# Arjun S

+91 9445308335 | email@arjun.guru | github.com/admiralarjun | linkedin.com/in/admiralarjun | arjun.guru

## Education

**KL University** June 2021 — May 2025
*Bachelor's of Technology, Computer Science and Engineering* *Andhra Pradesh, IN*

## Skills

**AI & LLMs:** LangChain, LangGraph, OpenAI/Gemini SDKs and Live APIs, Google ADK, OpenRouter, LiveKit Voice, RAG, Prompt Engineering

**Full Stack:** FastAPI, React, Next.js, Tailwind, TanStack, Node.js, Supabase, Docker, Git, AWS / Azure, Pinecone, Postgres, Redis, Nginx, Linux

## Work Experience

**AI Engineer** Feb 2026 — Present
Threatlens Inc *Bangalore, IN*

- Engineered a **Multi-Tenant cloud-native SaaS** platform, implementing advanced LLM token caching and prompt optimization strategies that reduced API latency by 40% and cut inference costs by over $10k+ monthly.
- Architected and deployed a **global honeypot network** spanning 15+ cloud regions, generating over 5TB of high-fidelity threat intelligence telemetry for **LLM fine-tuning and proprietary knowledge base creation**.
- Developed a **LangGraph-based AI agent orchestration framework** to automate SIEM/XDR alert triage, reducing manual incident response resolution times by 85% and increasing alert processing capacity to 50,000+ events daily.
- Built AgentShield, a dedicated security gateway providing **real-time protection for AI Agents**, successfully filtering out 99.9% of adversarial attacks including prompt injections and jailbreak attempts.

**Cybersecurity Analyst** Jan 2025 — Feb 2026
KPMG India *Bangalore, IN*

- Engineered a **cloud-native SaaS** platform for large-scale artifact analysis, leveraging AI-driven insights to accelerate incident response timelines.
- Developed a high-performance parsing engine to ingest and correlate heterogeneous data sources, including PCAP, EVTX, Linux logs, and multi-cloud audit trails.
- Built an AST-based, thread-safe analysis engine mapping real-time detections to the **MITRE ATT&CK framework** for reproducible and explainable threat hunting.
- Integrated **Google Gemini SDKs** to enable real-time enrichment and cross-artifact correlation, surfacing complex attack narratives from raw telemetry.
- Architected the **Agile Threat Hunting and Incident Response (ATHIR)** framework, streamlining iterative rule authoring and **LLM-assisted** triage.
- Orchestrated end-to-end VAPT and Vulnerability Management cycles for a **Bangalore International Airport (BIAL Ltd)**, securing **1,500+** critical assets across web applications, servers, and network infrastructure.

## Projects

1. **Hacklido** hacklido.com
   - Leading Infosec Blogging Platform with 6k+ Users and 150k+ Reads / Month, built with LAMP Stack and unmanaged VPS.
   - Generated over $2,000 in Annual Passive Revenue with 0 Marketing. I sold it to a private equity firm in 2026 January.
2. **RAID** github.com/admiralarjun/RAID
   - Developed an enterprise-grade Incident Response platform leveraging an AI-augmented analysis engine for automated cyber incident detection and investigation.
   - Built structured defense workflows and scalable containerized deployments using Docker and Django to streamline security operations.
3. **GoAgentShield** github.com/admiralarjun/GoAgentShield
   - Designed a real-time protection proxy in Go to block prompt injection, jailbreaks, and data exfiltration targeted at AI Agents.
   - Engineered a high-performance analytics integration with ClickHouse and a custom policy enforcement engine for continuous traffic monitoring.
4. **WebAppSec-Copilot** github.com/admiralarjun/WebAppSec-Copilot
   - Engineered a Model Context Protocol (MCP) backend integrated with a custom Burp Suite extension to automate web application vulnerability scanning.
   - Designed an intelligent security copilot utilizing LLMs to contextually orchestrate real-time penetration testing and prioritize mitigation strategies.
5. **PRVigil** github.com/admiralarjun/prvigil
   - Architected an AI-driven PR reviewer built with Django to autonomously differentiate between legitimate functionality and malicious code changes.
   - Automated code health enforcement to prevent supply chain vulnerabilities and ensure strict compliance before authorizing repository deployments.
6. **Woicex Live** github.com/admiralarjun/woicex-live
   - Built a real-time conversational Voice AI assistant using WebRTC, utilizing LiveKit SDK for the backend and Next.js for the dynamic frontend UI.
   - Orchestrated low-latency audio streaming, turn detection, and noise cancellation to enable seamless edge-to-edge intelligent voice interactions.

## Research Publications ORCID: 0009-0006-8874-6115

1. Beyond Text: Nefarious Actors Harnessing LLMs for Strategic Advantage.
2. Beyond Copy-Pasting - Contextualizing LLMs for Secure Code Generation.
3. Novel Attack Vector to Abuse AWS for Cryptojacking
4. Defending AWS Cloud Infrastructure Using Deceptive Defense