

Munish Kharb

Lead Security Engineer | Application, Cloud and Infrastructure Security · AI/LLM Security · DevSecOps

+91-8168139625 | munish@munishkharb.com | [linkedin.com/in/munishkharb](https://www.linkedin.com/in/munishkharb) | munishkharb.com | github.com/munishkharb | Gurugram, India

Summary

Lead Security Engineer with 6.5+ years across application, cloud and infrastructure security: threat modeling, secure code review in Java, Python and JavaScript, penetration testing across web, mobile, API and desktop, secure SDLC, AWS guardrails and detection. Owned the full security function for a three-entity healthtech group, then application and cloud security for an international gaming product. Built and ran a Wazuh SIEM across hundreds of endpoints, pulling in EDR, firewall, Suricata, AWS and VPN logs, found 200+ critical and high-severity vulnerabilities, and took an ASPM program from design to live enforcement. Secures AI features end to end, from prompt injection to agent tool access, and uses AI to widen threat modeling and code review.

Experience

Jungle Games

Gurugram, India

Lead Security Engineer

June 2026 – Sept 2026

- Role ended September 2026 when Jungle wound up operations after India's real-money gaming ban.
- Owned application and cloud security for two products under GDPR, one pre-launch and one live; threat-modeled the API gateway, payment, authorization and PII services and the identity, email and CRM integrations.
- Pentested Android, iOS, desktop, API and WebSocket surfaces with a self-built Python WebSocket tool; found account-takeover, SSRF and payment-integrity criticals and BOLA/IDOR flaws across both products.
- Designed and launched the secure-SDLC, ASPM and vulnerability management program, severity scored on exploitability, exposure and data sensitivity; took branch gating live on a production product and fixed a vendor default that was hiding real Criticals.
- Owned AWS cloud security: reviewed SCP and RCP guardrails, ran code-to-cloud scanning with Checkov and OX and posture with Wiz, and wired ASPM findings into the SIEM with SOC alerts and playbooks.
- Built an MCP server giving AI agents nine read-only investigation tools over a live SIEM, with a query allowlist and audit logging; runner-up of 33 teams at the company hackathon.

Connect and Heal

Remote, India

Lead Security Engineer

Sept 2025 – June 2026

- Owned the security function for three group entities (application, cloud, DevSecOps, detection, GRC, IT): quarterly and annual roadmaps, leadership metrics, incident response, and product security for 4 mobile and 9 web apps.
- Ran cloud and host vulnerability management on AWS and GCP (Inspector, Wazuh, Scalefusion, 580+ daily CIS and SOC 2 checks), scanned for dangling DNS, public snapshots and ECR exposure, and drove the CNAPP selection.
- Threat-modeled the CI/CD-to-production pipeline (Jenkins, Bitbucket, CodeBuild, ECR, EKS), found plaintext secrets and a cluster-admin CI identity, and directed the IAM and KMS remediation.
- Owned GRC on the company side, policy through audit evidence: ISO 27001, ISO 27701 and SOC 2 Type 2 across the group entities, access reviews, vendor assessments, Scrut rollout, customer security clearance calls.
- Led and mentored the security team and interns, coached IT and DevOps on domain security, and ran awareness and phishing training.
- Directed IT security across hundreds of MDM-managed endpoints: SentinelOne EDR, DLP, MDM baselines, Fortinet and Sophos firewall reviews, Google Workspace hardening, disk-encryption and OS end-of-life rollouts.
- Authored the AI usage policy into the ISMS, cut third-party OAuth access to company data down to an approved list with an approval workflow for new grants, and enforced it at the network with firewall and browser controls.

Senior Security Engineer

Jan 2023 – Sept 2025

- Set up the group's secure SDLC: design-time threat models, web, mobile and API pentests before release, and a CI/CD pipeline with live-verified secrets scanning, SAST and per-build SBOM and CVE correlation, rolled out from observe to enforce.
- Led the penetration test and security review of production healthcare chatbots built on Gemini: model integration, retrieval and data access, tool and API reach, abuse and data-leak paths; also pentested an ML claims system.
- Built and ran a Wazuh SIEM integrated with the commercial EDR (replacing it on part of the fleet to cut cost): 170+ ATT&CK techniques on SOCFortress and Sigma content, active response, CloudTrail detections, false positives cut by about two-thirds.
- Built and ran a daily external attack-surface pipeline (subdomain enumeration, port and tech fingerprinting, Nuclei with custom templates) with delta tracking across all domains.

PharmEasy

Security Engineer

Remote, India

Aug 2021 – Jan 2023

- Led penetration testing across PharmEasy, Retailio, Docon and Thyrocare (web and mobile on Java/Spring Boot, Python and ASP.NET) for apps serving millions of users; surfaced 100+ critical vulnerabilities, threat-modeled new features and took part in secure design reviews.
- Ran triage for the vulnerability disclosure program (validation, prioritization, researcher response); tracked findings in DefectDojo and evaluated Burp Suite Enterprise and Qualys in hands-on proofs of concept.
- Built an attack-surface monitoring tool on Nuclei for continuous scanning of public assets, ran network VAPT, added automated DAST, helped set up kube-bench CIS checks on EKS, and managed the Akamai WAF.

Acadbee

Security Engineer

Gurugram, India

Mar 2020 – Aug 2021

- Performed web application penetration tests and vulnerability assessments, and worked with developers to fix findings and improve secure-coding practices.
- Built Django and Python web applications in production alongside the security work.

Skills

Languages: Python, Java, JavaScript, Bash

Application Security: threat modeling (STRIDE, data-flow diagrams), secure design review, secure code review (Java, Python, JavaScript), web and API penetration testing, OWASP Top 10, OAuth 2.0, JWT and SAML, business-logic and payment-flow testing, multi-tenant authorization testing, third-party integration review

Mobile and Client Security: Android and iOS penetration testing (MASVS/MASTG), Flutter and Unity clients, macOS and Windows desktop clients, reverse engineering, dynamic instrumentation, TLS interception and pinning bypass, code-signing review

Cloud Security: AWS security architecture and hardening across multi-account estates, IAM, EKS and Kubernetes, VPC and network security, KMS, CloudTrail and GuardDuty, WAF, CSPM/CNAPP, IaC security (Terraform, Checkov), hands-on with GCP, working familiarity with Azure

DevSecOps, Supply Chain and Vulnerability Management: CI/CD security gates (SAST, DAST, SCA, secrets scanning), SBOM and CVE correlation, ASPM program design, severity and SLA design, branch protection, GitOps, phased developer rollout

Detection Engineering and Incident Response: SIEM architecture, MITRE ATT&CK-mapped rules, Sigma, YARA, CloudTrail detections, alert tuning and suppression, threat intelligence, ASPM-to-SIEM alerting, playbooks, incident-response automation

AI Security (LLM and agents): LLM application pentesting (prompt injection, data exposure, tool and API reach), RAG and agent/MCP threat modeling, OWASP LLM Top 10, MITRE ATLAS, AI usage governance, AI-assisted security analysis

Governance, IT and Corporate Security: ISO 27001, ISO 27701, SOC 2 Type 2, NIST CSF and SSDF, GDPR, DPDP Act, vendor and customer security assessments, EDR, DLP, MDM, firewall reviews, Google Workspace security, access reviews

Tools

Web, API and Recon: Burp Suite Professional and Enterprise, Caido, OWASP ZAP, Nuclei, httpx, Amass and the ProjectDiscovery suite, Shodan, Postman, sqlmap, ffuf, Nmap, Wireshark, Tenable Nessus, Qualys, DefectDojo, Cloudflare WAF, AWS WAF, Akamai WAF

Mobile and reverse engineering: Frida, Objection, MobSF, Jadx, Apktool, Drozer, Ghidra, radare2, Il2CppDumper, reFlutter, Blutter, Hopper, Charles Proxy

Cloud and IaC: AWS Organizations, IAM, KMS, CloudTrail, GuardDuty, Security Hub; Wiz (CNAPP), OX Security (ASPM, IaC scanning, runtime sensor), Prowler, ScoutSuite, Pacu, CloudFox, Checkov, tfsec, Trivy, Terraform, kube-bench; Plerion, Sysdig, Sweet Security, SentinelOne CNAPP

Pipeline: Semgrep, TruffleHog, Gitleaks, Syft and Grype, CycloneDX, Dependency-Track, OWASP Dependency-Check, pre-commit, SonarQube, Bitbucket Pipelines, GitHub Actions, Jenkins, Argo CD

Detection, IR and AI: Wazuh, OpenSearch, ELK stack, osquery, Sysmon, auditd, Suricata, YARA, ClamAV, Sigma and pySigma, Stratus Red Team, OpenCTI, VirusTotal, Coralogix, Velociraptor; MCP server development

Corporate and GRC: Scrut, SentinelOne EDR, Endpoint Protector DLP, Scalefusion, JumpCloud, Fortinet, Sophos, Google Workspace admin

Education

The NorthCap University (formerly ITM University)

Bachelor of Technology, Computer Science Engineering

Gurugram, India