# Avneesh Kasture

apkasture02@gmail.com

## SUMMARY

Security engineer and full-stack developer building AI-native platforms. Hands-on experience in SOC operations, detection engineering, and designing LLM-powered automation pipelines for lead intelligence, document generation, and project analytics.

## EXPERIENCE

**GRUVE** | Associate Solutions Engineer
04 2026 - Present | Pune

- Current focus: Generating efficiencies in critical business processes through blazing fast development of custom applications to solve pain points
- Built and deployed Helix, an internal AI sales enablement platform (Express.js, PostgreSQL, Redis, Prisma, Azure) with four components: engineering capability roadmap for sales visibility, automated pricing calculator for quotes, GPT-4o powered SOW generation pipeline, and a Service Navigator providing Assess-Design-Implement-Manage service mapping, pitch decks, Deal Weave artifacts, and a service comparison tool.

**GRUVE** | Security Operations Center Analyst
04 2025 - Present | Pune

- Performed advanced triage and investigation of security alerts across network, endpoint, and authentication telemetry using Splunk and Crowdstrike Falcon
- Conducted threat hunting that identified a vulnerability and led to a customer-wide advisory report.

**DELOITTE** | Digital Forensics Intern
07 2024 - 02 2025 | Mumbai

- Performed forensic acquisition and analysis of digital media using industry-standard forensic tools.
- Streamlined several business critical processes that cut down processing time by 80%
- Automated virus scanning and documentation of images using Python (RPA)

## PROJECTS

**PII DETECTION** | Personal Project
Feb 2025

- Built a filesystem-level PII detection tool to identify sensitive data exposure. Repository can be accessed here
- Enhanced with NLP-based entity recognition to identify structured and unstructured PII patterns.

## EDUCATION

**VELLORE INSTITUTE OF TECHNOLOGY**
Bachelor of Technology in Computer Science and Engineering
2024 | Chennai

## SKILLS

**SECURITY OPERATIONS**
Threat Hunting • Log Analysis • Detection Engineering • Splunk • Splunk Search Processing Language • Crowdstrike Falcon

**AUTOMATION & SOAR**
Document Generation Pipelines • Playbook Automation • LLM-driven Workflow Orchestration • Investigative Orchestration • Alert Enrichment

**FORENSICS & MALWARE**
Windows Forensics • Malware Analysis

**SYSTEMS & NETWORKING**
Linux • Windows • Networking

## CERTIFICATIONS

**ISC2 | CERTIFIED IN CYBERSECURITY**

**GOOGLE CLOUD AND DATA SCIENCE**

## SOCIETIES

ENACTUS VIT Chennai Chapter

## LINKS

Github:// **agileAlligator**
LinkedIn:// **Avneesh Kasture**