Product Requirement Document (PRD): Container Image Security Scanner

Background/Task

A security product is required to scan container images and provide users with vulnerability findings. Container images contain applications along with their dependencies, and these components may have known vulnerabilities. The goal is to help users:

- Identify which container images have vulnerabilities and assess their severity.
- Take necessary actions to fix high or critical vulnerabilities.
- Manage a large repository of container images effectively.

Objectives

- Provide an intuitive dashboard summarizing the security state of container images.
- Enable filtering and sorting mechanisms for efficient vulnerability management.
- Allow users to take immediate action on vulnerable images, such as updating or rolling back to previous versions.
- Implement a notification system for security updates and breaches.

Features In

Login & User Management

- Secure authentication and authorization.
- User roles and permissions for managing security scans.

Container Image Selection & Scanning

- Select container image registries (Docker Hub, Amazon ECR, Google Container Registry, etc.).
- Browse repositories and select container images for scanning.
- Initiate on-demand vulnerability scans.
- Scheduled periodic scans with customizable intervals.

Vulnerability Analysis

- Display scan results with severity levels (Critical, High, Medium, Low, Negligible).
- Provide detailed vulnerability descriptions, affected packages, and suggested remediation steps.
- Filters to sort by severity, repository size, alphabetical order, and recent updates.

Image Management & Actions

- Update an image to the latest secure version.
- Roll back to a previous, non-vulnerable version.
- Delete deprecated images to maintain repository hygiene.

Dashboard & Reporting

- [M] Overview of all container images with vulnerability status.
- [M] Charts/graphs displaying vulnerabilities by severity.
- [M] Drill-down view for individual image vulnerability reports.
- [M] Track recent scans and search history.

Notification System

- [M] Alerts for newly discovered vulnerabilities.
- [M] Notifications for security breaches or urgent remediation actions.
- [M] Option to keep repository connected or disconnected.

Features Out

- Automatic patching of vulnerabilities.
- Integration with third-party ticketing systems (e.g., Jira, ServiceNow) for issue tracking (future consideration).

Development Action Items

- Implement backend API for scanning container images and retrieving vulnerabilities.
- Develop UI components for image selection, scanning, and result display.
- Integrate filters and sorting options for vulnerability prioritization.
- Implement image update/rollback features.
- Set up real-time notifications for security breaches.