SAMI HAMEG

Ingénierie réseaux & Sécurité des infrastructures

Architecture réseau, segmentation et filtrage · Automatisation et ingénierie IA agentique

Île-de-France · 07 67 17 33 59 · shameg.pro@gmail.com

LinkedIn · GitHub · Portfolio

Alternance dès septembre 2027 · Cycle ingénieur

PROFIL

Futur ingénieur réseaux et sécurité des infrastructures, étudiant en BUT Réseaux & Télécommunications, je vise un cycle ingénieur en alternance dès septembre 2027. Expertise complémentaire : automatisation et systèmes agentiques (Claude Code, Codex).

EXPÉRIENCES

Administrateur Systèmes, Réseaux & Sécurité Junior · Mairie de Noisy-le-Grand 2 mois (11/2026 – 12/2026)

À la DSIN/SRN, en autonomie sur les objectifs fixés par le RSSI, mon tuteur de stage, et son adjoint.

Réalisations

Cartographie réseau : logs du pare-feu Stormshield, scans Nmap automatisés, tableau de bord des services exposés.

Administration systèmes : VM Linux sous Proxmox (provisionnement, mises à jour, sauvegarde), vulnérabilités (Cyberwatch).

Centralisation des journaux (projet Syslog) : collecte des événements du système d'information avec Rsyslog.

Missions en cours, nouvellement confiées

Audit des infrastructures réseau : analyse des flux internes ; étude d'une matrice des flux (objectif potentiel).

Découverte réseau et inventaire des équipements : identification et classification par VLAN (postes, imprimantes, serveurs), notamment avec Cyberwatch.

Microsegmentation réseau et filtrage NGFW Stormshield : analyse des dépendances réseau du serveur de l'autre stagiaire ; définition et mise en œuvre des politiques de filtrage (sources, destinations, protocoles, ports).

PROJETS IA AGENTIQUE

Speculynx · Sécurité des API pour agents IA (fondateur, développeur) · speculynx.dev 06/2026 – en cours

CLI Python publiée sur PyPI : analyse OpenAPI 3.0/3.1, cartographie des actions ouvertes à un agent IA (écriture, suppression, paiement), 14 contrôles de sécurité (BOLA, BFLA, SSRF, secrets, auth, rate limit).

Contrôle automatisé des contrats API en CI/CD ; le LLM ne peut pas assouplir la règle d'une action destructive.

Politiques réseau exportées en nftables et validées en CI ; SaaS FastAPI, PostgreSQL, Stripe ; plus de 1 000 tests automatisés.

Dotation · Agentic AI Engineering & Business Automation (fondateur, concepteur) · dotation.app 10/2026 – en cours

Agent pour artisans du bâtiment (21 outils, JSON Schema) : e-mails, avant-devis, relances ; orchestration, routines, validation.

Banc d'évaluation : 4 LLM × 414 appels, 12 critères (JSON, hallucination, injection, coût, latence) ; modèle retenu 12/12, 0 injection suivie sur 33.

Passerelle LiteLLM (bascule, budget par client) ; un serveur isolé par client, filtrage des sorties DNS/SNI, pseudonymisation, nftables, WireGuard.

Go, TypeScript, PostgreSQL, Flutter, API OVH ; environ 3 000 tests automatisés.

PROJETS RÉSEAUX & INFRASTRUCTURE

Réseau haute disponibilité : architecture LAN/WAN Cisco, routage et commutation, MPLS/LDP, HSRP, QoS ; panne absorbée sans coupure.

Segmentation réseau et filtrage : VLAN, ACL, supervision Zabbix.

Windows Server & Active Directory : unités d'organisation, comptes, groupes et stratégies GPO, documentés.

COMPÉTENCES

Architecture & ingénierie réseau : architecture LAN/WAN, routage et commutation, TCP/IP, IPv4/IPv6, VLAN, MPLS/LDP, haute disponibilité et redondance (HSRP), QoS, Cisco

Audit des infrastructures réseau : analyse du trafic réseau, cartographie des flux réseau, découverte réseau, inventaire des équipements, supervision Zabbix, Nmap, Cyberwatch

Sécurité réseau : ingénierie de sécurité réseau, segmentation et microsegmentation réseau, gestion des politiques de filtrage NGFW, Stormshield, nftables, ACL

Systèmes & automatisation : Linux, Windows Server, Active Directory, Proxmox, Docker, Python, Bash, Git, CI/CD

IA agentique & AI-native : tool calling, structured outputs, context engineering, orchestration d'agents, intégration d'outils et d'API, évaluation et routage de LLM (LiteLLM), MCP, Claude Code, Codex

Développement : Python (FastAPI), Go, TypeScript, PostgreSQL · Anglais : pratique courante

FORMATION

BUT Réseaux & Télécommunications, parcours Cybersécurité (2e année) · Sorbonne Paris Nord Depuis 2024