

# 2024/25\_N16 - Runtime Application Security and Observability

## Proposta de Bolsa/Estágio na Altice Labs



ID do Projeto	2024/25_N16
Departamento	SSO
Proponente	Mafalda Gimarães Nunes Paulo Miguel Vieira
Data de validade	31-Dec-2024

### IDI - Áreas Chave

Security & Privacy

### Tema / Título

Runtime Application Security and Observability

### 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. As attacks on applications continue to rise, businesses are finding it challenging to properly safeguard all of their applications, some of which may harbor vulnerabilities that were not identified or mitigated early on within the software development lifecycle (SDLC) or through various types of application security testing. This is why monitoring the runtime application and including protection within the application itself helps companies better balance security requirements with the imperative to roll out apps in a timely manner.

### Objetivos do Projeto

The main goal of this project is to improve the runtime application security and observability mechanisms in place at Altice Labs. It includes the gathering of state-of-the-art best practices in this scope, as well as the research and comparison of the available open-source and commercial tools that help address this issue. This comparison should result in the proposal of a minimalist toolset fit to implement the researched state-of-the-art best practices in Altice Labs applications. The researched best practices and proposed toolset should then be applied to an Altice Labs application deployment, to validate its feasibility and ability to address Altice Labs needs regarding runtime application security and observability.

### Aspetos Inovadores

- Security Information and Event Management (SIEM);
- Extended Detection and Response (XDR);
- Software supply chain security (runtime component analysis);
- Runtime Application Self-Protection (RASP);
- Cloud-Native Application Protection Platform (CNAPP).

### Ferramentas a utilizar

- Kubernetes;
- Private Cloud (OpenShift) and Public Cloud (AWS);
- Observability Tools (SIEM, XDR, etc.);
- Runtime Security Tools (component analysis, RASP, CNAPP, etc.).

### Referências Bibliográficas

- <https://www.techtarget.com/searchsecurity/ehandbook/Security-observability-tools-step-up-threat-detection-response>

- <https://www.infoworld.com/article/3691293/observability-will-transform-cloud-security.html>
- <https://coralogix.com/blog/observability-security-work-together/>
- <https://www.paloaltonetworks.com/cyberpedia/what-is-xdr-vs-siem>
- [https://owasp.org/www-community/Component\\_Analysis](https://owasp.org/www-community/Component_Analysis)
- <https://www.crowdstrike.com/cybersecurity-101/cloud-security/runtime-application-self-protection-rasp/>
- <https://www.synopsys.com/blogs/software-security/rasp-application-security-testing/>
- <https://www.wiz.io/academy/what-is-a-cloud-native-application-protection-platform-cnapp>
- <https://sysdig.com/learn-cloud-native/cloud-security/cloud-native-application-protection-platform-cnapp-fundamentals/>

## Atividades

- Research state-of-the-art best practices concerning runtime application security and observability;
- Research, compare, and select open-source tools for runtime security and observability;
- Research, compare, and possibly select commercial tools for runtime security and observability;
- Test the selected tools in the context of an Altice Labs application, including the analysis of the performance impact caused by such tools;
- Write a final report with the main findings of the project.

## Competências Chave Requeridas

- Security knowledge, more specifically regarding runtime security and observability;
- Critical thinking;
- Good communication skills.

## Orientador (nome e e-mail)

Mafalda Nunes - [mafalda-g-nunes@alticelabs.com](mailto:mafalda-g-nunes@alticelabs.com)

Paulo Vieira - [paulo-m-vieira@alticelabs.com](mailto:paulo-m-vieira@alticelabs.com)

Para concorrer podes enviar a tua candidatura, envia e-mail para o Programa GENIUS: [genius@nova-ria.pt](mailto:genius@nova-ria.pt)