2024/25_N15 - Secure Software Development Lifecycle - SSDLC

Proposta de Bolsa/Estágio na Altice Labs

ID do Projeto	2024/25_N15
Departamento	SSO
Proponente	Mafalda Gimarães Nunes Paulo Miguel Vieira
Data de validade	31-Dec-2024

IDI - Áreas Chave

Security & Privacy

Tema / Título

Secure Software Development Lifecycle

Contexto

Security is an important part of any application that comprises critical functionality or personal/sensitive data. Recent cyber attacks (such as MOVEit and AT&T attacks) and the approval of more strict regulations (like the European GDPR and the NIS2 Directive) put tremendous pressure on the need for various industries to ascertain the security of their products and services. Security applies at every phase of the software development life cycle (SDLC), starting from the requirements gathering stage to the deployment and maintenance of the application. It includes educating developers on the best secure coding practices and available frameworks for security, conducting an architecture risk analysis at the start, considering security when planning and building test cases, and using tools for automated security tests on the CI/CD pipeline. With dedicated effort, security issues can be addressed in the SDLC pipeline well before deployment to production. This reduces the risk of finding security vulnerabilities in an application and minimizes the impact when they are found.

Objetivos do Projeto

The main goal of this project is to improve the secure software development lifecycle methodology currently recommended at Altice Labs. Some work has already been done regarding the comparison and selection of open-source tools for static analysis, dependency analysis, and dynamic analysis. This project should continue that work, by adding to the comparison open-source tools for interactive analysis and commercial tools for static analysis, dependency analysis, dynamic analysis, and interactive analysis. Additionally, this project should establish effective rules to be applied in Altice Labs CI/CD pipelines as security gates, taking into account the selected tools' inputs and outputs. The proposed tools and security gates should then be applied to an Altice Labs application CI/CD pipeline.

Aspetos Inovadores

- Software supply chain security;
- CI/CD pipeline security;
- Automated validation of security best practices in modern architectures (e.g., Kubernetes).

Ferramentas a utilizar

- GitHub and GitHub Actions;
- CI/CD Security Tools (SAST, SCA, DAST, IAST).

Referências Bibliográficas

- https://www.trio.dev/blog/secure-sdlc
- https://www.hackedu.com/blog/what-is-the-s-sdlc-or-secure-sdlc

- https://books.google.pt/books?id=HmtgEAAAQBAJ&lpg=PT161&dq=Dagda%20containers%20notifications&hl=pt-PT&pg=PA1#v=onepage&q&f=false
- https://www.synopsys.com/blogs/software-security/integrating-automated-ast-tools/

Atividades

- Review the selected tools for CI/CD security;
- Research, compare, and select new promising open-source tools for interactive analysis;
- Research, compare, and possibly select commercial tools for CI/CD security;
- Define rules to be applied in CI/CD pipelines as security gates, considering Altice Labs' needs;
- Test the selected tools and defined rules in the context of an Altice Labs application;
- Write a final report with the main findings of the project.

Competências Chave Requeridas

- Security knowledge, more specifically regarding DevSecOps and security in the CI/CD pipeline;
- Critical thinking;
- Good communication skills.

Orientador (nome e e-mail)

Mafalda Nunes - mafalda-g-nunes@alticelabs.com

Paulo Vieira - paulo-m-vieira@alticelabs.com

Para concorrer podes enviar a tua candidatura, envia e-mail para o Programa GENIUS: genius@inova-ria.pt