Mainframe Vulnerability Scanning Against Regulatory Requirements

Company Overview:

This global financial firm manages over $2.6T in client assets with over 250,000 employees in offices spanning the globe.

Business Challenge:

The financial firm needed to meet compliance and regulation standards while protecting employee and customer data.

Challenge

In today's interconnected world, global companies are entrusted with vast amounts of highly sensitive client data—ranging from names and addresses to Social Security numbers and employment data. The stakes are exceptionally high when it comes to ensuring the integrity of mainframe systems and data security.

This invaluable information has traditionally been stored within the mainframe enterprise due to its built-in integrity. However, as this global financial firm transitioned towards a work-from-anywhere model for its thousands of employees, new and complex challenges have emerged. Balancing the need for seamless remote access while upholding the highest standards of data protection became an urgent and non-negotiable priority. The firm recognized it was critical to protect the integrity of the mainframe to ensure continued success in safeguarding client information.

The Challenge?

After moving to a work-from-everywhere model, the financial firm needed to mitigate risks and modernize its mainframe security operations within three months.

The financial firm faced the need to decrease security investigations and response times for mainframe security events. The goal was to expand coverage and automate tasks through integration with third-party products, all with the added challenge of having the new architecture in place within three months.

Solution

Facing a tight deadline and stringent requirements, the firm enlisted the expertise of Key Resources, Inc. (KRI), now a part of Rocket Software, to guide them in developing a mainframe vulnerability program.

But how would the organization be able to make that happen? No one on the customer side understood the issues with building mainframe vulnerability risk rankings and why analytics-driven reporting was necessary to analyze and score the vulnerabilities found on the mainframe.

The main challenge here centered around educating the security and risk teams at the financial firm on mainframe language and scheduling processes, to ensure they were equipped to handle the scanning results and vulnerability reporting schedules, as well as the mitigation processes.

As the financial firm looked for the correct way to make this transformation, a task force was formed to determine the best approach to integrate mainframe vulnerability scanning reporting with the current risk reporting. To break down the siloes that existed between enterprise operations and security operations, the financial firm decided to adopt an integrated and automated process that took the vulnerability scanning results from all the operational and technology layers to create consistent, automated reports.

Results

With the support of Rocket Software, the financial firm's mainframe vulnerability scanning responsibilities were successfully implemented and centralized. The team learned how to utilize the analytics-driven data and CVSS scoring that was being generated by Rocket® z/Assure® Vulnerability Analysis Program (VAP) and reported in a Vulnerability Analysis Report.

The Solution?

The firm implemented Rocket® z/Assure® VAP to expand the integrity of the mainframe and improve the organization's risk reporting.

Getting the financial firm's testing team up to speed quickly began paying dividends immediately, enabling them to take advantage of the automated vulnerability reporting which had a huge impact on their mainframe's integrity and risk reporting. Scan results were able to provide more contextual information during reporting. However, the benefits of the shift extended beyond the specific scanning operations. The organization was able to free up resources from its mainframe team, enabling the group to handle more pressing tasks and responsibilities in managing operations.

Impact

Expanded Mainframe Security Coverage

Improved Risk Reporting

Automated Vulnerability Scanning

Improved Mitigation and Optimization

Rocket® software

Modernization. Without Disruption.™

Learn more

Visit RocketSoftware.com ›