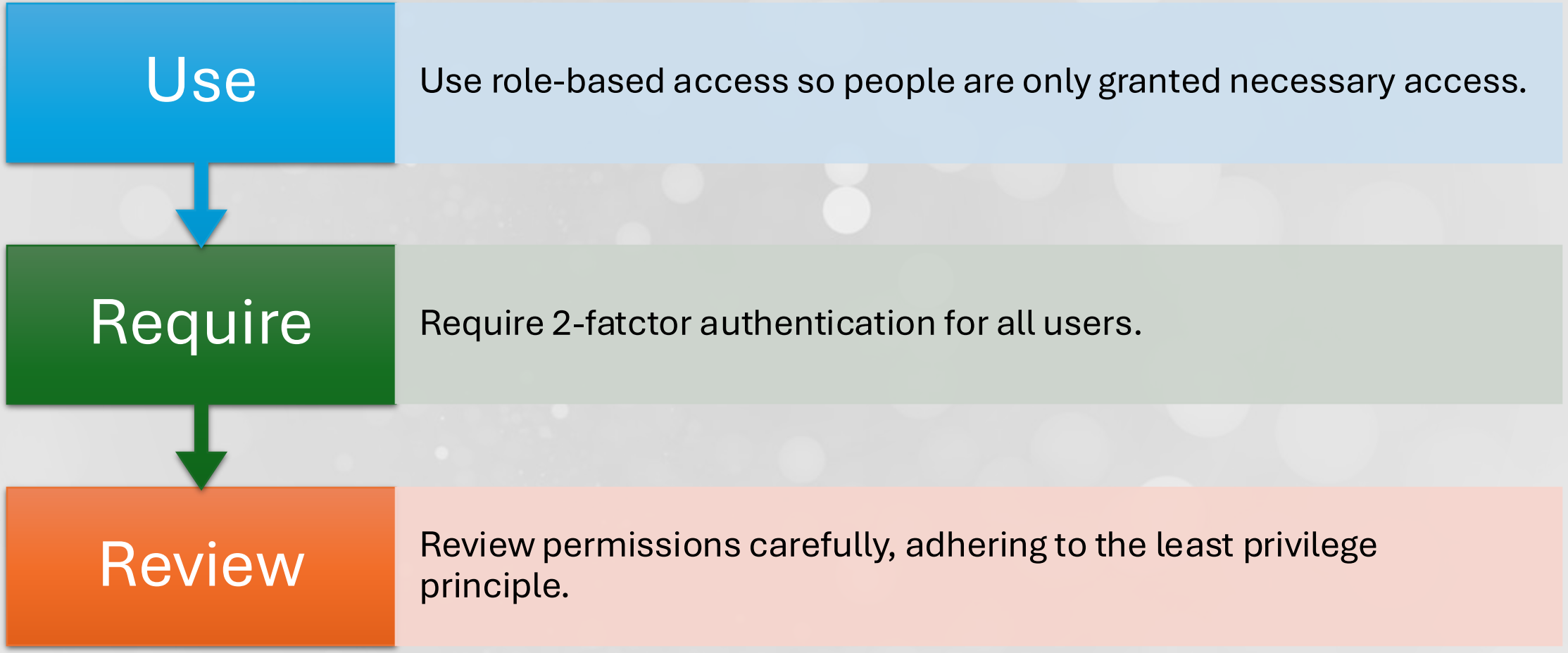
Security Controls in Shared Source Code Repositories

Kevin Ramirez
CSD 380

The Importance of security

- If proper security is not implemented, repositories can be target by hackers.
- Attackers can steal sensitive information, which can be subject to blackmail.
- Inserting malware in the code is also common.
- It is important to keep the systems secure to protect code and teams.

Managing Access Control



Credential and Authentication Protocols

- Never hardcode passwords, tokens, or keys into the code.
- Use secret manager tools that store and rotate credentials.
- Add secret scanners to catch mistakes before pushing code to the main repository.

Code Scanning and Analysis

Scanning is crucial, tools like SonarQube or Semgrep are helpful in catching security issues.

Set up these tools in your CI/CD pipelines.

It's best practice to manually reviews code to catch anything the tools might miss.

Enforcing Security in Repositories

01

Turn on branch protection, this will require pull requests to be reviewed.

02

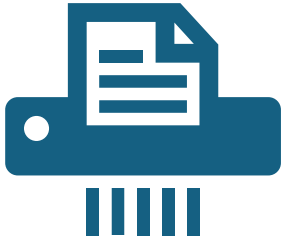
Used signed commits, ensuring that all the changes are being stored and accounted for.

03

Prepare a defined protocol for any data breaches.

Consistent Updates

Keep third party libraries updated.



Remove unused dependencies to reduce the attack surface on your libraries.

Update the team on new information and secure coding practices and mitigation strategies.

Conclusion and Next Steps

- Emphasize the importance of best security implementations in code to your team.
- Encourage immediate action in case of breaches and enforce up to date security practices.
- Take feedback from the team, and apply continuous improvement.

References

- Fernandes, C. (2023, August 7). *Source code security best practices: A complete guide*. Assembla. https://get.assembla.com/blog/source-code-security/
- TechTarget. (n.d.). *Top 4 source code security best practices*. SearchSecurity. Retrieved May 9, 2025, from https://www.techtarget.com/searchsecurity/tip/Top-4-source-code-security-best-practices
- GitHub. (n.d.). *Quickstart for securing your repository*. GitHub Docs. Retrieved May 9, 2025, from https://docs.github.com/en/code-security/getting-started/quickstart-for-securing-your-repository