

Lucas SOUMILLE

Né le 26/05/1994 (24 ans)
Permis B, véhiculé
<https://lsoumille.github.io/>

50 Avenue des Siffleuses
13090 Aix-en-Provence
06 82 45 18 12
lucassoumille@protonmail.com

INGÉNIEUR EN CYBERSÉCURITÉ

EXPÉRIENCES

Ingénieur en Cybersécurité, Thales Services ; Aix-en-Provence 2017-présent

Architecture open source de supervision de sécurité et de réponse aux incidents, Intégration de l'outil de chiffrement Thales, Gestion de vulnérabilités, Gestion d'identité et d'accès, Sécurité des environnements Microsoft.

Développeur iOS, Frontware International ; Bangkok 2016 (Stage)

Implémentation de la version iOS de l'application « Nearby ».

Développeur ASP.NET, SPIR Communication ; Aix-en-Provence 2014 (Stage)

Réalisation de deux applications web en ASP.NET destinées au DSI du groupe SPIR

FORMATION

Ingénieur en Sciences Informatiques (spécialité Cryptographie, Sécurité et Vie Privée dans les Applications et les Réseaux) — Polytech Nice Sophia — 2017

DUT Informatique — Université Aix Marseille site d'Aix-en-Provence — 2014

Baccalauréat S SVT — Lycée Ismaël Dauphin — 2012

COMPÉTENCES

Sécurité	SIEM (ELK, Splunk, Sigma), DFIR (TheHive, Cortex), IAM (Thycotic Secret Server, LAPS), Chiffrement (Vormetric), Audit (Nessus, OpenVAS, Nmap, Metasploit), Durcissement (Ubuntu 16, Windows Server), IDS (Snort, Suricata)
Langages de programmation	Java (OCA Java 8), PowerShell, Python, C, C++, Swift
Réseau	TCP/IP, TLS/SSL, SSH, Pare-feux (Iptables/CiscoASA), VPN (OpenVPN, Amazon Gateway), Repartition de charge (Radware Alteon)
Système d'exploitation	Linux (Ubuntu, Kali), Windows (Sysmon)
Logiciels	Ansible, Docker, Vagrant, Git, Jenkins, Office
Linguistique	Anglais - Conversationnel (TOEIC 935)

CENTRES D'INTÉRÊTS

Sports — Football, Basket, Cyclisme, VTT, Pétanque, Running

Hacking — Challenges (Root-me, SecGen), Livres

Culture — Intérêt pour les séries TV, les jeux vidéo et l'actualité sportive
Veille technologique (Mac4Ever, The Hacker New, Les Numériques, JDG)

PROJETS

Python, ELK - <i>Parseur Sigma pour Elastalert</i> Individuel - 1 mois - 2018	Extension de l'outil Sigma pour la génération de règles au format Elastalert à partir d'une règle générique.
Python, ELK - <i>Analyseur pour Elasticsearch</i> Individuel - 1 mois - 2018	Implémentation d'un analyseur Cortex pour réaliser des requêtes sur un cluster Elasticsearch depuis TheHive.
IDS, ELK - <i>IDS Portable</i> Individuel - 1 mois - 2017	Installation de BRO IDS sur une Raspberry PI avec indexation des alertes dans une pile Elasticsearch.
Java, ANTLR - <i>Preuve automatiques d'algorithmes cryptographiques</i> Quatre personnes - 2 mois - 2017	Implémentation d'un langage de programmation en utilisant ANTLR dans le but de prouver la résistance des algorithmes cryptographiques. Le programme permet de calculer toutes les exécutions possibles d'un algorithme cryptographique avec des paramètres fixés.
Java, Maven - <i>Algorithmes d'ordonnancement de VMs</i> Trois personnes - 1 mois - 2017	En s'appuyant sur le simulator CloudSim, l'objectif était d'implémenter différents algorithmes de placement de machine virtuelles dans un data center afin d'optimiser au maximum les revenus.
Python - <i>Analyse de réseaux sans fil grâce à une radio logicielle</i> Quatre personnes - 4 mois - 2016	Reverse engineering du protocole ZWave (domotique), ZAP (prises télécommandées) et Bluetooth LE (Montre OnMove 200/ Bracelet Mi Band). Extension d'un logiciel de conversion de signal afin de faciliter le reverse engineering en utilisant le HackRF One.
Android, PHP - <i>Conception d'un réseau social autour de la mode</i> Quatre personnes - 1 mois - 2016	Réalisation d'une application mobile permettant aux utilisateurs de partager leur garde-robe ou de demander l'avis de la communauté pour un prochain achat. L'architecture de l'application a été conçue afin de permettre le passage à l'échelle.
Hadoop, Spark, Scala - <i>Filtre anti-spam</i> Deux personnes - 1 mois - 2016	Conception d'une application déployable sur un cluster Hadoop, permettant de déterminer si les emails reçus sont légitimes. L'algorithme respecte le design pattern MapReduce.
Swift - <i>Application « Nearby »</i> Individuel - 2 mois - 2016	Implémentation de la version iOS de l'application « Nearby » permettant à l'utilisateur d'obtenir des informations sur les services à proximité. La géolocalisation se base sur l'utilisation de Beacons.
Java, Bash, Python - <i>Framework de tests par mutation</i> Trois personnes - 2 mois - 2016	Conception et implémentation d'une chaîne de build qui prend en entrée un projet Java et produit un rapport sur la qualité du banc de test. Le framework contient une documentation complète sur son fonctionnement.
HTML, JavaScript, PHP - <i>Classement des courses hippiques</i> Individuel - 1 mois - 2015	Développement d'une application web qui détermine le résultat final automatiquement par catégorie en fonction de l'arrivée de chaque course. Les résultats peuvent être exportés au format pdf.