SAJJIT SOTI

Cybersecurity Intern | GRC • Penetration Testing • Threat Detection | MSc Cybersecurity — EPITA Paris

sajjit.soti@epita.fr • +33 7 66 43 38 22 • Île-de-France (Open to Relocate) • www.linkedin.com/in/sajjit-soti/

PROFESSIONAL SUMMARY

Final-year MSc Cybersecurity student at EPITA Paris seeking a 6-month end-of-study internship in Cybersecurity. Broad hands-on expertise spanning offensive security (penetration testing, OSINT, vulnerability assessment), defensive operations (SIEM engineering, incident response, threat intelligence correlation), governance & compliance (NIST CSF 2.0, ISO 27001, risk management), and cloud security architecture (AWS WAF, IAM, Terraform). Experienced in delivering security-awareness training and communicating risk posture to non-technical stakeholders. **Language: English (bilingual), French (B1).**

TECHNICAL SKILLS

Offensive Security: Penetration testing (Metasploit), OSINT, Maltego, vulnerability assessment, network reconnaissance, web application security, exploit development awareness
Defensive Security & SOC: SIEM — ELK Stack, Wazuh, Kafka; threat intelligence correlation, anomaly detection, incident response, alert triage, IOC analysis, KPI reporting
GRC & Compliance: Risk assessment, NIST CSF 2.0, ISO 27001 awareness, security governance, compliance documentation, security policy design, awareness training delivery
Cloud Security: AWS (WAF, IAM, Cognito, S3, EC2), Terraform, cloud security architecture, DRP/PRA, disaster recovery, infrastructure hardening
IAM & Access Security: Okta, LDAP, OAuth, RBAC, lifecycle policies, least-privilege enforcement, MFA, SSO, Zero Trust
SRE & Observability: Metrics, logs, tracing, alerting; Grafana awareness, SLO/SLI/SLA, MTTR reduction, runbook design, monitoring dashboards
Languages & Tools: Python (security tooling, automation), Bash, SQL, Linux/Unix (CentOS, RedHat), Docker, Kubernetes, Git

EXPERIENCE

Project Manager | Eydean Inc, Nepal *Sept 2023 – Aug 2024*
- Designed and maintained Python-based deployment automation scripts and CI/CD pipelines for cloud infrastructure, eliminating manual steps and ensuring continuous, scalable delivery of production resources.
- Tracked operational KPIs via ERP dashboards to surface performance bottlenecks and drive continuous process improvements across platform operations.

IT Consultant | Kathmandu Metropolitan City, Nepal *Nov 2022 – Aug 2023*
- Designed and optimized on-premise IT infrastructure; documented system architectures focused on resilience and performance, enabling knowledge transfer and long-term maintainability.
- Delivered incident response and security-awareness training to 50+ users, covering threat detection, data protection policies, network protocols, and escalation procedures.

Web Development Intern | Muse Zade, Nepal *Aug 2021 – Oct 2022*
- Built and deployed scalable production web applications using Next.js; maintained Git-based version control and CI/CD pipelines, ensuring reliable, automated deployments with minimal downtime.
- Coordinated rigorous testing cycles in Jira, tracked issues systematically, and remediated technical debt before each release to maintain code quality and reduce production incidents.

KEY PROJECTS

Real-Time SIEM Pipeline | *Python, Kafka, ELK Stack, Docker*
- Engineered an event-driven pipeline to stream, enrich, and correlate network logs with live threat intelligence; built proactive alerting rules and observability dashboards covering the full kill chain.

Self-Healing Cloud SOC | *AWS, Terraform, Python*
- Built a 24/7 automated cloud auditor detecting and auto-remediating AWS infrastructure risks in real time — including instant deletion of exposed firewall rules and over-privileged IAM policies.

QR-SafeScan — Anti-Phishing Engine | *Python, API aggregation — Team of 4*
- Cross-platform detection engine achieving 96% accuracy using 27 local heuristics; emphasis on zero data retention, performance, and resilience against evasion techniques.

SOC & Observability Platform | *Wazuh SIEM, ELK Stack*
- Deployed a full observability stack (metrics, logs, tracing, alerting) on a simulated enterprise network with automated incident response workflows and threat hunting playbooks.

Telemedicine Cloud Security Architecture | *AWS, WAF, Cognito, EC2*
- Designed a HIPAA-aligned secure cloud architecture with network isolation, WAF rule sets, automated backups, and strict IAM access controls for sensitive healthcare data.

Identity & Access Management | *Okta, LDAP*
- Centralized authentication with lifecycle policies and least-privilege access controls across a simulated enterprise, including security event logging and anomaly detection integration.

EDUCATION

MSc Computer Science — Cybersecurity | EPITA, Paris *Graduation: 2026*
Core areas: cybersecurity governance, SOC operations, cloud security, penetration testing, SRE, IAM, DevOps.