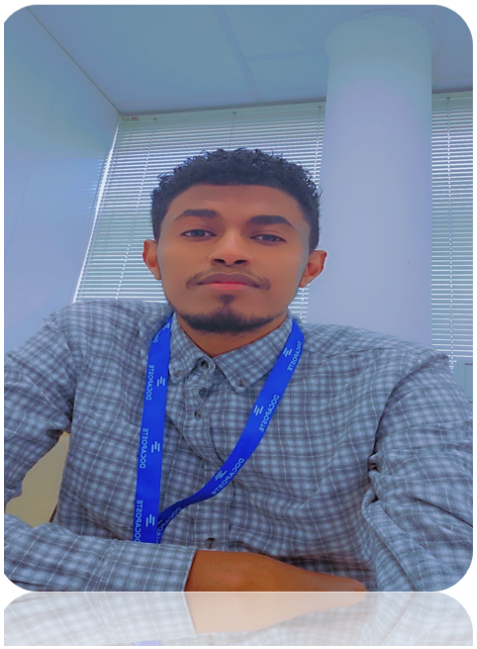
Résumé



DOCAPOSTE
l'avenir devient plus simple

Abdalla HAMD MOHAMED

Analyste Cybersécurité.



Titre professionnel :

Nom : HAMD MOHAMED

Prénom : Abdalla

En Formation à La Plateforme_, 8 rue d'Hozier 13002 Marseille,

Introduction

1.1. Présentation personnelle

Je m'appelle Abdalla Hamd Mohamed, je suis déjà actuellement Pentester/SOC analyste

Passionné par le monde de l'informatique depuis mon plus jeune âge, Malgré j'ai vécu une enfance marquée par une guerre civile dans mon pays, le Soudan. Malgré ces difficultés, je me suis beaucoup battu pour reprendre mes rêves et pouvoir travailler dans le domaine de la cybersécurité.

Ce choix a été mûrement réfléchi. Depuis mon enfance, attiré par l'informatique et les nouvelles technologies, j'ai toujours su que je voulais évoluer dans ce milieu.

Après mon arrivée en France il y a quatre ans, j'ai cherché comment allier l'utile à l'agréable. J'ai alors réalisé que j'aimais l'informatique et l'écriture en général, mais aussi que j'aimais accomplir des choses uniques et innovantes.

Je suis donc devenu développeur web, non pas pour faire carrière dans ce domaine, mais pour mieux comprendre les aspects techniques du développement. Après avoir acquis ces connaissances, j'ai rapidement décidé de me spécialiser davantage.

Après quelques mois de formation intensive qui m'ont permis de bien comprendre le métier de **Développeur Web/Web Mobile**, j'ai ensuite poursuivi ma carrière en tant que **Pentester**. J'ai pu découvrir environ 100 vulnérabilités dans de grandes entreprises, notamment **Nubia**, et **le groupe La Poste** afin de les signaler et leur proposer des correctifs.

Fort de cette expérience, j'ai décidé de poursuivre mon parcours en alternance afin d'intégrer un environnement professionnel et acquérir les compétences nécessaires à l'obtention du titre **Administrateur d'infrastructures sécurisées** Grâce à mes découvertes en matière de cybersécurité, j'ai eu l'opportunité d'être accepté en alternance chez **Docaposte**.

1.2.Résumé

Durant mon alternance, j'ai eu l'opportunité d'intégrer un poste **d'analyste en cybersécurité** au sein de **Docaposte**.

J'ai également eu la chance de rejoindre l'équipe **COSC** (Centre Opérationnel de Sécurité et de Cyberdéfense) du groupe, d'être un acteur clé dans plusieurs projets et de faire partie de la Blue Team de Docaposte.

L'objectif de mes missions était de travailler sur la Gestion des vulnérabilités, la détection et réponse aux incidents sur les endpoints (**EDR**), ainsi que la surveillance des alertes SIEM. J'étais également chargé de répondre aux attaques, de proposer des remédiations adaptées et de concevoir de nouveaux use cases pour améliorer la détection des menaces sur l'EDR et le SIEM.

1.3. Summary in English.

During my work-study program, I had the opportunity to take on a cybersecurity analyst position at **Docaposte**.

I was also fortunate to join the group's **COSC (Operational Security and Cyber Defense Center**) team, play a key role in several projects, and be part of **Docaposte's Blue Team**.

The objective of my missions was to work on vulnerability management, incident detection and response on endpoints (EDR), as well as SIEM alert monitoring. I was also responsible for responding to attacks,

Proposing appropriate remediations, and designing new use cases to enhance threat detection on both the EDR and SIEM

1.4.Présentation de l’entreprise

Docaposte est une filiale du Groupe La Poste et un référent majeur de la confiance numérique en France.
Elle accompagne les entreprises et les institutions publiques dans leur **transformation numérique**, tout en garantissant la sécurité et la conformité des données.

En 2024, Docaposte compte plus de **60 000 clients**, près de **6 500 collaborateurs**, et réalise un chiffre d’affaires de **879 millions d’euros**.
Elle est présente sur plus de 100 sites en France et à l’international.

Docaposte propose une offre complète combinant services numériques et physiques :
conseil, solutions sur-mesure ou clés en main, traitement de données sensibles, et accompagnement réglementaire.

Elle intervient sur toute la chaîne de confiance :
identification, authentification, signature électronique, certification et archivage sécurisé.

Elle est aussi leader des services numériques de confiance :
vote électronique, lettre recommandée électronique, archivage numérique, etc.
Et c’est le premier opérateur de données de santé en France, avec plus de **45 millions de dossiers médicaux**.

Docaposte possède de nombreuses **certifications de référence** :

- **ISO 27001**,
- **HDS** (Hébergement de Données de Santé),
- **SecNumCloud** (ANSSI),
- et elle est le **seul acteur en France labellisé eIDAS** sur toute sa gamme de services de confiance.

1.5. Présentation de l’équipe cybersécurité

Au sein de Docaposte, je fais partie de l’équipe COSC ("Centre Opérationnel de Sécurité et de Cyberdéfense"), composée plus de 20 personnes, dans plusieurs domaines : Net Sec, certificats, cryptographie, CSIRT - SOC (dont je fais partie) et identification des vulnérabilités (dont je fais également partie).

Ensuite, il y a le RSSI (Responsable de la Sécurité des Systèmes d’Information), qui est notre manager et dirige l’équipe sécurité.

Enfin, tout en haut de l’organigramme, se trouve le DSI (Directeur des Services Informatiques), responsable des équipes infrastructure, réseau, etc.

Mon équipe :

DOCAPOSTE

l'avenir devient plus simple

DSI

RSSI

Csirt/SOC

Moi

Vuln

2.1. Mon rôle au sein de l’entreprise

Au sein de **Docaposte**, j’ai été responsable de plusieurs missions liées à la **cybersécurité** et à la sécurité opérationnelle.
Je travaille au sein d’une équipe spécialisée, avec un système de ticketing qui nous permet de suivre les incidents, les alertes et les demandes de sécurité de manière organisée.

Voici un aperçu des principales tâches que j’ai réalisées:

- **Détection et Analyse des Incidents de Sécurité :**
  Surveillance continue des systèmes de sécurité avec l'EDR et SIEM pour détecter, analyser et répondre efficacement aux menaces (malwares, attaques réseau, etc.).
- **Gestion des vulnérabilités :**
  Utilisation d’outils de gestion des vulnérabilités pour lancer des scans réguliers, analyser les résultats, marquer (taguer) les failles détectées, et suivre leur traitement jusqu’à la résolution.
- **Propositions d'Améliorations en Cybersécurité :**
  Participation active à l’élaboration et à la mise en place de cas d’usage (use cases) sur le SIEM et l’EDR afin d’améliorer la détection des menaces et renforcer la posture de sécurité.
- **Réponse aux Incidents et Gestion des Alertes :**
  Analyse des alertes détectées, évaluation de leur gravité et application des mesures correctives adaptées.
- **Collaboration avec l’ANSSI :**
  Participation chaque mois à la coordination avec l’ANSSI pour le suivi et le traitement des vulnérabilités critiques,
  en lien avec les systèmes et environnements de nos client.

Présentation des dossiers

Dans cette présentation, je souhaite simplement vous donner une idée générale de ce que contiennent mes deux dossiers :

Le Dossier de Projet:

présente un travail sur l'infrastructure de sécurité, réalisé autour de la supervision avec **Splunk**, où j'ai centralisé plusieurs sources de logs afin d'améliorer la **protection de l'infrastructure** et la détection des incidents.

Le Dossier Professionnel :

présente mon travail en tant que pentester en ligne sur les plateformes comme **YesWeHack**, **HackerOne**(bug bounty), ainsi qu'un projet de supervision réalisé avec **Zabbix**.

⚠️ Je précise que je ne peux pas présenter un projet directement lié à mon travail à docaposte, car la diffusion d'informations est **non autorisée pour des raisons de confidentialité**.

🔷**THE END**

ThanKyou