Altice Labs Innovation Summer Camp 2024 - Threat Modeling in Modern Software Architectures

Código/Code	Summer Camp'24_Threat Modeling	
Departamento/Department	ISC21	
Orientador/Tutor	Mafalda Guimarães Nunes	
ID	N17	
Estagiário/Trainee	<a preencher pelos RH>	

Tema /Título/Title	Threat Modeling in Modern Software Architectures
Âmbito/Enquadramento /Freamwork	An interconnected world with an increasing number of systems, products, and services relying on the availability, confidentiality, and integrity of sensitive information is vulnerable to attacks and incidents. Unfortunately, the threat landscape expands and new threats, threat agents, and attack vectors emerge at all times. Threats can come from outside or within organizations, and they can have devastating consequences. Recent cyber attacks and the approval of more strict regulations put tremendous pressure on the need for various industries to ascertain the security of their products and services. Attacks can disable systems entirely or lead to the leakage of sensitive information, which would diminish the consumer's trust in the system provider. Defending against these threats requires that organizations are aware of such threats and threat agents. Threat modeling plays a vital role in architecting and designing systems with security in mind. It is a process by which potential threats, such as structural vulnerabilities, can be identified, enumerated, and prioritized all from a hypothetical attacker's point of view. By incorporating threat modeling into the design process, organizations can proactively address security concerns and build robust and resilient systems. Altice Labs incorporates security-by-design principles in its software development lifecycle, which includes performing threat modeling. In this regard, the Microsoft Threat Modeling Tool (TMT) is used to draw flow diagrams, identify threats, and propose mitigations.
Objetivos do Projeto/Goals	The main goal of this project is to improve the current threat modeling process at Altice Labs, by incorporating threats and mitigations specific to modern software architectures (microservices, Kubernetes, Cloud, etc.) in the used tool. This includes the gathering of state-of-the-art threats, mitigations, and best practices in these modern architectures, as well as the development of Microsoft TMT templates with the respective threats and mitigations.
Atividades/Activities	Plano de trabalhos: • Research state-of-the-art best practices concerning modern software architectures (e.g., Microservices, Kubernetes, Cloud); • Develop Microsoft TMT templates with the researched threats and mitigations for modern software architectures; • Test the developed templates in the context of an Altice Labs application; • Final report.
Tecnologias envolvidas/Involved technologies	• Microsoft Threat Modeling Tool (TMT); • Kubernetes; • Private Cloud (OpenShift) and Public Cloud (AWS).
Requisitos/Requirements	Basic security knowledge.
Orientador/Tutor	Mafalda Guimarães Nunes
Email (extenso)	mafalda-g-nunes@alticelabs.com
Local / Place	Aveiro
Modelo de Trabalho/Work Model (Remote/Mix/Local)	Mix

Duração/Duration	1 to 3 months
Data de Inicio/Start_Date	To be defined
Data de Fim/Due_Date	To be defined
Entre que datas/Between dates	Between July and September
Observações/Observations	