ILYASS KAOUAM

Ingénieur Senior Cloud, DevOps & Sécurité

Lille, France · Full remote · ilyassikai@gmail.com · linkedin.com/in/ilyass-kaouam · ilyasskaouam.com

PROFIL

Ingénieur infrastructure et sécurité senior, plus de 16 ans d'expérience dans la conception, la sécurisation et l'exploitation de systèmes critiques, de la virtualisation (VMware, Proxmox) aux environnements Cloud Native (GCP, AWS, Kubernetes). Je sécurise aujourd'hui de bout en bout une plateforme Kubernetes de trois clusters : détection runtime, SIEM et SOAR, policy-as-code, accès zero-trust et GitOps. Auparavant, six ans à construire et durcir une plateforme de production, du serveur physique à Proxmox, Ceph et Ansible. Orienté causes racines, attaché à la documentation, contributeur open source mergé sur le projet CNCF Falco.

COMPÉTENCES CLÉS

Détection & politiques	Wazuh (SIEM), Shuffle (SOAR), Falco (eBPF), OPA Gatekeeper, NetworkPolicies, Trivy, runbooks d'incident
Identité & accès	Zitadel (SSO OIDC, 2FA), Netbird/WireGuard, Vault + ArgoCD Vault Plugin, Bytebase, RBAC Kubernetes
Plateforme & GitOps	Kubernetes (OVHcloud, GKE, EKS, RKE2), ArgoCD ApplicationSets, Helm, Terraform, Ansible, cert-manager, GitLab CI
Réseau & périmètre	Traefik, Gateway API, Cloudflare, WAF (ModSecurity, anti-bot), pfSense, iptables/nftables/ipset, Keepalived/VRRP, HAProxy, F5, routage par politique
Observabilité	Prometheus, Alertmanager, Grafana, Loki, Fluent Bit, Elasticsearch/ELK, Zabbix, Nagios
Systèmes & données	Linux (Debian, RHEL), Proxmox & Ceph (expert), vSphere, PostgreSQL, MySQL, MongoDB, Bacula
Langages	Go (contributions open source), Python, Bash

EXPÉRIENCES PROFESSIONNELLES

ID6TM — Ingénieur DevSecOps / Platform Security (Cloud Native)

Depuis fév. 2026 · Remote

Sécurité de la plateforme Kubernetes de trois clusters sur OVHcloud (production, pré-production, outils internes) et refonte de l'architecture réseau & sécurité.

- **Sécurité runtime (Falco) :** driver eBPF, logs d'audit Kubernetes, règles sur mesure dans leur dépôt (shell dans un conteneur, reverse shell, accès aux secrets, conteneurs privilégiés), réduction du bruit, validation par tests d'attaque ; FalcoSidekick vers Wazuh, Prometheus et Slack.
- **SIEM (Wazuh) :** manager/indexer/dashboard déployés en Terraform, agents packagés en chart Helm via ArgoCD, SSO (OIDC) ; modules de corrélation, vulnérabilités et threat intel ; logs du compte cloud et des bases managées. Restructuration d'une règle déclenchée ~474 000 fois/jour.
- **SOAR (Shuffle) :** événements du fournisseur d'identité et du VPN indexés dans le SIEM, un ticket par événement critique, rapport sécurité hebdomadaire ; aucun secret dans les workflows ni dans leurs sauvegardes Git.
- **Policy-as-code (OPA Gatekeeper) :** une cinquantaine de politiques de la bibliothèque officielle sur 3 clusters via un ApplicationSet ArgoCD ; warn puis deny par environnement ; l'audit a révélé deux erreurs de configuration bloquantes avant l'enforcement ; 5 règles d'alerte Prometheus et une interface SSO.
- **Réseau :** origine joignable uniquement via Cloudflare (mTLS Authenticated Origin Pull, vraies IP clientes préservées) ; audit des NetworkPolicies et déploiement du default-deny en trois phases ; diagnostic d'une collision de marks Netfilter (Netbird / OVH OKS / kube-proxy) cassant les NodePorts, corrigée par DaemonSet et remontée à l'éditeur.
- **Accès :** administration zero-trust (VPN Netbird, SSO avec double authentification, RBAC fondé sur l'OIDC) ; setup keys VPN génériques révoquées après un départ, procédure de sortie ; Bytebase pour MySQL/PostgreSQL/MongoDB avec RBAC, séparation des rôles et break-glass.
- **Fiabilité & GitOps :** patch management via ApplicationSets avec canaux standard/stable ; revue du bruit d'alertes (alertes actives −23,5 %, critiques −25 %) ; rédaction du dossier d'architecture technique (DAT).
- **Open source (CNCF/Falco) :** correctif de résilience mergé dans falcosecurity/plugins, PR #1270 (k8saudit-ovh : reconnexion WebSocket, retry, gestion des erreurs JSON), publié en v0.4.1.

Environnement: Kubernetes (OVHcloud), ArgoCD, Helm, Terraform, Traefik, Cloudflare, Netbird, Zitadel, Vault, Wazuh, Shuffle, Falco, OPA Gatekeeper, Bytebase, Prometheus, Loki.

Cyllene — Ingénieur DevOps / SysOps, infogérance

Sept. 2021 – Déc. 2025

Lead technique pour l'infogérance et la modernisation d'infrastructures pour 10+ clients grands comptes (Paylib, Decathlon, Cotton Bird, H2O, Rouge Gorge, Cora).

- Architectures Cloud Native sur GCP (GKE, Cloud SQL) avec Terraform ; CI/CD avec ArgoCD, Argo Workflows, Helm et GitLab CI ; observabilité complète (Grafana, Prometheus, Alertmanager, Opsgenie).
- Référent sécurité Kubernetes : scan de vulnérabilités (Trivy, Starboard), hardening des clusters.
- Migration de Paylib d'OpenShift vers Kubernetes (GitOps) : environ 300 k€ économisés par an.
- Audit et consulting : haute disponibilité, reprise d'activité, optimisation des coûts.

Environnement: GCP, Kubernetes, Terraform, Helm, ArgoCD, Ansible, Grafana, Prometheus, Trivy, Gatekeeper.

Decathlon (via Néo Soft) — SysOps, Grande distribution

Janv. 2020 – Juil. 2021

Exploitation de la plateforme critique d'API management du groupe : 1,1 milliard d'appels par semaine.

- Extension d'AWS vers GCP (multi-cloud) pour la disponibilité et la latence ; infrastructure as code avec Terraform.
- Optimisation d'un cluster Elasticsearch de 30 To multi-région et migration vers un SaaS managé (Aiven) ; refonte du monitoring pour un alerting proactif ; Gravitee passé sur Kubernetes.

Environnement: AWS, GCP, Kubernetes, Terraform, Gravitee, Elasticsearch, Grafana.

Pictime Groupe (Auchan, Société Générale, Boulanger) — Ingénieur systèmes et réseaux

Fév. 2018 – Janv. 2020

Clients de la banque, de la finance, du retail et de l'assurance.

- Création de plateformes pour des grands comptes ; HA avec HAProxy et F5, clusters GlusterFS et Galera ; Linux, MySQL et MSSQL en production.

SIX Financial Information (Inforisk) — Administrateur système et exploitation

Oct. 2012 – Janv. 2018

Conception et réalisation de la plateforme : meilleure disponibilité et scalabilité, réduction drastique des coûts.

- **Virtualisation & IaC :** du physique au virtuel (vSphere, puis Proxmox) avec un cluster Ceph répliqué et sécurisé ; déploiement des VM entièrement automatisé et infrastructure codifiée avec Ansible pour une reconstruction automatique ; nombreux services critiques migrés vers Debian.
- **Sécurité :** WAF ModSecurity intégré à ELK, puis nouvelle version avec correcteur de faux positifs, règles personnalisées et anti-bot/bad-bot ; firewall dynamique ipset avec détection comportementale ; VPN pfSense ; réseau privé isolé ; tier d'entrée HA (Keepalived/VRRP) ; OpenLDAP, FreeIPA.
- **Traçabilité & supervision :** suivi des actions utilisateurs sur les serveurs critiques, logs centralisés (ELK, rsyslog) ; Zabbix entièrement mis à jour, Nagios, alertes améliorées en continu.
- **Données & continuité :** réplication PostgreSQL (RepMgr, PgPool), sauvegardes Bacula multi-sites, plans de continuité et de reprise, PowerDNS. **Équipe :** accompagnement des développeurs, formation d'un collaborateur N2 pour qu'il les accompagne en autonomie.

Premières expériences (2010 – 2012) : Médiane Communication, administrateur système et développeur freelance ; Groupe Scolaire Alkadissiya, formateur et administrateur du parc informatique.

FORMATION

CESASUP, Casablanca — Master 2 européen (Bac+5), 2016–2017 : management de projets informatiques

Institut Spécialisé Industriel, Mohammedia — Technicien spécialisé (Bac+2), 2008–2010 : réseaux informatiques

PIGIER, Mohammedia — Technicien spécialisé (Bac+2), 2007–2009 : développement informatique

CERTIFICATIONS

- GCP — Professional Cloud Architect (2023)
- GCP — Associate Cloud Engineer (2023)
- AWS Cloud Practitioner (2019)
- En cours : CKA → CKS (Kubernetes)

LANGUES

Arabe — langue maternelle · Français — courant · Anglais — avancé (B2, en progression vers C1)