



Simon "Plup" Rouault

Freelance cybersecurity engineer

plup@plup.io · plup.io · gitlab.com/plup
@plup@mastodon.social

BIO

Freelance cybersecurity engineer since 2015. My work includes long-term, full-time client missions and shorter projects.

Assessing threats, investigating security incidents, and designing effective response plans are the parts of my work I enjoy most.

I'm known to be an automation addict and a tireless traveler.

SKILLS

Application Security

Threat modeling
SAST/DAST/SCA integration
Secure CI/CD pipelines

Detection & Response

Detection engineering
Incident response
Threat hunting
Threat intelligence
Forensics

Security Architecture & Risk

IAM architecture
Risk assessment

Cloud & Automation

Cloud security
Container security
Infrastructure as Code
Security automation

Offensive Security

Redteam
Network analysis
Vulnerability research

EDUCATION

Engineering degree, École des Mines d'Albi-Carmaux, 2009

LANGUAGES

French (Native)
English (Full proficiency)
Spanish (Full proficiency)

INTERESTS

Traveling Climbing Sailing Hiking
Crafting

RECENT EXPERIENCE

Cybersecurity Engineer

Undisclosed, July 2022 - Present · Full-time freelance mission

Developed application security and threat detection capabilities across company applications and infrastructure.

- Developed threat models for all internal and third-party applications
- Integrated SAST, DAST, and SCA into GitLab CI pipelines, alongside AI-assisted merge request analysis
- Built AWS and Kubernetes pipelines to centralize company-wide infrastructure and application audit logs in Splunk
- Designed runtime detections for Kubernetes workloads using Falco/Sysdig

Kubernetes AWS Falco/Sysdig Terraform Splunk TheHive GitLab CI

Chief Information Security Officer

Startin'blox, Jan. 2018 - Nov. 2021 · Part-time freelance engagement

Oversaw product and production security, including decentralized IAM design, component validation, and infrastructure automation.

- Built component validation pipelines using GitLab CI
- Automated production provisioning with Ansible and built monitoring using the Prometheus stack
- Designed decentralized identity and access management for web components using WebID, OIDC, and WAC

GitLab CI OIDC Cryptography Web components Ansible Prometheus
Python

SOC Specialist

BNP Paribas, Feb. 2018 - Sept. 2020 · Full-time freelance mission

Managed SOC detection use cases and handled level-three incident response.

- Built an in-house detection orchestrator that queried logs in Elasticsearch and sent alerts to TheHive
- Deployed the SOC, including the in-house detection orchestrator, in Singapore and New York
- Established incident response plans, with a focus on insider threats
- Investigated security incidents and determined their scope through log, endpoint, network, and cloud analysis; executed containment and remediation
- Participated in red team exercises and threat hunting

Forensics Threat hunting SIEM SOAR ELK TheHive Python
Ansible

PREVIOUS EXPERIENCE

Selected DevSecOps and security projects

Multiple clients, Various dates since Sept. 2015 · Shorter freelance engagements

Delivered shorter DevSecOps engagements between long-term missions, with some projects running in parallel.

- Designed continuous deployment pipelines
- Set up log collection and monitoring architectures
- Pentested external and internal infrastructures
- Responded to cybersecurity incidents

Metasploit Forensics ELK Ansible Docker Kubernetes GitLab CI Python

Cybersecurity R&D expert

French Ministry of Defense, Nov. 2012 - Sept. 2015 · Full-time

Designed secure, covert communication devices.

- Developed security products using embedded Linux
- Implemented custom cryptography in C
- Developed and maintained a Public Key Infrastructure

Cryptography Embedded Linux Double VPN PKI Android C/C++ Java Python Smartcard

Lecturer on Information Security Management System

Ecole des Mines d'Albi-Carmaux, 2011 - 2015 (5 hours / year)

Taught risk analysis and security management processes to engineers.

- Developed and delivered lectures on risk analysis and information security management

ISSP ISO 27005 Teaching

Head of Operational Security

French Ministry of Finance, Oct. 2009 - Oct. 2012 · Full-time

Protected sensitive economic intelligence information.

- Led a team of 5 SecOps specialists
- Secured interconnections between departmental networks
- Handled a nationwide cybersecurity incident response
- Designed and tested the disaster recovery plan
- Managed DNS servers, firewalls and proxies

Management Risk assessment Disaster Recovery Splunk Firewall VPN DLP BYOD

Deputy Information Security Officer

French Ministry of Defense, Feb. 2009 - Sept. 2009 · Full-time

Assessed the interconnection network and scientific computing simulation platform for security accreditation.

- Conducted risk assessments using EBIOS
- Wrote an approval application for each subsystem
- Audited the critical elements

Risk assessment Compliance Technical writing