

## REFERENT CYBERSECURITE

### FORMATIONS & CERTIFICATIONS

2022 : Ecole d'ingénieur  
Informatique EFREI, majeure  
cybersécurité

### COMPÉTENCES

- Elaboration de politiques et de processus adaptés aux spécificités de l'entreprise
- Pilotage de projets transverses, de l'analyse des risques à la mise en œuvre technique
- Administration, automatisation et durcissement des systèmes
- Traitement proactif des vulnérabilités, alertes et incidents
- Coordination et l'accompagnement des équipes techniques et métiers

#### COMPETENCES TECHNIQUES

- Analyse de risques : EBios
- Normes réglementaires : RGPD
- Cybersécurité : Qualys, Cyberreason, CyberArk, BitLocker, OpenSSL, Zabbix
- Systèmes : Windows, Linux (RHEL/CentOS), Active Directory, Entra ID, VMware, Docker
- Développement : PowerShell, Bash, Python, Git, SQL
- ITSM : Jira Service Management, Confluence
- Référentiels : CIS Benchmarks, CIS Controls v8

### LANGUES

Anglais : courant

## EXPÉRIENCES

Société :

ALBIOMA

03/2023 à 06/2025

Poste :

Référent sécurité

Environnement technique :

AD, Entra ID, BitLocker  
Qualys, Cybereason, Vade365, OpenSearch, KnowBe4  
PowerShell, Bash  
Fortinet, Stormshield  
Veeam, QNAP, Synology

Missions réalisées :

Contexte :

- Producteur d'énergie renouvelable implanté sur 33 sites en France (hexagone et outremer) et à l'international (Brésil, Turquie, Canada, Australie)
- Cyberattaque majeure en 2021, ayant conduit à la création d'un pôle cybersécurité
- 850 PC, 160 serveurs OnPremise, 230 applications métiers

Objectifs :

Sur l'ensemble du groupe, bureautique comme industriel :

- Mettre en conformité le SI avec le niveau 2 du référentiel CIS Controls v8
- Maintenir l'ensemble du SI en conditions de sécurité
- Découvrir et répondre aux vulnérabilités, alertes et incidents

Réalisations :

- Gouvernance et communication
  - Rédiger les politiques (tests d'intrusion, chiffrement, sauvegardes, etc.)
  - Sensibiliser les collaborateurs à travers le tournage de vidéo et la préparation de modules de formations
  - Rédiger et présenter un compte rendu mensuel aux directeurs ainsi qu'un comité de cybersécurité trimestriel à mes collègues
- Projets
  - Déployer BitLocker (par scripts et GPO) sur l'ensemble des PC
  - Chiffrer l'ensemble des sauvegardes
  - Bloquer les périphériques de stockage amovibles
  - Rédiger les processus de configuration sécurisée des PC, serveurs et équipements réseau
  - Rédiger les processus de gestion des vulnérabilités
  - Développer un script PowerShell générant un rapport de conformité des PC et serveurs, interconnecté via l'API de Qualys et de Cybereason
- Exploitation opérationnelle
  - Remédier ou piloter la remédiation des alertes, vulnérabilités et incidents (phishing, équipements exposés, malwares, veille technologique, etc.)

- Vérifier chaque jour la réussite des sauvegardes chiffrées et prendre en charge les malwares détectés par notre EDR
- Rendre compte chaque semaine des alertes en cours et de la conformité des systèmes
- Amélioration continue et automatisation
  - Durcir les systèmes et désactiver les protocoles obsolètes
  - Automatiser la maintenance des PC via Qualys (mises à jour, désinstallations, configurations, redémarrages)
  - Maintenir et améliorer continuellement Vade365, Qualys et Cybereason
  - Auditer mensuellement notre Active Directory et Entra ID (conformité des PC et serveurs, configurations améliorables, etc.)

#### Résultats :

- Création de 15 procédures et 4 politiques (maintenues et utilisées au quotidien)
- Réduction de 63 à 28 vulnérabilités par PC ou serveur
- Traitement de plus de 500 alertes de vulnérabilités (hors faux positifs) et de 10 incidents
- Mise en conformité de plus de 100 applications métier vis-à-vis de nos exigences

#### Société

MAGELLAN

09/2023 à 11/2023

#### Poste :

Consultant tests d'intrusion

#### Environnement technique :

nmap, Nessus, Nikto, wpscan, gobuster, sslscan  
Burp Suite Pro, OWASP ZAP, Postman  
Metasploit, Hydra, SQLMap,

#### Missions réalisées

##### Contexte :

- Équipe spécialisée en cybersécurité offensive
- Clients en banque, éducation, énergie etc.

##### Objectifs :

- Émettre des recommandations de sécurisation des systèmes de nos clients afin de leur émettre des recommandations

##### Objectifs et réalisations :

- Conduire des tests d'intrusion sur des applications et API web afin de découvrir vulnérabilités
- Produire des rapports de vulnérabilités incluant analyse des risques et recommandations de remédiation
- Présenter et expliquer les résultats aux équipes techniques et métiers pour favoriser leur mise en œuvre

##### Résultats :

- 11 tests d'intrusion réalisés avec rapports et restitutions

**Société****CAP GEMINI****04/2021 à 09/2022****Poste :****Consultant IAM****Environnement technique :**

**CyberArk**  
**Jira Service Management, Confluence**  
**Zabbix**  
**Terraform, Ansible**

**Missions réalisées****Contexte :**

- Société de conseil IT
- Service spécialisé sur CyberArk ; solution de PAM (Gestion des accès privilégiés)
- Volonté de créer un centre de service afin d'optimiser et automatiser les actions récurrentes

**Objectifs :**

- Garantir le support et la supervision des environnements clients
- Automatiser ou formaliser des procédures, dans le but d'améliorer la qualité de service tout en réduisant le temps dépensé

**Réalisations :**

- Support N2 CyberArk
  - Diagnostiquer et résoudre les incidents
  - Répondre aux demandes d'évolutions
  - Vérifier quotidiennement les environnements de nos clients, et automatiser cette vérification
- Création d'un ITSM
  - Le configurer (types de demandes, SLA, routage automatique des tickets, vue des clients, etc.)
  - L'interconnecter avec un autre ITSM via API REST
  - Rédiger les procédures N1 et N2
- Supervision CyberArk
  - Déployer Zabbix sur l'ensemble de nos instances
  - Développer un script de connexion en Bash afin de vérifier la disponibilité du service
  - Automatiser le déclenchement d'astreintes via des alertesSMS en cas d'anomalie
- Concevoir et animer des formations sur Linux et les PKI (OpenSSL) pour mes collaborateurs.

Ces formations combinaient présentations théoriques et travaux pratiques sur machines virtuelles.

Résultats :

- Efficacité accrue du processus de déclaration et de résolution des demandes N1/N2
- Détection automatique d'incidents de disponibilité ayant permis des résolutions hors horaires ouvrés
- Gain de temps pour les N3 qui peuvent déléguer les tâches N1/N2 à l'aide de procédures rédigées

Société

PLATYPUS

01/2019 à 01/2020

Poste :

Développeur fullstack

Environnement technique :

Angular (TypeScript/HTML/CSS)

Google Sheets / MariaDB

Contexte : projet visant à mettre en relation et faciliter l'administratif entre professeurs et écoles

Objectifs :

- Développer l'application web principale (servant à faciliter les démarches, à gérer la comptabilité, etc.)
- Migrer une base de données afin de l'accélérer

Réalisations :

- Développement FullStack
  - Ajout de nouvelles fonctionnalités (calcul du temps de trajet entre deux écoles, gestion des emplois du temps des professeurs, etc.)
  - Résolution de bugs
- Migration progressive de la base de données depuis Google Sheets vers MariaDB
  - Création de requêtes SQL pour reproduire la structure des formules Google Sheets

Résultats :

- Interfaces améliorées pour les enseignants
- Fonctions de comptabilité ajoutées
- Accélération des requêtes de la base de données (de plusieurs minutes à quelques dixièmes de seconde)