C P KARTHIK

Cybersecurity Engineer | Backend Engineer | AI Security | Cloud & DevSecOps

Hyderabad, Telangana, India | +91-9866591766 | karthikkunal1122002@gmail.com

LinkedIn | GitHub | Medium

Professional Summary

Cybersecurity and software engineering professional with hands-on experience across security operations, email security, threat intelligence, incident response, backend engineering, AI-assisted security automation, and cloud-native systems. Skilled in Python, Golang, REST APIs, distributed systems, Docker, Kubernetes, AWS, Azure, SIEM platforms, Microsoft Defender, KQL, vulnerability intelligence, and secure software development. Experienced in building security platforms, backend services, automation workflows, RAG pipelines, multi-agent systems, and threat-analysis tools. Strong foundation in networking, application security, cryptography, cloud security, DevSecOps, observability, and incident response.

Technical Skills

Programming:	Golang, Python, SQL, JavaScript/TypeScript, C/C++, Java Basics, Bash, PowerShell
Backend Engineering:	Gin, GORM, FastAPI, REST APIs, gRPC, WebSockets, Microservices, Goroutines, Channels, Worker Pools, Context, JWT, Swagger
Cybersecurity:	SOC Operations, Incident Response, Threat Intelligence, Threat Hunting, Vulnerability Assessment, DFIR, Email Security, Application Security, IAM
Email Security:	Microsoft Defender for Office 365, Defender XDR, KQL, SPF, DKIM, DMARC, ARC, Message Trace, Safe Links, Safe Attachments, ZAP, Quarantine
SIEM & Detection:	Microsoft Sentinel, ELK Stack, Wazuh, Zeek, Suricata, Event Correlation, Detection Engineering, Log Analysis, IOC Enrichment
Network Security:	TCP/IP, DNS, HTTP/S, Routing, Firewalls, VPN, IDS/IPS, Wireshark, Nmap, Scapy, Network Traffic Analysis
Application Security:	OWASP Top 10, VAPT, API Security, Burp Suite, Nessus, OWASP ZAP, CSRF Protection, Secure SDLC, Threat Modeling
Cloud & DevOps:	AWS EC2, S3, IAM, VPC, CloudWatch, Azure, GCP, Docker, Kubernetes, Terraform, Jenkins, GitHub Actions, GitLab CI, NGINX
AI / ML / LLM:	LangChain, FAISS, RAG, OpenAI APIs, Embeddings, LLM Agents, Transformers, spaCy, NLTK, scikit-learn, MCP
Databases:	PostgreSQL, MySQL, MongoDB, NeonDB, Vector Databases
Cryptography:	Symmetric Encryption, Asymmetric Encryption, Hashing, PKI, TLS, Digital Signatures, Key Management, Secure Protocols, Post-Quantum Cryptography Concepts
ServiceNow:	Certified System Administrator, Certified Application Developer, SecOps Concepts, Workflow Automation, ServiceNow Platform Fundamentals

Professional Experience

Cyber Security Analyst | LTIMindtree **Oct 2025 – Present**

Microsoft Defender for Office 365 – Security Operations *Hyderabad, India*

- Monitor and investigate enterprise security incidents involving phishing, spoofing, business email compromise, malicious URLs, suspicious attachments, compromised identities, and authentication anomalies.
- Use Microsoft Defender XDR, Defender for Office 365, KQL, message tracing, email headers, and security telemetry to determine incident scope, severity, impact, and recommended containment actions.
- Analyze SPF, DKIM, DMARC, ARC, Received headers, domains, IP addresses, URLs, sender infrastructure, threat reputation, and user activity during investigations.
- Perform root-cause analysis of false positives and false negatives, identify detection gaps, and support tuning of sender signals, authentication logic, policies, and detection workflows.
- Develop Python utilities for IOC enrichment, log processing, investigation support, report generation, and repetitive security operations.
- Create investigation reports, SOPs, handoff notes, runbooks, dashboards, remediation guidance, and structured case documentation.
- Collaborate with security engineering, detection, cloud, infrastructure, and incident-response teams in a global 24x7 environment.

Backend Engineer / Open Source Contributor | Swecha **Mar 2022 – May 2025**

Backend Engineering, Security Automation and Open Source *Hyderabad, India*

- Developed Golang and Python services for backend systems, vulnerability intelligence, security automation, data ingestion, and API integrations.

- Built concurrent CVE and vendor-advisory collectors using goroutines, worker pools, structured parsing, retries, validation, and JSON/CSV output pipelines.
- Contributed to secure backend applications, REST APIs, Linux tooling, debugging, testing, documentation, and Git-based collaborative development.
- Worked with Docker, Kubernetes, databases, cloud deployment, network-security tooling, and distributed-system concepts.

SOC / Security Intern | Ideathon Axis **Aug 2024 – Apr 2025**
Security Monitoring and Incident Analysis *Hyderabad, India*

- Supported SIEM monitoring, IDS/IPS analysis, incident triage, network-security investigations, and log-correlation activities.
- Assisted with alert investigation, IOC validation, incident documentation, escalation, and security monitoring workflows.

Major Projects

Adaptive Threat Response Orchestrator (ATRO) *Python, LLMs, MCP, SIEM, Zeek, Suricata*

- Architected a multi-agent cyber-defense platform with agents for network analysis, log analysis, vulnerability assessment, threat intelligence, and automated incident response.
- Integrated RAG, MCP, LLM reasoning, SIEM telemetry, CVE data, FAISS retrieval, MITRE ATT&CK mapping, risk scoring, and automated incident reporting.
- Built workflows for evidence correlation, prioritization, containment guidance, and analyst-facing decision support.

AI-Powered Autonomous Threat Hunting System *Python, Streamlit, FAISS, spaCy, scikit-learn*

- Developed a threat-hunting platform combining anomaly detection, CVE intelligence, NLP-based insights, threat enrichment, and response playbooks.
- Integrated security analytics, searchable knowledge, dashboarding, and automated threat-analysis workflows.

Go Vulnerability Intelligence Platform *Go, Gin, Colly, chromedp, Docker*

- Built a concurrent vulnerability intelligence platform collecting OEM advisories, CVEs, severity data, affected products, and remediation references.
- Exposed REST APIs with worker pools, retries, structured logging, validation, JSON/CSV export, and containerized deployment.

Phishing OSINT & Email Security Analysis Platform *Python, DNS, WHOIS, URL Intelligence*

- Designed workflows to ingest EML, PDF, DOC, URLs, QR codes, images, headers, authentication results, and attachments.
- Implemented reputation checks, redirect analysis, domain intelligence, SPF/DKIM/DMARC validation, IOC enrichment, risk scoring, and verdict generation.

Security & Infrastructure Projects

Wireless Intrusion Detection System *Python, Scapy, Zeek, Suricata*

- Built detection logic for Evil Twin access points, deauthentication attacks, rogue wireless activity, and WPA2-related anomalies.
- Integrated packet inspection, rule-based detection, and security-event analysis.

Decentralized Intrusion Detection System *Python, AI, Raspberry Pi, Blockchain*

- Designed a distributed IDS architecture combining edge devices, AI-assisted anomaly detection, secure node communication, and decentralized trust mechanisms.

Web Application Security Automation Framework *OWASP ZAP, Selenium, Playwright, CI/CD*

- Built automated web-security testing workflows for OWASP Top 10, regression testing, security validation, reporting, and CI/CD integration.

OpsForge / Debian Composer Advanced *Go, Terraform, Docker, Kubernetes, OPA*

- Designed an infrastructure automation platform with signed recipes, policy enforcement, drift detection, remote agents, SBOM generation, vulnerability scanning, rollback, canary deployment, and RBAC concepts.

Software & Platform Engineering Projects

RAG Knowledge Assistant *Python, LangChain, FAISS, REST APIs*

- Built a retrieval-augmented generation platform for document ingestion, embeddings, semantic search, contextual responses, and API-based knowledge retrieval.

Go + CSRF Protection Web Application *Go, REST APIs, Security Middleware*

- Implemented CSRF token middleware, secure REST endpoints, request validation, authentication controls, and testing workflows.

Microservices Backend Platform *Go, Gin, GORM, PostgreSQL, MongoDB*

- Developed REST APIs and microservices using Golang, Gin, GORM, JWT authentication, concurrent processing, and containerized deployment.

Job AI Automation System *Go, Next.js, APIs, Automation*

- Designed backend modules for scraping, matching, resume processing, authentication, notifications, and automated job-workflow orchestration.

Employee Tracking Platform *Django, React, Leaflet*

- Built a web application with backend APIs, authentication, employee tracking, map visualization, and database integration.

Go-Sec Cybersecurity Learning Platform *Go, Web, Security Education*

- Designed a cybersecurity learning platform combining structured lessons, hands-on challenges, technical exercises, and AI-assisted guidance.

Cryptography & Security Research

- Working knowledge of symmetric and asymmetric encryption, cryptographic hashes, digital signatures, PKI, TLS, key exchange, and secure communication protocols.
- Familiar with encoding vs. encryption, classical and modern cipher structures, authenticated encryption, key derivation, and password hashing concepts.
- Explored post-quantum cryptography concepts including lattice-based, code-based, hash-based, and multivariate cryptographic approaches.
- Applied cryptographic concepts in secure API design, authentication, CSRF protection, JWT workflows, TLS-secured services, and security challenge experimentation.

Publications & Technical Writing

- Published **Adaptive Threat Response Orchestrator (ATRO)** on Medium, covering AI-assisted threat detection, multi-agent orchestration, and automated incident response.
- Write and build around AI security, cybersecurity automation, backend engineering, MLOps, cloud infrastructure, and secure software systems.

Achievements

- **Third Prize – National Techno-Exhibition 2025** for Adaptive Threat Response Orchestrator.
- Built multiple end-to-end projects spanning cybersecurity, AI, threat intelligence, backend engineering, cloud-native systems, DevSecOps, and distributed architectures.
- Contributed to open-source backend and security initiatives through Swecha and related community projects.
- Hands-on enterprise experience with Microsoft Defender, KQL, email threat investigations, detection tuning, incident response, and automation.

Education

Bachelor of Technology – Cyber Security **Dec 2021 – May 2025**
Vignana Bharathi Institute of Technology *Hyderabad, India*

CGPA: 7.7/10

Certifications

- ServiceNow Certified System Administrator (CSA)
- Certified Network Security Practitioner (CNSP)
- Developing Secure Software – Linux Foundation
- Linux Foundation LFD121
- ServiceNow Certified Application Developer (CAD)
- Certified Phishing Prevention Specialist (CPPS)
- JNCIA – Juniper Networks
- Zscaler Cloud Associate

Core Strengths

Cybersecurity Engineering • Backend Engineering • AI Security • Threat Intelligence • Cloud Security • DevSecOps • Distributed Systems • Cryptography • Incident Response • Secure Software Development • Automation