Case Study
Reducing Cost and Risk

INDUSTRY
Financial Services

SIZE
300 employees serving over 1,400 financial partners, nationwide

LOCATION
United States

Challenges
With the organization unable to deliver software products on time and lacking infrastructure and security automation, the CTO and CISO wanted assistance in strengthening their ability to meet compliance and federal regulations in an efficient way.

Solution
Lean Security Assessment and implementation using DevSecOps automation and orchestration integration services, provided by New Context.

Achievements
Improved infrastructure deployment time and efforts by 99.93%, while maintaining strict security and compliance and meeting federal regulation requirements.

With proper security in place, financial organizations can reduce risk to systems and infrastructure while improving their capacity to innovate.

As a leader in financial technology, our client has been delivering innovative payment and risk solutions for more than 25 years. Providing protection for a diverse network of financial, government, and payment entities and the customers they serve, our client ensures safe, secure, and convenient financial transactions, nationwide.

Innovation, growth, and new business are critical for organizations in any industry. With the proper security in place, even organizations governed by stringent compliance and regulatory measures can reduce risk to their legacy systems and infrastructure and improve their capacity to innovate, enter new markets, and capture market share. The banking industry is no stranger to these conditions, and our client has realized the benefits an investment in security and automation can yield.

Struggling to keep up with market needs, our client was failing to deliver products on time and unable to keep up with accelerating changes in regulations ... placing them in legal jeopardy, in danger of losing compliance with FINRA (Financial Industry Regulatory Authority) in order to continue conducting certain types of transactions, and potentially at risk for going out of business.

In an effort to better understand the organization's current state and to determine the most effective approach for improving their IT business practices, New Context performed a Lean Security Assessment. An expert conducted the assessment within the client's location by measuring aspects of an organization's security operation, including use of Agile, DevSecOps culture, security and compliance. Additionally, they observed meetings and surveyed employees across varying levels of the business to get a feel for what was going well and where performance needed to improve. These findings were compiled with a framework developed by New Context, to develop a story around the client's current state and desired outcome, and to lay out a roadmap to demonstrate how to achieve it.

The answer was clear. The client needed New Context's help, beginning with collaboration and automation. In the Fall of 2015, two of the firm's engineers joined the client's on-site DevOps department.

Solving Security Challenges Using Automation
One of the initial accomplishments delivered by New Context for the client was automating the host provisioning process. Due to their strict system of controls, when a developer needed a new server to work on, they had to submit a ticket and then wait six weeks or more to receive it - often incomplete, requiring them to spend additional time communicating back and forth to get what they needed. By automating provisioning, developers were able to stand up new servers on their own, cutting the wait time to under one week. It also improved the quality of the deliverable, creating a reproducible outcome and helping to ensure that audit and compliance requirements were met.

The next challenge New Context encountered was helping the client with a mission critical, short deadline to comply with Federal Disaster Recovery audit requirements. In order to meet these terms, the team needed to automate server and application installations and updates in the client's system so that they could replicate and stand the system up in another region.

The situation was dire, as none of the existing staff knew how to configure the organization's legacy tools. New Context's engineers hunkered down with the client's team and collaborated to recreate these configurations based on what was known to be working. The already massive effort posed additional challenges, such as application architecture changes occurring while automating the configurations, which added to the workload of the moving target. As any automation effort is also an audit, compliance errors discovered during the process also required resolution.

The client realized over 99% efficiency through infrastructure automation.

By the end of the process, the team was able to recreate several legacy systems and serve up applications on them within a couple of hours, on a repeatable basis. This enabled the team to automate 25 of the client's 50 applications in less than one year.

Breaking Down Barriers With Collaboration

New Context's Lean Security Assessment had also identified a lack of collaboration among the client's Technology and Security teams. The teams worked in silos, communication was predominantly managed through email, there were many extensive, ineffective meetings – and it was hurting overall productivity. After reviewing these findings and considering the expert's recommendations, the client began assigning members from Security and other areas to attend meetings for other teams to initiate collaboration. They also added persistent video conferencing to connect and create presence for remote staff, enabling them to participate in "hallway" conversations and other scenarios that were not previously possible.

The client's Security team embodied a "can't do it" culture – a roadblock, where the team threw darts at everyone around them, but never contributed to the task at hand. New Context worked diligently with Security and DevOps to improve collaboration and communication across the teams. Eventually, the Security team started pitching in, providing code, participating in the code review process for pull requests, and reviewing project workload. This enabled the business to move forward and both the Security and DevOps teams began recognizing and acknowledging the value of input from their peers.

With the help of New Context, the team was able to automate application deployments and server provisioning and remove communication barriers. As a result, provisioning and deployment time was reduced from six weeks down to one hour -- with some applications taking only a few seconds to deploy and fully provisioned, new servers taking as little as ten minutes. With the ability to innovate and deliver on their mission more quickly, collaboratively, and securely, the client is now compliant with Federal regulations, can better serve their customers, and grow their bottom line.

Lean Security reduced deployment time for a new server from six weeks to 10 minutes.

Looking Ahead to Full Lean Security Transformation

New Context continues to guide the client's technology advancements and enable them to make changes to their technology at a faster rate, satisfy regulatory requirements, and do business more competitively in their space. They also strive to evolve the organization and its culture to align with the technology transformation in order to become a fully agile shop.

New Context has deep experience driving the successful, holistic transformation of organizations, their technology, and how they do business by implementing automation, collaboration, and increased security, leading to increased efficiency, effectiveness, resilience, and reduced costs.

DevSecOps Services and Consulting

DevSecOps automation, orchestration, and solution provider

Full stack platform development using Lean Security methodology

Contact us to learn how you can benefit from New Context's DevSecOps services and consulting.

888.773.8360 / newcontext.com
New Context / @newcontext / sales@newcontext.com

NEW CONTEXT