Chainguard

FedRAMP Checklist for Containers

When it comes to initial build-out, ongoing operation, and management of FedRAMP accreditation, having a clear understanding of your containers and maintaining them regularly to keep vulnerability counts low is critical. Here are three steps you can take to simplify the ongoing operations and management of your FedRAMP journey when it comes to container security.

- [ ] **Implement asset management best practices:** Identifying and tracking assets is a critical component required for an Authorizing Official (AO) to assess risk and the overall trustworthiness of a FedRAMP accreditation package. This should include first and third party components built or ingested during the software development life cycle (SDLC) and deployed within the accreditation boundary. Some best practices include:
  - Maintain up-to-date software in images
  - Generate software bill of materials (SBOMs) at build time rather than runtime
  - Validate vendor and open source artifacts
  - Don't overlook software dark matter (software not picked up by vulnerability scanners or software composition analysis (SCA) tools)

- [ ] **Automate container supply chain and hardening:** Once you understand your container security landscape, apply industry frameworks and best practices for hardening images. Leverage automated tools to streamline container hardening controls to all assets within the accreditation boundary. Here are some other tips on your way to FedRAMP accreditation:
  - Deploy hardened, minimal container images to reduce attack surface
  - Close any remaining gaps with automated checks and tooling
  - Use images that contain detailed provenance and have digital signatures
  - Integrate automation to open and triage vulnerable packages

- [ ] **Create a continuous vulnerability management plan:** Once you have a solid asset management and container supply chain plan in place, vulnerability management becomes less of a burden. Evaluating your assets against vulnerability management guidelines is a great first step to identify potential gaps and address any known vulnerabilities before submitting your FedRAMP accreditation package. This is critical to a successful FedRAMP certification process. Here are some ways to get started:
  - Start with images that are updated frequently with fixes to keep vulnerabilities low
  - Employ automated scanning early and often
  - Scan images during build and run phases
  - Revisit your organization's vulnerability plan to ensure timely remediation
  - Prioritize vulnerabilities based around risk and follow NIST guidance