



# **secure(UA)ll**

## Security Exposure Sentinel

Licenciatura em Engenharia Informática - PI

Grupo 4 - Projeto 6

## **Milestone 2**

# Functional Requirements



## Dashboard

Web platform available 24/7 through UA IDP access that allows the system management and vulnerability monitoring



## Alerts

Email sent every time a vulnerability is detected. It informs the manager of its existence and suggests possible corrections



## Scrapping

With a configurable periodicity and with several levels (from the less to the most evasive), it recurs to external pluggable tools



## Vulnerability Analysis

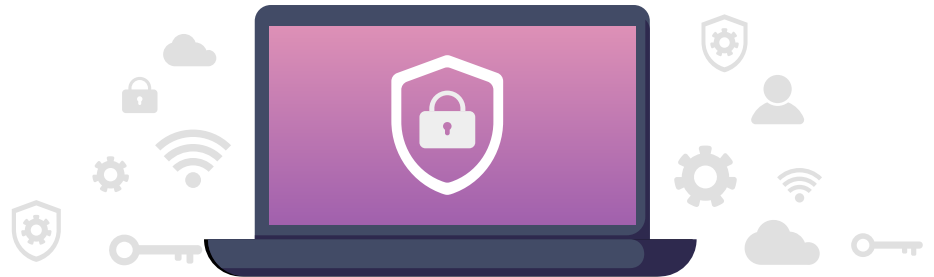
Based on the data gathered by scraping tools, the risk is computed based on CVSS and the vulnerability scan

# 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.

This domains provide services that need to be checked periodically to prevent malfunction and/or not working at all.



# State-of-art

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

# Personas



**Rafaela Fernandes**

**Profession:** Servers manager at STIC

**Age:** 31

**Gender:** Female

**Education:** Master in Software Engineering

**Goals:** Rafaela is the responsible for STIC's servers. She has a goal to assist the machines in fault recuperation, risk mitigation and searching/eliminating threats.

**Stories:** As the server's manager I want to be able to keep the servers updated on a security level, preventing possible attacks. I also want to know which machines are obsolete.



**Carla Pereira**

**Profession:** Professor at DETI

**Age:** 42

**Gender:** Female

**Education:** PhD in Software Engineering

**Goals:** Besides teaching at DETI Carla is also a researcher at IT. Through the years, both in her investigation and teaching, she has created multiple web services that are available inside and outside UA's network. However, she can not maintain all the systems updated and with no vulnerabilities because she does not have the amount of time needed to check every machine frequently.

**Stories:** As a professor and researcher I want to focus on my new projects and maintaining the existent ones only when strictly needed.



**Ricardo Ferreira**

**Profession:** Member of UA's Cibersecurity Office

**Age:** 38

**Gender:** Male

**Education:** Master in Computer Science

**Goals:** Ricardo is a member of UA's Cibersecurity Office, whose mission consists on promoting awareness and the adoption of a safer behavior regarding the usage and treatment of devices and digital information.

**Stories:** As an office member I want to be sure that safety measures are being correctly implemented.

# Actors

## Admin

The admin has access to the entire system and its features.

## Owner

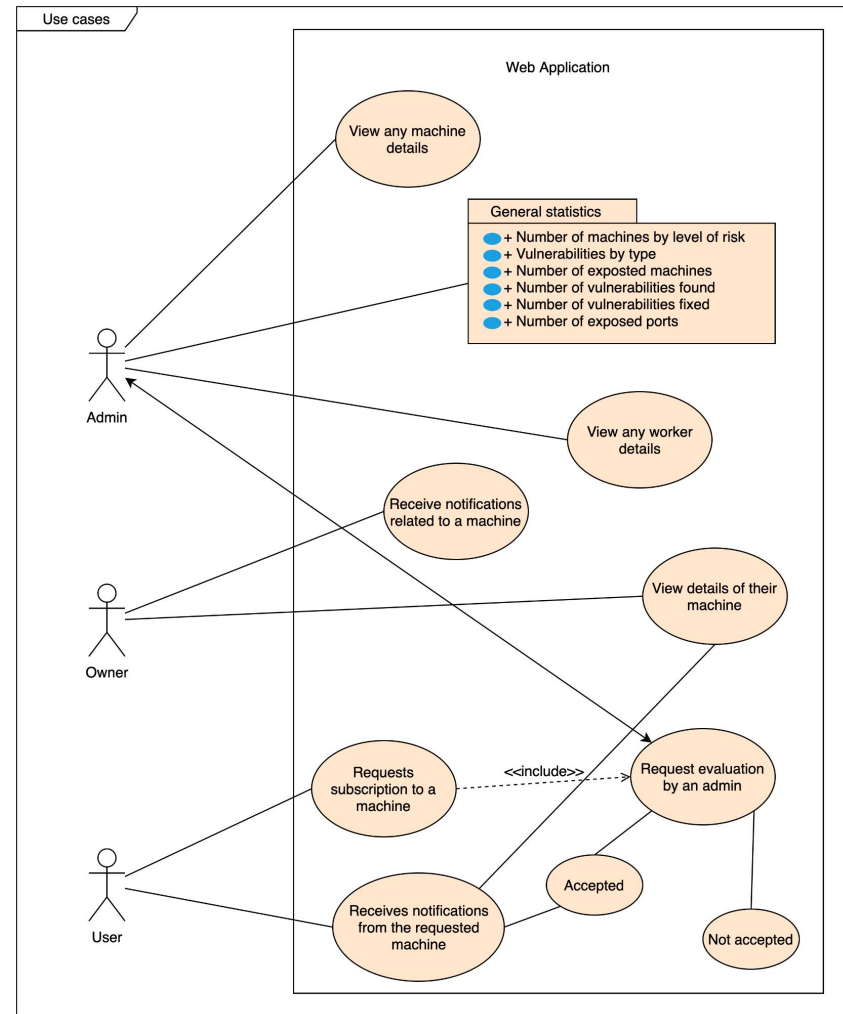
The owner can manage her/his machines, check statistics/vulnerabilities found, define a scrapping level for a specific machine, and receives notifications whenever a vulnerability is found.

## User

The user can check global statistics about the system, and can request to receive notifications about a specific machine.

# Core use cases

- Machine details
- General statistics
- Notifications
- Machine subscription
- Worker details





# Non-Functional Requirements

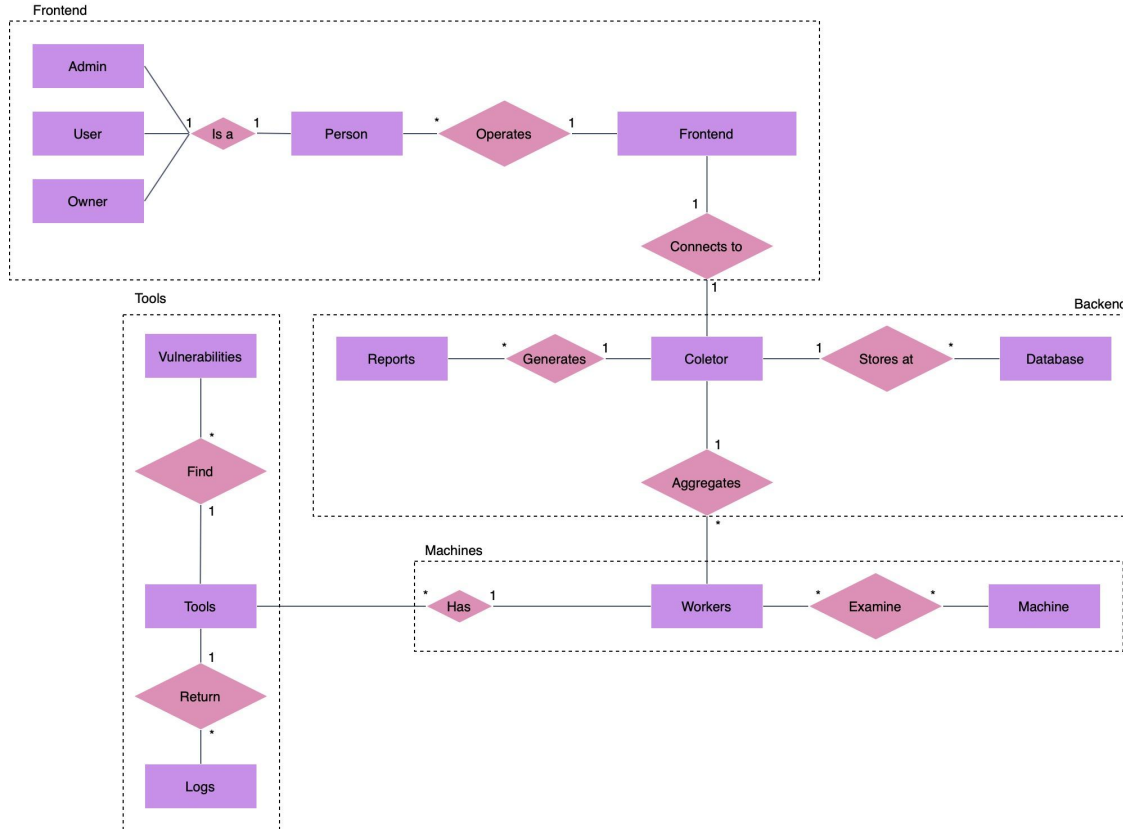
Requirement	Description	Priority
Scalability	Distribution of work between several workers in order to respond to high workloads.	Low
Portability	Containerization allows simple implementations in simple execution environments.	Low
Usability	Intuitive management and control interface creates a good user experience.	Medium
Privacy	Ensure that any sensitive or personal data retrieved during scans is not stored.	Maximum
Security	Only authorized users (administrators and subscribers) have access to the data and vulnerability reports for each machine.	Maximum

# Assumptions & Dependencies

In order for the application to work as expected the following assumptions are made. The first requirement to operate this product is that the user must have a stable connection to the Internet, as well as the programs needed to access it (web browser, etc.). It is also expected that the user has an active UA account, because the login process is made through UA's IdP.



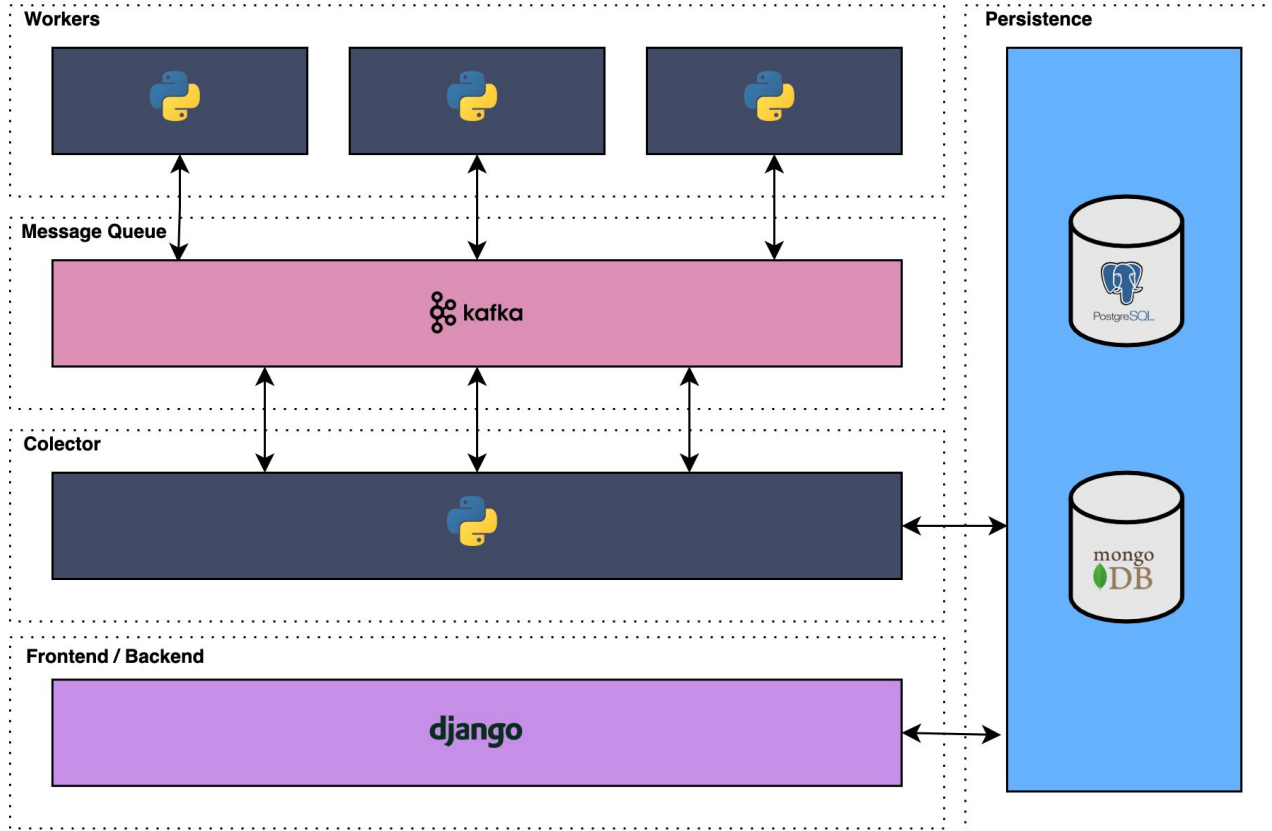
# Domain Model



## Entities:

1. Person
  - a. Admin
  - b. User
  - c. Owner
2. Frontend
3. Colector
4. Reports
5. Database
6. Workers
7. Vulnerabilities
8. Tools
9. Logs
10. Machine

# Architecture



# Mock-ups

For the mockups, we used a prototyping tool called [Figma](#)

