

[Stage] Audit de sécurité et cybersécurité IoT

Description

Get Your Way est une startup technologique belge qui développe des solutions matérielles et logicielles destinées aux secteurs hospitalier et industriel. L'entreprise conçoit notamment *aRdent ScanDisplay*, un terminal portable connecté permettant d'accompagner les opérateurs dans leurs tâches quotidiennes grâce à l'affichage d'informations métier, la communication sans fil et l'interaction utilisateur.

Nos produits combinent applications web, APIs, infrastructures cloud et systèmes embarqués. Ils sont déployés dans des environnements sensibles où la sécurité des systèmes et des données est essentielle.

Dans ce contexte, la cybersécurité représente un enjeu majeur, tant pour la protection de nos solutions que pour la confiance de nos clients. L'entreprise souhaite renforcer sa posture de sécurité, améliorer ses pratiques internes et anticiper les exigences réglementaires applicables aux environnements hospitaliers et industriels.

L'objectif de ce stage est d'évaluer la sécurité de nos produits, d'identifier les vulnérabilités potentielles et de contribuer à l'amélioration continue de notre cybersécurité. Vous travaillerez aussi bien sur les applications web que sur les infrastructures cloud, les APIs, les systèmes embarqués ESP32 et les procédures internes de l'entreprise.

Missions

- Réaliser des analyses de vulnérabilités et des tests d'intrusion sur les applications web, APIs et systèmes embarqués développés par Get Your Way.
- Identifier les risques de sécurité et proposer des mesures correctives adaptées aux contraintes de l'entreprise.
- Étudier les bonnes pratiques de cybersécurité applicables aux environnements hospitaliers, industriels et IoT.
- Participer à l'amélioration des procédures internes liées à la gestion des accès, des incidents et des données sensibles.
- Contribuer à la mise en œuvre de premières améliorations techniques permettant de renforcer la sécurité des produits et services.
- Formaliser les résultats sous forme de recommandations, de procédures et de plans d'actions prioritaires.

Challenges

- Analyser des systèmes variés combinant applications web, infrastructures cloud et firmware embarqué.
- Identifier et prioriser les vulnérabilités les plus critiques dans un environnement en constante évolution.
- Comprendre les enjeux de cybersécurité propres aux environnements hospitaliers et industriels.

- Trouver un équilibre entre sécurité, simplicité d'utilisation et contraintes opérationnelles.
- Traduire des problématiques techniques en recommandations concrètes et applicables par l'équipe.

Profil recherché

Nous recherchons une personne curieuse, rigoureuse et passionnée par la cybersécurité, qui aime comprendre comment fonctionnent les systèmes, identifier leurs faiblesses et imaginer comment ils pourraient être attaqués ou sécurisés. Étudiant·e en cybersécurité, informatique, réseaux, systèmes embarqués ou domaine équivalent.

- Intérêt marqué pour la cybersécurité offensive, les tests d'intrusion ou l'analyse de vulnérabilités.
- Bonne compréhension des systèmes informatiques, des réseaux ou du développement logiciel.
- Curieux·se des technologies web, cloud, IoT et systèmes embarqués.
- Autonome, méthodique et capable de prendre des initiatives.
- Une expérience avec des outils tels que OWASP ZAP, Burp Suite, Kali Linux, Wireshark ou des outils similaires constitue un atout, mais n'est pas indispensable.

Ce que nous offrons

Un stage au sein d'une startup technologique en pleine croissance, où tu travailleras sur des problématiques concrètes ayant un impact direct sur la sécurité de nos produits et de notre organisation.

- Une vision complète de la cybersécurité appliquée aux applications web, aux infrastructures cloud et aux objets connectés.
- L'opportunité d'analyser et de tester des systèmes réels utilisés dans les secteurs hospitalier et industriel.
- Une grande autonomie dans l'exploration des sujets, les méthodes utilisées et les recommandations proposées.
- Un environnement startup dynamique, avec une équipe de 7 personnes accessible et à l'écoute.
- L'opportunité de contribuer directement à l'amélioration de la sécurité de l'entreprise et de ses produits.
- Des horaires flexibles et la possibilité de télétravail partiel.

Disponibilités

À partir de **juin 2026**, dates flexibles avec une durée de 3 mois

Lieu

Centre-ville de **Liège – Belgique**

Contact

Antoine Malherbe, CTO, a.malherbe@getyourway.be, [+32492034525](tel:+32492034525)