ILYASS KAOUAM

Senior Cloud, DevOps & Security Engineer

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

PROFESSIONAL SUMMARY

Senior infrastructure and security engineer with 16+ years of experience designing, securing and operating critical systems, from virtualization (VMware, Proxmox) to Cloud Native environments (GCP, AWS, Kubernetes). Currently securing a three-cluster Kubernetes platform end to end: runtime detection, SIEM and SOAR, policy-as-code, zero-trust access and GitOps. Earlier, six years building and hardening a production platform from physical servers to Proxmox, Ceph and Ansible. Root-cause oriented, documentation-minded, merged open-source contributor to the CNCF Falco project.

TECHNICAL SKILLS

Detection & policy	Wazuh (SIEM), Shuffle (SOAR), Falco (eBPF), OPA Gatekeeper, NetworkPolicies, Trivy, incident runbooks
Identity & access	Zitadel (OIDC SSO, 2FA), Netbird/WireGuard, Vault + ArgoCD Vault Plugin, Bytebase, Kubernetes RBAC
Platform & GitOps	Kubernetes (OVHcloud, GKE, EKS, RKE2), ArgoCD ApplicationSets, Helm, Terraform, Ansible, cert-manager, GitLab CI
Network & perimeter	Traefik, Gateway API, Cloudflare, WAF (ModSecurity, anti-bot), pfSense, iptables/nftables/ipset, Keepalived/VRRP, HAProxy, F5, policy routing
Observability	Prometheus, Alertmanager, Grafana, Loki, Fluent Bit, Elasticsearch/ELK, Zabbix, Nagios
Systems & data	Linux (Debian, RHEL), Proxmox & Ceph (expert), vSphere, PostgreSQL, MySQL, MongoDB, Bacula
Languages	Go (open-source contributions), Python, Bash

PROFESSIONAL EXPERIENCE

ID6TM — DevSecOps / Platform Security Engineer (Cloud Native)

Since Feb 2026 · Remote

Security of the three-cluster Kubernetes platform on OVHcloud (production, pre-production, internal tools) and redesign of the network & security architecture.

- **Runtime security (Falco):** eBPF driver, Kubernetes audit logs, custom rules in their own repo (shell in container, reverse shell, secret access, privileged containers), noise reduction, validation by attack tests; FalcoSidekick to Wazuh, Prometheus and Slack.
- **SIEM (Wazuh):** manager/indexer/dashboard deployed with Terraform, agents packaged as a Helm chart via ArgoCD, SSO (OIDC); correlation, vulnerability and threat-intel modules; cloud-account and managed-DB logs. Re-tiered a rule firing ~474,000 times/day.
- **SOAR (Shuffle):** identity-provider and VPN events indexed into the SIEM, one ticket per critical event, weekly security report; secrets kept out of workflows and Git backups.
- **Policy-as-code (OPA Gatekeeper):** ~50 policies from the official library on 3 clusters via an ArgoCD ApplicationSet; warn then deny per environment; audit caught two cluster-blocking misconfigurations before enforcement; 5 Prometheus alert rules and an SSO policy UI.
- **Network:** origin reachable only through Cloudflare (mTLS Authenticated Origin Pull, real client IPs preserved); NetworkPolicy audit and three-phase default-deny rollout; diagnosed a Netfilter mark collision (Netbird / OVH OKS / kube-proxy) breaking NodePorts, fixed with a DaemonSet and reported upstream.
- **Access:** zero-trust administration (Netbird VPN, SSO with 2FA, OIDC-based RBAC); generic VPN setup keys revoked after a departure, offboarding procedure; Bytebase for MySQL/PostgreSQL/MongoDB with RBAC, separation of duties and break-glass.
- **Reliability & GitOps:** patch management through ApplicationSets with standard/stable release channels; alert-noise review (active alerts −23.5%, criticals −25%); wrote the infrastructure technical architecture document (DAT).
- **Open source (CNCF/Falco):** resilience fix merged in falcosecurity/plugins, PR #1270 (k8saudit-ovh: WebSocket reconnection, retry, JSON error handling), released in v0.4.1.

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

Cyllene — DevOps / SysOps Engineer, IT outsourcing

Sep 2021 – Dec 2025

Technical lead for infrastructure outsourcing and modernization across 10+ enterprise accounts (Paylib, Decathlon, Cotton Bird, H2O, Rouge Gorge, Cora).

- Cloud-native architectures on GCP (GKE, Cloud SQL) with Terraform; CI/CD with ArgoCD, Argo Workflows, Helm and GitLab CI; full observability (Grafana, Prometheus, Alertmanager, Opsgenie).
- Kubernetes security referent: vulnerability scanning (Trivy, Starboard), cluster hardening.
- Paylib migration from OpenShift to Kubernetes (GitOps): about 300k€ per year saved.
- Audit and consulting: high availability, disaster recovery, cost optimization.

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

Decathlon (via Néo Soft) — SysOps Engineer, Retail

Jan 2020 – Jul 2021

Operated the group's critical API management platform: 1.1 billion API calls per week.

- Extended AWS to GCP (multi-cloud) for availability and latency; infrastructure as code with Terraform.
- Optimized a 30 TB multi-region Elasticsearch cluster and migrated it to a managed SaaS (Aiven); redesigned monitoring for proactive alerting; Gravitee moved to Kubernetes.

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

Pictime Groupe (Auchan, Société Générale, Boulanger) — Systems & Network Engineer

Feb 2018 – Jan 2020

Banking, finance, retail and insurance clients.

- Delivered new platforms for enterprise clients; HA with HAProxy and F5, GlusterFS and Galera clusters; Linux, MySQL and MSSQL in production.

SIX Financial Information (Inforisk) — Systems & Operations Administrator

Oct 2012 – Jan 2018

Designed and built the platform: better availability and scalability, drastically reduced costs.

- **Virtualisation & IaC:** physical to virtual (vSphere, then Proxmox) with a replicated, secured Ceph cluster; VM deployment fully automated and infrastructure codified with Ansible for automatic rebuild; many critical services migrated to Debian.
- **Security:** ModSecurity WAF with ELK, then a new version with false-positive corrector, custom rules and anti-bot/bad-bot; dynamic ipset firewall with behavioural detection; pfSense VPNs; isolated private network; HA entry tier (Keepalived/VRRP); OpenLDAP, FreeIPA.
- **Traceability & monitoring:** user actions on critical servers tracked, logs centralised (ELK, rsyslog); Zabbix fully upgraded, Nagios, alerting continuously improved.
- **Data & continuity:** PostgreSQL replication (RepMgr, PgPool), Bacula backups across sites, continuity and recovery plans, PowerDNS. **Team:** supported the developers, trained a level-2 engineer to support them autonomously.

Early career (2010 – 2012): Médiane Communication, freelance systems administrator and developer; Groupe Scolaire Alkadissiya, IT instructor and network administrator.

EDUCATION

CESASUP, Casablanca — European Master's degree (Bac+5), 2016–2017: IT project management

Institut Spécialisé Industriel, Mohammedia — Specialized Technician (Bac+2), 2008–2010: network engineering

PIGIER, Mohammedia — Specialized Technician (Bac+2), 2007–2009: software development

CERTIFICATIONS

- Google Cloud — Professional Cloud Architect (2023)
- Google Cloud — Associate Cloud Engineer (2023)
- AWS Certified Cloud Practitioner (2019)
- In progress: CKA → CKS (Kubernetes)

LANGUAGES

Arabic — native · French — fluent · English — professional working proficiency (B2, progressing to C1)