



## Cyber Security Architect / Polyglot Developer / DevSecOps

### Résumé

*Développeur de formation et passionné de sécurité, j'aime traiter des projets alliant ces deux compétences. Mon expérience en développement, ainsi que ma curiosité pour les technologies me permet d'avoir un regard tourné vers l'avenir. J'attache de l'importance au partage des connaissances et compétences au sein de mon environnement de travail. Avidé de connaissances, je recherche des postes permettant l'apprentissage et l'exploitation de nouveaux savoirs.*

*Profils de postes souhaités : Architecte; Formateur; Expert Technique; DevSecOps; Slasher;*

*Domaines souhaités : Cyber Sécurité; Big Data; IoT; Blockchain;*

### Expérience Professionnelle

#### **Continental Digital Services [Industriel Automotive - R&D]**

**Toulouse - France**

*Cyber Security Architect / Ninja Developer / SecOps / PO*

*June 2017 -*

- › Product Owner pour produits Sécurité / DevOps.
- › Technical leader / Golang guru.
- › Définition des services de cyber risk monitoring (AWS).
- › Définition plateforme de production (Data, Services, Produits, Operations).
- › Définition stratégie "Security By Design".
- › Plateforme de communication sécurisée Voiture connectée / IoT <-> Cloud. (HTTP, MQTT, CoAP)
- › Plateforme d'identification et contrôle d'accès distribuée. (AWS, Go, OIDC / SAML2)
- › Protocole d'identification respectant la vie privée. (Crypto, ZKP)
- › Etude d'intégration de blockchain. (Data Sharing, Licensing)
- › Mesures techniques CyberSécurité liées au RGPD. (Crypto, Go, Java, Scala)
- › Rédaction des guides de durcissement. (AWS, Docker / K8S)
- › Audits et conseils d'architecture. (Threat Model)
- › Audits et conseils de code sécurité. (Java / J2EE, NodeJS, Python, Go, Crypto)
- › Formation / Support aux équipes. (Go, Crypto, Blockchain)

#### **Sogeti ESEC [Sécurité - SSII]**

**Toulouse - France**

*Cyber Security Expert / Data Architect / Full Stack Developer / DevOps*

*October 2013 - June 2017*

- › Développement outils CERT / SOC.
- › Outil de gestion d'incidents Jira / QRadar (Go, Javascript, RethinkDB)
- › Plateforme d'analyse de malware automatisée pour extraction d'IOC. (Go, RethinkDB, RabbitMQ, Docker, Cuckoo, VirusTotal, Yara, AngularJS 2)
- › Etude des regroupements de données IoC / IoA / observables. (R, Neo4j, ElasticSearch, Machine learning, Clustering)
- › Plateforme de centralisation d'indicateurs pour analyse sécurité "Technical Threat Intelligence". (Go, RabbitMQ, ElasticSearch, Neo4j, AngularJS)
- › Plateforme de centralisation et corrélation des bulletins sécurité. (Go, RabbitMQ, MongoDB, AngularJS)
- › Conception et réalisation d'un système embarqué type "boîte blanche" pour décontamination virale. (Go, AngularJS, Qt, ZMQ, Docker)
- › Microservices: email (composition, envoi, signature), identification / autorisation, jetons, licences (Go, gRPC, Consul, Vault, Docker, Rancher)
- › Audit qualité et sécurité. (Java / J2EE)
- › Encadrement stagiaires.

#### **Infotel [Mainframe - Editeur / R&D]**

**Toulouse - France**

*Ingénieur R&D / Scrum Master*

*January 2010 - October 2013*

- › Plateforme de dépôt sécurisé de fichier à haute valeur probante. (RabbitMQ, Protobuf, Scala/AKKA, Java, Spring, ElasticSearch, AngularJS)
- › Conception et réalisation d'un SSO basé sur OAUTH 2.0. (Java, Spring, JWT, PKI, PKCS#11, HOTP)
- › Industrialisation de la chaîne documentaire. (Git, Jenkins, Maven, Docbook5, XSLT, FOP)
- › Revue de code qualité et sécurité. (Java, J2EE)
- › Maintenance de produits. (ClearCase, Java, Struts2, Eclipse RCP, Z/OS)
- › Encadrement stagiaires.

## SCASSI Conseil [Sécurité - SSII / Conseil]

### Ingénieur Sécurité

- › Conception et réalisation d'un outil d'analyse de risques basé sur la méthodologie EBIOS (SOA, J2EE, .Net)
- › Généralisation des méthodes d'analyse de risques (UML)
- › Audit de code (Java/J2EE, C/C++, PHP)
- › Reverse engineering, analyse de malware
- › SOC (Security Operating Center) auprès d'un grand compte (Gestion des événements sécurité, gestion des requêtes sécurité, maintien en condition opérationnelle)
- › Instructeur pour des ateliers techniques (Virtualisation / Firewall & Contrôles d'accès) auprès d'une vingtaine de personnes

### Stagiaire - Développeur

October 2007 - July 2008

## Opencube Technologies [Média Numérique - Editeur / R&D]

### Stagiaire - Développeur

Toulouse - France  
March 2007 - September 2007

## MEDES IMPS [Santé / Espace - Editeur / R&D]

### Stagiaire - Développeur

Toulouse - France  
March 2006 - September 2006

## Karobas [Jeux Vidéo - Editeur / R&D]

### Stagiaire - Administrateur Système et Réseau

Sophia Antipolis - France  
March 2005 - August 2005

## Nice-antiques.com [Art - Antiquaire]

### Stagiaire - WebMaster

Nice - France  
March 2004 - July 2004

## Formation

### IUP ISI

#### M2 ISI - Métamodélisation et Temps réel critique

- › Métamodélisation UML; J2EE; Programmation temps réel (ADA, C, SCADE); Droit;

#### M1 Ingénierie des Systèmes Informatiques (ISI)

- › Conception / Modélisation UML; Programmation distribuée (Java / J2EE, C); Base de données (avancé); Mathématiques; Gestion / Economie;

#### L3 Ingénierie des Systèmes Informatiques

- › Conception / Modélisation UML; Programmation (Java / C++ / C / ASM); Base de données; Mathématiques; Gestion / Economie;

### IUT Informatique

#### Licence Professionnelle, Administration des Systèmes et des Réseaux (ASR)

- › Réseau; Administration Systèmes (Unix, Windows); Base de données (Oracle); Mathématiques; Gestion / Economie; Droit;

#### DUT Informatique, Génie Logiciel

- › Base de données; Programmation (Java / C++ / C); Réseau; Mathématiques; Gestion / Economie;

### Lycée Albert Camus

#### Bac S, Science de l'Ingénieur, spécialité Mathématiques

- › Mathématiques; Mécanique; Electronique; Informatique;

## Langues

- › Français - Langue maternelle
- › Anglais - Lu, écrit et parlé

## Compétences

Eléments de catégorie classés : [5] "Expertise", [4] "Je sais", [3] "Je connais", [2] "J'apprends" et [1] "Vraiment si besoin".

### Fonctionnelles

Creative Thinking <sup>5</sup>; Veille technologique <sup>5</sup>; Slasher <sup>5</sup>; Gestion de projet / Scrum Master <sup>4</sup>; Conduite de réunion <sup>4</sup>; Pédagogie / Vulgarisation <sup>4</sup>; Rédaction publications scientifiques <sup>3</sup>; Présentation en public <sup>3</sup>;

### Sécurité

Programmation défensive <sup>5</sup>; Contre-mesures sécurité <sup>5</sup>; OWASP Top 10 <sup>5</sup>; SANS Top 25 <sup>5</sup>; Audit de code <sup>4</sup>; Cryptographie / Chiffrement <sup>4</sup>; Durcissement Logiciel / Conteneur <sup>4</sup>; Threat Modeling (DFD, AT) <sup>4</sup>; Threat Intelligence <sup>4</sup>; Cuckoo Sandbox <sup>4</sup>; Analyse de risque (EBIOS) <sup>3</sup>; RGPD <sup>3</sup>; Suricata <sup>3</sup>; Bro IDS <sup>3</sup>; Honeybots (Cowerie / Kippo) <sup>3</sup>; Sinkhole <sup>3</sup>; QRadar SIEM <sup>3</sup>; Splunk <sup>3</sup>; Elasticsearch / LogStash / Kibana <sup>3</sup>; Reverse Engineering <sup>2</sup>; Penetration Testing <sup>2</sup>;

### Langages

Go <sup>5</sup>; JavaScript <sup>5</sup>; Java <sup>5</sup>; C/C++ <sup>4</sup>; Rust <sup>4</sup>; Ruby <sup>4</sup>; Python <sup>4</sup>; Scala <sup>3</sup>; ASM (x86, ARM7) <sup>3</sup>; PHP <sup>3</sup>; Elixir <sup>2</sup>; Erlang <sup>2</sup>;

### Ingénierie des données

Modélisation Sémantique <sup>5</sup>; Préparation des données <sup>5</sup>; Data Wrangling <sup>5</sup>; Data Scraping <sup>5</sup>; Protégé <sup>4</sup>; Anonymisation <sup>4</sup>; Elasticsearch / LogStash / Kibana <sup>4</sup>; Traitement du signal <sup>3</sup>; Détection d'anomalies <sup>3</sup>; Statistiques <sup>3</sup>; Python / Jupyter / Pandas <sup>3</sup>; SciKit Learn <sup>3</sup>; Machine learning (SVM, PNN, RF, GBM) <sup>3</sup>; H2o <sup>3</sup>;

## Affinités FullStack

Développement Backend <sup>5</sup>; DevOps <sup>5</sup>; Développement Frontend <sup>4</sup>; UI/UX Designer <sup>1</sup>;

## Backend Framework

Clean Architecture <sup>5</sup>; Microservices Patterns <sup>5</sup>; Resilience Patterns <sup>5</sup>; gRPC / Protobuf <sup>5</sup>; REST / GraphQL <sup>5</sup>; NodeJS <sup>4</sup>; Express <sup>4</sup>; Ruby on Rails <sup>3</sup>;

## Cloud

RabbitMQ <sup>5</sup>; NATS <sup>5</sup>; NSQ <sup>5</sup>; ZMQ <sup>5</sup>; WebSocket <sup>5</sup>; Serverless <sup>5</sup>; MQTT / eMQTTd <sup>4</sup>; Apache Kafka <sup>4</sup>; Amazon IAM / Cognito <sup>4</sup>; Amazon EC2 <sup>4</sup>; Amazon SNS <sup>3</sup>; Amazon IoT <sup>3</sup>; Amazon API Gateway / Lambda <sup>3</sup>; CoAP / DTLS <sup>3</sup>;

## DevOps

Docker <sup>5</sup>; Rancher <sup>5</sup>; Prometheus <sup>5</sup>; Consul <sup>5</sup>; Vault <sup>5</sup>; Grafana <sup>4</sup>; GitlabCI <sup>4</sup>; Kubernetes <sup>4</sup>; Helm <sup>4</sup>; Istio / Envoy <sup>4</sup>; Sentry <sup>4</sup>; Jenkins <sup>3</sup>; Terraform <sup>3</sup>; Ansible <sup>2</sup>;

## Frontend / UX

VueJS / Vuex <sup>4</sup>; Apollo <sup>4</sup>; HTML5 <sup>3</sup>; CSS3 / SASS / LESS <sup>3</sup>; WebAssembly <sup>3</sup>;

## Blockchain

General concepts (Proofs, Algorithms, Protocols) <sup>4</sup>; Ethereum <sup>4</sup>; J.P. Morgan Quorum <sup>3</sup>; IBM Hyperledger <sup>3</sup>; Parity <sup>3</sup>; Smart Contract <sup>2</sup>; Solidity <sup>2</sup>;

## Liens

---

- › [site] - <http://zenithar.org>
- › [blog] - <https://blog.zenithar.org>
- › [facebook] - <https://www.facebook.com/zenithar>
- › [github] - <https://github.com/zenithar>
- › [linkedin] - <https://www.linkedin.com/in/zenithar>
- › [mastodon] - <https://mamot.fr/@zenithar>
- › [twitter] - <https://twitter.com/zenithar>

## Autres Activités hors Curriculum

---

- › Instruments musique: Batterie & Saxophone
- › Amélioration continue grâce à la veille technologique, l'expérimentation et les projets personnels (Sécurité, Logiciels, Techniques de management)
- › Rédacteur (Blog)
- › Explorateur technologique
- › Impression 3D
- › Domotique
- › Développement personnel
- › Cuisine du monde
- › Microbrasserie
- › Pâtisserie / Boulangerie
- › Rénovation maison (Maçonnerie, Isolation, Electricité)