chainguard

FedRAMP Checklist for Containers

When it comes to initial build-out, ongoing operation and management of FedRAMP accreditation, having an inventory of what software you are running and where can save you time and resources. Here are three steps you can use to simplify the ongoing operations and management of your FedRAMP journey.

- □ **Assess Current Container Image Landscape**: Evaluating your existing container images security is a great first step to identify potential gaps and address any known vulnerabilities before undergoing the official security assessment is critical to a successful FedRAMP certification process. You can start by:
  - □ Reduce your attack surface with minimal container images
  - □ Incorporate scans earlier in the software development lifecycle
  - □ Update images frequently with fixes to keep vulnerabilities low

- □ **Implement Best Security Practices**: Once you understand your container image vulnerability surface, apply industry frameworks and best practices for securing images. This includes hardening the operating system, restricting access, and using the latest security patches. You can also consider:
  - □ Maintaining software updates in images
  - □ Generating SBOMs at image build rather than runtime
  - □ If images are from others parties, be sure to prove provenance with signatures

- □ **Automate Image Scanning**: Leverage automated tools to streamline all the work you've done to prepare for FedRAMP. That means employing automation to check your organization's container images for security issues regularly to aid in early detection and timely remediation. Here are some other tips on your way to FedRAMP accreditation:
  - □ Scan images during build and run phases
  - □ Don't overlook dark matter (software not picked up by scanners)
  - □ Integrate automation to open and triage vulnerable packages