SRIRAAM NAGARAJAN

Cloud Security & AI Systems | AWS · SIEM · Autonomous AI Agents
Coimbatore, India • +91 97517 16283 • nosriraam7@gmail.com • linkedin.com/in/sriraam-nagarajan • GitHub Portfolio

Cybersecurity undergraduate specializing in Cloud Security and SIEM operations, with hands-on experience building AWS security tooling, MITRE ATT&CK-mapped detection workflows, and automated cloud monitoring systems. Also active in AI systems development — built a fully local autonomous AI assistant with multi-agent orchestration and persistent memory architecture. 10+ self-built projects across cloud security, detection engineering, and AI automation.

EXPERIENCE

Cyber Security Trainer Jul 2025 – Present
Pynevera • Internship • Hybrid

- Deliver cybersecurity training sessions to students as part of Pynevera's technical team, covering network security, threat awareness, and security fundamentals
- Develop and structure course content for a private limited tech education company, translating complex security concepts into accessible curriculum for beginner-to-intermediate learners

PROJECTS

Portfolio: github.com/nssriraam | AWS-CSPM-Tool | AI-CloudTrail-Analyzer | SOC-Home-Lab

Rika — Autonomous AI Assistant Apr 2026 – Jun 2026
Python · Groq API · Ollama · ChromaDB · FastAPI · Playwright · Multi-Agent Orchestration

- Architected a fully local autonomous AI assistant in Python with voice-first interaction, 6-layer persistent memory (vector, graph, SQL), OS-level automation, and multi-agent swarm orchestration — achieving sub-300ms voice response latency with zero cloud data exposure
- Integrated a modular security assessment engine featuring automated surface discovery, vulnerability chain mapping, and MITRE ATT&CK-aligned findings synthesis — delivering structured reports via automated Telegram notification pipeline

SSH Honeypot & Attack Analysis Mar 2026
Cowrie · AWS EC2 · Python · MITRE ATT&CK

- Deployed a Cowrie SSH honeypot on AWS EC2 (EU-North-1) exposed to live internet traffic, capturing 16 real attack sessions within 35 minutes including credentials, commands, and attacker TTPs
- Mapped 4 observed techniques to MITRE ATT&CK (T1110.003, T1082, T1087.001, T1105), performed malware analysis on an intercepted live wget payload — producing a threat intelligence report with 5 defensive recommendations

AI-Powered CloudTrail Anomaly Detector Jan 2026 – Feb 2026
Python · Ollama · Qwen 2.5 · AWS CloudTrail

- Developed an offline AI triage tool using Python and Ollama (Qwen 2.5) to analyze AWS CloudTrail logs — cutting manual log review to zero by automating severity classification per event
- Integrated MITRE ATT&CK technique mapping and SOC action recommendations into every event output — generating analyst-ready incident reports without sending data to external services

AWS Cloud Security Posture Management (CSPM) Tool Dec 2025 – Jan 2026
Python · AWS Boto3 · Cloud Security

- Engineered a Python/Boto3 misconfiguration scanner covering 20+ AWS attack surfaces (S3, IAM, EC2, Security Groups, CloudTrail) — reducing manual audit time to under 60 seconds per account
- Uncovered 4 confirmed vulnerabilities (1 HIGH, 3 MEDIUM) on a live AWS account using automated severity scoring and vulnerability assessment — outputting timestamped JSON reports consumable by any SIEM pipeline

Phishing Email Analysis Nov 2025 – Dec 2025
Email Forensics · IOC Extraction · MITRE ATT&CK

- Conducted structured forensic analysis of phishing emails, extracting 3 IOC categories (malicious URLs, spoofed sender identities, header anomalies) using manual investigation methodology

- Correlated attack chain to MITRE ATT&CK T1566 and produced a formal threat analysis report documenting analyst findings, decision logic, and containment actions — replicating real SOC workflow

SOC Incident Case Study — MITRE ATT&CK Mapping Jun 2025 – Nov 2025

Threat Analysis · Incident Response Documentation

- Simulated end-to-end SOC incident handling across 5 stages — alert triage, threat hunting, investigation, severity classification, escalation, response, and closure — with analyst decisions documented at every step
- Attributed 5+ attack behaviors to MITRE ATT&CK techniques, producing a case study demonstrating structured incident response capability equivalent to L1 SOC analyst workflow

Wazuh SIEM Deployment & Troubleshooting Jun 2025 – Nov 2025

Wazuh · SIEM/IDS Administration

- Stood up a self-hosted Wazuh SIEM/IDS from scratch on Linux and resolved 3+ critical failures across the indexer, REST API, and dashboard — cutting downtime by diagnosing root causes and documenting repeatable fixes

EDUCATION

United Institute of Technology, Coimbatore 2027

Bachelor of Engineering in Computer Science & Engineering

CGPA: 8.40 / 10 • **Relevant Coursework:** Computer Networks, Network Security, Operating Systems, Cloud Computing, Digital & Mobile Forensics

SKILLS & OTHER

Cloud Security: AWS IAM, EC2, S3, CloudTrail, CSPM, Boto3, Security Groups, Firewall Rules, Vulnerability Assessment, Cloud Monitoring, Cloud Detection
Detection & SOC: Splunk, Wazuh, SIEM, Detection Engineering, Security Monitoring, SOC Operations, Incident Triage, Alert Triage, Log Analysis, Security Event Correlation, Anomaly Detection, Threat Detection, False Positive Analysis, Security Analytics
Threat & Frameworks: MITRE ATT&CK, Threat Hunting, Threat Intelligence, IOC Extraction, Malware Analysis, Incident Response, Escalation Procedures, Severity Classification, IDS/IPS, Phishing Analysis, Security Automation
AI & Engineering: Python, Bash, REST API, AWS Boto3, Groq API, Ollama, ChromaDB, FastAPI, Multi-Agent Orchestration, LLM Integration, MCP Protocol, JSON Log Parsing, Automation Scripting
Networking & OS: TCP/IP, DNS, HTTP/S, SSH, Windows Event Logs (4624/4625), Linux Auth Logs, Network Protocol Analysis
Certifications: Fortinet NSE1 & NSE2 (2026), Cisco Intro to Cybersecurity (2026), CCEP — Red Team Leaders (Nov 2025), PCAP: Python Essentials — Cisco (2022)