Adnan Koroth

Phone: +91 9094 97 9494 • LinkedIn: adnankoroth • Github: adnankoroth • Email: adnankoroth@gmail.com • Web: adnan.koroth.xyz

Experience

Pintu Crypto Exchange Pvt Ltd - Indonesia's largest OJK-regulated crypto exchange

Staff Security Engineer — *Mar 2025 - Present*

Lead Security Engineer — *Sep 2022 - Feb 2025*

Owned security engineering across cloud, identity, detection, and AI-enabled operations. Identified problems, scoped MVPs, and shipped internal platforms covering vulnerability management, IAM risk, cloud posture, secrets governance, and agentic security workflows - adopted by the security and engineering teams as the primary tooling for their domains. All running across AWS and GCP under fintech regulatory constraints (OJK SEOJK-38, ISO 27001, NIST CSF, CIS).

Internal Security Platforms - designed and shipped end-to-end

- Cerberos suite - 4-scanner cloud security platform on ECS Fargate covering container image exposure (Trivy across 10+ AWS service types), AWS CIS v5.0.0 compliance across all org accounts (Steampipe/Powerpipe), EKS CIS benchmarks (Kubescape), and EKS node CIS validation per-AMI via dynamically deployed Kubernetes Jobs with matching nodeSelector and tolerations. Findings flow to OpenSearch dashboards and auto-create Jira tickets. Replaced what would otherwise be 4 separate commercial tools.
- IAMGuru - Multi-cloud IAM risk platform built end-to-end (Python scanners, Go HTTP backend, PostgreSQL, web dashboard) deployed on ECS Fargate Spot for ~$8/month. Enumerates AWS IAM across every org account via STS assume-role chains; computes privilege escalation attack paths and per-role blast radius; maps findings to MITRE ATT&CK. GCP coverage includes org-wide service-account enumeration and Workload Identity Federation (WIF) binding analysis - surfaces all AWS→GCP cross-cloud trust paths, a gap most commercial tools miss. Risk scoring is database-driven (JSONB rules), tunable by the security team without code changes.
- Pentagon (co-architected) - Unified security operations platform consolidating findings from 6+ scanners into a single PostgreSQL warehouse with a 4-dimensional taxonomy (finding_type × scan_category × security_domain × framework) and SHA-fingerprint deduplication. Became the unified posture view for security and engineering leadership across cloud, application, and IAM risk. Owned the scanner job pipeline (ephemeral ECS Fargate Spot tasks → S3 JSONL → async ingest) and contributed compliance mapping for CIS AWS v3.0.0, ISO 27001, NIST CSF, and OJK SEOJK-38.

AI-Enabled Security Operations - bounded agents and pipelines

- AI-enriched SOC alert pipeline - CrowdStrike → SQS → ECS Fargate processor queries LogScale, sends raw events to Claude for structured assessment (severity, impact, actor, recommendation, confidence), resolves the affected user across Okta/GitHub/Jira/Slack, and posts a structured analyst summary to Slack. Includes an interactive clarification loop - analysts and affected users converse with the bot inside the alert thread until the case auto-closes at confidence ≥ 75 with no open questions. Bounded by design: deterministic temperature for classification, structured JSON output schema, no autonomous remediation actions, model inputs and outputs audit-logged for review.
- Pentagon AI agents (co-designed) - Three production agentic services on Fargate Spot using LangChain + Anthropic Claude: App Triage for vulnerability priority scoring and false-positive filtering; DNR Enrichment for IOC correlation and detection tuning; GRC Analyst for compliance gap analysis. Bounded by design: deterministic temperature for classification, scoped read/write surfaces (read findings, write enrichment, no destructive actions), shared PostgreSQL state, human review on disputed classifications.
- AI-powered WAF triage - Cloudflare Worker (TypeScript) that catches CF WAF spike alerts, aggregates the firewall event log via GraphQL, sends to Claude for threat classification, and posts a pre-classified Slack alert in under 30 seconds - replacing 10+ minutes of analyst dashboard work per spike.

Identity & Zero-Trust IAM

- Designed and enforced zero-trust IAM across all AWS accounts: Okta + AWS IAM Identity Center federation, hardware MFA, role-based least-privilege - eliminated standing long-term credentials org-wide.
- Built a cross-system identity resolution service (Lambda HTTP API) mapping one user across Okta, GitHub, Jira, Slack, and Google Sheets - consumed by the SOC pipeline, onboarding automation, and device-trust enforcement.
- JIT Access portal - Slack-native just-in-time AWS access (ECS + DynamoDB, Slack Socket Mode): engineers request elevated access via Slack, the request is routed to the account owner with Approve/Deny actions in-channel, and on approval the role is granted for a bounded session and auto-revoked at expiry. Replaces both standing elevated permissions and a vendor-PAM line item with an in-house bounded-trust workflow - satisfies ISO 27001 A.9 / CIS / OJK least-privilege requirements with a concrete control.
- Built Okta event-hook-driven device-limit enforcement that auto-suspends devices on policy breach.

Secrets Governance & GitHub Posture

- Multi-cloud secrets pipeline - Collectors for AWS Secrets Manager, GCP Secret Manager, and HashiCorp Vault gather metadata and HMAC value fingerprints, deliver HMAC-signed batches to a central ingestor, and write to BigQuery - providing org-wide secrets visibility and fingerprint-based change detection across all three stores.
- GitHub Enterprise Cloud auditing - 39 automated security checks across enterprise/org/repo scopes, week-over-week drift detection, automated Notion + Slack reports on a weekly EventBridge schedule.

Detection, Telemetry & Platform Engineering

- Built a security telemetry ingestion pipeline (Python) collecting from CrowdStrike EDR, Cloudflare WAF, NextDNS, Google Workspace, Office 365, and Falco - each a stateless collector with S3-persisted checkpoints and partition-aware queries for cost.
- Owned cloud-security and detection domains in a Go security automation monorepo: 26+ production services across 5 domains, 37 shared infrastructure client libraries (AWS/GCP/GitHub/Okta/CrowdStrike/Vault/Slack/Jira/Notion/Anthropic). Co-designed the domain-driven layout, dependency injection, and plugin auto-registration patterns.
- Infrastructure-as-code via Terraform (Pentagon) and AWS CDK (Cerberos), least-privilege IAM per service, KMS-encrypted secrets, private-subnet-only deployments. Real PostgreSQL in tests via testcontainers-go (no DB mocking). Pre-commit gates: golangci-lint, ruff, gitleaks, actionlint, zizmor, tflint, trivy.

Cars24 Services Pvt Ltd (India, Australia, Thailand & UAE)

Security Engineer - III (Cloud & Infrastructure) *Jul 2021 - Sep 2022*

- Established and built Cars24's security posture from scratch, managing and leading their Cloud Security (AWS & GCP), Endpoint Security (Palo Alto Cortex) and SASE Solution for Secure Engineering Workflows (Palo Alto Prisma)
- Spearheaded and completed the XDR (Palo Alto Cortex) roll-out across 4 countries and 6000+ employees in less than 90 days.
- Collaborated with application owners, end-users, and other stakeholders to gather requirements and ensure interoperability of cloud security controls implementation.
- Provided expertise on cloud security initiatives, vision & roadmaps by designing, implementing & maintaining open-source security solutions in cloud infrastructure.
- Drove the adoption of modern cloud-native IAM solutions; designed and implemented Authentication and Authorization policies and practices aligned with AWS's well-architected framework across all pillars.
- Defined, led, and executed architecture design workshops and white-boarding sessions to build implementation plans and improve DevSecOps.
- Designed backup, redundancy, and information-security continuity controls in the AWS/GCP environment to support ISO 27001 certification.

Castellum Labs (India)

Team Lead - Cloud & Network Security - Cloud Security Engineer - Associate Cyber Security Consultant *Aug 2019 - Jul 2021*

- Managed, modelled and held responsible for the company's AWS Cloud Infrastructure.
- Designed cloud security architecture, controls, and roadmaps for enterprise clients on AWS and on-prem.
- Built ThreatN!XD - a virtual SOC training environment (Docker, WAFs, IDS/IPS, firewalls) for blue-team drills with red-team C2 simulations
- Deployed SIEM platform (ELK, Wazuh, TheHive, Cortex, MISP, OpenCTI) with agent and agentless log forwarding from AWS.
- Built an internal Certificate Authority with CFSSL; enforced MFA and PKI-backed service authentication.
- Built an S3 misconfiguration scanner that harvests hostnames from Certificate Transparency logs, probes for public access, and scans exposed contents for credentials and PII.
- Conducted advanced phishing simulations (PhishCHK) for MNC clients using an in-house OSINT framework, self-hosted mail servers, and browser exploitation (BeEF).

IT Engineer Roles (Oman & India)

Freelance Consultant *Jun 2017 - Jul 2019*

- Diagnosis, configuration and maintenance of desktop, network and infrastructure issues,
- Worked efficiently as an IT contractor to provide small businesses with IT, Networking, Hardware, Software, Web Design and Graphic Design services.

Education

Sathyabama University, Chennai, TN, India
Bachelor of Engineering Computer Science (B.E - C.S).

- Thesis: Detection of Cyber Terrorism using Web Data Mining - system to mine User-Aware Rare Sequential Topic Patterns (URSTPs) from streaming web data.

Certifications

- **AWS - Security Speciality Certified**
- Cisco **CCNA, CCNP** (Routing and Switching)
- Fortinet NSE 1 & 2 Network Security Associate
- ICSI - Certified Network Security Speciality

Skills

- Languages: Python, Go (AI-assisted workflow), TypeScript, Bash
- Cloud & Infrastructure: AWS (IAM, STS, ECS Fargate, Lambda, S3, Secrets Manager, CloudTrail, GuardDuty, EKS, Organizations, EventBridge, KMS), GCP (IAM, Secret Manager, BigQuery, Resource Manager, WIF), Terraform, AWS CDK, Cloudflare Workers, Cloudflare Tunnel, Tailscale
- Security Engineering: Trivy, Kubescape, Steampipe/Powerpipe, Semgrep, Gitleaks, Falco, Wazuh, CrowdStrike Falcon, Palo Alto Cortex XDR, Palo Alto Prisma Access (SASE), AWS Access Analyzer, PKI/CFSSL
- Identity & Access: Okta, AWS IAM Identity Center, federated SSO, OIDC, RBAC, Workload Identity Federation (AWS→GCP); legacy directory auth (Kerberos, LDAP)
- AI & Agentic Systems: Anthropic Claude API, LangChain, agentic pipeline design (domain-specialized agents, deterministic classification, shared state over PostgreSQL), LLM workflow design for security triage, structured classification, enrichment, and human-in-the-loop review, Cloudflare Workers + LLM routing. AI safety practices: bounded autonomy, structured output schemas, confidence thresholds, human-in-the-loop on uncertain cases, audit-logged inputs/outputs, no destructive autonomous actions.
- Detection & Data: OpenSearch / ELK, SIEM design, MITRE ATT&CK mapping, IOC correlation, BigQuery, PostgreSQL, SQS event-driven pipelines
- Compliance & Frameworks: CIS AWS v3.0.0 / v5.0.0, CIS EKS T1.7.0, ISO 27001, NIST CSF, MITRE ATT&CK, OWASP Top 10, PCI-DSS, OJK SEOJK-38
- Engineering Practices: Domain-driven design, dependency injection, testcontainers-go (real-DB testing), Infrastructure-as-Code (Terraform, CDK), least-privilege IAM per service, KMS-by-default, pre-commit security gates

Personal Projects, Hobbies and Interests

- Outside of working hours - you can find me hiking, travelling, weight lifting and playing soccer.
- Automobile and Science Enthusiast.