Enhancing Cyber Resilience in the **Transportation** Sector

Case Study

AGILEBLUE   NFTA

Company Profile

COMPANY:
The Niagara Frontier Transportation Authority (NFTA)

HEADQUARTERS:
Buffalo, New York

INDUSTRY:
Transportation (Bus, Rail, & Airlines)

FOUNDED:
1834

AGILEBLUE SOLUTION:
- Cerulean AI Platform
- vCISO Consulting Services

WEBSITE:
www.nfta.com

Overview

NFTA set out to enhance their cybersecurity posture by building out a comprehensive program based on a recent CMMC assessment. Their primary goal was to elevate their cybersecurity maturity from CMMC Level One to Level Two. Facing challenges in defining the necessary controls and technologies, NFTA sought a partner who could provide clear direction and support. AgileBlue stepped in to fulfill this need, initially focusing on developing a detailed roadmap to guide NFTA through the implementation of essential cybersecurity controls and capabilities.

About NFTA

The Niagara Frontier Transportation Authority is unique, serving both transit and aviation communities, embracing travelers from both the U.S. and Canada. With roots going back to 1834, the NFTA builds on its traditions every day and across the region. The NFTA proudly keeps their region moving by air, land, and rail, ensuring Western New York's people and businesses continue to thrive.

Security Challenges

___

(1) **Cybersecurity Roadmap**

NFTA faced several significant security challenges that required expert guidance and strategic implementation. Initially, they struggled to define the specific controls and technologies necessary to advance their cybersecurity program. Without a dedicated cybersecurity team and relying on third-party providers for parts of their IT infrastructure, NFTA needed a clear, actionable plan. AgileBlue's first objective was to develop a comprehensive roadmap to help NFTA navigate the complexities of cybersecurity enhancements.

(2) **Compliance (CMMC, TSA Mandates & DHS Mandates)**

AgileBlue's initial involvement began with aiding NFTA in achieving CMMC compliance. However, the landscape quickly evolved as NFTA received new mandates from the TSA and DHS. These mandates introduced four core principles that NFTA needed to adhere to: user access, vulnerability management, continuous monitoring and auditing (SOCaaS), and network segmentation. Over the past year, AgileBlue has focused on these critical areas, providing tailored solutions to ensure compliance and bolster NFTA's cybersecurity defenses.

Overall Business Impact

Initial Goal Achievement:

NFTA aimed to enhance its cybersecurity posture by partnering with a security expert to develop a comprehensive program aligned with CMMC standards. Their objective was to progress from CMMC Level 1 to Level 2 compliance. To achieve this, AgileBlue created a detailed roadmap outlining the necessary improvements for NFTA to strengthen its security measures and meet CMMC Level 2 requirements.

Compliance with New Mandates:

As new mandates from the TSA and DHS introduced additional requirements, AgileBlue's impact on NFTA expanded. These mandates centered around four core principles: user access, vulnerability management, continuous monitoring and auditing (SOCaaS), and network segmentation. AgileBlue's tailored solutions in these areas have been instrumental in strengthening NFTA's cybersecurity framework.
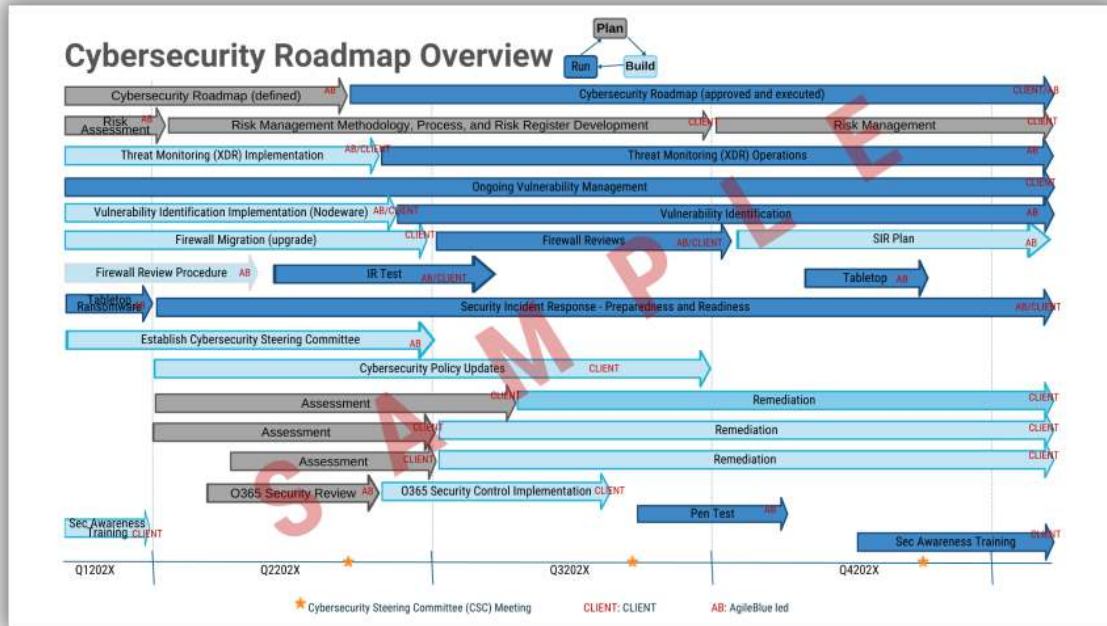
Enhanced Security Infrastructure:

By implementing robust user access controls, streamlining patch management processes, establishing continuous monitoring and auditing capabilities through SOCaaS, and ensuring effective network segmentation, AgileBlue has significantly enhanced NFTA's overall security posture. This comprehensive approach has enabled NFTA to build a resilient defense against evolving cyber threats.

Confidence and Peace of Mind:

This strong partnership has not only ensured compliance with regulatory requirements but also provided NFTA with confidence and peace of mind in their cybersecurity capabilities. The positive business impact extends beyond compliance and technical improvements; it encompasses the strategic value and trust that NFTA places in AgileBlue. This relationship has enabled NFTA to navigate the evolving cybersecurity landscape with confidence, knowing they have a dependable partner to support them in an instant.

AB AgileBlue.com

Addressing Security Challenges & Roadmap Development:

NFTA faced significant challenges in defining the necessary controls and technologies required to achieve their cybersecurity goals, particularly given their IT team lacked dedicated cybersecurity expertise and relied on third-party providers for parts of their IT infrastructure. AgileBlue provided clear direction and support, helping NFTA navigate these complexities effectively.

Example of AgileBlue Cybersecurity Roadmap

Why AgileBlue

AgileBlue's partnership with NFTA has resulted in an enhanced security infrastructure, compliance with regulatory requirements, and increased confidence in NFTA's cybersecurity capabilities. Valued for their vCISO services and SOCaaS, AgileBlue has established a trusted and reliable relationship, enabling NFTA to navigate the evolving cybersecurity landscape with assurance. This partnership ensures the safety and security of Western New York's transit and aviation communities, upholding NFTA's tradition of excellence.

AgileBlue.com

AGILEBLUE

AgileBlue Cerulean AI combines AI-powered cybersecurity with the human touch you trust. Our SecOps platform autonomously detects, investigates, and responds to endpoints, network, and cloud cyber-attacks faster and more accurately than a traditional SOAR.

Our technology is both intelligent and automated, but we take a custom approach for every client we work with, analyzing and detecting exactly what matters most. Our products are entirely cloud-based with advanced machine learning and user behavior analytics, all supported by our U.S.-based team of cyber experts.

For more information, visit our website: AgileBlue.com.

Ready to start protecting your company?

Request a Demo