EFR

Consultant Gestion des vulnérabilités

FORMATIONS & CERTIFICATIONS

2017-2019 : Diplôme Master 2 Expert en ingénierie de l'informatique et des systèmes d'information : ESGI (Ecole Supérieure de Génie Informatique).

2017 : Formation Sécurité informatique chez Sysdream Levallois (92) : Hacking et sécurité avancée, détection, identification et éradication de malwares

2025 : Formation et Certification CompTIA, CompTIA Security Plus.

2025 : Formation Microsoft Sentinel TECH LAB (détection & IA avec Copilot for Security)

2025 : Formation Splunk Administering Splunk Enterprise Security

2024 : Formation et Certification Falcon Crowdstrike / Falcon Administrator

2022 : Formation et Certification EC-Council | Certified SOC Analyst.

2022 : Formation ECCouncil, Computer Hacking Forensic Investigator

2022 : Formation PECB, ISO 27001 Lead Implémenter

COMPETENCES FONCTIONNELLES & TECHNIQUES

- SOC et SIEM (Splunk) : Détection, analyse et réponse aux incidents
- Gestion des vulnérabilités : Scans (Qualys), reporting, plan de remédiation et suivi, coordination avec les équipes IT.
- Gestion des dérogations
- Gestion des habilitations,
- Sécurité des infrastructures
- Outils et solutions : CrowdStrike, Qualys, Splunk ES, Logpoint, Microsoft Sentinel et Copilot for Security, Vectra, ServiceNow

Anglais : opérationnel

EXPERIENCES PROFESSIONNELLES

GRTGAZ, Janvier 2024 à Février 2026

Ingénieur cybersécurité

Contexte du projet : Consultant cybersécurité référent pour la chaîne de valeur Infrastructure et Data Center. Mon rôle est d'accompagner l'équipe d'infrastructure Datacenter pour sécuriser les infrastructures vis-à-vis des menaces de cybersécurité, tout en assurant la conformité aux réglementations et en maintenant une coordination avec les parties prenantes internes et externes.

Réalisations :

- **Pilotage sécurité opérationnelle sur le périmètre Infrastructure & Data Center.**
- **Contribution à la détection et suivi de vulnérabilités (Qualys, Nessus) et coordination des actions correctives.**
- **Support opérationnel aux équipes SOC (logs, incidents).**
- **Gestion des comptes à privilèges et suivi des habilitations administrateurs.**
- **Suivi de la conformité sécurité et gestion des dérogations.**
- **Recette Cyber : Intégration Sécurité Projet (ISP)**

Environnement technique : Qualys, Nessus, Splunk, ServiceNow

INA (Institut National de l'Audiovisuel), Septembre 2020 à Décembre 2023

Analyste cybersécurité et gestion des vulnérabilités

Contexte du projet : Analyse SOC (N1, N2/N3) : détection, prévention et réponse aux incidents.

Tâches réalisées :

- **Gestion des vulnérabilités : Définition de périmètres de scans, réalisation de scans avec Qualys et de leurs suivis (reporting et remédiation).**
- **Détection et gestion des incidents de sécurité remontés par le SIEM (Logpoint) et par IDS (Vectra)**
- **Investigations sur incidents de sécurité (portée, causes, remédiations).**
- **Participation active à la gestion de crise lors d'attaques DDoS et propagation du ver ayant affecté le SI ;**
- **analyse, diagnostic, coordination et maintien de la communication en salle de crise.**
- **Intégration et enrichissement de nouvelles sources de logs dans le SIEM (applicatifs, serveurs, réseau) afin d'améliorer la détection d'incidents.**
- **Optimisation des règles de corrélation, tuning des alertes SIEM et amélioration du pipeline de détection SOC.**
- **Production de rapports d'investigation et présentation en COMOP sécurité.**

Environnement technique : Qualys, Splunk, Logpoint, Vectra, ServiceNow

PRICE WATERHOUSE COOPERS, Septembre 2029 à Septembre 2020

Analyste cybersécurité

Contexte : Membre de l'équipe CISO PWC France et en étroite collaboration avec les équipes basées aux Royaume-Uni, en charge des activités cybersécurité

Tâches réalisées :

- **Gestion des vulnérabilités : Définition de périmètres et réalisation de scans avec Qualys**
- **Reporting et suivi de remédiation des vulnérabilités**
- **Gestion des incidents : analyse et traitement des incidents de sécurité via ServiceNow.**
- **Suivi des tests d'intrusion et coordination des remédiations**

Environnement technique : Qualys, Splunk, ServiceNow

BITDEFENDER, Septembre 2015 à Août 2019

Ingénieur cybersécurité

- **Installation, administration et support technique avancé (solutions antivirus B2B/B2C)**
- **Investigation incidents sécurité et proposition de mesures correctives.**