



Senior Cyber Security Expert

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 Solution; Développeur FullStack; Expertise Technique; Conseil;

Domaines souhaités : Cyber Sécurité; Big Data; Machine learning; Blockchain; IoT;

Expérience Professionnelle

N/C [Industriel - R&D]

Senior Cyber Security Expert / Golang Guru

Toulouse - France

June 2017 -

- › Plateforme d'identification et contrôle d'accès distribuée. (AWS, Go / Rust)
- › Etude d'intégration d'une blockchain privée (Ethereum)
- › Audits et Exigences infrastructure sécurité pour projets "Cloud". (AWS)
- › Mesures de sécurité pour "Privacy by Design" de projets "Cloud" internationaux. (RGPD, ISO270xx)
- › Audits de code sécurité. (Java / J2EE / NodeJS / Python / Go / Crypto)

Sogeti ESEC [Sécurité - SSII]

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

Toulouse - France

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]

Ingénieur R&D / Scrum Master

Toulouse - France

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

Toulouse - France

July 2008 - December 2009

- › 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

- › Conception et réalisation d'un outil d'analyse de risques basé sur la méthodologie EBIOS (Ruby, RoR)
- › Administration système et réseau dans un environnement hétérogène
- › Penetration Testing sur applications Web J2EE.

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

Toulouse - France

Stagiaire - Développeur

March 2007 - September 2007

- › Réalisation d'une API d'exploitation de format d'échange de sous-titre DFXP. (Qt, C++)
- › Traitement du signal pour récupération de signaux télétexte. (Qt, C++)

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

Toulouse - France

Stagiaire - Développeur

March 2006 - September 2006

- › Conception et réalisation d'un composant graphique pour afficher des informations géolocalisées. (Java, Eclipse, RCP)
- › Etat de l'art des systèmes d'informations géolocalisées libre (PostGIS, GRASS)
- › Architecture réseau, mise en place d'un domaine libre (OpenLDAP, Samba, Kerberos, DHCP, DNS, NTP)
- › Virtualisation Serveurs (Gentoo, Xen, VMWare)

Karobas [Jeux Vidéo - Editeur / R&D]

Sophia Antipolis - France

Stagiaire - Administrateur Système et Réseau

March 2005 - August 2005

- › Conception / Restructuration du réseau de l'entreprise.
- › Haute disponibilité et Sécurité.
- › Mise en place d'un domaine Exchange 2003.
- › Migration technologique de base de données, et prise en charges des impacts logiciels.
- › Modélisation mondes ludo-éducatifs (Virttools).

Nice-antiques.com [Art - Antiquaire]

Nice - France

Stagiaire - WebMaster

March 2004 - July 2004

- › Conception et réalisation d'un site web dynamique. (PHP / MySQL)
- › Optimisation du référencement commercial.

Formation

IUP ISI

Toulouse - France

M2 ISI - Métamodélisation et Temps réel critique

2008

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

M1 Ingénierie des Systèmes Informatiques (ISI)

2007

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

L3 Ingénierie des Systèmes Informatiques

2006

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

IUT Informatique

Nice - France

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

2005

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

DUT Informatique, Génie Logiciel

2004

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

Lycée Albert Camus

Fréjus - France

Bac S, Science de l'Ingénieur, spécialité Mathématiques

2002

- › 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 ⁵; Veille technologique ⁵; Gestion de projet / Scrum Master ⁴; Conduite de réunion ⁴; Pédagogie / Vulgarisation ⁴; Rédaction publications scientifiques ³; Présentation en public ³;

Sécurité

Programmation défensive ⁵; Contre-mesures sécurité ⁵; OWASP Top 10 ⁵; SANS Top 25 ⁵; Audit de code ⁴; Cryptographie / Chiffrement ⁴; Durcissement Logiciel / Conteneur ⁴; Cuckoo Sandbox ⁴; Analyse de risque (EBIOS) ³; RGD ³; Suricata ³; Bro IDS ³; Honeypots (Cowerie / Kippo) ³; DNS / SMTP Sinkhole ³; QRadar SIEM ³; Splunk ³; FileBeat / PacketBeat ³; Reverse Engineering ²; Penetration Testing ²;

Langages

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

Base de données

MongoDB ⁵; RethinkDB ⁵; Redis ⁵; Neo4j ⁴; Elasticsearch ⁴; MySQL / MariaDB ⁴; PostgreSQL ⁴; Hadoop / HBase ³; Oracle ³; SQL Server ³; DB2 ³; DGraph / GraphQL ²;

Système d'exploitation

Linux / Archlinux ⁵; MacOS X ⁴; Windows ³;

Affinités FullStack

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

Backend Framework

Microservices Patterns ⁵; Resilience Patterns ⁵; gRPC / Protobuf ⁵; NodeJS ⁴; Express ⁴; MeteorJS ³; Ruby on Rails ³; Laravel ²;

Cloud

RabbitMQ ⁵; NSQ ⁵; ZMQ ⁵; WebSocket ⁵; MQTT ⁴; Apache Kafka ⁴; Amazon IAM / Cognito ⁴; Amazon EC2 ⁴; Amazon SNS ³; Amazon IoT ³; Amazon API Gateway / Lambda ³; CoAP DTLS ³;

DevOps

Docker ⁵; Rancher ⁵; Prometheus ⁵; Consul ⁵; Vault ⁵; Grafana ⁴; GitlabCI ⁴; Sentry ⁴; Kubernetes ³; Jenkins ³; Amazon ECS / ECR ³; Ansible ²; Istio / Envoy ²; Linkerd ²; Terraform ²;

Frontend / UX

AngularJS 1.x ⁵; ES 6/7 ⁴; TypeScript ⁴; AngularJS 2.x ⁴; VueJS ⁴; WebPack ⁴; Bootstrap ⁴; HTML5 ³; CSS3 / SASS / LESS ³; Web Design ³; ReactJS ²;

Ingénierie des données

Modélisation Sémantique ⁵; Préparation des données ⁵; Data Wrangling ⁵; Data Scraping ⁵; Protégé ⁴; Anonymisation ⁴; Elasticsearch / LogStash / Kibana ⁴; Traitement du signal ³; Detection d'anomalies ³; Statistiques ³; Python / Jupyter / Pandas ³; SciKit Learn ³; Machine learning (SVM, PNN, RF, GBM) ³; H2o ³; R ²; DataViz ²; D3 ²;

Blockchain

Ethereum ⁴; J.P. Morgan Quorum ³; IBM Hyperledger ³; Solidity ²; Truffle ²; ERC20 Token ²;

Java

Spring (Core, MVC, Security, Data) ⁵; Spring Boot ⁴; J2EE ⁴; Apache Storm ⁴; Apache Spark ³; Apache Kafka ³; Zookeeper ³; Vert.x ³;

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

- › Batterie depuis Septembre 2013
- › Saxophone depuis l'âge de 11 ans dont 6 ans en conservatoire
- › Amélioration continue grâce à la veille technologique, l'expérimentation et les projets personnels (Sécurité, Logiciels, Techniques de management)
- › Rédacteur (Blog)
- › Explorateur technologique