Rocket® software

Mainframe Security Services

Regulations like the Digital Operational Resilience Act (DORA), PCI DSS 4.0, NIST, and others, are buckling down to ensure optimal risk oversight across organizations. When it comes to risk management, legacy systems like the mainframe need to be prioritized in your cybersecurity strategy.

Regular penetration testing, integrity assessments, compliance assessments, and vulnerability management on mainframes are critical to maintaining the rigorous compliance that is required by DORA and other regulations.

01

Integrity Assessments

Vulnerability scanning across all operating systems is crucial for mitigating threats, and it's now required by DORA and other regulations. Rocket® z/Assure® Vulnerability Analysis Program (VAP) is the only vulnerability management solution that automatically and precisely scans for and identifies vulnerabilities in mainframe operating system (OS) code. Rocket Software partners with you to leverage our Integrity Assessment Services, to determine risk exposure, and to enable you to take steps to protect your business from the types of breaches that lead to financial harm or regulatory violations.

First, a scan of your mainframe operating system layer is conducted using z/Assure VAP, measuring the severity of each vulnerability using the Common Vulnerability Scoring System (CVSS) methodology. As a trusted industry standard for ranking the severity of vulnerabilities, CVSS allows Rocket to report on program coding errors found in your systems. The detailed reporting you receive will enable you to understand and communicate mainframe risks to your internal development team or software providers for remediation. As a result, you're empowered to proactively protect your business from emerging mainframe threats.

02

Penetration Testing

While a vulnerability scan uses automated tools to search for vulnerabilities, a penetration test is a more in-depth assessment. According to DORA, "Threat led penetration testing shall cover at least the critical functions and services of a financial entity and shall be performed on live production systems supporting such functions."[1]

Penetration testing utilizes a combination of machine and human-driven, or even physical approaches to identify hidden weaknesses.

With threats constantly evolving, it's recommended that every organization commission penetration testing at least once a year, but more frequently when:

- Making significant changes to infrastructure
- Launching new products and services
- Preparing for compliance with security standards
- Bidding for large commercial contracts
- Utilizing or developing custom applications

Rocket recommends vulnerability scanning and penetration testing be done so your organization receives a comprehensive evaluation.

1. Source: https://www.digital-operational-resilience-act.com/DORA_Article_23_(Proposal).html

03 Compliance Assessments

Assessing compliance to ensure your critical system configurations don't drift from organizational policy is crucial. Mainframe Compliance Assessments are imperative for organizations in passing a Security Readiness Review (SRR) for a z/OS® mainframe environment with RACF®, CA Top Secret, or CA ACF2® as the Access Control Program (ACP) / Enterprise Security Manager (ESM). Passing an SRR brings mainframe system security into compliance with the security guidelines developed by the Defense Information Security Agency (DISA) for the Department of Defense (DoD), and PCI regulations.

The assessment will provide answers to questions like:

- Are security parameters in sync with the corporate security policy?
- Do your users have the appropriate access?
- How pervasive is excessive access?
- Is audit logging appropriate for the level of access given to privileged authorities?

Are you planning on converting from CA ACF2 or CA Top Secret to IBM® RACF®?

Lastly, it's imperative to leverage a team of experts when moving from CA ACF2 or CA Top Secret to IBM RACF. Converting to IBM RACF plays a key role in the initiative to standardize vendors. Rocket Software has a trusted 30-year strategic partnership with IBM with over 40 years of expertise leading these successful complex migrations. So why partner with Rocket in your conversion initiative to RACF?

- Significant reduction in manpower; limited staff augmentation required during the conversion.
- The Security Conversion Utilities provide a proven and tested methodology for converting to or from CA ACF2™, CA Top Secret® or IBM RACF. These tools automatically convert 90% of the commands, keeping manual intervention to a minimum.
- SCU4ACF2 and SCU4TSS increase data accuracy and the quality of the content of the newly-generated security database, allowing you to architect a solution that's easy to administer and performs up to your expectations.
- z/Assure Password Propagation Software will optionally propagate your existing passwords to the targeted security package using one-way encryption.
- Easy to read conversion reports.

Digital transformation, emerging technologies, and evolving regulations have made the world of managing IT infrastructure security a complex one to navigate. But that doesn't mean IT leaders need to face those complexities alone. Taking advantage of services delivered by a trusted expert and partner like Rocket Software, your security teams can tackle even the most complex security challenges, ensuring and maintaining compliance and preventing disaster before it ever has a chance to strike.

Learn more about how Rocket Software security services can help keep your IT operations protected.

Rocket software

MAR-9728_MF-SecurityServices_OnePager_v2