(Recap) Next steps

Goal: guarantee continuous operation of scientific services and applications after EL7 EOL

- Start developing guidance for the use of containers:
  - Common guidance for both cases: services and user applications. Specific guidance when required.
  - 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 capture telemetry and enhance visibility
  - Schedule weekly vulnerability scans for container image registries

Risks

1) Vulnerable, misconfigured or infected container image leads to compromise of:
   - Host OS --> leading to further compromise of the Fermilab network
   - Sensitive/protected data used by the container during runtime
2) Misconfiguration of container runtime environment or container orchestration tool leads to compromise of:
   - Container during runtime
   - Scientific computing services
3) Records of container-specific activity are not available for investigation and incident response:
   - Container image creation
   - Container image registries including authentication and access control
   - Container orchestration tools and container runtime environment

Common guidance

- For every container image, there should be records/logs/evidence to answer:
  - What the container image is for? Service or user application?
  - Where did it come from? Provenance
  - Does it have any known vulnerabilities?
  - During runtime:
    - Host OS details: machine name, kernel version, user identity
    - File system config, namespaces, credentials, capabilities, control groups, user identity (unprivileged user for every case?)
    - Download of additional content --> connection to external resources
    - Any attempts for privilege escalation, unallowed system calls, access to host OS resources
- (TBD) Where these records will be stored?