Sanay Krishna

Cloud Security · Security Operations · BCA Honours, Chanakya University, Bangalore
sanay.rein@gmail.com | linkedin.com/in/sanaykrishna | github.com/SanayKrishna | tryhackme.com/p/mochi1 | +91 7510554785

EDUCATION

Bachelor of Computer Application (BCA Honours) Expected Jun 2027
Chanakya University, Bangalore, Karnataka · CGPA: **9.29 / 10**

TECHNICAL SKILLS

Cloud & AWS	AWS S3 · CloudTrail · EventBridge · Lambda · SNS · IAM · Boto3 · Terraform
Security	MITRE ATT&CK · SIEM · SOAR · Incident Response · Threat Detection · CIS Benchmark
Languages & Frameworks	Python · JavaScript · TypeScript · Java · SQL · Bash · Flask · FastAPI · React · Next.js · Scikit-learn
Tools & Platforms	Nmap · Wireshark · Metasploit · Burp Suite · Linux · Git · PostgreSQL · SQLite · MySQL

TECHNICAL PROJECTS

S3 Security Dashboard (CloudScanner) · github.com/SanayKrishna/CloudScanner *Cloud Security & AWS Threat Detection*

- Built an event-driven AWS S3 security framework using CloudTrail, EventBridge, Lambda, and SNS to detect and alert on suspicious API activity in real time; deployed infrastructure via Terraform.
- Implemented continuous misconfiguration auditing mapped to AWS CIS Foundations Benchmark, classifying findings across four severity levels with a FastAPI and Jinja2 dashboard.

MITRE ATT&CK Cloud TTP Detection Engine · github.com/SanayKrishna/Mitre-Cloudtrail-Detection *Cloud Threat Detection & ATT&CK Mapping*

- Engineered 39 detection rules mapping CloudTrail events to 20 MITRE ATT&CK Cloud techniques across 9 tactics; rules-as-data architecture separates detection logic from the engine for zero-code rule additions — 33 unit tests, all passing.
- Integrated the official MITRE STIX bundle for real-time alert enrichment with technique metadata; FastAPI backend with filterable alert store, coverage gap dashboard, and live CloudTrail ingestion via Boto3.

AI-Powered SOAR Engine · github.com/SanayKrishna/Ai-Powered-Soar-Engine *Automated SOC Orchestration*

- Developed a SOAR prototype using a trained RandomForestClassifier to assign dynamic risk scores (1–100) per alert, triggering conditional automated playbooks to reduce analyst alert fatigue.
- Integrated Slack Webhooks for real-time notifications and built a Chart.js analytics dashboard with SQLite audit logging for full incident trail and compliance visibility.

EXPERIENCE

Application Security Intern Dec 2025 – Present
Asia to Genki LTD, Japan · Remote

- Applied OWASP Mobile Top 10 security principles to the Kokomata mobile application — implementing secure JWT authentication, input validation, encrypted local storage, and HTTPS-enforced API communication.
- Conducted security-focused code reviews during feature delivery cycles, identifying vulnerabilities in user data handling, session management, and third-party API integration points.

ACHIEVEMENTS

2nd Place — IKS Hackathon 2026 · Chanakya University ChandaEngine · 8 Days · Team of 4

- Built a computational implementation of Chandas Shastra: rule-based syllabifier with consonant-cluster lookahead, 15+ classical meter validators, FastAPI backend, Next.js frontend, Sarvam AI TTS/STT integration, and 21 passing unit tests — shipped in 8 days.

3rd Place — Srujana Hackathon 2025 · Chanakya University Netā-Nomics · Governance & AI

- Built an AI pipeline using Tesseract OCR and Google Gemini API to structure government expenditure data from unstructured PDFs, with multi-agent anomaly detection and automated RTI/PIL document generation (Next.js · FastAPI · PostgreSQL · Docker).

CERTIFICATIONS

Introduction to Cybersecurity Cisco · 2023
Google IT Automation with Python Specialisation Coursera / Google · 2023