

Yassine KACEM

29 ans

Nationalité Française, Permis B

Domicilié en France, zone frontalière

Consultant SSI PAM

Compétences Fonctionnelles

- Référentiels de sécurité : ISO 27001, 27002, 27005
- Méthodologies/Référentiels : critères communs, RGS ANSSI
- Analyse de risques EBIOS 2010 Risk Manager
- Continuité d'activité (PCA, Plan de Reprise d'Activité, Plan de Secours Informatique)
- Intégration de la Sécurité dans les Projets
- RGPD et ses impacts techniques
- Gestion de projets et juridique (Différente lois liée à la cybersécurité)
- Cyberdéfense (état de l'art de la Cyberdéfense « hardening » et utilisation des services pour la protection d'une infrastructure)

Compétences Techniques

Technologies Cartes à puce, TPM (Trusted Platform Module)

Cryptographie Symétrique / asymétrique, mécanismes de chiffrement / signature / authentification

Réseau Proxy, Firewall, modèle OSI, Configuration matériel CISCO

Langages Java, C, C++, PowerShell, Python

Bureautique Suite Office (Word, Excel, PowerPoint), VBA, Macros

IAM MFA, SSO, OKTA verify, SAML 2.0, OAuth

Expériences Professionnelles

SQUAD, Paris

Depuis 01 / 2024

Product Owner CyberArk

- 1. Tâches de configuration et de déploiement
- Configurer les coffres-forts et les stratégies de gestion des mots de passe.
- Ajouter et configurer des comptes privilégiés dans CyberArk.
- Mettre en place des politiques de rotation des mots de passe selon les exigences du client.
- Effectuer des configurations simples, comme les workflows d'approbation ou les intégrations de base (LDAP/AD).
- 2. Support technique
- Fournir une assistance aux utilisateurs finaux pour des tâches courantes comme :
 - La récupération ou l'enregistrement des mots de passe.
 - L'utilisation des sessions PSM pour l'accès distant sécurisé.
 - Résoudre des problèmes techniques de niveaux N1 N2 N3 (erreurs de connexion, accès aux coffres-forts, etc.).
- 3. Documentation
- Rédiger et maintenir des documents techniques, tels que :
 - Les guides d'installation et de configuration.
 - Les plans de test (test cases) pour valider les configurations.
- Contribuer à la documentation des incidents et des résolutions dans un système ITSM.

- 4. Audit et reporting
- Collecter des données pour les audits de sécurité à l'aide des rapports CyberArk.
- Vérifier la conformité des comptes privilégiés gérés par rapport aux exigences de sécurité du client.
- Aider à générer et analyser des rapports d'accès et d'activité
- 5. Formation et sensibilisation
 - Former les utilisateurs finaux ou les administrateurs sur des fonctionnalités basiques de CyberArk.
 - Assister dans les sessions de transfert de compétences.
- 6. Participation à des projets d'intégration
- Travailler sur des intégrations de base entre CyberArk et d'autres outils, comme Active Directory, SIEM ou des systèmes ITSM.
- Tester et valider les intégrations existantes avec les équipes.
- 7. Tests et validation
- Exécuter des tests et des mises à jour ou des changements dans l'environnement.
- Tester des scénarios de gestion des mots de passe, d'accès aux sessions, et d'intégration

Neverhack, Paris

01 2023 / 01 2024

Consultant PAM CyberArk

- Installation et Administration de l'infrastructure CyberArk
- Embarquement de comptes et d'applications dans la solution CyberArk
- Gestion et Traitement d'incidents (Support N2/N3)
- Développement de connecteurs PSM automatisant les connexions à des applications métiers à travers CyberArk
- Installation de la solution Core PAS en v12.2 (Vault, DR, PVWA, CPM, PSM, PSMP, Backup)
- Upgrade des composants PVWA, PSM et PSMP en 12.2.12
- Configuration de la haute disponibilité des composants PVWA, PSM et PSMP (configuration de VIP)
- Raccordement aux outils tiers (AD, Syslog, SIEM, SMTP...)
- Configuration MFA avec PointSharp (Radius)
- Assistance dans les phases de recette
- Automatisation des actions CyberArk via script REST API pour (création de des coffres-forts, des groupes locaux CyberArk, des groupes et users dans l'Active Directory, mapping les groupes locaux CyberArk au groupe AD, embarquement des comptes, etc)
- Développement de script PowerShell pour automatisation (module AD, REST API et PACLI) Support de niveau N2/N3
- Rédaction de fiches incidents N2/N3
- Animation d'ateliers techniques
- Rédaction de documentation de production et de cahiers de recette
 - Développement sur PSM /CPM:
 - connecteurs PSM avec AutoIT (Toad, Squirrel, RSAT [DNS, ADUC et GPMC])
 - connecteurs Web PSM (VCenter, Palo Alto, Panorama, Fortigate, F5)
 - plugin CPM AS400

MGEN Technologie, Paris

06/2022 à 12/2022

Consultant IAM

- Administrer et faire évoluer les briques IAM :
- Projet CIAM (en cours)
- Reprise de la TMA (Tierce Maintenance Applicative Groupe Vyv et Prestataire)
- Accrochage SSO (**Forgerock**) sur différente application en fonction du besoin étudié
- Prise en compte et analyse des besoins
- Paramétrages recettes fonctionnelles
- Gestions des demandes de livraisons
- • Coordination des acteurs Investissement sur les projets d'IAM:

- Organisation, participations aux réunions et ateliers, rédaction de compte rendus, rédaction des spécifications, supports de présentation
- Participation à l'activité de revue des habilitations (contrôle), échanges avec les équipes, pilotage et exécution des remédiations
- Mission transverses : Reporting sur les projets au RSSI, rétro-documentation, identification et mise en place d'actions d'amélioration

Axicom Security, Paris

09/2021 à 06/2022

Consultant Architect Security Edr

Au sein d'Axicom Security, j'étais en charge d'accompagner les projets d'intégration de solution EPP et EDR (SOPHOS) chez différents clients et dans la mise en œuvre de la sécurité et de la mise en conformité à la politique sécurité suivant le contexte client. Monter en compétence sur la solution **OKTA**.

- Rapport et documentation technique Gestion de l'architecture d'Antivirus
- Supervision des alertes de sécurités remontées par l'EDR
- Définition de règle de filtrage web des postes de travail (Sophos)
- Projet de migration on-premise vers SAAS
- Détection des fichiers malveillants téléchargés par les utilisateurs.
- Participation à la mise à jour des postes de travail
- Lancement des scans AV sur les postes de travail, mise en quarantaine et isolation des machines à risque.
- Veille et analyse des menaces
- **OKTA** : Projet de mise en place de la solution, intégration, SSO, MFA pour des applications en internes

Elandis, Paris

02/2021 09/2021

Chef de Projet

- Revue et amélioration de la méthode d'analyse de risque projet
- Projet d'aménagement des nouveaux locaux, mise en place fibre noire et bornes wifi suivant les normes
- Analyse du besoin et cahier des charges
- Conduite et coordination de projet (Gantt et retro-planning)
- Réunions avec les différents acteurs
- Gestions des ressources
- Gestion des budgets

KOMET France, Paris

11/2018 02/2021

Administrateur Systèmes Réseaux et Bases de Données (Alternance)

Assurer et maintenir les services et le réseau informatique de l'entreprise. Gestion de projets, déploiement, sauvegarde des données, formation et support aux utilisateurs :

- Projet mise en production du MDM de Microsoft
- Support et formation aux utilisateurs
- Configuration et maintenance du parc informatique (ordinateurs, smartphones, imprimantes)
- Maintien de l'infrastructure réseau (HPE) et des services virtualisés (Microsoft Serveur 2016 - Hyper-V)
- Gestion des services réseaux (DNS, DHCP, VPN SSL et IPSEC)
- Téléphonie Fixe Mitel, 3CX
- Gestion des lignes mobile (Orange Business Services)
- Interlocuteur avec les prestataires informatique.

Formations et Diplômes

2021-2022 Expert en Sécurité Digital – ESD Diplôme BAC+5

2020-2021 Chef de projet informatique – Titre de Niveau 7 – ASTON ECOLE IT

2018-2020 Administrateur Systèmes Réseaux et BDD Niveau 6 – ASTON Certification Diplôme BAC+4

2018-2019 Formation niveau II Administrateur Système et Réseaux – IPI Groupe IGS, Paris
2017-2018 Technicien Supérieur en Support Informatique -Niveau III - GECCEL, Garges
2017-2018 Administrateur réseaux en télécommunication Cisco - GECCEL, Garges
2016-2017 Technicien en informatique Niveau IV Titre RNCP– GECCEL, Cergy
2015-2016 Bac professionnel Gestion Administration - Lycée Camille Claudel, Mantes la Ville

Certifications

Sailpoint certification	En cours
CyberArk certification Sentry	Validée
CyberArk certification Defender	Validée
OKTA Certification Professional – OKTA Certification Administrator	Validée
CYBERARK certification TRUSTEE	Validée
Sophos Certification Engineer – Sophos Certification Architect	Validée
Expert en Sécurité Digitale Niveau 7 – ASTON Certification CEH et ISO27001	Validée

Langues

Français	Langue maternelle
Anglais	Technique