Assignment: Security Controls in Shared Source Code Repositories

CSD 380

MODULE 11.2 ASSIGNMENT

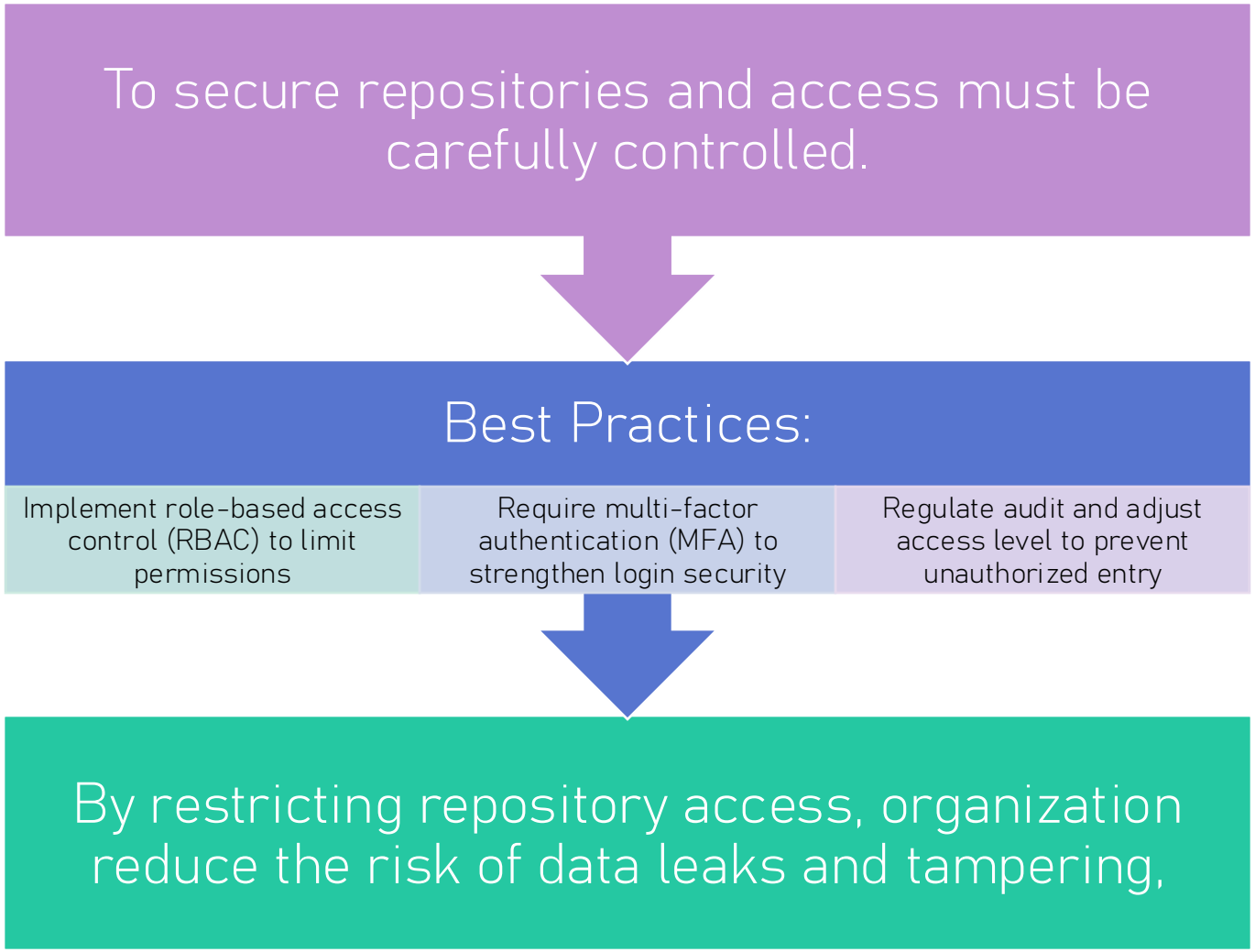
JULIE SAKAI

5/10/25

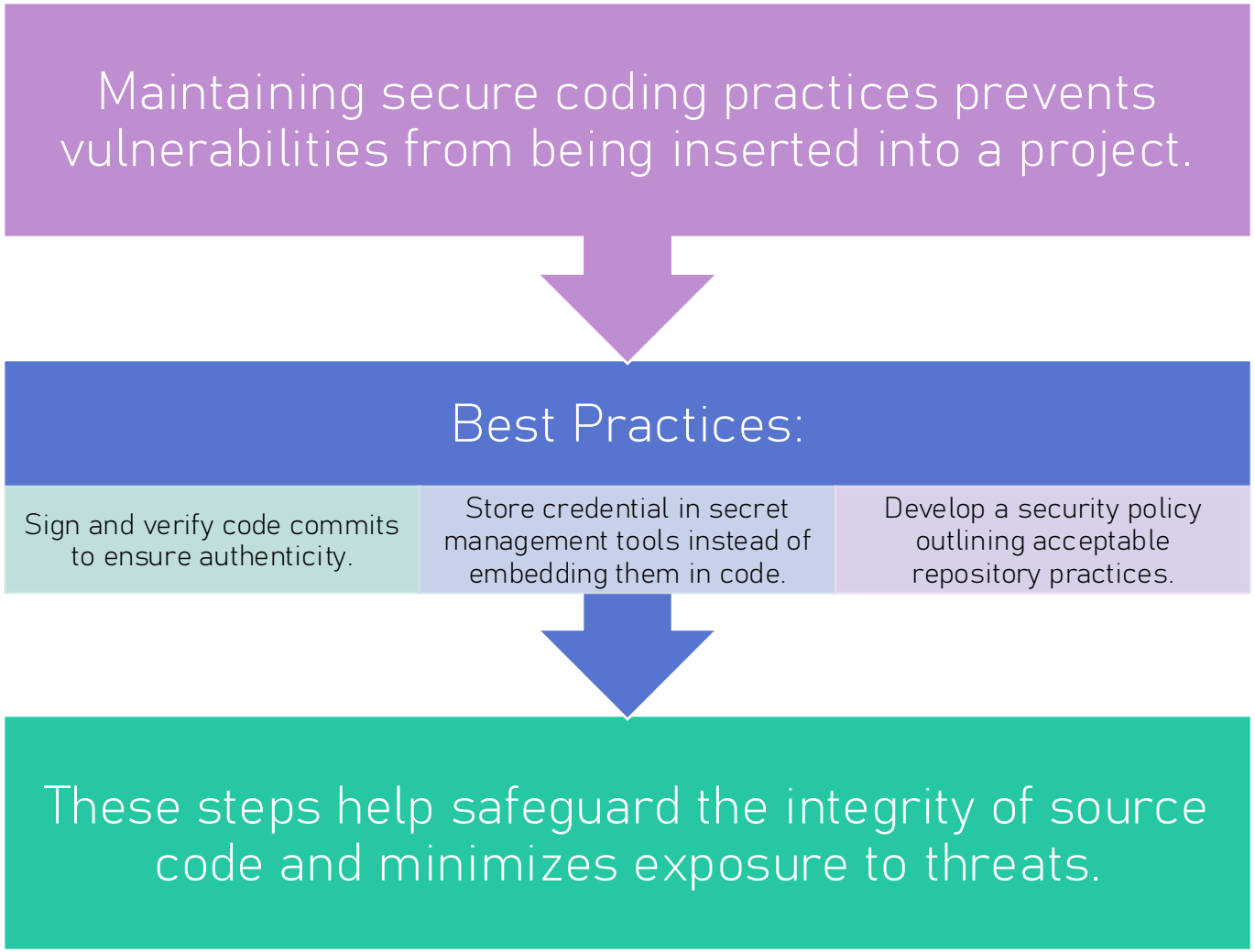
Introduction

- Shared source code repositories is important in software development, but it does post security risks if not properly protected.
- Without strong security measures, repositories can become vulnerable to breaches, unauthorized modifications, and supply chain attacks.
- Security is necessary
  - Protect intellectual property and sensitive data.
  - Prevent cyber threats like malware injections.
  - Ensure software integrity and compliances.

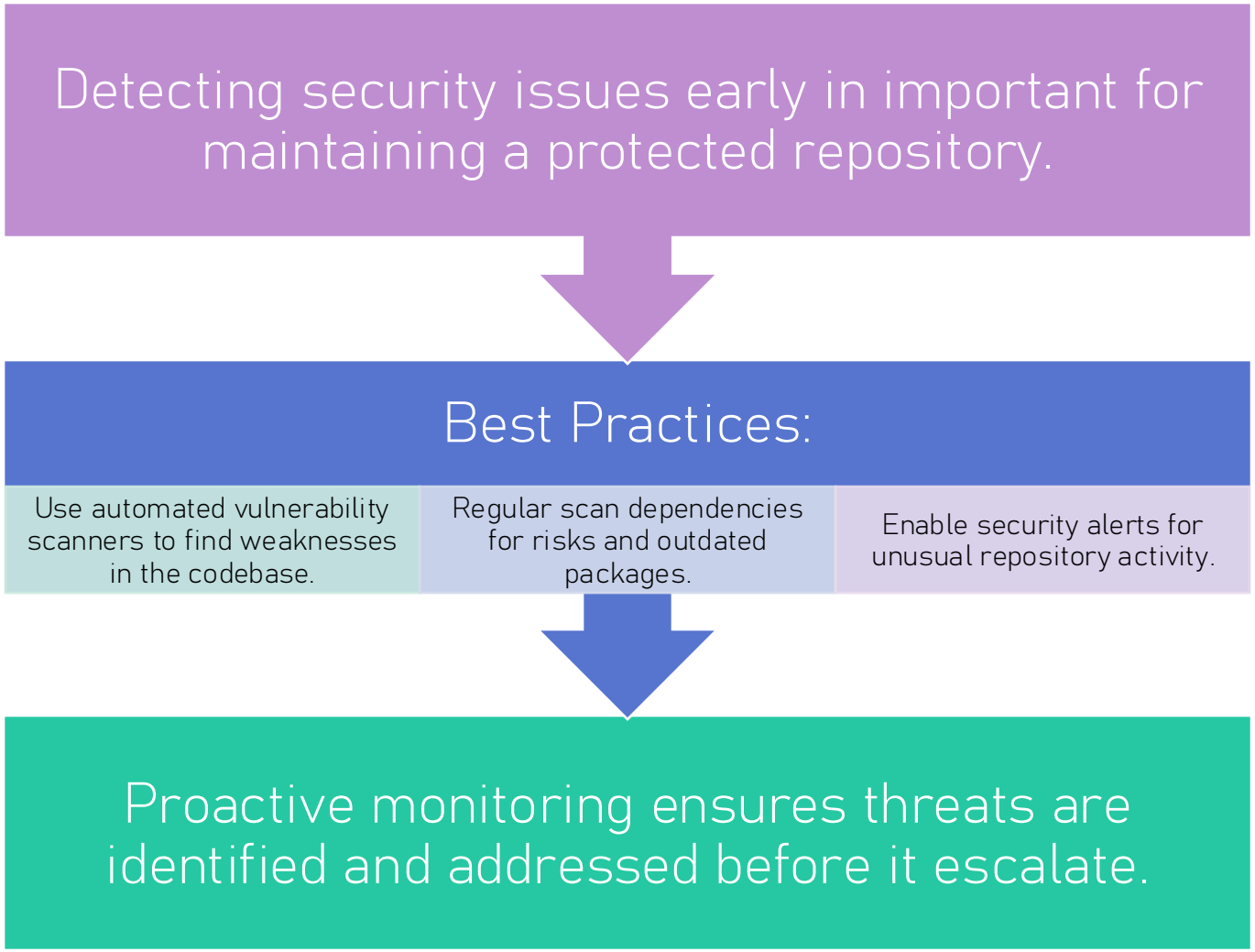
Managing Access and Authentication



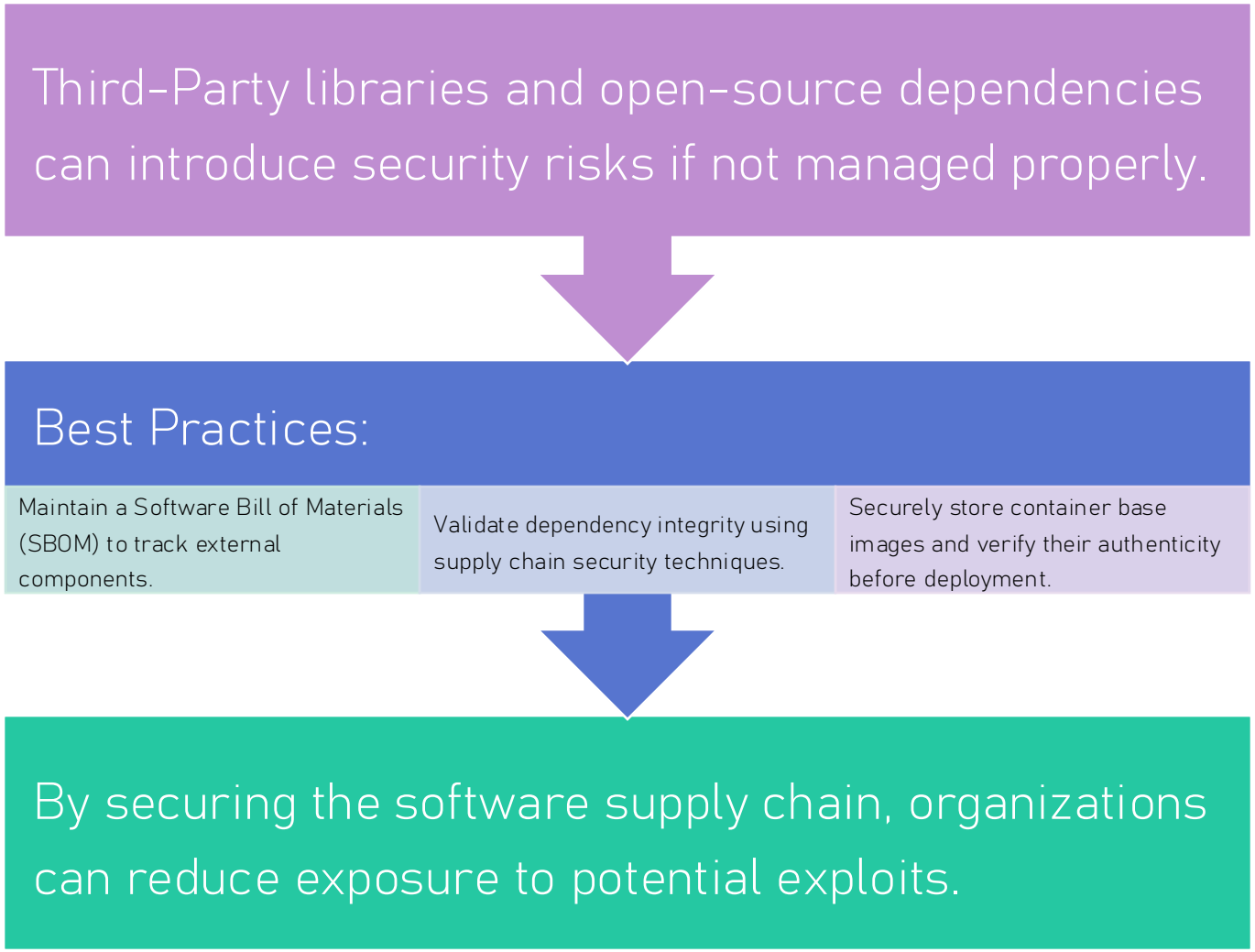
Secure Development Practices



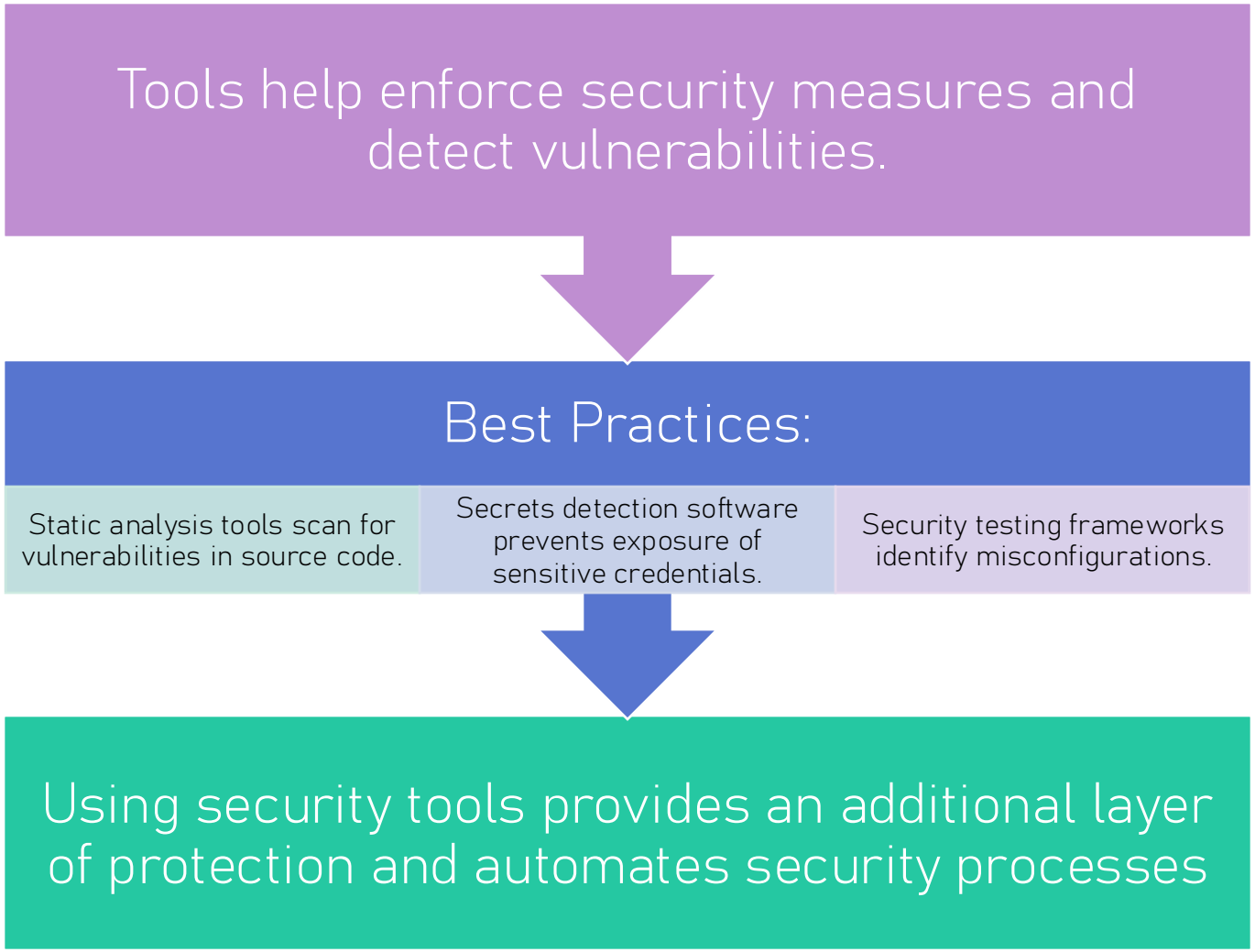
Automated Threat Detection and Monitoring



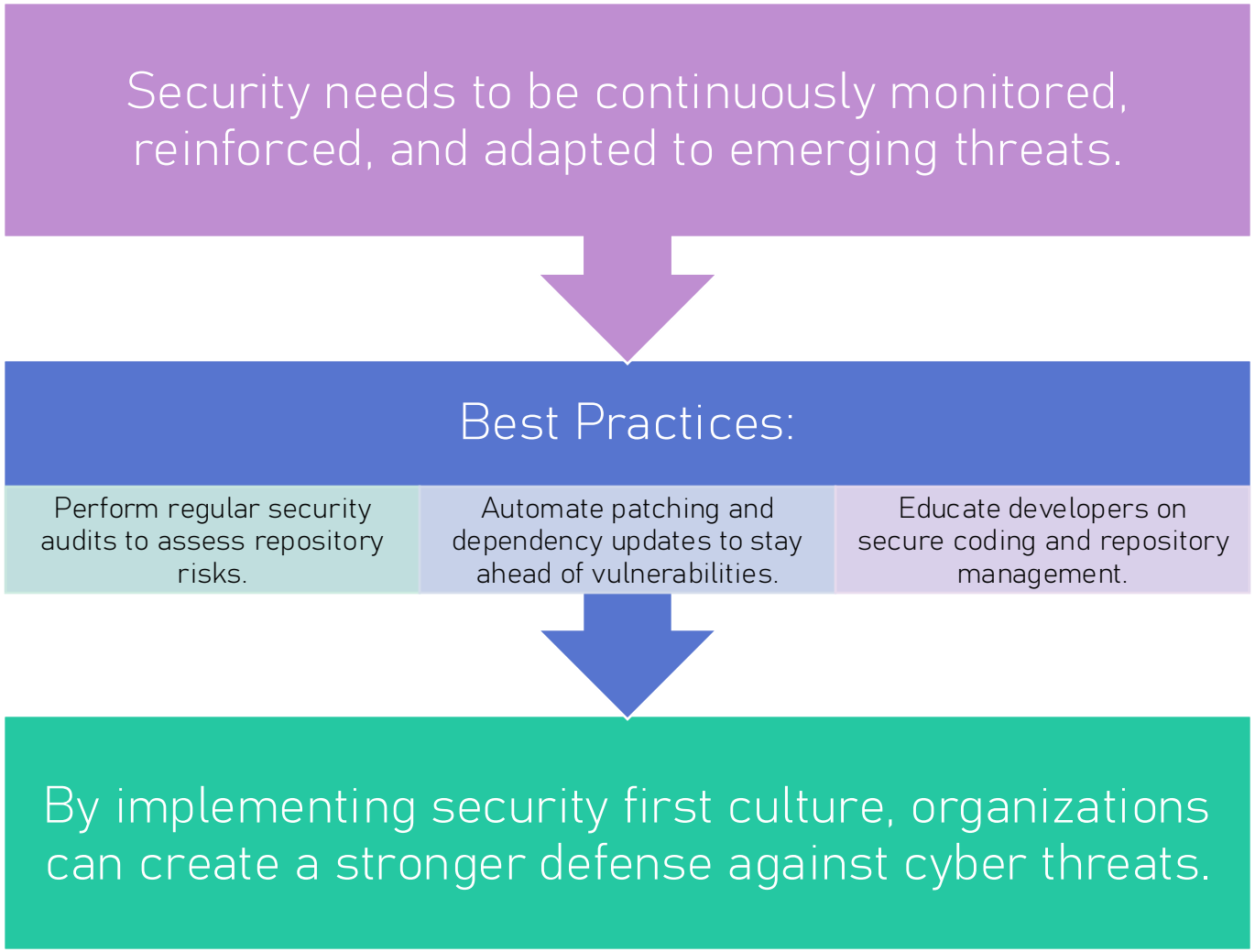
Protecting Open Source and Supply Chain Security



Security Tools for Repository Protection



Continuous Security Practices



Conclusion

- Securing shared source code repositories is important for software development.
- Control access with RBAC and MFA.
- Use secrets management tools to protect credentials.
- Automate vulnerability detection with security tools.
- Monitor repository activity for any unusual changes and threats.
- Implementing these security measures ensure that repositories remains safe and reliable.

References

- G. (n.d.). *Quickstart for securing your repository*. GitHub Docs. https://docs.github.com/en/code-security/getting-started/quickstart-for-securing-your-repository
- H. (2025, May 5). *Best Practices for Securing Code Repositories*. Harness. https://www.harness.io/harness-devops-academy/secure-code-repositories-best-practices
- Tal, L. (n.d.). *Securing Source Code in Repositories is Essential: How To Get Started*. Snyk. https://snyk.io/articles/securing-source-code-repositories/