Lucas SOUMILLE

Né le 26/05/1994 (26 ans)
06 82 45 18 12
lucassoumille@protonmail.com

24 Avenue de la Cascade
13100 Aix-en-Provence
Permis B, véhiculé

INGÉNIEUR CYBERSÉCURITÉ

EXPÉRIENCES PROFESSIONNELLES

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

- 2020 - Présent STMicroelectronics Analyste SOC Niveau 3
- 2017 - 2020 ITER Organization Assistance RSSI
- 2020 SmartPush Audit OWASP
- 2019 VSB Energies Nouvelles Analyse forensic
- 2017 Louis Dreyfus Company Déploiement d'une enclave de collecte
- 2017 Planet Of Finance Intégration de l'outil de chiffrement Vormetric
- 2017 CMA CGM Intégration d'un collecteur d'événements

2016 (Stage) **Développeur iOS, Frontware International ; Bangkok**

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

FORMATION

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

2014 **DUT Informatique** ; Université Aix Marseille ; Aix-en-Provence

2012 **Baccalauréat S SVT ;** Lycée Ismaël Dauphin ; Cavaillon

COMPÉTENCES

Sécurité	SIEM (ELK, QRadar, Splunk), Investigations numériques (TheHive, Cortex, MISP), Chiffrement (Vormetric), Audit (Nessus, BloodHound, Nmap, Metasploit, OWASP Zap), Sécurité des environnements Microsoft (Active Directory, Sysmon, ATA, Defender ATP), IDS (Suricata), Bac à sable (Cuckoo)
Langages de programmation	Java, PowerShell, Python, C, C++, Swift
Réseau	Pare-feux (Palo Alto, IPFire), Repartition de charge (Radware Alteon), Pare-feux applicatif (Radware AppWall), Netflow, VPN (OpenVPN)
Système d'exploitation	Windows, Linux (Ubuntu, Kali)
Logiciels	Ansible, Docker, Vagrant, Git, Jenkins, Office
Linguistique	Anglais - Conversationnel (TOEIC 935)

CERTIFICATIONS

2018 **Radware AppWall Level 1**

2018 **Radware Alteon Specialist**

2017 **Oracle Certified Associate Java 8**

PROJETS PERSONNELS

Python, ELK - *Parseurs Sigma pour Elastalert et Defender ATP* Individuel - 2020	Extension de l'outil Sigma pour la génération de règles de détection d'intrusion au format Elastalert et Defender ATP à partir d'une règle générique et échangeable.
Python, ELK - *Analyseur pour Elasticsearch et Active Directory* Individuel - 2019	Implémentation d'un analyseur Cortex pour réaliser des requêtes sur un cluster Elasticsearch depuis TheHive dans le but de faciliter les investigations.
IDS, ELK - *IDS Portable* Individuel - 2017	Installation de Suricata sur une Raspberry PI avec indexation des alertes dans une pile Elasticsearch.
Java, ANTLR - *Preuve automatique d'algorithmes de chiffrement* Quatre personnes - 2017	Implémentation d'un langage de programmation en utilisant la librairie ANTLR dans le but de prouver la résistance des algorithmes de chiffrement. Le programme permet de calculer toutes les exécutions possibles d'un algorithme de chiffrement avec des paramètres fixés.
HTML, JavaScript, PHP - *Classement des courses hippiques* Individuel - 2015	Développement d'une application web pour la société hippique de Cavaillon. Cette dernière détermine le résultat final automatiquement par catégorie en fonction de l'arrivée de chaque course. Les résultats peuvent être exportés au format pdf.

L'ensemble de mes projets est disponible à l'adresse suivante https://lsoumille.github.io/

CENTRES D'INTÉRÊTS

Brassage amateur

Sports Football, Ski, Cyclisme, VTT, Pétanque, EDPM

Hacking Actualités, Challenges (Root-me), Livres

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