



# Mondher Ouled Ahmed

Ingénieur en Cybersécurité

contact@mondherouledahmed.com

+21654059246

Tunisie

linkedin.com/in/mondher-ouled-ahmed

## Résumé Professionnel

Expert en cybersécurité avec plus de 4 ans d'expérience dans la protection des infrastructures critiques et la gestion des environnements SOC/CERT. Spécialiste en détection et réponse aux incidents, implémentation de solutions Splunk, analyse avancée des logs et hardening Linux (Samhain, AIDE, auditd). Maîtrise des technologies de sécurité réseau (TLS, filtrage IPS) et email (DKIM, SPF, DMARC). Pionnier dans l'application de l'IA à la cyberdéfense avec développement de solutions innovantes de pentest automatisé et CMDB sécurisée. Rôle stratégique à l'interface entre équipes techniques, direction et fournisseurs de services de sécurité. Expertise en gouvernance et conformité avec une approche axée sur l'automatisation, l'intégrité et la non-répudiation des systèmes.

## Domaines d'Expertise

### Sécurité

Réponse aux incidents & gestion de crise

Analyse de vulnérabilités & remédiation

Surveillance SOC/CERT & analyse de logs

Gouvernance de sécurité & conformité

Forensics & investigations numériques

### Réseau

Migrations TLS & protocoles sécurisés

Filtrage IPS & sécurisation des flux

Configuration DKIM, SPF, DMARC

Architecture réseau sécurisée

Gestion des accès & authentification

### Système

Administration Linux avancée

Automatisation Ansible/AWX

Durcissement & sécurisation

Patch management & mise à jour

Scripting Bash/Python pour sécurité

## Expérience Professionnelle

- ### Cyber Security Engineer

Sopra HR Software

Juillet 2021 - Présent

#### Sécurité Opérationnelle

  - Mise en œuvre des règles de sécurité opérationnelles et élaboration de plans de contrôle sécurité
  - Suivi des alertes internes/SOC et pilotage proactif des plans de remédiation critiques
  - Réalisation et analyse des campagnes de scans de vulnérabilité avec priorisation des mesures correctives
  - Traitement des incidents de sécurité et participation à la mise à jour des plans de réponse aux incidents majeurs
  - Analyse et validation des demandes liées à la sécurité (règles Firewall, dérogations, etc.)
  - Implémentation et configuration des Universal Forwarders Splunk pour la centralisation des logs de sécurité
  - Intégration des clients dans le SOC via déploiement d'agents spécifiques ou configuration de rsyslog
  - Analyse approfondie des logs de sécurité pour la détection et l'investigation d'incidents

#### Infrastructure & Réseau

  - Gestion des migrations TLS et sécurisation des protocoles de communication entre composants applicatifs
  - Configuration et maintenance des mécanismes de filtrage IPS pour la protection des flux clients
  - Implémentation et optimisation des mécanismes de sécurité email (DKIM, SPF, DMARC) pour prévenir l'usurpation d'identité
  - Analyse et sécurisation des flux réseau entre les différents environnements (production, préproduction, développement)
  - Suivi des services de sécurité en production : alertes, escalades, améliorations continues

#### Systèmes & Automatisation

  - Accompagnement des équipes techniques sur les meilleures pratiques et mesures correctives en matière de sécurité
  - Développement de scripts d'automatisation (Ansible/AWX) pour le déploiement sécurisé des environnements
  - Pilotage des campagnes de patching des systèmes avec définition des procédures techniques de sécurité
  - Veille technologique sur les composants applicatifs (Apache, Tomcat, Java, OpenLDAP, Oracle) et évaluation des besoins de mise à jour
  - Participation aux projets de déploiement de nouvelles solutions de sécurité et amélioration des processus existants
  - Conception et implémentation de solutions de hardening Linux pour garantir l'intégrité des systèmes (Samhain, AIDE)
  - Configuration d'auditd pour assurer la non-répudiation et la traçabilité des actions systèmes critiques

#### Gouvernance & Reporting

  - Point de contact stratégique entre sous-traitants et fournisseurs de services de sécurité
  - Participation aux comités de sécurité clients et internes en tant qu'expert technique
  - Conduite et coordination des tests d'intrusion avec vérification des prérequis juridiques et techniques
  - Contribution à la création de reportings et tableaux de bord sécurité pour le suivi des indicateurs clés

#### Compétences Transversales

Gestion d'incidents

Filtrage avancé

Automatisation

Plans de remédiation

Veille sécurité

Sécurité email

IAM

Conformité
- ### Call Center Agent

Teleperformance

Mars 2021 - Juillet 2021

  - Gestion des appels clients et support technique de premier niveau
  - Résolution des problèmes techniques courants
  - Documentation des incidents et suivi des procédures
- ### Technicien support

Tunisie Télécom

Mars 2019 - Août 2019

  - Support technique aux utilisateurs
  - Diagnostic et résolution des problèmes informatiques
  - Maintenance des équipements réseau

## Formation

- ### Diplôme d'ingénieur en Cloud security engineer

Université Sesame

2021 - 2024
- ### Master en Sécurité / sûreté de l'information des systèmes informatiques

ISIMM | Higher Institute of Informatics and Mathematics of Monastir

2020 - 2021
- ### Licence professionnelle en Administration réseaux et systèmes

ISIMM | Higher Institute of Informatics and Mathematics of Monastir

2019

## Projets & Innovations

### Pentest IA Automatique

Développement d'une solution innovante utilisant l'intelligence artificielle pour automatiser les tests d'intrusion et la découverte de vulnérabilités.

**Apports business:** Réduction des coûts d'audit, identification proactive des risques, optimisation du temps de réponse aux vulnérabilités.

### CMDB de Sécurité Automatisée

Conception et implémentation d'une base de données de configuration dédiée à la sécurité avec automatisation des audits et de la détection de dérives.

**Apports business:** Visibilité permanente sur l'état de sécurité des systèmes, traçabilité des configurations, conformité facilitée.

## Certifications

### Fortinet

#### NSE1

License: LsDFWRjYrYA, validité jusqu'au 30/04/2025

Compétences: Fondamentaux de la cybersécurité, menaces actuelles

#### NSE2

License: 40G4Q5gd0H, validité jusqu'au 30/04/2025

Compétences: Produits de sécurité Fortinet, architecture sécurisée

#### NSE3

Compétences: Solutions Fortinet avancées, protections spécifiques

### EC-Council

#### Ethical Hacking Essentials (EHE)

License: 217273

Compétences: Méthodologies de pentest, détection de vulnérabilités

#### Digital Forensics Essentials (DFE)

Compétences: Investigation numérique, analyse de preuves digitales

### Qualys

#### Qualys certified professional

Compétences: Scanning de vulnérabilités, compliance monitoring

#### Cloud security assessment and Response

Compétences: Évaluation de sécurité cloud, réponse aux incidents

### Autres certifications

#### CCNA1 (Cisco)

Compétences: Fondamentaux des réseaux, configuration d'équipements

#### Incident Response Process ((ISC)²)

License: 5egy1568f

Compétences: Gestion d'incidents, procédures de réponse

#### Cyber threat intelligence 101 (arcX)

Compétences: Veille sur les menaces, analyse de renseignements

## Formation & Sensibilisation

### Animation de sessions de formation et sensibilisation:

- Formation des collaborateurs aux bonnes pratiques de sécurité informatique et à la détection des tentatives de phishing
- Sensibilisation aux risques de sécurité et aux comportements à adopter face aux menaces émergentes
- Accompagnement des équipes dans l'application des normes de sécurité (ISO 27001, RGPD)
- Élaboration de documentation technique et de guides de sécurité adaptés aux différents profils utilisateurs
- Organisation d'exercices pratiques de gestion d'incidents et de réponse aux attaques

## Compétences Techniques

### Sécurité

SOC/CERT

EDR

Splunk UF

Analyse de logs

SIEM

Gestion des vulnérabilités

Forensics

Plans de remédiation

Incident Response

Tests d'intrusion

Veille sécurité

ISO 27001

RGPD

### Réseau

Migration TLS

Filtrage IPS

DKIM

SPF

DMARC

Architecture réseau

Rsyslog

Sécurité des flux

Révision des accès

SFTP sécurisé

Gestion IAM

### Système

Linux (RedHat/CentOS)

Debian

Bash

Python

Ansible

AWX

Samhain

AIDE

auditd

Apache

Tomcat

Java/Karaf

OpenLDAP

Oracle

Durcissement systèmes

Patch management

## Langues

Arabe	Français	Anglais	Allemand
Langue maternelle	Professionnel	Professionnel	Notions de base