



Antony Audic

Informations personnelles

audic.antony@gmail.com

Permis de conduire
B

OUTILS DE SECURITE :
SentinelOne, Sekoia, Varonis
Proofpoint, Wazuh, MDE

LANGAGES: Bash, MySQL,
Ansible, Python, SIGMA

PLATEFORME CLOUD:
AWS, Azur, GCP

SYSTEMES: GNU/Linux
(Debian, Ubuntu, Redhat),
Windows clients/servers (XP, 7,
8, 10, 2008, 2012, 2016)

PROTOCOLES : DNS, SSH,
FTP, SFTP, DHCP, HTTP(S),
NTP

JOURNALISATION: Elastic
Search, Logstash, Kibana

DEVOPS: Ansible, Gitlab CI,
Jenkins, Terraform

MIDDELWARE: Apache,
Nginx

Langues

Espagnol

Anglais

Français



Profil

- **Ingénieur Système**
Solides compétences analytiques
- **Compréhension des enjeux sociaux**
- **Bonne communication**
- **Flexibilité et adaptabilité**
- **Connaissance des outils de recherche**
-



Expertise Métier

- **Connaissance des menaces et vulnérabilités**
- **Surveillance et détection des incidents de sécurité**
- **Réponse aux incidents de sécurité**
- **Gestion des logs et des données de sécurité**
- **Connaissance de la conformité**



Expertise Technologique

- **Analyse de code malveillant**
- **Outils de sécurité : EDR XDR SIEM**
- **Langage de programmation : Python, Bash, YAML**
- **Plateforme Cloud: AWS AZURE**
- **DevOps/GitOPS Tools: Ansible, Git, Rundeck**
- **Terraform Middleware: Apache, Nginx**



Expérience Professionnelle

Consultant SOC, SYNETIS, Cesson-Sévigné

octobre 2022 - mars 2025

CLIENTS: Cora, Asn, Portalp, Groupe Partnaire, Nge, Asn, Le Verdier, Nuxe, La martiniquaise, SABC, Tiime, Lynred, Emova, Odalys,

CONTEXTE : MSSP IR

MISSIONS:

- Suivi de détection de vulnérabilités, attaques malveillantes
- Utilisation d'outils de sécurité, d'analyse de code malveillant et de gestion des informations et des événements de sécurité (SIEM)
- Maintenance des agents SentinelOne
- Préparation des comités de pilotage clients et animation

TECHNOLOGIES

- SentinelOne, Wazuh, Jira, Sekoia, Varonis, Proofpoint, MDE

Administrateur WebOPS, Claranet, Cesson-Sévigné

janvier 2019 - octobre 2022

- Gestion / Architecture de l'infrastructure d'un client grand compte dans le domaine du luxe
- **Plateformes Cloud:** AWS
- **DevOps/GitOps Tools:** Ansible, Git, Rundeck • **CI/CD:** Azure, GitLab, Bitbucket
- **Middleware:** Apache, Nginx, Tomcat
- **Intégration/Build:** Terraform • intégration et optimisation de l'architecture des plateformes clients
- Analyse et Résolution des dysfonctionnements remontés par les équipes de supervision
- Intervention en escalade sur des incidents affectant le bon fonctionnement des services

Administrateur Backup, Claranet, Cesson-Sévigné

2016 - 2018

- Intégration, maintenance et MCO outils de backups multiplateformes clients
(Avamar Veeam)

Administrateur Système et Web, Claranet , Cesson-Sévigné

novembre 2010 - 2015

- Infogérance de plateformes clients pour des sites de type: E-commerce, média / presse
- Traitement de demande de mise en production et préproduction,
- Rédaction de documentation



Formation

SANS SEC450 Blue Team Fundamentals: Security Operations and Analysis

décembre 2023

SEKOIA.IO Certified Security Analyst 301

février 2023

BTS TSSI, DIAFOR

août 2019