

✓ ouledahmedmondher@gmail.com +21654059246

Tunisie, Tunis, Nouvelle Soukra linkedin.com/in/mondher-ouledin



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. 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. Expertise en gouvernance et conformité avec une approche axée sur l'automatisation, l'intégrité et la non-répudiation des systèmes.

Domaines d'Expertise



Réponse aux incidents & gestion de

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 (Samhain, AIDE, auditd) Patch management & mise à jour Scripting Bash/Python pour sécurité

Projets Innovants

Pentest IA Automatique

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

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

CMDB de Sécurité Automatisée

Conception d'une base de données de configuration dédiée à la sécurité avec automatisation des audits et détection de dérives. Apports business: Visibilité permanente sur l'état de sécurité des systèmes, traçabilité des configurations, conformité facilitée.

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
- 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

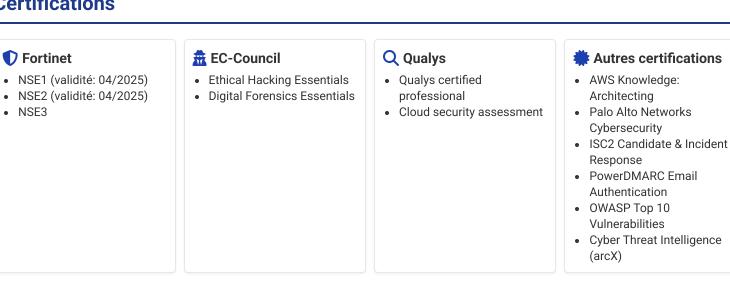
Expériences précédentes

- Call Center Agent Teleperformance (Mars Juillet 2021) : Support technique et gestion des appels clients
- Technicien support Tunisie Télécom (Mars Août 2019) : Support utilisateurs et maintenance équipements réseau

Formation

Diplôme d'ingénieur Licence professionnelle Master Cloud security engineer Sécurité des systèmes informatiques Administration réseaux et systèmes Université Sesame, 2021 - 2024 ISIMM, 2020 - 2021 ISIMM, 2019

Certifications



Compétences Techniques

