BILEL KHARRATI

Ingénieur Sécurité | Réseau | Cybersécurité

06 95 39 79 69 @ www.bilel.eu
34 boulevard de Stalingrad, 94600 Choisy-le-Roi

RÉSUMÉ

Ingénieur sécurité avec plus de 10 ans d'expérience en maintenance et administration d'infrastructures informatiques. Passionné par les aspects techniques de la sécurité des systèmes d'information, je recherche des défis pour approfondir mes compétences et contribuer à la protection des infrastructures critiques.

EXPÉRIENCE

Ingénieur Sécurité

Chantelle / CNRS

05/2022 - Présent Val de Marne

- Détection, qualification, analyse et investigations des incidents de sécurité, gestion des événements et veille sur les menaces
- Automatisation, améliorations continues et renforcement de la sécurité des infrastructures, contrôle de conformité et rapport d'audits de sécurité
- Sensibilisation des équipes, rédaction de procédures et contribution aux plans de continuité et de reprise d'activité (PCA/PRA)
- Threat Hunting avec les outils disponibles, en utilisant les indicateurs de compromission
- Analyse forensic approfondie lors d'un incident, en utilisant les processus documentés et les outils disponibles.
- Développement et maintien des règles de détection sur différents outils (SIEM, EDR, IDS/IPS, Firewall)
- **Environnement technique** : Windows Server, CentOS, Ansible, Palo Alto, Docker/K8s, ELK, AWS, Meraki, SentinelOne, Qualys, Withsecure, Wazuh

Ingénieur Sécurité des Systèmes / DevSecOps

Thales Digital Factory / Gandi

08/2018 - 04/2022 Paris

- Supervision des événements de sécurité et déploiement d'environnements sécurisés
- Hardening de la sécurité des infrastructures Linux, gestion des firewalls et création de règles d'alerte
- Scan de vulnérabilités, patch management, et veille sur les menaces et vulnérabilités
- Audit de configuration, Rédaction des HLD/LLD
- PoC des outils de sécurité, actions préventives nécessaires pour assurer la haute disponibilité des infrastructures réseau et sécurité
- Automatisation des processus récurrents, gestion les demandes d'ouverture de flux, création de règles de firewall en fonction du DAT
- Analyser les alertes de sécurité en provenance du SOC, et proposer/appliquer des actions de remédiation, recherche de tentative de compromission
- **Environnement technique** : Linux, Splunk, VMware, Docker, Terraform, PowerShell, Ansible, GitLab CI/CD, Jenkins

Ingénieur Systèmes, Réseaux et Sécurité

École Supérieure de Physique et de Chimie Industrielles (ESPCI)

2015 - 2018 Paris

- Maintien en condition de sécurité des infrastructures, automatisation de la production
- Analyse et traitement des événements de sécurité, pentest des labos de recherche et sensibilisation à la sécurité
- Collecte et analyse d'artefacts sur environnements Windows et Linux
- Mise en production, maintenance et sécurisation des applicatifs métiers, cartographie du réseau, audit de la couverture wifi et gestion des flux réseau
- **Environnement technique** : Python, C, JS, Selenium, MySQL, Bash, NetBSD, Metasploit, LDAP, Aruba, Linux/CentOS, MailInBlack, Veeam backup, CloudFlare, Fortinet, KVM

RÉALISATIONS

Intégration du réseau de l'IAM

Faire dialoguer les api OKTA et MERAKI afin d'intégrer les éléments réseau des sites distant dans l'IAM

Refonte de l'architecture de sécurité

Création et déploiement d'une stack complète de brique et service sécurisé

Déploiement d'une solution SIEM

Déploiement d'un SIEM ELK et intégration des assets et des règles de détection, automatisation des règles de corrélation

Intégration d'une solution NAC

Intégration du la solution PacketFence afin de sécuriser les labos en zones à régime restrictif (ZRR) du CNRS

COMPÉTENCES

SIEM EDR | Réseau

Python PowerShell C ASM

Évaluation des risques | Firewall

Web services, RESTfull API

Intrusion Detection

Windows Linux Cloud computing, virtualisation Docker

FORMATION

Formation Analyse inforensique réseau
2024

Formation Okta Essential
2023

Formation Splunk
2022

Formation Palo Alto
2020

Formation Aruba Switch
2019

Formation Docker
2016

EXPÉRIENCE

Administrateur Systèmes et Réseaux

Osiatis / Docaposte / RATP

2006 - 2015 Ile de France

- Gestion et maintenance de l'infrastructure IT, support applicatif, résolution d'incidents de niveau 1 à 3
- Installation, configuration et maintenance des serveurs et réseaux, automatisation des tâches récurrentes
- Développement de scripts d'exploitation et de playbooks Ansible, rédaction de procédures d'exploitation et de rapports d'activité
- Surveillance des opérations d'exploitation, maintenance matérielle, gestion de la téléphonie et des systèmes embarqués
- **Environnement technique** : VMware, Citrix, Active Directory, SCCM, GLPI, Ansible, Ubuntu, RS485/232, équipements de réseaux industriels

ÉDUCATION

Licence informatique

Conservatoire National des Arts et Métiers

09/2015 - 07/2016 Paris

BTS Solutions informatiques aux organisations (option solutions logicielles et applicatives)

Candidat libre

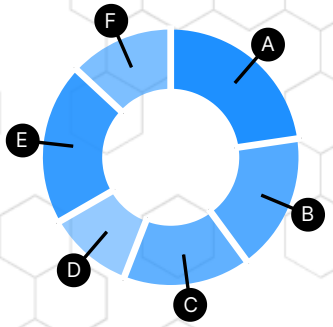
09/2014 - 07/2015 Paris

LANGUES

English
Avancé

Arabe
Intermédiaire

MON QUOTIDIEN



- A Gestion des firewall
- B Détection et analyses des menaces
- C Automatisation des tâches récurrentes
- D Déploiement des briques de sécurités
- E Amélioration continu de la sécurité
- F Rédaction de la documentation