Security Controls in Shared Code Repo's

Shared Repo's

- Shared repo's are a great place to store code for projects
- It allows developers easy access to the latest code base
- It's great for information sharing
- One central repository to easily find what is being looked for
- Easy to implement security measures

Libraries

- Collection of code which serve a particular function
- Can introduce vulnerabilities making it a security threat
- Many libraries are written by third-parties
- Introduction of a library should be sense checked and vetted

...continued

- Can be used as an offset to vulnerabilities
- They should contain security libraries to make it easier for developers to implement security measures
- Can include but not limited to: 2FA, hashing and logging
- Documentation should be provided on how and when to use libraries

Secret Management

- Storage of information and instructions on the software should be housed in their repo
- This include applications and tools utilized
- Providing a central repo that houses all information for easy of use
- Allows the team to stay updated on the latest instance being used

Software

- Other software that is typically found are:
- OpenSSL configs
- OSSEC
- NTP
- The same benefits apply here as well

Build Images

- The central repo is a good place to store build images
- The images can be operating systems, databases and web servers
- The images are of the recommended configurations
  - allow for the team to quickly test programs in a safe environment

Dev pipeline

- The repo should hold information about tools and processes related to testing
- Including security configurations
- “How to” documentation should be included here as well
- Results of the testing should be held here too

Collaboration

- The repo should be a place of collaboration
- Everyone should have a voice and be able to raise their concerns is an item is misused
- Changes should be reviewed with scrutiny and approved cautiously
- The space should encourage challenging the status quo and organizational tools

Sources

- Kim. G, et al. (2016). The DevOps Handbook - How to Create World-Class Agility., Reliability, & Security in Technology Organizations. IT Revolution Press LLC.