Résumé de projet

1. Présentation Personnelle

Je m'appelle Mylène Rodrigues Dos Santos et j'ai commencé ma reconversion dans le monde de l'informatique, plus précisément la cybersécurité en 2022. Ma reconversion fait suite à quelques années d'expérience dans le monde de la restauration.

Durant ces années, je me suis rendue compte que je ne voulais pas continuer en restauration jusqu'à ma retraite, j'ai donc commencé à me poser des questions et à réfléchir à ce qui m'intéressait et à ce que je pourrais faire durablement.

Enfant, j'étais passionnée par les ordinateurs et les logiciels attractifs, je me suis donc tournée vers l'informatique en général et la cybersécurité étant en plein essor, je me suis renseignée et documentée sur ce domaine. J'ai trouvé des domaines en cybersécurité tellement intéressants et passionnants que j'ai su que je voulais travailler dans ce milieu.

Curieuse par l'étendue du monde de la cybersécurité et des nouvelles technologies et avec une grande envie d'apprendre, je me suis donc dirigée vers l'école de La Plateforme afin de reprendre mes études et faire carrière dans la cybersécurité.

J'ai donc commencé une première année à l'école de la plateforme en IT puis je me suis spécialisée en cybersécurité la seconde année. C'est également cette année-là que j'ai trouvé et commencé mon alternance chez CortexEra, une entreprise de cybersécurité qui aide les entreprises à rester aux normes à respecter dans la cybersécurité mais également des pentests, et à protéger les entreprises de cybercriminel et des procédures à suivre en cas de cyberattaque.

2. Présentation de l’entreprise

CortexEra est une jeune entreprise spécialisée dans la cybersécurité pour aider les petites et moyennes entreprises à se défendre contre divers cyberattaques.

CortexEra intervient pour plusieurs types de services: audits, audits sur IoT, pentests, réponse sur incident, gestion de crise, analyse de risques, récupération des données, installation et maintenance en informatique générale … . Nous traitons la demande du client et intervenons si nécessaire selon la demande de service du et/ou des clients.

CortexEra est également certifié Qualiopi et référencé par Cybermalveillance et Dynabuy et nous participons également à des CTF et des conférences

3 Summary In English

During my internship, I had the opportunity to work at Cortexera, a cybersecurity company that specializes in supporting organizations targeted by cyberattacks. The company also conducts security audits to help businesses strengthen their digital defenses. In addition to its operational services, Cortexera is involved in educational initiatives, providing cybersecurity training and awareness programs in various schools and academic institutions. This experience allowed me to gain valuable insight into both the technical and strategic aspects of cybersecurity.

1.4 Résumé entreprise:

J’ai travaillé chez CortexEra, une petite entreprise de quatres personnes dont je fais partie et où j’ai la chance d’avoir un patron qui a plus de 25 ans d’expérience dans le domaine de la cybersécurité qui m’a énormément appris.

Mon patron m’a fait revoir toutes les bases de l’école:

- en réseau: VirtualBox et réseau des entreprises à auditer,
- en code: HTML, CSS, Javascirpt, C/C++,
- en virtualisation,
- en analyse de log: parsing de log,

- en cloud: Acronis,
- les normes ISO 27xxx/RGPD
- …

J’ai également appris les bases en soudure, électronique et en reverse engineering.

Je prépare également l’examen du CEH (Certified Ethical Hacker) qui est une certification reconnue, délivrée par l’organisation EC-Council qui forme sur la sécurité offensive comme les techniques de piratage utilisées par les cybercriminels (dans un cadre légal et éthique). Le CEH a pour but d’enseigner les compétences nécessaires pour tester les défenses d’un système informatique, prévenir les intrusions, renforcer les mesures de sécurité et connaître les techniques, outils et méthodes d’attaque les plus utilisées dans le monde réel .

J’ai aussi pu participer au renouvellement et à la préparation de plusieurs certifications de mon entreprise.

Concernant le cloud, mon entreprise travaille avec Acronis, une application Cloud qui permet de protéger son infrastructure avec un choix de services tiers à activer ou non. Elle est spécialisée dans la sauvegarde, la récupération après sinistre, la cybersécurité et la protection des données. Cette solution permet entre autres de:

- faire des backups du systèmes,
- planifier des sauvegardes,
- de créer des images complètes du système afin de pouvoir restaurer l’environnement en cas de perte ou de corruption,
- de sécuriser ses données, de pouvoir avoir un plan de remédiation si les données sont chiffrées,
- d’isoler un programme ou logiciel lorsque l’agent d’Acronis détecte un code malveillant
- protéger les fichiers critiques avec des fonctions de chiffrement, d’authentification et de contrôle d’intégrité
- effectuer des tests de restauration pour valider l'efficacité du plan de reprise d’activité (PRA)

Ce logiciel est constamment mis-à-jour. On peut visualiser tout cela avec un dashboard qui nous permet de voir rapidement ce qu’il se passe et s' il y a un problème.

On peut également via Acronis synchroniser les mails et ainsi pouvoir bloquer des attaques de type phishing, spear phishing, business email compromise ou encore des malspams.

Nous gérons donc la cybersécurité de plusieurs clients via ce logiciel.

J’ai également eu l’opportunité d’intervenir avec mon entreprise directement chez des clients pour faire des audits de sécurité, voir comment ça pouvait se passer sur le terrain et comprendre comment et pourquoi des cyberattaques peuvent se produire que ce soit en distanciel ou directement sur le terrain. J’ai également vu quels équipements les entreprises possédaient et quels moyens elles utilisaient pour sécuriser leur système. J’ai donc pu participer à la rédaction de rapports en incluant aussi plusieurs schéma réseau des dites entreprises.

A la suite de ces interventions chez les clients pour des audits de sécurité, j’ai travaillé sur un code en HTML, CSS et Javascript pour faire une application qui automatise le schéma réseau d’une entreprise. Sur la première page, on peut mettre toutes les informations de l’entreprise. Sur la deuxième page nous avons un rack avec plusieurs boutons pour choisir quels équipements (marque et model) on veut rajouter dans le rack, y compris des boutons pour modifier la place de l’équipement dans le rack. Sur la dernière page on peut rajouter des photos des racks prisent directement chez le client et ajouter des informations supplémentaires si nécessaire.

Dans le cadre de mon alternance chez CortexEra, j’ai eu l’opportunité d’accompagner mon patron et collègue de travail lors de sessions d’enseignement dans plusieurs établissements scolaires. Cortexera donne des cours allant du niveau Bachelor 1 jusqu’au Master 2 sur la cybersécurité. On a donné des cours sur de l’OSINT, du web, des adresses IP, sur Wireshark … . J’ai pu assister à ces cours et même co-animer un cours aux côtés de mon patron. Cela m’a permis de revoir et consolider certaines bases, mais également de découvrir les méthodes pédagogiques utilisées pour transmettre les connaissances.

J’ai également pu assister à des conférences sur la cybersécurité comme Barbhack et assisté à des meetings où je présentais mon entreprise à d’autres entreprises.

J’ai ainsi été formé sur plusieurs logiciels comme wireshark, ghidra, openstreetmap, Acronis, Visual Studio Code … .

1.5 Résumé Projet

Pour valider mon titre RNCP AIS, je vais monter une infrastructure docker sécurisée au sein d'une entreprise fictive. Cette infrastructure à pour but de fournir un environnement SIEM (Security Information and Event Management) robuste, modulaire et sécurisé. Je vais déployer les services suivant avec docker:

- Grafana pour la visualisation et les dashboards de supervision
- Prometheus pour la collecte et la surveillance des métriques système
- Wazuh pour la détection des intrusions, l'analyse de logs et la supervision de la sécurité
- OpenVPN pour sécuriser l'accès distant à l'infrastructure
- Nginx utilisé en tant que reverse proxy sécurisé (HTTPS) afin de centraliser et sécuriser les accès aux services

Chaque service sera isolé dans son propre environnement docker et relié à des réseaux docker dédiés. La configuration repose un usage des dockerfiles, du fichier .env et des certificats SSL auto-signés. Plusieurs scripts bash seront mis en place pour déployer et stopper l'ensemble des conteneurs proprement.

Parallèlement, pour pouvoir valider la partie réseau, j'ai conçu et documenté une architecture réseau sécurisée pour une entreprise fictive sur Cisco Packet Tracer en:

- configurant et segmentant les sous-réseaux,
- les pare-feux,
- les VLANs,
- mise en place de protocole
- les routes Inter-VLAN
- serveur de sauvegarde TFTP
- simulation d'accès à Internet
- DMZ

Chaque équipement sera configuré et testé pour assurer le bon fonctionnement de l'infrastructure.