

# CAHIER DES CHARGES



Thomas Genin - Nicola Piemontese - Valentin Tournier - Thomas Violent

CPE Lyon – 5ICS

## Table des matières

I Définition du projet .....	2
II Objectifs du projet.....	2
III Périmètre.....	2
IV Rôles.....	2
V Cas d'utilisation.....	3
VI Spécifications fonctionnels .....	3
VII Contraintes techniques.....	3
VIII Planning prévisionnel .....	4
IV Maquettes .....	4

## I Définition du projet

Le projet s'inscrit dans une volonté d'étendre l'offre de détection des mails malveillants en proposant un outil similaire au fonctionnement de VirusTotal qui permettrait entre autres, l'analyse de mail sur demande. L'idée a émergé sur un besoin, celui pour un analyste SOC de détecter simplement et automatiquement le caractère suspicieux (ou non d'un mail) au travers de différents facteurs.

## II Objectifs du projet

Nous voulons développer une solution permettant une analyse complète des emails. Celle-ci permettra d'avoir une analyse approfondie afin de détecter les emails malveillants à partir de plusieurs indicateurs.

Les utilisateurs pourront soumettre des emails à la solution et un score de risque sera calculé afin de définir si celui est malveillant.

## III Périmètre

Cette application se destine principalement au professionnel de la cybersécurité, notamment les analystes SOC.

En effet, les analystes doivent régulièrement étudier des emails tagués comme potentiellement malveillant par les systèmes de détections automatisée ou signalés par les utilisateurs. Le site permet de réaliser une analyse approfondie de manière automatique.

## IV Rôles

Product Owner  
Nicola Piemontese

Scrum Master  
Sprint 1  
Valentin Tournier

Scrum Master  
Sprint 2  
Thomas Violent

Scrum Master  
Sprint 3  
Thomas Genin

Security  
Compliance Officer

## V Cas d'utilisation

- Les utilisateurs doivent pouvoir uploader sur l'interface web un email à analyser
- Les utilisateurs doivent pouvoir visualiser le résultat de l'analyse
- Les utilisateurs doivent pouvoir lancer l'analyse d'un email via l'API
- Les utilisateurs doivent pouvoir visualiser l'historique et les résultats des précédentes analyses.

## VI Spécifications fonctionnels

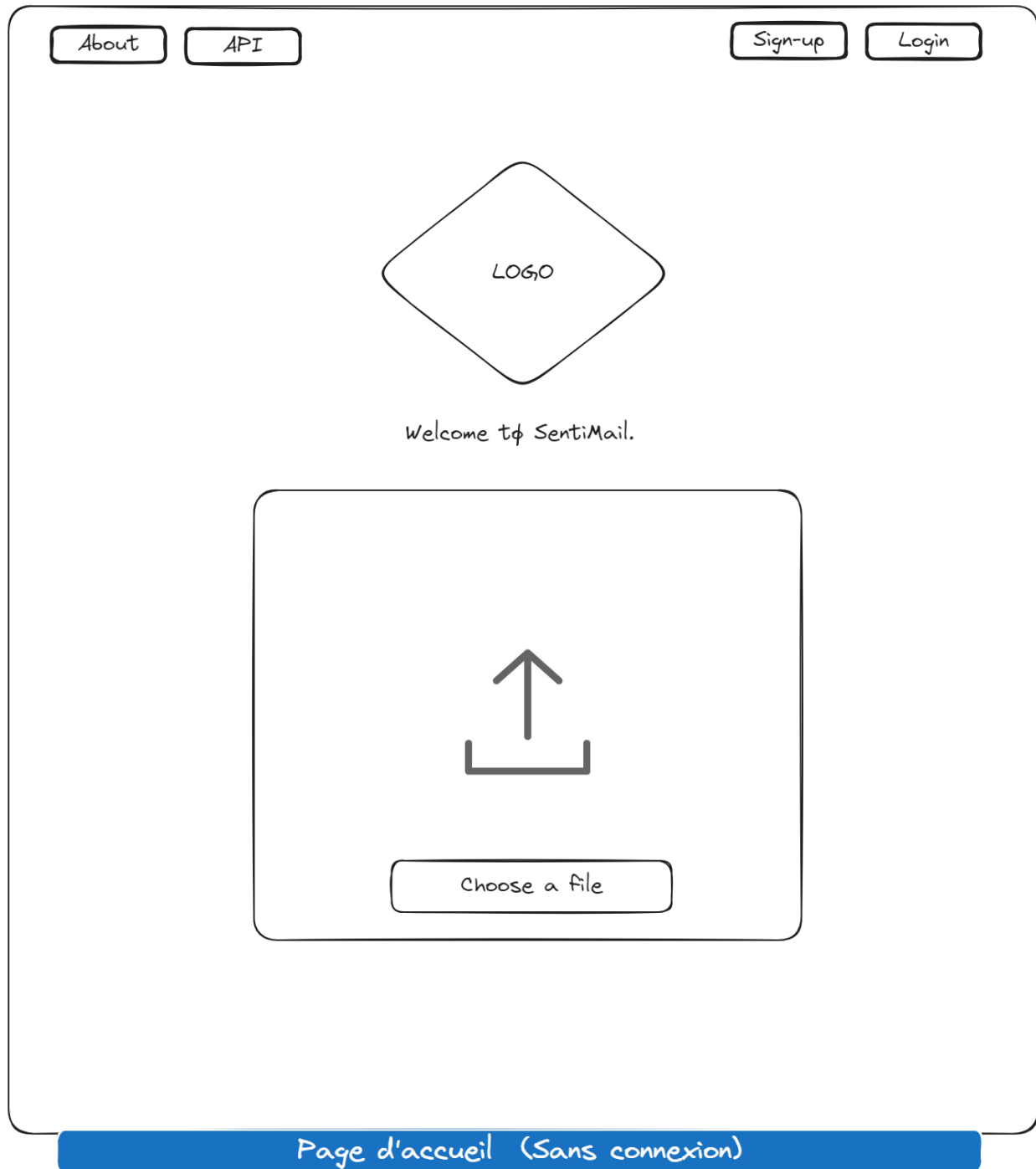
- Le site web doit être en anglais
- Les utilisateurs
  - o Doivent pour s'authentifier
  - o Voir leur mails/fichier envoyés par le passé
  - o Soumettre un mail ou un fichier qui sera scanné par l'appli
  - o Obtenir un retour de l'application, qui se traduira par un score de fiabilité concernant les mails envoyés
- Analyse des mails
  - o Les métadonnées des emails doivent être vérifiées à chaque scan, incluant :
    - La réputation du nom de domaine et de l'adresse IP.
    - Certains headers spécifiques (SPF, DKIM)
  - o Le contenu des emails doit passer une batterie de tests :
    - Fautes d'orthographe
    - Caractères dans une police non conventionnel
    - Liens web et toutes autres url présentes
      - Vérifier la réputation du domaine et l'adresse IP derrière le nom de domaine,
      - Vérifier si le lien écrit est bien le lien voulu (par exemple, si un site web amène vers google.fr, s'assurer qu'il n'est pas écrit google.fr)
    - Similaire à d'ancien mail reconnu comme spam
    - Typosquattage (par exemple un l et un I)
- Analyse des fichiers
  - o La potentielle présence de code malveillant doit être vérifiée, incluant :
    - Une analyse complète (Virus total)
    - L'ouverture des fichiers dans des sandbox dédiées (si applicable)
  - o Le type de document doit être vérifié
  - o Si le fichier est un contenant (un fichier zip par exemple), le contenu de chaque fichier doit être vérifié.

## VII Contraintes techniques

- La solution doit utiliser une base de données relationnelle ou noSQL.
- Le stockage des mails et des pièces jointes doit se faire sur un bucket S3 ou équivalent.



Page N°1 : Page d'accueil



Page N°2 – Page de connexion

The wireframe shows a login page layout. At the top center is a circle labeled "Logo". Below it is the text "Log in to SentiMail". This is followed by two rounded rectangular input fields, the first labeled "email" and the second labeled "password". Below the password field is the text "Forgot password ?". Further down is a rounded rectangular button labeled "Log in". At the bottom of the main content area is the text "Don't have an account ? Sign up". The entire page content is enclosed in a large rounded rectangle. Below this rectangle is a solid blue horizontal bar containing the text "Page de connexion" in white.



### Page N°3 – Page de création de compte

Logo

Sign up to SentiMail

email

password

Sign up

Already have an account? Log in

Page de création de compte

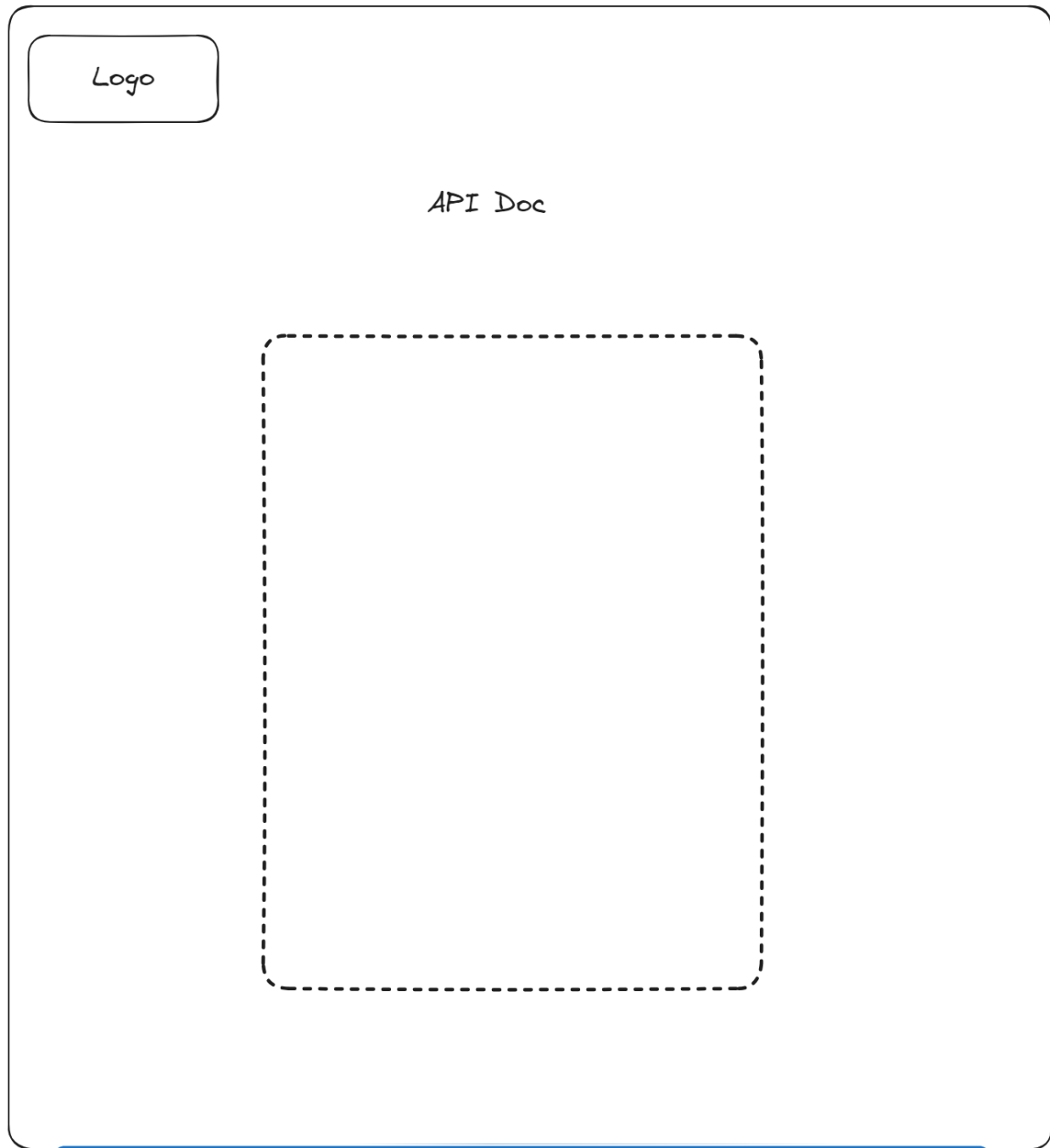
Page N°1 - Page d'accueil

— Cliquez sur le bouton  
Sign Up —>

Page N°3 - Page de creation de  
compte



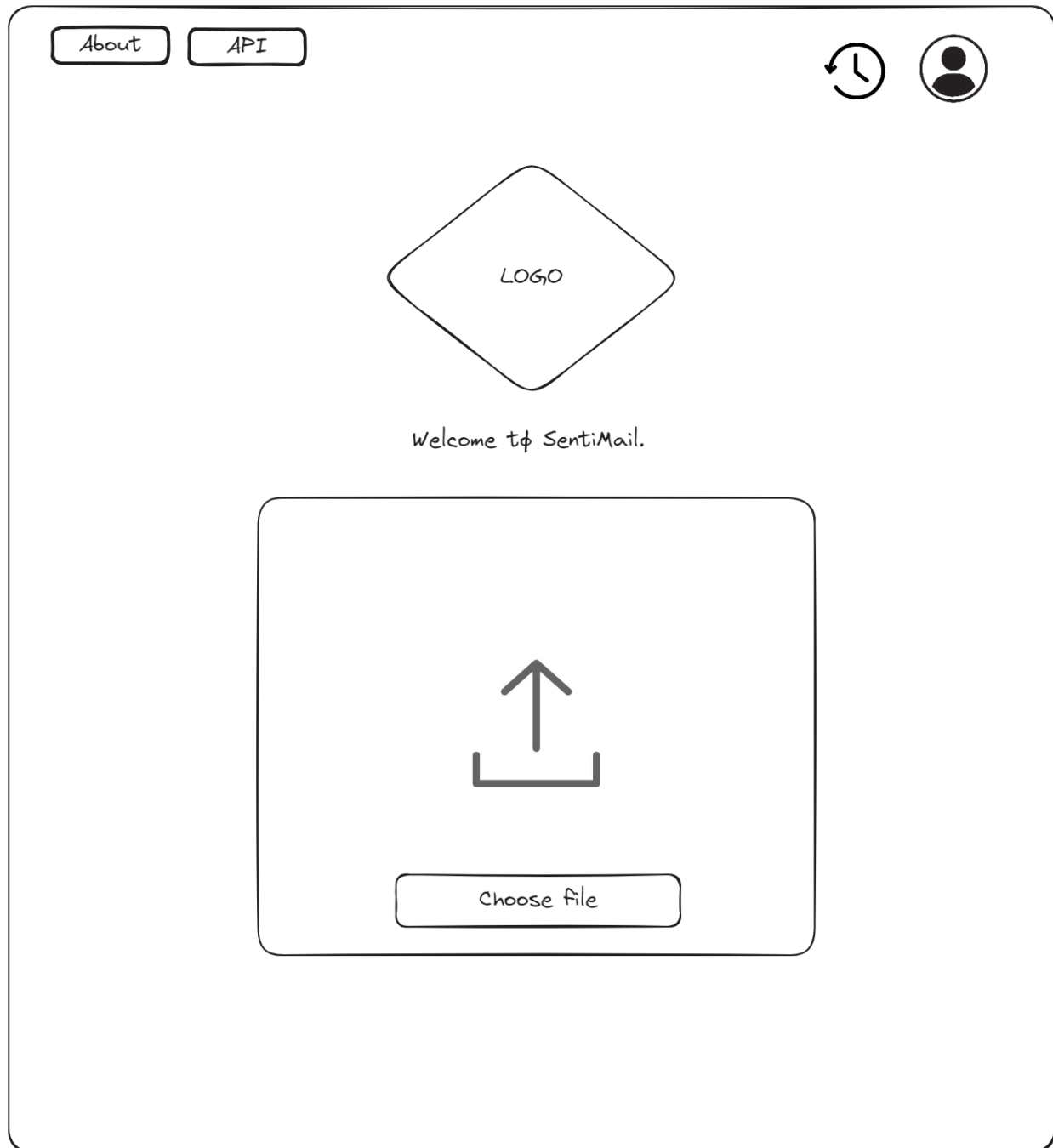
Page N°4 – Page de documentation d'API



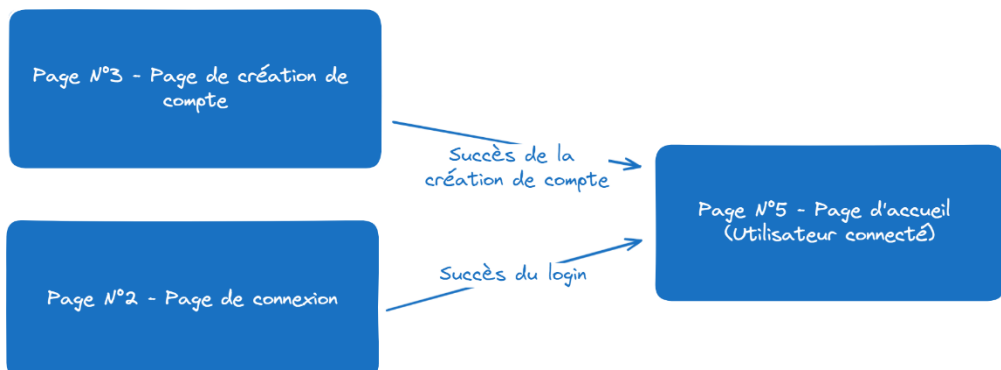
Documentation API de l'application



## Page N°5 – Page d'accueil (Utilisateur connecté)





### Page d'accueil (Utilisateur connecté)



## Page N°6 – Page d'administration utilisateur

Logo



Account

Name

John

Change name

Email

John@mail.fr

Change email

Password

Change password

API Token

Generate token

Page d'administration utilisateur



Page N°5 - Page d'accueil  
(Utilisateur connecté)

— Clique sur le bouton  
user →

Page N°6 - Page d'administration  
utilisateur

## Page N°7 – Page d'historique scan

AboutAPI



LOGO

Name

Historic

Sort by nameSort by date

Date : dd/mm/yyyy  
Result : Success / fail  
Details :

Context :  

Sender : example@example.com  
To : example@example.com  
Subject : example  
xxxxxxxxx xxxxxxxx xxxx

Date : dd/mm/yyyy  
Result : Success / fail  
Details :  
Context :

### Page historique utilisateur



Page N°5 - Page d'accueil  
(Utilisateur connecté)

— Cliquez sur le bouton  
Historique →

Page N°7 - Page historique de  
scan

## Page N°8 – Page de résultat scan

Logo



XX %  
Score

Results

Description

Date  
From  
To  
Sujet

Recap

Indicators

Details

Metadata

Content

Attachments

### Page de résultat (après scan)

