Loreto E Eclevia

Module 9.2 DevOps

Bellevue University

July 14, 2024

THIS PRESENTATION IS ABOUT SECURING A PROJECT RELATED TO SECURITY CONTROLS IN SHARED SOURCE CODE SUCH AS WORKING THROUGH REPOSITORIES

- The groups focused on security and creating software are starting to see how crucial it is to understand the components of the software that companies use and buy. Keep an eye out for updates on new weaknesses found in these components. Being aware of these weaknesses can allow security groups to respond to new dangers faster. More often, software source code includes a list of its parts, known as a software bill of materials. Another option is for security groups to use software that analyzes source code to find any components from other companies being used.

Making Just Culture a Reality: One Organization's Approach

- Acquire secure external source code
- Protect source code access and storage
- Analyze source code
- Identify source code components

- Practices and Processes
- Background
- Methods
- Conclusion

Acquire secure external source code

Confirm the authenticity of every piece of code obtained from external sources, whether it's intended for internal purposes or for integration into products or services. Ensure that you only download code from reputable sites and employ methods to ensure its integrity, like checking cryptographic hashes. Depend on automated processes to prevent mistakes made by humans, like misspelling a URL or neglecting to compare cryptographic hash values (Scarfone, 2022).

PROTECT SOURCE CODE ACCESS AND STORAGE

Ensure the protection of source code by storing it in highly secure code repositories. Limit access to only those who need it, including individuals, applications, and services, and pay close attention to granting access for code modification. Verify each user in the repository, regardless of their role, and set up the repositories to record all modifications in audit logs. Make it a requirement for developers to place all code from third-party sources into these repositories (Scarfone, 2022).

Analyze source code

- Whether you create your source code or obtain it, employ static analysis tools to look for weaknesses and harmful code. Don't only examine the code upon acquisition. Ensure you have tools that conduct scans regularly, or even continuously. Although tools are capable of performing the majority of the tasks, it's important for individuals to examine and probe the findings of these tools. Make sure your plans for responding to incidents and procedures are ready to address the identification of harmful code (Scarfone, 2022).

Identify source code components

The groups focused on security and creating software are starting to see how crucial it is to understand the components of the software that companies use and buy. Keep an eye out for updates on new weaknesses found in these components. Being aware of these weaknesses can allow security groups to respond to new dangers faster. More often, software source code includes a list of its parts, known as a software bill of materials. Another option is for security groups to use software that analyzes source code to find any components from other companies being used (Scarfone, 2022).

REFERENCE

Techtarget (Scarfone, 2022): https://www.techtarget.com/searchsecurity/tip/Top-4-source-code-security-best-practices

National Library of Medicine: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3776518/#:~:text=In%20a%20just%20culture%2C%20both,Above%20all%2C%20Safety.

DevOps Handbook: Kim. (2016). DevOps Handbook (2nd ed.). National Book Network.