SAJJIT SOTI

Ingenieur Cybersecurite | SOC & Detection · Tests d'Intrusion · Securite Cloud

sajjit.soti@epita.fr | +33 7 66 43 38 22 | Ile-de-France (mobilite totale) | sajjitsoti.com.np | linkedin.com/in/sajjit-soti

Recherche un stage de fin d'etudes de 6 mois a partir de septembre 2026 · Convention de stage EPITA disponible

PROFIL

Etudiant en derniere annee de Master Cybersecurite a l'EPITA Paris, a l'aise sur les volets offensif et defensif. J'ai mene un test d'intrusion en boite grise enchainant 14 vulnerabilites jusqu'a l'execution de code a distance et la compromission complete de la base de donnees. J'ai construit un SOC sur Wazuh et la stack ELK, redige moi-meme ses regles de detection, puis lance quatre attaques Red Team pour verifier qu'elles se declenchaient. J'ai egalement durci une plateforme SaaS en production jusqu'a une notation A+ sur les en-tetes de securite. Projets documentes sur sajjitsoti.com.np.

COMPETENCES TECHNIQUES

Securite Operationnelle & Detection: SIEM (Security Information and Event Management) : Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana), Apache Kafka ; ingenierie de detection et redaction de regles, collecte, enrichissement et correlation de logs, threat intelligence, triage d'alertes, reponse a incident, tableaux de bord d'observabilite

Securite Offensive: Tests d'intrusion, evaluation et enchainement de vulnerabilites, injection SQL, RCE (execution de code a distance), upload de fichiers non restreint, failles de session et de cookies, Burp Suite, Metasploit, Nmap, Wireshark, OSINT et Maltego, rapports de remediation

Securite Cloud & Infrastructure: AWS (EC2, S3, IAM, WAF, Cognito), Terraform, IaC (Infrastructure as Code), audit et remediation automatises de configuration, Docker, pipelines CI/CD, administration Linux et Windows, TCP/IP, DNS, VPN, pare-feu, durcissement systeme

Gouvernance, Risques & Conformite (GRC): Mapping des controles ISO/IEC 27001, NIST CSF 2.0, analyse de risques IT, gouvernance et politiques de securite, IAM (Identity and Access Management) : Okta, LDAP, MFA, moindre privilege, Row-Level Security PostgreSQL, en-tetes de securite (CSP, HSTS)

Developpement & Outils: Python, Bash, SQL, JavaScript, React, Next.js, Git et GitHub, PostgreSQL, ligne de commande Linux, documentation technique

EXPERIENCE PROFESSIONNELLE

Developpeur Full-Stack Freelance | Uply - SaaS de gestion des approvisionnements (client francais) *Avr. 2026 - Present*

- Durcissement d'une plateforme SaaS multi-tenant en production jusqu'a une notation A+ sur les en-tetes de securite (CSP, HSTS, X-Frame-Options), et mise en place d'un workflow staging-first pour livrer les evolutions du client en toute securite
- Conception d'un schema PostgreSQL avec Row-Level Security pour une isolation stricte des tenants, et developpement du frontend React/Vite ainsi que des interfaces admin et client par role, de bout en bout, pour un client payant

Chef de projet | Eydean Inc, Nepal *Sept. 2023 - Aout 2024*

- Conception et maintenance de scripts d'automatisation de deploiement en Python et de pipelines CI/CD pour l'infrastructure cloud, supprimant les etapes manuelles et assurant une livraison continue et reproductible

Consultant IT | Mairie de Katmandou, Nepal *Nov. 2022 - Aout 2023*

- Delivrance de formations en reponse a incident et en sensibilisation securite aupres de plus de 50 utilisateurs, couvrant la detection des menaces, les politiques de protection des donnees, les protocoles reseau et les procedures d'escalade

PROJETS CLES

Test d'intrusion applicatif web | *Burp Suite, injection SQL, RCE ; equipe de 4:* Mission en boite grise enchainant 14 vulnerabilites, des cookies non signes et l'upload de fichiers non restreint jusqu'a l'injection SQL, aboutissant a l'execution de code a distance et a la compromission complete de la base de donnees, avec rapport de remediation ecrit.

Plateforme SOC & Observabilite | *Wazuh SIEM, ELK Stack:* Deploiement d'un SOC cloud et execution de quatre attaques Red Team reelles, dont une regle personnalisee detectant l'enumeration de noms d'utilisateur SSH des la premiere tentative ; metriques, logs, tracing, alerting et playbooks de reponse automatises.

Auditeur cloud auto-reparateur | *AWS, Terraform, Python:* Auditeur automatise 24/7 detectant et corrigeant en temps reel les risques d'infrastructure AWS, incluant la suppression instantanee des regles de pare-feu exposees et des politiques IAM sur-privilegiees.

FORMATION

Master of Science - Informatique, specialite Cybersecurite | EPITA, Paris *Obtention : 2026*

Licence en Informatique - BSc (Hons) Computing | Islington College, Nepal *2021*

Domaines cles : gouvernance cybersecurite, operations SOC, securite cloud, tests d'intrusion, SRE, IAM, DevOps.

LANGUES

Anglais (courant) · Francais (B1, en progression) · Nepalais (langue maternelle) · Hindi (conversationnel)