Container Security

Jeny Teheran
FIFE meeting
10 November 2023

Cyber and Container Security

- Traditional cybersecurity defenses and configuration might not directly apply to containerized environment and applications.
- Cybersecurity risks or areas of concern:
  a) Vulnerable container images due to: vulnerable components, misconfiguration
  b) Mismanagement of credentials and secrets
  c) Use of untrusted images
  d) Vulnerable container image registries
     - Authentication and access controls
     - Application security
  e) Container deployment and management: choice of solution, authentication and access controls
  f) Container runtime: lack of telemetry and visibility for IR

Cyber and Container Security

- 4 target areas for guidance on best security practices:
  a) Container image creation and integration
  b) Container image registries
  c) Container deployment and management
  d) Container runtime
- Use of EOL containers → policies to be amended
  a) Host OS must be fully patched
  b) Container (or application running on it) should not be exposed to the Internet
  c) Compensatory controls following guidance on container security above

Next steps

- Start developing guidance for the use of containers:
  - Common guidance for both cases: services and user applications
  - Specific guidance when applicable
  - Target date for CSBoard review: Feb 2, 2024
- Work in parallel starting Jan 2024:
  - Policy review to include the use of EOL containers in CCE, including CCE security plan.
    - Cybersecurity policy might be required to do a controls test
- Second half of 2024 (After EL7 EOL)
  - Design a strategy for container image vulnerability scanning
  - Deploy EDR technologies as appropriate to address telemetry and visibility
  - Container image registries should be scanned weekly for application vulnerabilities