ANIRUDDHA KHANDWE

SECURITY PRACTICE LEADER · SECURITY ARCHITECT

Nagpur, Maharashtra, India +91 95612 15406 aniruddha1khandwe@gmail.com
linkedin.com/in/aniruddha-khandwe

CERTIFICATIONS

- **CISA** — ISACA
- **CISM** — ISACA
- **CEH v11** — EC-Council
- **ISO/IEC 27001** Lead Auditor
- **ISO/IEC 20000-1** Lead Auditor
- **ISO 22301** Lead Auditor
- **ISO 31000** Risk Manager
- **Certified Penetration Tester** — National Security Database
- Google Cloud — Core Infrastructure & Security

EDUCATION

M.Tech (Executive), Cloud Computing
Indian Institute of Technology, Patna
2024 – 2026

B.E., Electrical & Electronics Engg.
Yashwantrao Chavan College of Engineering, Nagpur
2021

SECTORS SERVED

BFSI · Insurance · Stock Exchange · Power Utilities · Smart City · Government & PSU · Critical Infrastructure

COMPLIANCE FRAMEWORKS

- ISO 27001 / 22301 / 20000-1 / 31000
- PCI DSS & SOC 2
- NIST CSF
- RBI & SEBI security guidelines
- CERT-In directions & empanelment
- DPDP Act readiness

PROFILE

Cybersecurity leader with 6 years of experience across security practice management, security architecture, governance and offensive security. Currently Principal Security Engineer at Aurionpro Solutions Limited, leading the cybersecurity practice end-to-end — VAPT, Red Team, SOC, GRC and Security Solutioning — with ownership of delivery, presales, OEM partnerships and practice P&L. Serves 20+ enterprise and government customers across BFSI, insurance, stock exchange, power utilities, smart city and public sector. Executive M.Tech (Cloud Computing), IIT Patna; CISA, CISM, CEH and ISO Lead Auditor certified. Part of the team contributing to the CERT-In AI Cyber War Room.

CORE COMPETENCIES

Security Leadership — practice build-out, delivery ownership, budgeting & P&L, multi-team leadership, OEM and partner management, hiring and capability development

Governance, Risk & Compliance — policy and control frameworks, compliance checklists, audit working papers, internal and IT audit, regulatory readiness

Security Architecture — Zero Trust, SOC / SIEM / SOAR / UEBA, IAM & PAM, WAF, EDR & XDR, DLP, MDM, network segmentation, secure cloud design, threat modelling

Offensive & AI Security — web, API, mobile, network and cloud VAPT; red teaming; secure code review; LLM and GenAI application testing; NIST AI RMF, ISO 42001, OWASP LLM Top 10

Presales & Solutioning — RFP and tender response, technical proposals, BoM and costing, effort estimation, evaluation-committee presentations, PoC and bid defence

PROFESSIONAL EXPERIENCE

Aurionpro Solutions Limited
Aug 2021 – Present

Cybersecurity Practice — India

Principal Security Engineer — Security Practice Lead *2024 – Present*

- **Lead the cybersecurity business end-to-end** across five delivery functions — VAPT, Red Team, SOC, GRC and Security Solutioning — covering strategy, staffing, capability build-out and delivery quality.
- **Own practice delivery, budgeting and P&L** — effort and cost modelling, resource planning, margin tracking and commercial governance for the security portfolio.
- **Manage a portfolio of 20+ active customers** across BFSI, insurance, stock exchange, power utilities, smart city and government, acting as escalation and assurance owner.
- **Design enterprise security architectures** for greenfield and modernisation programmes — SOC / SIEM / SOAR, IAM, Zero Trust and ZTNA, WAF, EDR / XDR, MDM, DLP and cloud security.
- **Own the OEM and partner ecosystem** across 20+ vendors (SailPoint, Arcon, Sophos, Zscaler, Array Networks, FireMon, Wazuh, Gurucul, Cyble, Indusface and others) — running product demos and PoCs, assessing fitment against client risk posture and regulation, and maintaining commercial and technical relationships.
- **Drive presales and tender solutioning** for large public-sector and BFSI RFPs: solution documents, compliance matrices, costing and BoM, pre-bid queries, and presenting the solution to client evaluation committees.
- **Build the governance layer for the practice** — policies, SOPs, audit working papers and control checklists mapped to ISO 27001, ISO 22301, PCI DSS, SOC 2, NIST CSF, RBI and CERT-In requirements.
- **Built the AI security service line** — AI-augmented VAPT, LLM and GenAI application testing and AI governance — and contribute to the CERT-In AI Cyber War Room on Blueprint drafting and governance.

FOCUS AREAS

- Security Architecture & Design
- Governance, Risk & Compliance
- VAPT & Red Teaming
- Presales & Tender Solutioning
- SOC Build & Operations

OEM ECOSYSTEM

SailPoint · Arcon · Sophos · Zscaler · Array Networks · FireMon · Wazuh · Gurucul · BluSapphire · Cyble · Indusface · Haltdos

TOOLS & PLATFORMS

- Burp Suite, OWASP ZAP, Nessus, Acunetix, Metasploit
- Splunk, Wazuh, SIEM / SOAR / UEBA platforms
- Docker, Kubernetes, Jenkins, GitHub, Azure DevOps
- AWS, Azure, GCP, NIC Cloud
- Python, Shell scripting

COMMUNITY

- Organizer — TensorFlow User Group, Nagpur
- Co-organizer — GDG Cloud, Nagpur
- Guest speaker — DevFest Nagpur and engineering colleges across Maharashtra
- Vice-Chair — IEEE YCCE Student Branch
- **Languages:** English · Hindi · Marathi

SELECTED ENGAGEMENT HIGHLIGHTS

Market Infrastructure Institution — SEBI CSCRF system & cyber audit
300+ regulatory controls, 300+ technology assets, 50+ critical applications across production, DR and support environments; 79 risk-ranked observations lifting Cyber Capability Index maturity.

Cooperative bank — digital banking assessment & DPDP readiness
12+ banking applications, 4 mobile platforms, 25+ APIs, 80+ servers and 150+ controls assessed; 95% of critical and high findings closed and validated on re-test.

State transport NCMC programme — secure cloud transformation
On-premise to AWS migration with Zero Trust, 300+ cloud and security controls validated, SAST/DAST and SBOM / HBOM / AIBOM coverage; 92% reduction in critical exposures, PCI DSS achieved and maintained.

ALPHV / BlackCat ransomware response — state transport department
Containment, clean DR recovery and hardening: full restoration in 48 hours, 1-hour RTO, 15-minute RPO, zero data loss, no ransom paid.

Managed threat hunting — enterprise SOC
ATT&CK-mapped hunting across 10,000+ endpoints and 50+ telemetry sources; detection 60% faster, containment 50% faster, dwell time down 70%.

Embedded VAPT programme — SEBI-regulated broker
Scaled tested estate from 40 to ~290 applications and 300 to 500 APIs across web, mobile, network and API domains under an always-audited model.

EARLIER EXPERIENCE

Cloud & Cyber Security Expert — Aurionpro Solutions Limited *Aug 2021 – 2024*

- VAPT and security audits across applications, APIs, cloud workloads and network infrastructure; secure cloud and DevSecOps design (AWS, Azure, GCP, NIC Cloud) with CI/CD pipeline security and container hardening.

Ministry of Social Justice & Empowerment, Govt. of India **Aug 2021 – Sep 2022**
Test Engineer (Cyber Security) — deputed through Aurionpro

- Owned cybersecurity for national citizen-facing portals — SACRED, SAGE, AGRASR, NMBA and SEED — covering VAPT, patch management, hardening and NIC-hosted infrastructure.

All India Council for Technical Education (AICTE) **Jul 2020 – Sep 2022**
Cyber Security Intern → Project Lead Trainee — Ministry of Education, GoI

- Led the cyber team for NATS, the AICTE Internship Portal and AMRUTUM 2.0 — web and network auditing, API security, patching and load testing.

KEY PROJECTS & INNOVATION

AI Trishul — in development
Unified AI-assisted platform for architecture review, configuration review, source code review and AI-driven VAPT on a single console.

Abhedya — GUI-based indigenous firewall
IP, region and country-level blocking, attacker geolocation, bot protection and live traffic monitoring.

Registered patent (2021)
Named inventor on a registered patent in the security and technology domain.