Ines Ayoub, Raphaël Letourneur, Maela Schmidt, Théo Vigreux

Projet G11 : CVE Warn

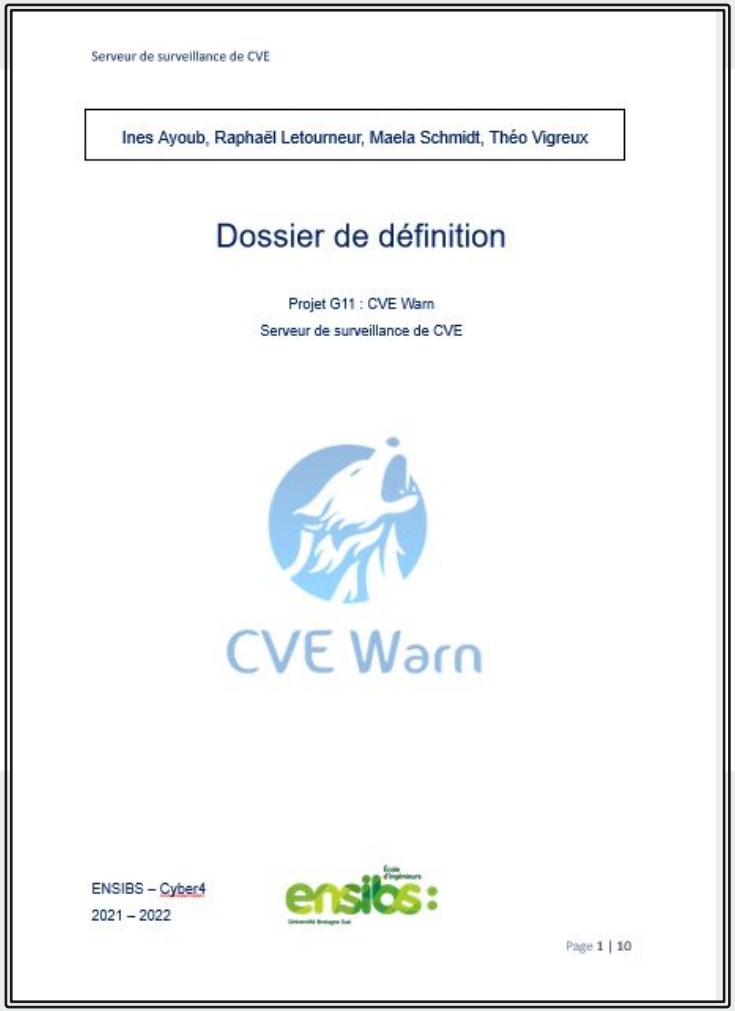
Serveur de surveillance de CVE

ENSIBS - Cyber4
2021 - 2022

Sommaire

- Introduction
- Rappel Jalon 1
- Dossier de définition : Pourquoi en faire un ?
- Présentation schéma d’architecture
- Présentation du scénario opérationnel
- Conclusion

Introduction



Serveur de surveillance de CVE

Ines Ayoub, Raphaël Letourneur, Maela Schmidt, Théo Vigreux

Dossier de définition

Projet G11 : CVE Warn

Serveur de surveillance de CVE

CVE Warn

ENSIBS – Cyber4

2021 – 2022

Page 1 | 10

Rappel Jalon 1

- Les différents objectifs de ce projet
- Les raisons pour lesquelles nous avons choisis ce sujet
- L’ organisation du projet
- Les moyens nécessaires pour la réalisation du projet

Dossier de définition : Pourquoi en faire un ?

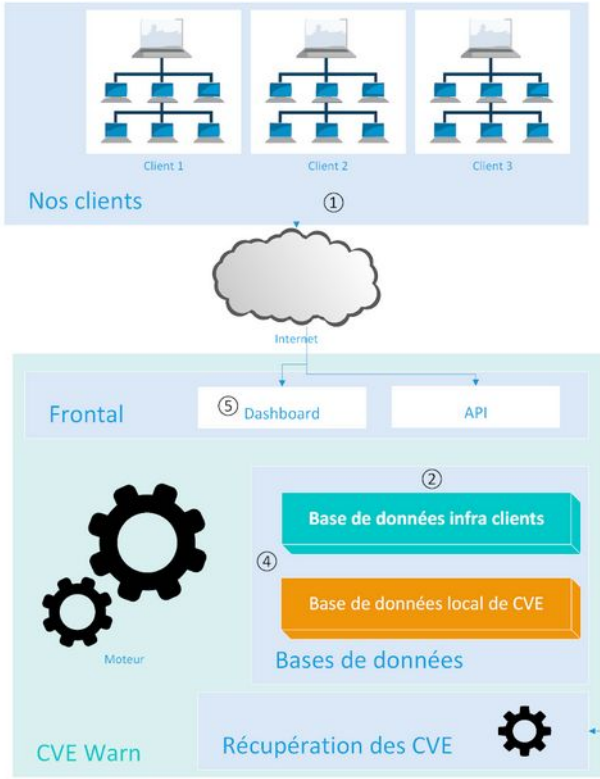
- Présenter les différentes interacteurs de notre projet au client (acteur, bien support, informations traitées) ainsi que les fonctions principales du produit.

- Présentation détaillée de notre système :

  - Scénario opérationnel

  - Schéma architecture

Schéma d'architecture



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

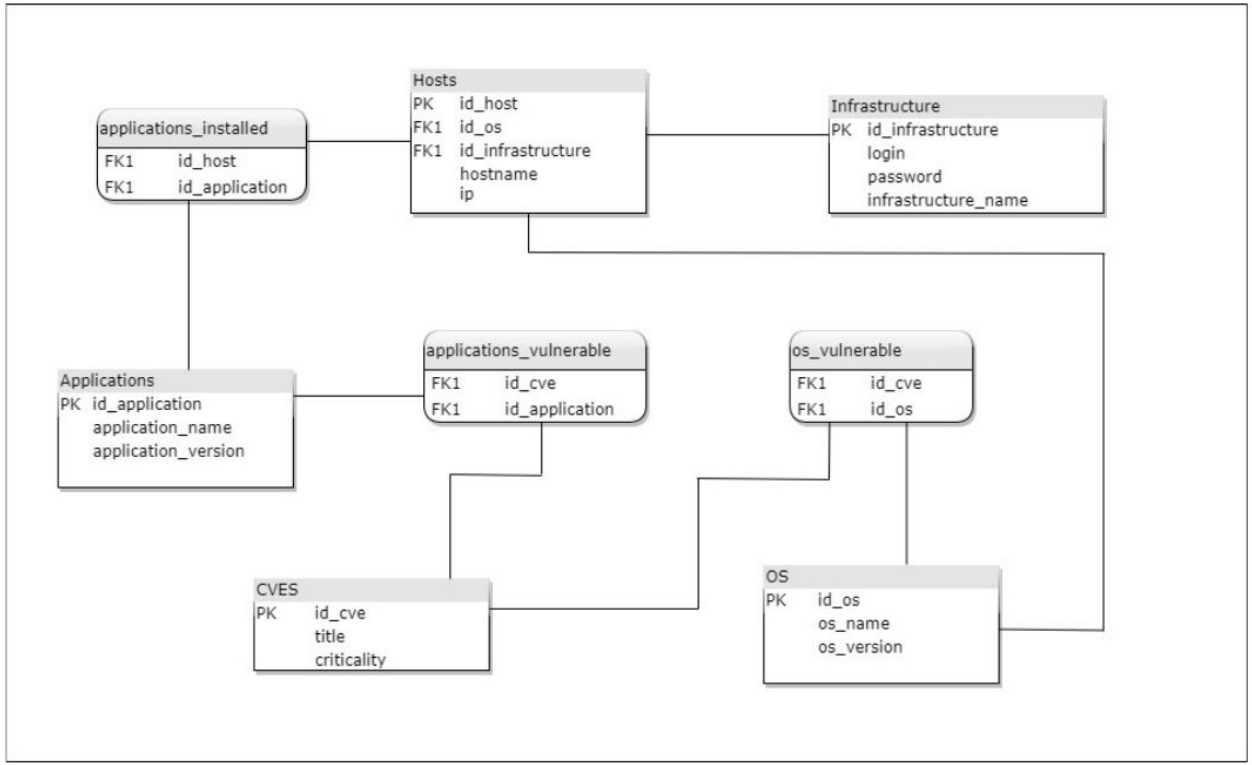
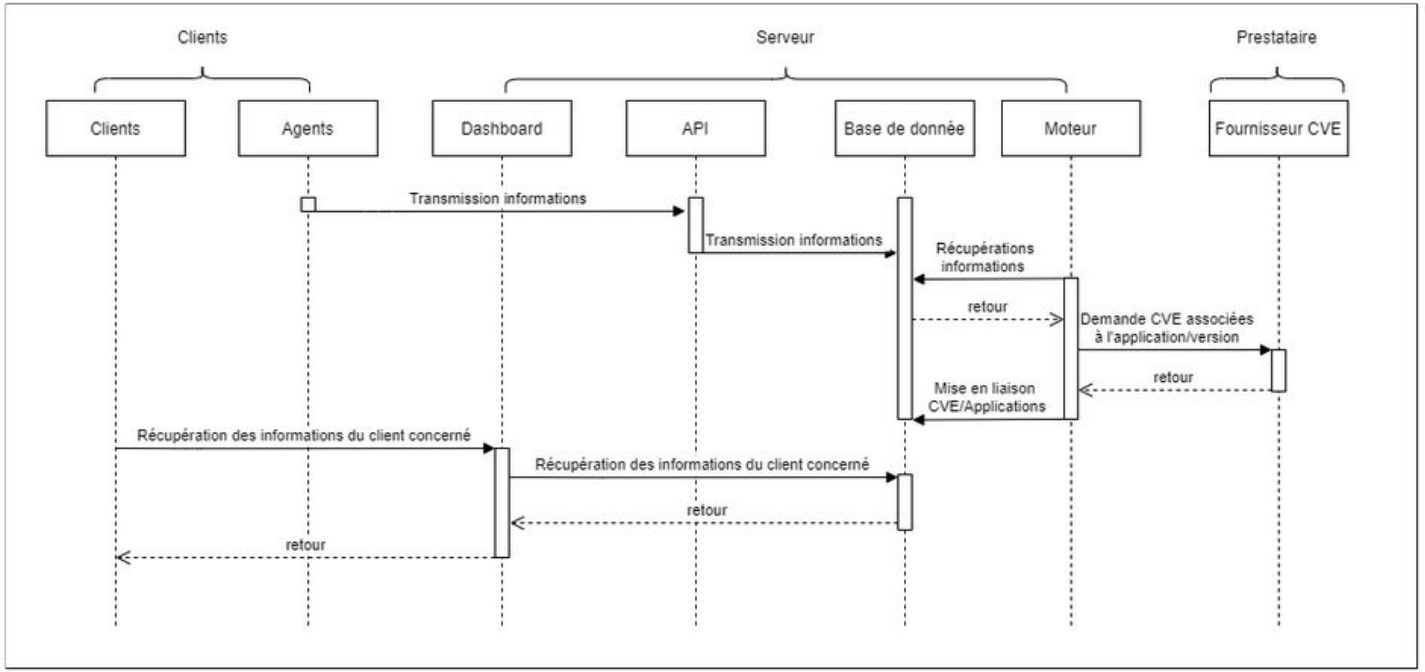


Diagramme de séquence global



Scénario opérationnel

Données applications / OS → Base de données

Entrée n°1 : [‘Chrome’, ‘96.0.4664.45’, ‘Application’]

Entrée n°2 : [‘Blender’, ‘2.78’, ‘Application’]

Entrée n°3 : [‘Windows Server’, ‘2016’, ‘OS’]

Scénario opérationnel

CVE → Base de données

Entrée n°1 : [‘Chrome’, ‘95.0.4683.54’, ‘Application’]

[‘CVE-2021-37996’,’2021-11-02’, ‘Faible’, ‘Insufficient validation of untrusted …..’]

[‘CVE-2021-37990’, ‘2021-11-02’, ‘Moyenne’, ‘Heap buffer overflow …..’]

Entrée n°2 : [‘Blender’, ‘2.78’, ‘Application’]

[‘CVE-2017-2906’, ‘2018-04-24’, ‘Moyenne’, An exploitable integer overflow …..’]

Entrée n°3 : [‘Windows Server’, ‘2016’, ‘OS’]

[‘CVE-2018-8420’,’2018-09-13’, ‘Haute’, ‘A remote code execution vulnerability ……’]

Conclusion

La prochaine étape sera de finaliser le dashboard, continuer à établir notre base de données, corriger quelques éventuelles bug et enfin de réaliser le jalon 3

Avez vous des questions ?