

SIMON THÉMIOT

Architecte Infrastructure et Cybersécurité

07 78 82 16 24 | simon.themiot@stockageprive.net | Quincieux, France
Site web: <https://www.stprive.net> | LinkedIn: <https://www.linkedin.com/in/simon-th%C3%A9miot-3733911ba/>

PROFIL / PROFESSIONAL SUMMARY

Architecte Infrastructure et Cybersécurité avec 10+ ans d'expérience dans la conception, la sécurisation et l'exploitation d'environnements Linux, cloud privé et services exposés sur Internet. Profil hybride infrastructure, réseau, sécurité et développement, capable de concevoir, déployer, durcir, superviser et exploiter une architecture en production.

Cibles : Architecte Infrastructure, Architecte Technique Cybersécurité, Expert Infrastructure et Sécurité, Consultant Infrastructure Sécurisée.

IMPACT ET CHIFFRES CLÉS / KEY ACHIEVEMENTS

- 10+ ans d'expérience en système, réseau, infrastructure, développement et cybersécurité.
- PrivCloud Sharing conçu pour des transferts sécurisés jusqu'à 250 Go par opération.
- Infrastructure critique refondue avec objectif de disponibilité 99,9 % et amélioration des temps de réponse jusqu'à 40 %.
- Stack sécurité multi-couche : WAF, IDS/IPS, SIEM/XDR, durcissement Linux, filtrage DNS, supervision et alerting.
- Exploitation d'environnements de production avec contraintes de disponibilité, sécurité, logs, sauvegardes et support.

EXPÉRIENCE PROFESSIONNELLE / PROFESSIONAL EXPERIENCE

Auto-entrepreneur - Architecte Infrastructure et Cybersécurité | 2015 - Présent

- Conception et déploiement d'architectures sécurisées Linux/cloud privé pour environnements PME : VPN, virtualisation, segmentation réseau, services exposés, durcissement OS et réduction de surface d'attaque.
- Pilotage de projets de bout en bout : cadrage, choix techniques, migration, clustering, haute disponibilité, segmentation et sécurisation des flux.
- Audits de configuration, analyse de vulnérabilités, recommandations de durcissement CIS/ANSSI et priorisation des remédiations.
- Automatisation de tâches d'exploitation et de sécurité via Bash, Python, GitLab CI/CD, Ansible, Terraform et scripts système.
- MCO/MCS Linux, réseau, mail, web et sauvegardes avec objectifs de disponibilité, supervision, alerting, patching sécurité et continuité de service.

Apprenti Cybersécurité - Blanc Météore | 2 ans - durant Mastère

- Administration système et réseau en production, supervision et sécurisation des services.
- Durcissement de serveurs Linux, suivi d'incidents, maintenance préventive et corrective d'infrastructures critiques.
- Contribution à des projets d'intégration sécurisée, migration d'infrastructures et amélioration de l'exploitation.

PROJETS MAJEURS / KEY PROJECTS

PrivCloud Sharing - Fondateur et Architecte Technique | 2025 - Présent

- SaaS de partage sécurisé de fichiers sensibles, orienté confidentialité, souveraineté, simplicité d'usage et auditable.
- Architecture Security by Design : chiffrement E2EE côté client, AES-256, logique Zero Knowledge, secrets non exposés serveur et réduction de la surface d'attaque.
- Gestion de transferts volumineux jusqu'à 250 Go avec optimisation performance, reprise, sécurité et expérience utilisateur.
- Workflows de signature électronique : traçabilité, preuves techniques, horodatage TSA/RFC 3161 et vérification documentaire.
- Déploiement et durcissement : Linux, Docker, reverse proxy sécurisé, TLS, WAF, logs, supervision et préparation à l'audit public du code.

Migration Infrastructure Critique et Sécurisation Globale | 2024 - 2025

- Refonte d'un environnement de production multi-VM sous Proxmox, avec contraintes de disponibilité, sécurité, supervision, sauvegardes et conformité RGPD.
- Proxmox VE, isolation réseau, routage dual-stack IPv4/IPv6, segmentation des flux sensibles et défense en profondeur.
- Intégration Zabbix, Wazuh, Suricata, ntopng, MalwareDetect et ClamAV pour améliorer la visibilité opérationnelle et la détection.

Cloud Privé Entreprise et VPN Sécurisé | 2021 - 2022

- Nextcloud, suite collaborative, accès VPN obligatoire, reverse proxy, DNS sécurisé, sauvegardes, Talk, WOPI, Coturn, Janus et NATS.
- Supervision, maintenance, filtrage réseau avancé, gestion des flux temps réel et réduction de l'exposition publique.

DOMAINES D'INTERVENTION / SCOPE

- Audit, durcissement et migration d'infrastructures Linux critiques.
- Architecture cloud privé, SaaS sécurisé, VPN, DNS, mail, reverse proxy et services collaboratifs.
- Mise en place de supervision, alerting, SIEM/XDR, WAF, IDS/IPS et procédures MCO/MCS.
- Accompagnement technique : cadrage, recommandations, documentation, exploitation et amélioration continue.

COMPÉTENCES TECHNIQUES / TECHNICAL SKILLS

Cybersécurité (Cybersecurity) : Zero Trust, Security by Design, Defense in Depth, Linux Hardening, WAF, IDS/IPS, SIEM/XDR, Incident Response, Risk Management, ISO 27001, NIS2, RGPD, hygiène informatique ANSSI.

Architecture sécurité (Security Architecture) : Network Security, Cloud Security, Cloud Architecture, cloud privé/on-premise, architecture hybride, segmentation, micro-segmentation, sécurité applicative et services exposés.

Audit et tests (Security Assessment) : analyse de vulnérabilités, audit de configuration, Pentest applicatif/infrastructure en contexte projet, recommandations de remédiation, priorisation des risques et durcissement CIS/ANSSI.

Infrastructure : Linux, Debian, Ubuntu, Kali, Proxmox VE, KVM, LXC/LXD, Docker, stockage S3 compatible, sauvegardes, PRA/PCA, services web, mail et SaaS sécurisé.

Réseau (Network) : IPv4/IPv6, WireGuard, OpenVPN, routage, NAT, DNSSEC, DNSCrypt-Proxy, DNSDist, DoH/DoT, reverse proxy, load balancing, firewalling.

DevOps et automatisation : Bash, Python, GitLab CI/CD, Ansible, Terraform, Infrastructure as Code (IaC), Zabbix, Wazuh, Suricata, ntopng, dashboards et alerting.

SÉCURITÉ OPÉRATIONNELLE / SECURITY OPERATIONS

- Durcissement de serveurs Linux exposés : SSH, TLS, Nginx, permissions, isolation, logs et services critiques.
- Mise en place de défenses multicouches : reverse proxy sécurisé, WAF, IDS/IPS, SIEM/XDR, filtrage DNS et supervision centralisée.
- Analyse d'incidents, tuning de règles Wazuh/Suricata/NAXSI, réduction du bruit d'alerte et priorisation des actions.
- Sécurisation des flux applicatifs : accès VPN, micro-segmentation, règles firewall, contrôle des endpoints et exposition minimale.
- Maintien en condition de sécurité : patching, sauvegardes, surveillance, alerting et amélioration continue des procédures.

ENVIRONNEMENTS ET OUTILS / TOOLS

- Virtualisation : Proxmox VE, KVM, LXC/LXD, Docker, Docker Compose.
- Services : Nginx, Postfix, Dovecot, Nextcloud, GitLab, MariaDB, PostgreSQL, S3.
- Sécurité : NAXSI, SafeLine, Suricata, Wazuh, ClamAV, MalwareDetect, iptables.
- DNS/VPN : WireGuard, OpenVPN, DNSSEC, DNSCrypt-Proxy, DNSDist, DoH/DoT, IPv4/IPv6.
- Observabilité : Zabbix, ntopng, métriques système, logs, dashboards, alerting et seuils personnalisés.

FORMATIONS / EDUCATION

- **Mastère Expert en systèmes d'information sécurisés - Niveau 7 RNCP** - Obtenu.
- **Mastère Administrateur Système et Réseaux - Niveau 7 RNCP** - Obtenu.
- Prépa Cybersécurité - IPSSI Paris - 2022 - 2023.
- Piscine 42 - États-Unis - C et Python - 2019.
- Certificat Développement Web - OpenClassrooms - HTML/CSS - 2018.
- Formation continue : ANSSI, NIS2, ISO 27001, ISO 27005, RGPD, Linux Hardening, WAF, SIEM, Incident Response, Risk Management et Compliance.

LANGUES / LANGUAGES

- Français : langue maternelle.
- Anglais : niveau professionnel - documentation technique, veille, tickets et échanges techniques internationaux.

POSITIONNEMENT / STRENGTHS

- Profil hands-on : capacité à concevoir une architecture, la déployer, la durcir, l'exploiter et la documenter.
- Culture production : disponibilité, sécurité, supervision, sauvegardes, logs, performance et continuité de service.
- Approche pragmatique : arbitrage entre risque, coût, dette technique, maintenabilité et contraintes métier.
- Autonomie forte sur les environnements Linux, réseau, sécurité applicative, messagerie, cloud privé et outils de supervision.