Ines Ayoub, Raphaël Letourneur, Maela Schmidt, Théo Vigreux

Dossier de définition

Projet G11 : CVE Warn

Serveur de surveillance de CVE

ENSIBS – Cyber4

2021 – 2022

Table des matières

Introduction

Il est important de définir les différents éléments composant notre système ainsi que le fonctionnement de ce dernier. C'est pour cela que nous avons créé un dossier de définition contenant les définitions des éléments du système, un scénario opérationnel et une architecture de notre système. Cela va ainsi nous permettre de bien encadrer et comprendre ce projet.

Définition des éléments du système

Informations

- Application (nom, version)
- CVE impactant l'infrastructure (titre, criticité)
- Système d'exploitation (nom, version)
- Infrastructure (identifiant, mot de passe, nom de l'infrastructure)
- Machine hôte (système d'exploitation, infrastructure, adresse IP)

Biens supports

- Agents des machines clients (parc informatique)
- Serveur
- Sites de récupération des CVE (externes)
- Machines client
- Client

Acteurs

- Administrateurs du système
- Clients
- Prestataires

Fonctions

- Récupération des applications et des systèmes d'exploitation installés.
- Transmission chiffrée des informations clientes récupérées.
- Récupération des CVE.
- Affichage des différentes CVE impactant les applications et systèmes d'exploitation.
- Mise en place d'un service d'authentification sécurisé pour les clients.

Scénario opérationnel

L'avancement de notre projet nous a permis de mieux évaluer notre produit et d'avoir une vision plus globale de son utilisation. Ainsi, nous avons pu mettre en place un scénario opérationnel. Il s'agit d'une description de plusieurs séquences d'événement imaginées afin de mettre en situation notre produit et l'interaction avec le client. Notre scénario est le suivant :

Une entreprise cliente en pleine croissance souhaite surveiller son parc informatique afin d'évaluer s'il existe des vulnérabilités au sein de leurs applications ou systèmes d'exploitations. Elle fait donc appel à notre produit.

- ➔ Installation des agents clients sur leurs postes de travail et serveurs.
- ➔ Attribution à l'entreprise d'un accès personnel (login/mdp) sur notre site web pour la consultation de leurs vulnérabilités.
- ➔ Remontées d'informations concernant leurs applications/OS, chaque entrée est composée du nom de l'application, de sa version et de son type.
- ➔ Le serveur réceptionne les informations et vérifie dans la base de données des CVE si des CVE correspondent à chaque entrée reçue.
  - ◆ Si des CVE sont présentes, le serveur les lie à l'application concernée.
  - ◆ Si aucune CVE ne correspond, le serveur va récupérer les CVE correspondant sur 3 sites d'informations de CVE :
    - https://nvd.nist.gov/
    - https://cve.mitre.org/
    - https://www.cvedetails.com/

    → Une liaison est ensuite créée entre les CVE récupérées et les applications concernées.
- ➔ Génération d'un dashboard propre à chaque client accessible depuis l'extérieur.
- ➔ Affichage des applications/OS clientes ainsi que les CVE correspondantes sur le dashboard client.

Architecture du système

Présentation de l'architecture du système

Notre architecture se compose en 3 parties.

La partie principale est notre serveur de surveillance, c'est là que sont stockées toutes les données et que tout le traitement est effectué.

Ensuite nous avons le parc informatique client. Le parc client communique avec nous à travers internet. Nous disposons d'agents qui nous transmettent les données du parc que nous traitons sur notre serveur. Avec ce traitement, nous mettons à disposition un dashboard référençant toutes les informations du parc ainsi que les CVE impactantes que nous avons trouvées.

Enfin, nous agrémenterons notre base de données de vulnérabilité à l'aide de services externes tels que *CVE détails*, *NVD*, *Mitre*, etc.

Notre serveur dispose donc d'une partie frontal web composé de l'API pour la remontée des agents ainsi que des dashboard de retour d'information, d'une partie backend pour télécharger les CVE dans notre base de données, et d'un moteur mettant en corrélation les applications et les CVE.

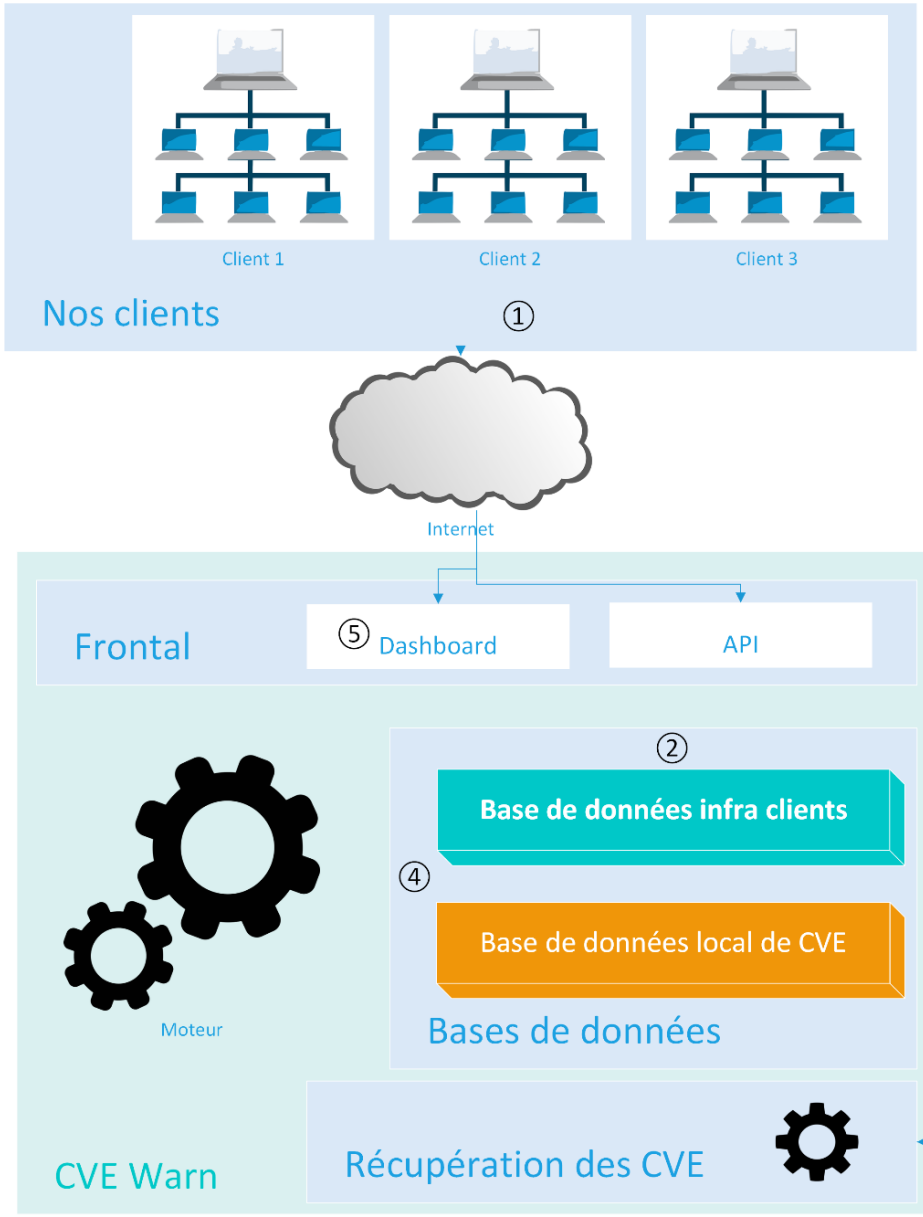
Pour notre démonstration, nous avons réuni la base de données de CVE et la base de données des informations clientes dans une même base.

Schéma d'architecture

Les schémas d'architecture nous sont très utiles afin de visualiser la structure globale de notre produit. Ils permettent de s'assurer que notre système répond bien à nos attentes et au besoin client.

Nous avons donc réalisé les quatres schémas d'architecture suivants :

- Un schéma d'architecture global reprenant les principaux composants de notre produit et permettant de comprendre le fonctionnement.
- Un schéma de notre base de données comprenant les informations sur les machines hôtes, les applications, les systèmes d'exploitation, les CVE et les informations clients.
- Un schéma de notre architecture frontale permettant de comprendre ce qui sera exposé aux clients, c'est-à-dire notre dashboard et l'API présent sur les machines clientes. Pour des raisons de sécurité, l'API ne dispose que de fonctions d'écriture afin d'éviter la fuite de nos informations clientes.
- Un schéma de diagramme de séquence afin de représenter les interactions entre les différents éléments du système dans un ordre chronologique.



Architecture CVE Warn

① Nos agents sont déployés sur les PC de nos clients et envoient les informations relevées à notre API.

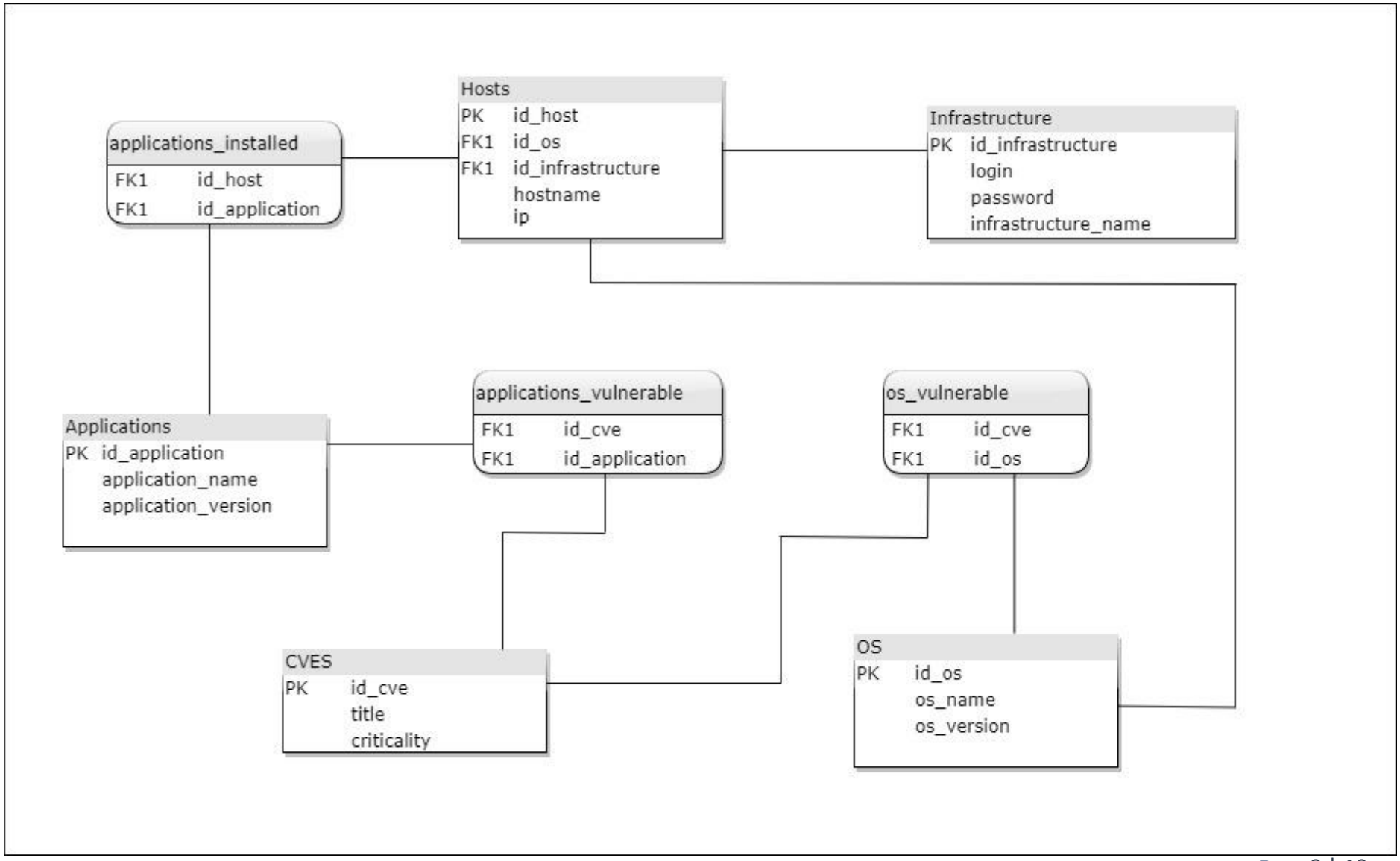
② Notre moteur analyse la remontée d'informations pour stocker les données clientes en base de données.

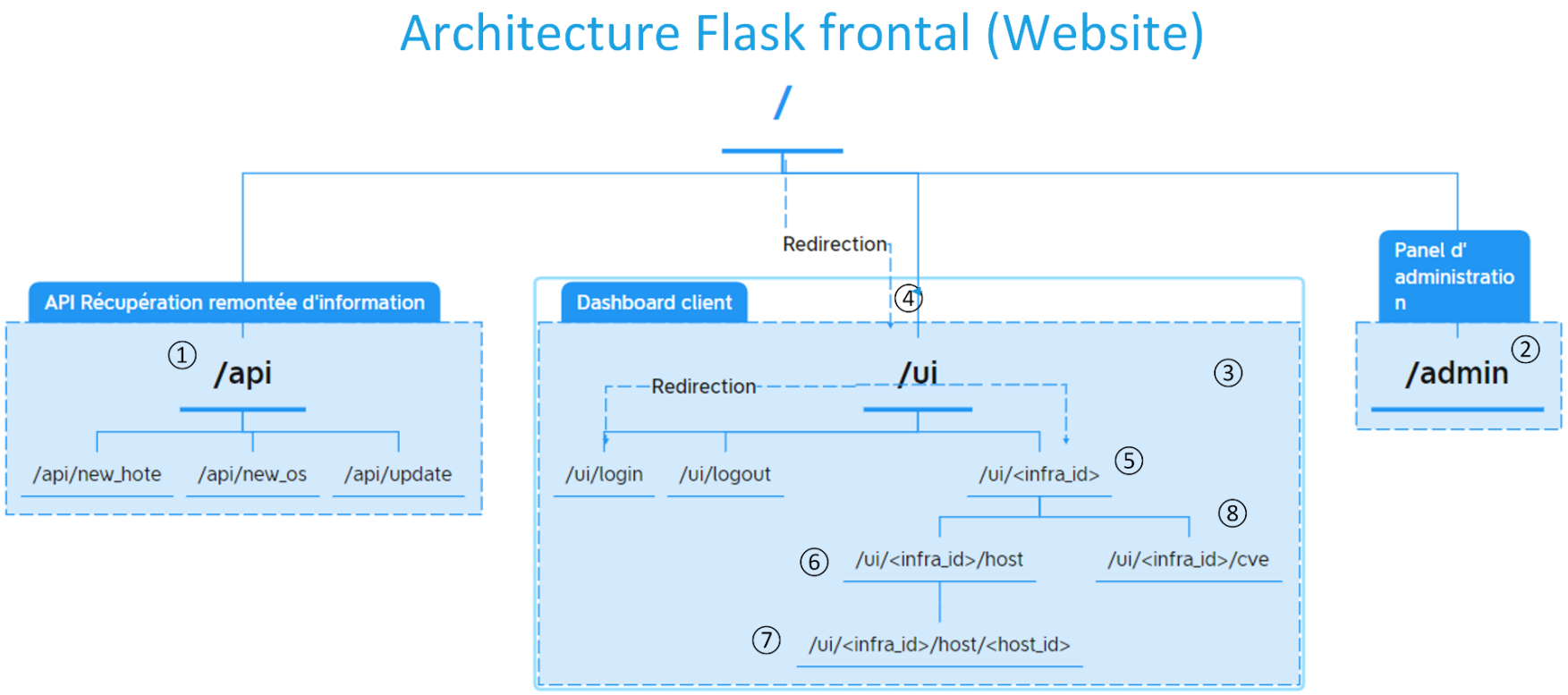
③ Nous gardons notre base de données de CVE à jour en nous basant sur plusieurs référentiels de CVE en ligne.

④ Les informations des CVE et de nos clients sont confrontées afin de déterminer quelles CVE impactent leurs services.

⑤ Toutes les informations sont ensuite transmises au client sous forme de dashboard qu'il peut consulter.

Schéma base de données





① L'API est le point d'entrée des informations clientes vers la base de données

② Le panel d'administration est notre panel permettant de gérer nos clients (créer des utilisateurs, des infrastrcutures, etc.)

③ L'interface UI est le dashboard que voit les clients avec toutes les informations les concernant (leurs matériels, cve impactante etc...)

④ La racine redirige automatiquement vers l'infrastructure du client s'il est connecté ou sur la page de connexion.

⑤ Page affichant leur dashboard d'accueil ⑥ Page listant leur infrastructure ⑦ Page affichant les informations d'un hote

⑧ Page affichant les CVE impactant l'infratrusture

Diagramme de séquence global