Jaskarn Singh

Cloud Security & DevSecOps Engineer | AI/Agentic Security (USAP)

Berlin, Germany | +49 176 2094 7408 | jaskaranhundal0001@gmail.com
linkedin.com/in/jaskarnsinghcybersec | github.com/jaskaranhundal | jaskarnsingh.vercel.app

Summary

Cloud Security & DevSecOps Engineer with 8+ years across security engineering, cloud infrastructure, and networking. Designs and ships security architecture for cloud-native production systems in a regulated healthcare environment (ISO 27001, GDPR): fleet-wide CI/CD security pipelines, infrastructure-as-code platform services, container hardening to zero HIGH/CRITICAL CVEs, and TLS automation. Author of USAP, an open-source AI-security agent platform, and focused on securing AI and agentic systems on cloud.

Core Skills

Security: SAST/DAST/SCA (Semgrep, OWASP ZAP, Trivy, Gitleaks, npm-audit), Vulnerability management (Nessus, Qualys), Incident response, SIEM (ELK Stack), Sentry, ISO 27001, GDPR, PCI-DSS, Secure SDLC

AI/LLM Security: OWASP LLM Top 10, MITRE ATLAS, NIST AI RMF, Agentic security (USAP), garak, PyRIT, promptfoo

Cloud: AWS, Azure, Open Telekom Cloud (OpenStack), Hetzner

Containers & Orchestration: Docker, Kubernetes, Non-root hardening, nginx

CI/CD & Automation: GitLab CI/CD, Jenkins, Python, Bash, paramiko, WireGuard, cron

Networking: FortiGate, Juniper, Cisco, Palo Alto, WAF, IDS/IPS

Experience

DevSecOps Engineer (Cloud Security) — Lindera

Apr 2025 – Present | Berlin, Germany

- Designed and rolled out a hardened CI/CD security pipeline - Semgrep SAST, OWASP ZAP DAST, npm-audit SCA, Trivy container/IaC scanning, and Gitleaks secrets detection, with all scanner images pinned by SHA-256 digest - across 15+ production repositories.
- Built a fleet-wide TLS certificate auto-renewal platform solo: scheduled GitLab pipelines renew and deploy certificates to every host over WireGuard and rotate Open Telekom Cloud load-balancer certificates via API, with dry-run mode, preflight diagnostics, and MS Teams reporting.
- Eliminated 29 HIGH and 6 CRITICAL CVEs from the primary base image, drove production containers to zero HIGH/CRITICAL vulnerabilities, and enforced non-root containers across the frontend and backend fleet.
- Own the observability stack: operate self-hosted Sentry with daily backups to object storage and automatic issue creation from qualifying alerts; rolled out Sentry SDKs to 6 applications; operationalized the ELK monitoring stack.
- Built hardened Redis and RabbitMQ platform services with TLS, ACL-based authentication, and encrypted configuration, deployed via CI/CD; automated cloud server scheduling to reduce infrastructure costs.
- Shipped 160 merge requests across 26 projects and 1,200+ CI pipeline runs; driving fleet-wide standardization of pipeline architecture (merge-request gates, tiered post-merge checks, nightly security scans).

Cybersecurity & DevOps Engineer (Working Student) — Lindera

Oct 2023 – Mar 2025 | Berlin, Germany

- Implemented and maintained ISO 27001 security controls and audit-readiness documentation in a regulated healthcare environment (GDPR, HIPAA-aligned processes).
- Ran vulnerability assessments across cloud and application layers with remediation tracking to closure.
- Monitored and responded to security incidents using the ELK stack, OSSEC, and Wireshark under established incident-response procedures.
- Automated Docker builds and Hetzner server deployments in GitLab CI for web and mobile applications, including non-root container hardening.
- Drove secure-coding practices and delivered security awareness sessions for development teams.

NOC Engineer II — Zeta

Oct 2019 – Mar 2023 | Bangalore, India

- Configured and managed WAF and IDS/IPS systems (FortiGate); ran vulnerability scanning with Nessus and Qualys for banking-technology infrastructure.
- Maintained 99.99% uptime of wired and wireless network infrastructure serving card-issuing and core-banking platforms.
- Migrated servers to AWS with infrastructure-as-code, improving production efficiency 17% with no added downtime.

- Implemented and audited ISO 27001 and PCI-DSS security controls.
- Reduced network downtime 30% through continuous monitoring and incident management; documented 22 client networks.
- Reviewed, audited, and onboarded 15 external vendors handling billions of concurrent network requests.

Associate Network Engineer — KocharTech
Sep 2016 – May 2019 | Amritsar, India

- Provided first- and second-level support for network security incidents, including firewall configuration and intrusion-detection analysis.
- Performed scheduled Juniper upgrades and configuration changes with zero service downtime.
- Executed 75% of all firewall changes, installs, and upgrades; remediated 13 quarterly IDS/IPS findings.
- Led 6 major network design, implementation, and automation projects.

Projects

USAP - Unified Security Agent Platform
github.com/jaskaranhundal/usap-skills

79 cybersecurity skills and 12 orchestrator agents across SOC, incident response, threat hunting, and DevSecOps, exposed over the Model Context Protocol. Typed output contracts, resolvable-evidence gating, hash-chained audit log; tiered autonomy (L1-L4) with human approval gates.

ARIA
Private research, evaluation phase - write-up on request

7-agent architecture driven by a locally fine-tuned model (Llama 3.1 8B, 181k-sample training corpus, MLX), in evaluation phase against DVWA and OWASP Juice Shop in an isolated lab. Not deployed against production systems.

Education

MSc Cybersecurity
IU International University of Applied Sciences | Jul 2023 – Mar 2025 | Berlin, Germany

B.Tech Computer Science
Satyam Institute of Engineering and Technology (Punjab Technical University) | 2016 – 2019 | Amritsar, India

Certifications

- Certified in Cybersecurity (CC) — ISC2, 2023
- Junior Cybersecurity Analyst Career Path — Cisco Networking Academy, 2024
- Azure Fundamentals — Microsoft, 2020
- PCI Compliance — Qualys, 2023
- Vulnerability Management Foundation — Qualys, 2023
- AWS Cloud Practitioner Essentials — AWS, 2022
- JNCIA-Junos — Juniper, 2020
- JNCIA-Sec — Juniper, 2020
- NSE 1 & NSE 2 — Fortinet, 2022
- Splunk Fundamentals — Splunk, 2019

Languages

English (Proficient), Punjabi (Native), Hindi (Native), German (A1 - in active study)