Julien Larzul

Cybersecurity Intern — Security Engineer Intern — SOC Analyst Intern
Available for a 6-month internship starting July 2026

Habère-Poche, France | +33 (0)6 99 19 03 32 | julienlrzl@gmail.com | linkedin.com/in/julien-larzul | github.com/julienlrzl
larzuljulien.com | tryhackme/julienlrzl

Education

Université du Québec à Chicoutimi (UQAC) **Expected Graduation: 2026**
Master's in Cybersecurity *Chicoutimi, QC, Canada*

Polytech Lyon **2021 – Expected Graduation: 2026**
Diplôme d'ingénieur en informatique (Computer Engineering) *Lyon, France*

- Double degree program: Engineering and Master's studies in Cybersecurity
- Relevant coursework: Cybersecurity, Data Analysis, Computer Networks, Software Engineering, Algorithms, ML

Work Experience

Lizeo Group **Sep 2024 – Jan 2025**
R&D Intern – Machine Learning *Lyon, France*

- Optimized **Large Language Models (LLMs)** for **opinion mining**, testing prompt engineering strategies and automating CSV pipelines for large-scale sentiment analysis, reducing manual processing time.
- Benchmarked and integrated alternative models via **AWS Bedrock (Claude 3.5 Sonnet)** to reduce monthly costs of GPT-4 usage, learning **YAML** configuration and API deployment.
- Developed an image compliance verification pipeline for **Rolex**, leveraging **ResNet50 embeddings** and **cosine similarity** to automate retailer homepage conformity checks.
- Evaluated multiple feature extraction methods (SIFT, ORB, SURF) and selected SURF for layout validation through **gravity center distance matrices**.

Projects

Mobile Forensics (UQAC) | *2025* **Autopsy**

- Performed forensic acquisition and analysis of **200+ artefacts** (SMS, GPS metadata, images, call logs) from Android disk images.
- Designed a formal **chain-of-custody workflow** ensuring forensic integrity.

Log Management & Anomaly Detection (UQAC) | *2025* **ELK | Kibana | syslog-ng | Suricata**

- Deployed a full **SIEM pipeline** ingesting thousands of logs in real time.
- Configured Suricata to detect **5 intrusion scenarios** (scan, DoS, exploit attempt, etc.).
- Deployed automated alerting (email/SMS) for confirmed threats.

Web Application Security Assessment (UQAC) | *2025* **OWASP Top 10 | ZAP | DVWA**

- Identified, exploited, and documented **20 vulnerabilities** across 3 vulnerable applications (bWAPP, DVWA, WebGoat).
- Implemented remediation steps and produced a structured report including reproduction steps, exploit paths, and mitigation strategies.

Technical Skills

Security: OWASP ZAP, Suricata (IDS/IPS), ELK, syslog-ng, Autopsy, Burp Suite
Technical: Python, Java, SQL, AWS, Git, Docker, YAML
Networking & Systems: Network fundamentals (TCP/IP, routing, DNS, HTTP), Linux, Windows
Languages: French (native), English (B2 – TOEIC 885/990)