



# **secure(UA)ll**

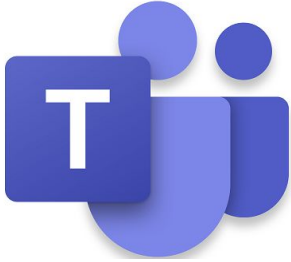
## Security Exposure Sentinel

Licenciatura em Engenharia Informática - PI

Grupo 4 - Projeto 6

# **Milestone 1**

# Communication plan



Mentoring

**Teams**

mentoring communication



Documentation

**Drive**

Repository for docs



Git Platform

**Github**

Private repository



Team Communication

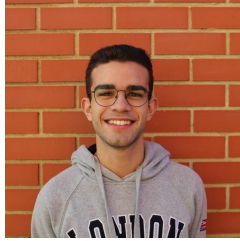
**Slack**

internal discussion

# Team Members



Eduardo Santos  
Product Owner



Gonçalo Matos  
Architect



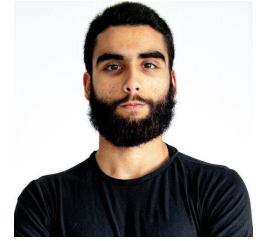
Pedro Bastos  
Team Manager



Margarida Martins  
DevOps



Isadora Loredó  
Tester



André Morais  
Lead Developer



João Paulo Barraca  
Advisor



André Zúquete  
Co-Advisor



Ricardo Martins  
Colaborator

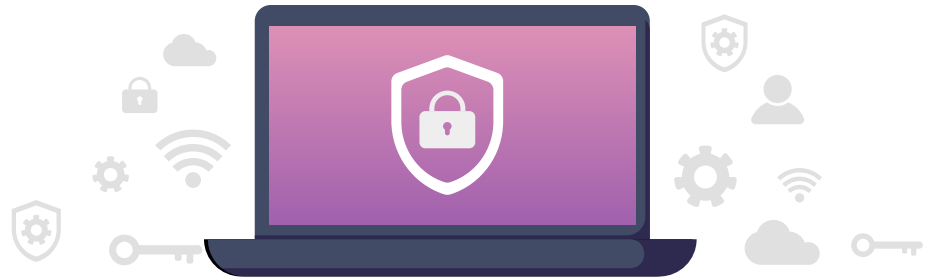


Vitor Cunha  
Colaborator

# Context

The **University of Aveiro** has a **very high** exposure to the outside world, through webpages/machines that export services.

The number of public domains of this institution exceeds **1500**, each of which can potentially **disseminate** information or even allow **exploitation** of flaws in its software.



# Problem

The **compromise** of any of these systems, even if the specific system is not much relevant itself, can lead to the **attack** being scaled laterally to others, either with **more sensitive data** or with **higher criticality**.

It is therefore vital to have systems that can monitor a wide range of systems, detecting and alerting to potential **security issues**.

This alert can be carried out for the **UA services**, but it can also include the **owners** of this services.



# Project Goals

## Detect Vulnerabilities

Constant monitoring in all the IP address space of UA

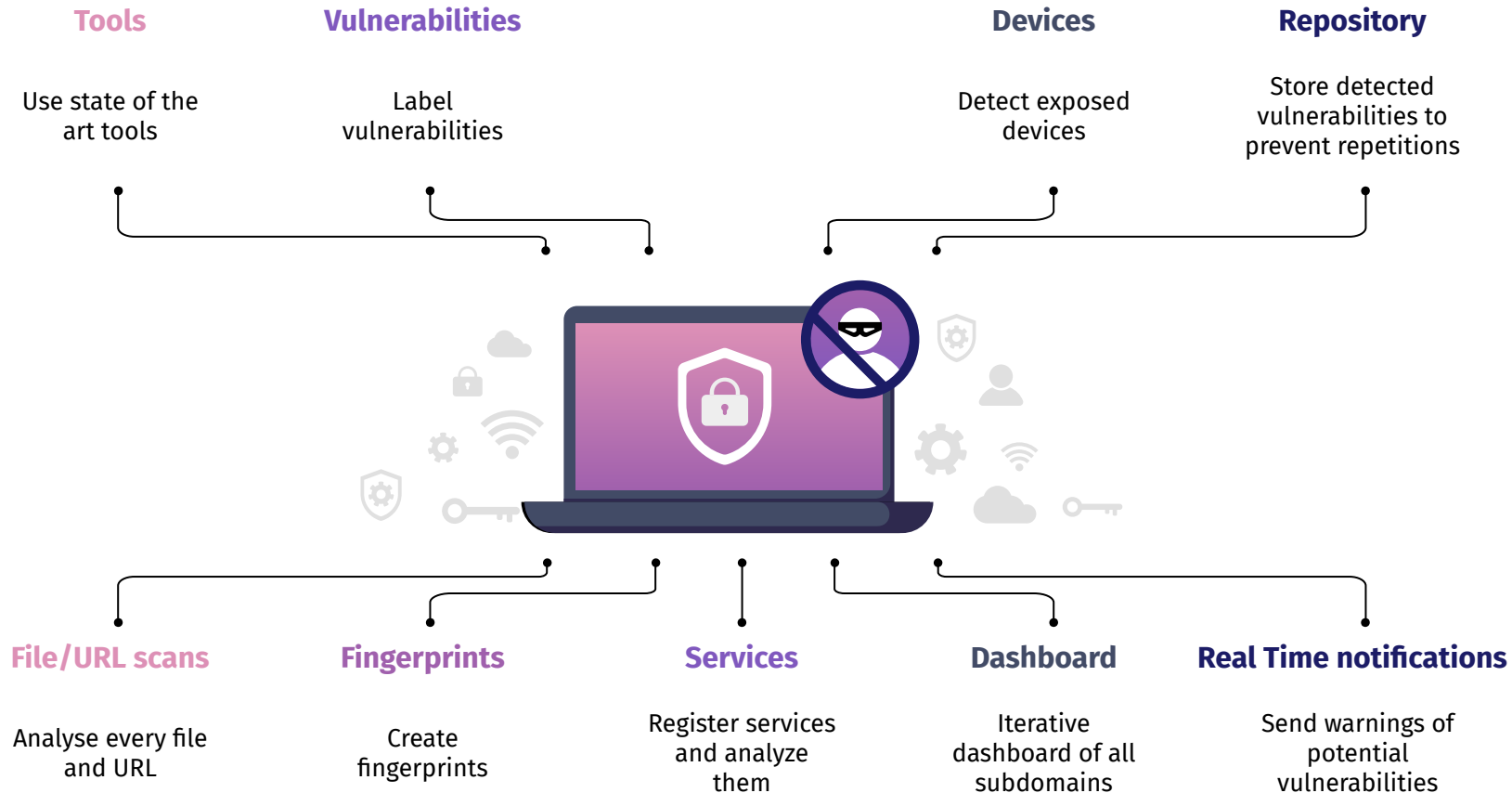
## Prevention Culture

By encouraging fixes before they become a problem

## Reduce Risk

Alert the owners about the problems found

# Project Tasks





# Expected Results

## Scanning

Automatic scanning for vulnerabilities of the UA's exposed services.



## Dashboard

- A usable dashboard containing:
- Overall information about the vulnerabilities detected.
  - Vulnerabilities found for a specific machine.



## Notifications

Automatic notification via e-mail to the responsible of the machine when a new vulnerability is found.



# Related Work

There are applications that allow us to scan URLs, IP addresses, Domains and Files to find potential malwares and exposures



Our application must be more focused on scanning for potential vulnerabilities, services, subdomains, etc

# Calendar

Inception	Week 1	Client's project scope presentation; team building; website construction; calendar; M1 presentation.	
	Week 2	M1	Understanding and researching the scope and objectives; derivables definition; architecture definition.
Elaboration	Week 3	Backlog management system setup; core stories defines.	
	Week 4	M2	Validate architecture.
	Week 5	M2	Setup the tools; prioritize user stories.
Construction	Week 6, 7	Development of a few core user stories; demonstrate architecture end-to-end.	
	Week 8, 9	M3	New user stories required for a functional MVP deployed, specially covering data aggregation/ visualization.
	Week 10	Required user story: alarms/events detection on data streams.	
	Week 11	Implement integrations with external services; integrate the cypher-physical layer.	
	Week 12	Stabilize presentation layer and production environment; update documentation (project specific. and software documentation).	
Transition	Week 13, 14	M4	Bug-fixing; stable iteration built for project presentation.
	Week 15	Product release; demo, video and public version of the website.	

M1: presentation of the life cycle objectives and calendar for the project.

M2: presentation of the lifecycle architecture; the milestone is achieved when the architecture has been validated.

M3: prototype; mid-term presentation with supervisors; peer evaluation.

M4: project presentation; all functionality has been developed