

Auteurs : Maxime KEJIKIAN – Etienne ARNAUD-GODDET - Eduardo Robson CARDOSO GUEDES FILHO

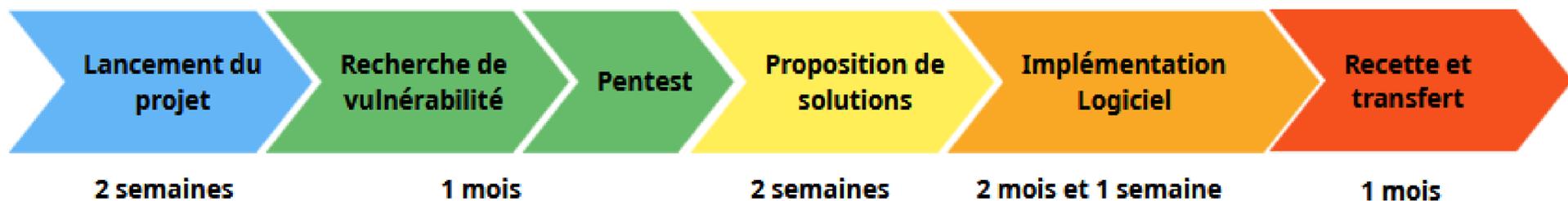
CONTEXTE ET OBJECTIF

Chauvin Arnoux est une entreprise française spécialisée dans la conception d'instruments de mesures. Ils produisent notamment le CA8345 sur lequel nous avons travaillé.

L'entreprise souhaite améliorer la cybersécurité de cet appareil pour le rendre conforme aux futures normes de cybersécurité liées à la directive RED et au Cyber Resilience Act.



MÉTHODES ET DÉVELOPPEMENTS



Le projet était composé de 3 phases:

- ❖ Recherche de vulnérabilités et pentest
- ❖ Propositions de solutions
- ❖ Implémentation de certaines solutions en utilisant Yocto

Méthodes de travail:

- ❖ Réunions toutes les 2 semaines
- ❖ Utilisation de Docker

yocto
PROJECT



RÉSULTATS ET CONCLUSION

- ❖ Rapports sur les attaques réalisées et les vulnérabilités trouvées
- ❖ Propositions de solutions
- ❖ Mise à jour du firmware
- ❖ Nouveau système de mise à jour sécurisé
- ❖ Début de montée de version

Les rapports ont permis à Chauvin Arnoux de connaître les points faibles du CA8345. Les propositions ont permis de développer des corrections en fin de projet. La réalisation d'une base de travail de montée de version sera poursuivie par l'entreprise. Ce projet servira également à améliorer la sécurité d'autres appareils de Chauvin-Arnoux.

MOTS-CLÉS : Cybersécurité, Embarqué, Yocto, Docker