Julien LEQUEN

Ingénieur Cyberdéfense

Six-Fours-les-Plages | linkedin.com/in/julien-lequen | Permis B

PRÉSENTATION

Ingénieur cyberdéfense, quinze ans d'expérience en sécurité des systèmes d'information — du SOC opérationnel au pilotage RSSI. J'interviens sur toute la chaîne : détection et réponse à incident (DFIR), threat intelligence, gouvernance et conformité (PSSI, LPM, RGPD). Mon parcours, mené au sein du Ministère des Armées et de grands groupes (Bouygues, SNCF, Capgemini) et nourri par un engagement actif dans la communauté cyber, m'a forgé une approche technique et rigoureuse de la protection des infrastructures sensibles.

COMPÉTENCES

Cybersécurité

Gouvernance SSI, Supervision (SOC), Réponse à incident (DFIR), Threat Intelligence

Systèmes & scripting

Windows, Linux, PowerShell, Bash, Sysinternals

Réseau

Firewall, Routeur, Switch

Virtualisation & conteneurs

VMware, Proxmox, VirtualBox, Docker

Outils sécurité

DFIR-ORC, Splunk, MISP, APT Defender

INTÉRÊTS

Plongée sous-marine

Tir sportif

Informatique

Domotique

Impression 3D

EXPÉRIENCES

Ministère des Armées — **Octobre 2019 - aujourd'hui**
Ingénieur Cyberdéfense

Bouygues SA — **Octobre 2017 - Septembre 2019**
RSSI — Paris

- Gouvernance de la sécurité
- Rédaction d'une PSSI
- Gestion des dérogations
- Pilotage du durcissement Active Directory
- Rédaction d'un cahier des charges pour la mise en place d'un SOC

C2S Bouygues — **Mai 2017 - Septembre 2019**
Responsable CERT — Île-de-France

- Mise en place et pilotage du service de réponse aux incidents de sécurité (CSIRT)
- Mise en place et pilotage de la cellule de veille et de renseignement sur les menaces (Threat Intelligence)
- Conseil sur l'application de la LPM (Loi de Programmation Militaire)
- Conseil sur la mise en conformité RGPD

Squad — **Janvier 2017 - Mai 2017**
Consultant Sécurité pour SNCF — Île-de-France

- Animation de la cellule de recherche d'information du CERT SNCF (COTIC)
- Détection et qualification des fuites de données de l'entreprise

Euriware / Capgemini — **Septembre 2011 - Janvier 2017**
Analyste Sécurité — Cherbourg

- Réponse à incident de sécurité
- Création de règles de corrélation SIEM pour la détection d'incidents
- Investigation forensique
- Analyse comportementale
- Analyse de malwares
- Audit d'architecture et de configuration
- Pilotage de l'activité de scans de vulnérabilités

FORMATIONS

Bac +4 — **2012 - 2014**
Formation RARE (Responsable Administrateur de Réseaux d'Entreprise) — CESI

BTS — **2010 - 2012**
BTS Informatique de gestion Administration réseaux d'entreprises — E2SE

Bac Pro — **2008 - 2010**
Bac Pro SEN TR (Systèmes Électroniques Numériques, Télécommunications et Réseaux) — Lycée Charles TELLIER

BEP — **2006 - 2008**
BEP Électronique — Lycée Alexis de TOCQUEVILLE

EXPÉRIENCES DE BÉNÉVOLAT

Tedomum **2020 - aujourd'hui**

Membre actif

https://tedomum.net/

Hébergement de services sécurisés, respectueux de la vie privée et des libertés.

ARCSI **2017 - aujourd'hui**

Membre actif

https://www.arcsi.fr/

Association des Réservistes du Chiffre et de la Sécurité de l'information.

FR/AC **2017 - aujourd'hui**

Membre actif

Communauté French Abuse et CSIRT.

Crypt-0n **2016 - aujourd'hui**

Fondateur et trésorier

https://www.crypt-0n.fr/

Fondateur, trésorier et webmaster d'une association ayant pour but de promouvoir la sécurité informatique.

FFESSM **1999 - aujourd'hui**

Plongeur bouteille et apnée

Plongée bouteille :

- Niveau 4
- Initiateur
- Technicien en Inspection Visuelle (TIV)
- Nitrox confirmé

Plongée apnée :

- Niveau 2
- Initiateur