Mestour Med Amine

Consultant Sénior en Expertise Sécurité

Anglais bilingue

11 années d'expériences

Email : mestour.m.amine@gmail.com **Tel : 0620465250**

FORMATIONS & CERTIFICATIONS

2026	**CISM (en cours)**
2018	**ISO 27005 Risk Manager**
2018	**ISO 27001 Lead Implementor**
2014	**CEH (Certified Ethical Hacker) version 8**
2014	**CCNA Security**
2014	**Diplôme ingénieur d'Etat en génie informatique option « Sécurité des systèmes d'information » - ENSIAS**

CONNAISSANCE TECHNIQUES

- Implémentation d'un SMSI conforme à l'ISO 27001 (27002 et 27005)
- Intégration de la gestion des risques dans les projets
- Appréciation et traitement des risques : ISO 27005, EBIOS RM
- Sécurité Cloud (Azure, AWS), Active directory-tiering ,, SCCM, Architecture réseau, Switchs Cisco, Harshi corp, Sécurité d'infrastructure réseaux, Qualys, Tenable Windows server, IDS/IPS, Wallix, RSA, Anyconnect, NSX, IAM, PAM 802.11x, Micro-segmentation, Pingcastle, Oradad, OPENSCAP, Satellite/Forman, DEVSECOPS, securité API, DLP pureview , sécurisation des IAs , LLM Guard
- PCI DSS, standard ANSSI, LPM, RGPD, NIST, NIS 2, DORA, DRP.
- Test intrusion, Firewall, SIEM, Scan de vulnérabilité, Sonde IPS,System Hardening, IAM.

EXPERIENCES PROFESSIONNELLES

Depuis Janvier 2019 **Wancore**

Consultant Senior GRC

De Février 2025 à Décembre 2025 Chez BNP ITGP Prod SEC

Mission : Analyste en Sécurité IT et Expert SoD

- **Analyse des demandes de dérogation RSSI et instruction des fiches de risque liées à la production IT sous ServiceNow(création, renouvellement, clôture de fiche de risques) sur le perimetre Workspace (Azure, Entra ID ,Copilot)**
- **Analyse des demandes soumises à validation RSSI (droits d'accès distants, applications, systèmes, bypass de contrôles/mesures de sécurité, exception Av, …)**
- **Revue et MAJ des analyses de risques dans le cadre de la revue de risque**
- **Réalisation, participation ou accompagnement à des analyses de risque IT dans un contexte Cloud privé/public.**
- **Expertise SoD : définition et mise en place de règles de séparation des tâches (SoD) sur le périmètre de la production IT du groupe afin de limiter les droits des utilisateurs à privilèges**
- **Pilotage de chantier de durcissement (création de guide, implémentation et contrôle de mise en place règles) environnement : OS, Réseau, Middleware, Cloud IBM**

- **Suivi des vulnérabilités sur la surface externe via Qualys et Bitsight**

- **Suivi de Pentest et remédiation et validation des preuves de correction.**

- **Préparation des Dashboards Sécurité.**

Depuis Avril 2022 décembre 2024 **secteur bancaire**

Mission : Chef de projet et expert Cybersécurité et conformité

- Mise en place de la gouvernance du programme Cyber
- Définir le planning et les livrables attendus
- Gère les interactions avec les autres projets en adhérence
- Prépare et pilote la conduite du changement
- Mise en plan de remédiation des recommandations issue des différents audits (LPM, PCI DSS)
- Mise en place d'une infrastructure d'administration pour infrastructure LPM
- Mise en place d'infrastructure de collecte de Log pour SIEM(sysmon, rsyslog,sekoia)
- Renforcement du processus d'habilitation : Définition des matrices RBAC, mise en place des Revues périodiques.
- Mise en place d'indicateurs Règlementaire de l'ANSSI
- Définition et mise en place des process de gestion d'obsolescence et du processus MCS
- Mise en place d'une infrastructure d'outillage d'administration conforme ANSSI et PCI DSS (Constriction des ADs, DNS, WSUS, Satellite, Openscap,…….)

- Pilotage chantier de durcissement (Windows server, Laptop, AD, Linux, AIX VMware)
- Rédaction d'architecture pour les infrastructures liées au MCS, EDR et infra d'accès (HLD , LLD et de DAT) en respectant les bonne pratiques (MCS, segmentation…)
- Animation des différents comités de suivi, COPROJ et COPIL

De Août 2021 à Mars 2022 **Decathlon**

Mission : Responsable Security Officer

- Rédaction et revue des politiques sécurité
- Revue du tooling sous AWS (audit et Pan d'action)
- Réalisation des revues sécurités des applications et définition des plans d'action pour remédier aux non-conformités
- Préparation des exercices DRPs/PCA
- Animation des équipes pour le suivi de compliance CSPM via Prisma Cloud et de vulnérabilité CWPP Tenables dans les environnements AWS et GCP (analyses des vulnérabilité, identification des risks, et priorisation des remédiations selon la priorité définies)
- Rédaction des guides et préparations des classes puppets pour les hardening Os
- Production de KPI sécurité

De Septembre 2019 à Juin 2021 **BNP Paribas BDDF**

Mission : Consultant en Instruction Sécurité SI Projets

- Déploiement des instructions de risque sécurité des projets de BDDF (analyse des besoins, des menaces potentielles, évaluation des risques et proposition de plan de remédiation (mesures organisationnelles ou techniques), l'élaboration des fiches sécurité, la mise en conformité des contrats des prestataires de services externalisés le cas échéant (clauses sécurité), suivi des Tests d'intrusion, revue SATS , DAST ...
- Gestion des différentes demandes d'autorisations et d'habilitations spécifiques des personnes de BDDF aux ressources IT (accès internet, poste de travail, infrastructure, etc ...)
- Études et validation de la légitimité de demandes ponctuelles : d'ouverture de flux, d'extraction de données de production, ...
- Accompagnement et Assistance sécurité nécessaire aux différentes sollicitations métier
- Accompagnement aux réponses aux appels d'offres (AO Métier, conformément à notre Plan d'Assurance Sécurité)
- Reporting

Mars 2019 à Aout 2019 **John Paul**

Mission : Accompagnement Conformité PCI-DSS

- Rédaction des politiques de sécurité (PSSI , habilitations, MCS,…..).
- Suivi de Déploiement de l'implémentation de l'antivirus.
- Suivi de Déploiement de l'implémentation du processus du Patch management.
- Suivi Implémentation File Integrity Management.
- Mise en place du processus de gestion d'incident.
- Rédaction de Méthodologie de test d'intrusion.
- Analyse de Risque.

Décembre 2017 à mai 2018 **CREDIT DU MAROC**

Titre : **Ingénieur sécurité SI :**

- Evaluation des risques Sécurité SI :
  - Accompagner le métier dans la définition de leurs exigences sécurité pour un projet et l'élaboration des analyses de risque suivant de la méthodologie MESARI inspirée de EBIOS.
- Pilotage du plan d'action SSI :
- Contribuer aux actions de sensibilisation et de formation des utilisateurs :
- Contrôle : Pilotage des contrôles de niveau 2.1 (reporting des indicateurs de sécurité, audits de conformité aux politiques SSI) et suivi des plans de remédiation issus des audits et des non-conformités sur la gestion des habilitations.
- **Environnement Techniquement : ISO 27001, Qualys, ISO 27005, MESARI.**

Janvier 2015 à novembre 2017 **LEAR Corporation**

Titre : **ingénieur système et sécurité**

- Déploiement de la solution de Mcafee drive encryption dans les laptops du parc.
- Gestion de l'anti-virus sur le parc informatique avec la solution McAfee Endpoint
- Installation des différents patches de sécurité sur les serveurs et ordinateurs via SCCM :
  - Préparation des preuves pour l'audit SOX et ISO 27001.
  - Definition des RTO et RPO avec la production pour leur application Metier
  - Etude et réalisation du Business Impact Analyses des systèmes de production.
  - Mise en place des scénarios de Disaster Recovery Plan annuel.
  - Administration de l'infra de prod : AD, solution backup Acronis, Vmware , Oracle
  - Résolution et suivi des incidents et gestions des problèmes sous ServiceNow.

  Environnement Technique : Mcafee, SCCM, Windows server, SOX, BIA, DRP,