

CURRICULUM VITAE

Badathala Jaisurya

AI Security · DevSecOps · MLOps · Cloud Security

Chennai, India · +91 8143516981 · jaisurya524126@gmail.com · linkedin.com/in/badathala-jaisurya · github.com/jaisurya93945 · jaisurya93945.github.io/portfolio

PROFESSIONAL SUMMARY

DevOps and cybersecurity engineer bridging security operations, cloud infrastructure and applied AI. Certified Ethical Hacker with hands-on experience in SIEM monitoring, vulnerability assessment and incident response, now applying that foundation to DevSecOps and cloud infrastructure as a DevOps Engineer at Stackly. Founder of CipherAI, a production AI SaaS platform serving a live paying client, and author of SentinelCore and IdenSec — open-source defences for prompt injection and agent tool-call provenance.

Targeting AI Security Engineer, DevSecOps, MLOps and Cloud Security roles.

CORE SKILLS

AI & LLM Security

Prompt-injection and jailbreak detection, LLM guardrails, MCP tool-poisoning checks, AI red teaming (garak, PyRIT), OWASP LLM Top 10, MITRE ATLAS, NIST AI RMF, detection engineering, evaluation harnesses.

Cloud, DevSecOps & MLOps

AWS, GCP, Docker, CI/CD pipelines, Kubernetes (in progress), Linux administration and hardening, Git/GitHub, dependency and secret scanning, pip-audit, dataset validation, regression testing.

Security Operations

SIEM monitoring, incident response, vulnerability assessment (VAPT), penetration testing, malware analysis, endpoint security, TCP/IP, DNS, firewalls, Splunk, ELK, Wireshark, Nmap, Metasploit, Burp Suite.

Development

Python, Bash, JavaScript/TypeScript, React, FastAPI, PyTorch, scikit-learn, Firebase, Supabase, LLM API integration (OpenAI, OpenRouter).

PROFESSIONAL EXPERIENCE

DevOps Engineer

Mar 2026 – Present

Stackly

- Manage cloud infrastructure and CI/CD pipelines supporting scalable backend deployment.
- Operate containerised applications with Docker, improving system reliability and deployment consistency.
- Drive DevOps and DevSecOps practice across build, release and deployment workflows.

Founder & Engineer

Jan 2025 – Present

CipherAI — cipherai.in

- Architected and built a multi-product AI SaaS platform spanning LLM chat, image and video generation, cybersecurity education, a job portal, hackathons and certification.
- Integrated LLM APIs (OpenAI, OpenRouter) with Clerk authentication, Firebase Firestore and Supabase storage to power 50+ AI tools on a credit-based usage system.
- Implemented Razorpay payment processing and an admin dashboard; delivered the platform to a real paying client, generating revenue from a live production SaaS product.

Cybersecurity Intern

Jan 2024 – Dec 2024

Tata Consultancy Services

- Conducted vulnerability assessments and risk analysis for enterprise systems, identifying security gaps across infrastructure.
- Monitored security alerts using SIEM tooling, supported incident triage and response, and prepared technical remediation reports.

Cybersecurity Intern

Jan 2024 – Jun 2024

CFSS Pvt Ltd

- Assisted penetration testing and ethical hacking exercises across web and network applications.
- Performed Linux system hardening and configuration security reviews; documented secure operating procedures.

SELECTED PROJECTS

SentinelCore

Python 3.11, FastAPI, SQLite, Docker, pytest

- Model-agnostic security layer between AI applications and their models, tools and data sources; inspects prompts, documents, tool calls and model output.
- Detects prompt injection, obfuscation (zero-width, bidirectional text, homoglyphs, encoding), PII and secrets, and MCP tool-poisoning; enforces allow / warn / sanitise / approve / block policy.
- 96.8% precision and 17.7% recall across 744 labelled examples, with an attack-replay lab tracking improvements across versions; OpenAI-compatible reverse proxy with queryable audit trails.

IdenSec

Python, deterministic taint tracking

- Provenance enforcement for agent tool calls: the check asks not who is calling but what determined this argument, and denies values that came from untrusted content.
- No model in the decision path, no network calls and no runtime dependencies, so a verdict is reproducible and reviewable rather than a score.
- 96.7% security ceiling measured against AgentDojo; the project reports a trade-off surface rather than a single headline score.

NeuroGenesis

Python, PyTorch, symbolic methods

- Verification framework converting LLM reasoning into structured representations and independently checking logic, factual and constraint violations before an answer is accepted.
- Implements a reasoning-shortcut oracle that enumerates shortcut spaces before training, testing whether identifiability predicts correct concept learning.

SOC Detection Lab

ELK, Splunk, detection engineering

- Deployed ELK and Splunk SIEM stacks in an isolated lab; wrote detection rules, simulated real-world attacks and documented end-to-end incident-response workflows.

Endpoint Monitoring & Malware Lab

Python, sandboxing, automation

- Built an isolated sandbox to safely analyse malware behaviour and evaluate defensive countermeasures.
- Built a USB/device monitor that flags unauthorised activity to prevent data exfiltration, plus scripts automating log analysis and network scanning.

CERTIFICATIONS

- Certified Ethical Hacker (CEH) — EC-Council
- DevSecOps — Linux Foundation
- Linux Essentials — Linux Foundation
- Cloud Computing Foundations — Google Cloud
- Python and AI certifications
- CompTIA Security+ and Network+ (in progress)

EDUCATION

B.Tech, Computer Science and Business Systems

Aug 2021 – May 2025

Rajalakshmi Institute of Technology, Chennai

ACHIEVEMENTS

Solved 100+ Capture the Flag (CTF) challenges across multiple platforms.

Runner-up, National Cybersecurity Hackathon.

Ranked in the top 3% globally in security competitions and on TryHackMe.

Generated revenue from a live production AI SaaS product delivered to a paying client.