for a Digitized Trade Finance Platform with Virtual CISO Services

The Context

The client, a digitized global trade finance platform using blockchain technology to manage global liquidity for supply chain and trade assets, needed a dedicated CISO and an information technology and cybersecurity team. This gap meant that associates with limited cybersecurity expertise were handling critical tasks, pulling them away from their core responsibilities and reducing productivity.

Nexdigm stepped in to fill this gap, offering a comprehensive solution with our Virtual CISO services, effectively acting as the client's dedicated information technology and cybersecurity team.

The Objective

The client required third-party resources to manage their Information and Cybersecurity (ICS) team to save time and costs while ensuring robust cybersecurity measures. The success of the project depended on:

Enhanced Security: Strengthening the security framework by implementing advanced tools, policies, and procedures to mitigate potential threats and vulnerabilities.

Reduced Risk: Conduct simulations and proactive assessments, such as phishing exercises and penetration testing, to identify and minimize real-time risks.

Case Highlights

- Delivered cost-efficient security solutions, achieving 70% savings compared to a full-time CISO.
- Strengthened risk mitigation and overall security posture with tailored strategies.
- Ensured full compliance with industry regulations and standards.
- Supported incident response readiness, ensuring seamless business continuity.

Increased Operational Efficiency: Streamlining daily security operations and incident management processes to ensure timely resolution of security issues and optimize resource utilization.

Policy Compliance and Governance: Ensuring adherence to industry standards, like CIS v8, by reviewing, updating, and mapping security policies and controls.

Seamless Tool Configuration: Researching, configuring, and setting up key tools like Windows Autopilot and Apple Business Manager to automate security workflows and enhance system management.

Incident Management Support: Providing Level 1 support for handling and resolving cybersecurity incidents promptly to maintain business continuity.

Cost and Time Efficiency: Leveraging third-party cybersecurity resources to save time and reduce operational costs while maintaining robust security measures.

The Solution

Nexdigm acted as the virtual Chief Information Security Officer (CISO) and implemented a suite of solutions to achieve the outlined objectives.

Strengthened Authentication: Implemented Single Sign-On (SSO) and controlled local admin access for improved security.

Security Awareness Enhancement: Conducted phishing simulations to elevate security awareness among users.

API Governance Improvement: Identified vulnerabilities through penetration testing to enhance (Application Programming Interface) API governance.

Optimized Entra ID Policies: Customized Entra ID policies for diverse user groups to ensure tailored security measures.

Security Risk Mitigation: Applied critical updates to mitigate potential security risks.

Endpoint Security Enhancement: Strengthened endpoint security through comprehensive policy improvements.

Web Security Optimization: Enhanced web security by implementing effective content filtering solutions.

Mac Device Management: Streamlined management and security of Mac devices for better oversight.

Daily Security Checks: Maintained consistent daily security checks and effective incident response protocols.

Software Vulnerability Mitigation: Assessed and mitigated software vulnerabilities while ensuring compliance with security standards.

Third-Party Risk Assessment: Conducted thorough assessments to identify and mitigate third-party risks.

Visual Insights: Provided visual insights through the Quartey Dashboard for enhanced monitoring and decision-making.

Windows Autopilot Research: Conducted research, configuration, and testing of Windows Autopilot for improved deployment processes.

The Impact

Nexdigm's extensive array of cybersecurity not only enhanced the client's security measures but also deliver significant business benefits, showcasing a successful partnership in navigating today's complex threat landscape.

- Implemented strategies that ensured continuous monitoring and adherence to industry standards, minimizing potential risks.
- Delivered robust security solutions that optimized resources and improved overall effectiveness.
- Achieved significant reductions in operational costs while maintaining high-security standards, resulting in a 70% cost saving on an annual basis.
- Strengthened the client's defenses against cyber threats through a holistic approach to cybersecurity.
- Addressed vulnerabilities systematically, resulting in a more resilient security framework.

For more information on this case study, please write to us at:

ThinkNext@nexdigm.com

You can also visit our website to know how our services resulted in tangible business benefits:

www.nexdigm.com