SANGAMESH GIRISH DANDIN

AI Security Engineer | Vulnerability Research | Automation Tooling | Penetration Testing
(+353) 089-255-9418 | sangameshs2003@gmail.com | Dublin, Ireland
Linkedin | Github | Portfolio

Professional Summary

AI Security Engineer with hands-on experience building automated vulnerability intelligence platforms, malware classification engines, adversarial ML systems, and AI-powered penetration testing tooling. Experienced in CVE analysis, exploit prediction, Active Directory attack chains, phishing simulation, and LLM security. Built and deployed production-ready security tools using FastAPI, Docker, XGBoost, FAISS, and modern cloud infrastructure. Published IEEE author currently pursuing PNPT certification through TCM Security

Technical Skills

Languages:	Python, Bash, JavaScript, SQL
AI & ML:	XGBoost, LightGBM, Random Forest, LSTM, Scikit-learn, PyTorch, TensorFlow, SHAP, FAISS, Sentence Transformers, NLP
Security Tooling:	Nmap, Metasploit, Burp Suite, Wireshark, Shodan, OSINT Frameworks, Impacket, CrackMapExec, BloodHound
Vulnerability Research:	CVE/NVD/CISA KEV Analysis, CVSS Scoring, Exploit Prediction, PoC Generation, OWASP Top 10, SQLi, XSS, CSRF, Prompt Injection Defense, Adversarial ML, Penetration Testing
Data Engineering:	Large-scale CVE Ingestion Pipelines, FAISS Vector Search, REST API Integration, WebSocket Real-time Streaming, Batch Processing
Infrastructure:	Docker, Docker Compose, FastAPI, Flask, React, AWS (EC2, S3, IAM, VPC), Supabase, Vercel, Git, CI/CD
OS & Networking:	Windows PE, Win32 API, Linux Administration, TCP/IP, DNS, HTTP/S, SPF/DKIM/DMARC, Network Protocol Analysis
Active Directory:	Kerberoasting, Pass-the-Hash, BloodHound Enumeration, Active Directory Attack Chains

Security Research & Projects

- **ByteHunter: AI Malware Classification Engine** *Python, LightGBM, XGBoost, SHAP, LIEF, FastAPI, Docker, React*
  - Engineered a 4-model ensemble achieving 89.67% accuracy on EMBER 2018 using a 2,381-dimensional PE feature vector extracted via LIEF covering section entropy, import table, and entry-point heuristics.
  - Developed malware family attribution pipeline using XGBoost on Microsoft BIG-2015 for threat actor classification and campaign tracking across known adversary toolsets.
  - Implemented batch scanning, SHA-256 caching, Win32 API behaviour simulation, and automated forensic PDF report export for high-throughput malware processing pipelines.
- **ZeroTrace AI: Threat Intelligence Platform** *Python, XGBoost, FAISS, Groq, NVD API, CISA KEV, ExploitDB, Docker*
  - Built a full-stack CTI platform ingesting CVE feeds from NVD, CISA KEV, and ExploitDB, aggregating threat data across 3 authoritative sources into a unified risk-ranked intelligence pipeline.
  - Trained XGBoost exploit-prediction model on enriched CVE features including CVSS score, exploit availability, CWE category, and vendor data to rank vulnerabilities by active exploitation likelihood.
  - Integrated FAISS vector search for semantic CVE lookup and Groq NLP summarisation to automate analyst-ready threat narratives and accelerate vulnerability investigation workflows.
- **RedTeam Copilot: AI-Powered Penetration Testing Assistant** *Python, FastAPI, Groq LLM, Nmap, Shodan, NVD API, Supabase, React, Vercel*
  - Developed an agentic red team assistant automating a full recon-to-report pipeline covering OSINT enumeration, Nmap port scanning, NVD CVE matching, and AI-driven security analysis.
  - Integrated Shodan for passive internet-wide recon and pre-engagement footprinting, replicating large-scale network scanning operations used in modern adversary simulations.
  - Generated structured PDF pentest reports with risk matrix, attack chain visualisation, and remediation roadmap, delivering actionable intelligence from raw scan data in a single automated pipeline

- **ZeroInject Shield: Prompt Injection Defence System** *Python, FastAPI, Groq LLaMA, Multi-Agent Consensus, React, Docker*
  - Built a 6-stage zero-trust middleware pipeline intercepting prompt injection attacks, jailbreak attempts, and adversarial inputs targeting LLM-integrated applications.
  - Engineered a multi-agent consensus engine using ensemble LLM voting to reduce false negatives, benchmarked against JailbreakBench for rigorous adversarial evaluation.
  - Designed a zero-trust defensive architecture combining prompt sanitisation, policy enforcement, and multi-agent validation to secure LLM-integrated applications against adversarial inputs
- **SpearSim: AI Phishing Simulation Platform** *PPython, FastAPI, Groq, React, Supabase, SendGrid, Docker, GDPR*
  - Built a GDPR-compliant phishing simulation platform generating LLM-crafted role-targeted emails with real-time click and credential-capture tracking, modelling social engineering TTPs used by real threat actors.
  - Implemented multi-tenant RBAC isolation, signed authorisation PDF generation, and post-phish awareness training modules replicating enterprise security awareness operations
  - Deployed full CI/CD pipeline with Docker, enabling production-grade multi-tenant operation with complete audit logging and campaign analytics dashboard

Professional Experience

Data Science Intern | CodeClause, Remote *2024*
- Developed an Image Caption Generator using CNN-RNN encoder-decoder architecture with TensorFlow and NLP preprocessing pipelines for automated image-to-text generation.
- Built a Loan Status Prediction system across 5 machine learning models with automated preprocessing, feature engineering, and Tkinter-based deployment interface.
- Standardised reusable preprocessing and evaluation pipelines, reducing model experimentation and deployment iteration time across projects.

Vice President | ACM NMIT Student Chapter, Bengaluru *Jan 2024 – Jul 2025*
- Led **10+ technical workshops** and cybersecurity training sessions covering vulnerability research, offensive security, and AI system design for 200+ participants.
- Managed cross-functional student teams and coordinated faculty partnerships to execute semester-long technical programs and security events.
- Organised AI security and adversarial ML research seminars while serving concurrently as Vice Secretary of IEEE CIS NMIT, contributing to 30% chapter membership growth.

Education

MSc in Artificial Intelligence – National College of Ireland, Dublin, Ireland *Jan 2026 – Jan 2027 (Expected)*

B.E. in AI and Data Science – Nitte Meenakshi Institute of Technology, Bengaluru, India *Feb 2023 – Oct 2025 | CGPA: 7.49/10*

Diploma in Computer Science – N.V. Polytechnic College, Kalaburagi, India *Aug 2019 – Aug 2022 | 80%*

Certifications

- **PNPT**: Practical Network Penetration Tester (In Progress) *TCM Security*
- **CompTIA Network+** (N10-008) *CompTIA*
- **AWS Academy Graduate**: Cloud Architecting – EC2, S3, VPC, IAM *Amazon Web Services*
- **Tata Group Cybersecurity Analyst** Job Simulation *Tata Group / Forage*

Publication

AlertSphere: Alerting About Disasters and Ensuring Safety Using AI
Nayana B.P., K.S. Prakruthi, Ananya Rekha Ashok, Sangamesh Girish Dandin, Tanveer Akhlaque Ahmed.
IEEE ICAMIDA 2025, Aurangabad, India DOI: 10.1109/ICAMIDA64673.2025.11209472