Ritika Verma

(669) 499-7975 | Cupertino, CA 95014
ritika.tanwar7@gmail.com | linkedin.com/in/ritikaverma7| github.com/RitikaVerma7 | ritikaverma.tech

Innovative **cybersecurity professional with 7.5+ years** of expertise in securing critical infrastructure and enterprise applications, bringing a blend of traditional security and AI security capabilities. Proven track record of implementing robust security frameworks across diverse industries including enterprise software and technology consulting, while pioneering **AI-driven security solutions** including an offensive security agent for next-generation threat detection. Currently advancing offensive security expertise through **OSWA certification** and pursuing a **master's in information systems (GPA: 3.9/4.0)** with research focus on **AI/ML security** methodologies. Recognized for driving security excellence through deep technical expertise in **MITRE ATT&CK, OWASP Top 10**, and **Infrastructure Security**, complemented by a passion for mentoring next-generation security professionals as **President of the AI Club** at Santa Clara University and **WiCyS mentor**.

EXPERIENCE

Santa Clara University Santa Clara, California
AI Security Research Assistant - Prometheus Lab July 2024 – Dec 2024

- Led comprehensive evaluations of market tools and AI/ML security methodologies, driving the development of an in-depth research paper.

Box, Inc. Cupertino, California
Natural Language Processing (NLP) Intern Jan 2024 – June 2024

- Engineered a recurrent neural network (RNN) with LSTM architecture, achieving 94% precision in classification tasks, enhancing data extraction capabilities from textual content.

SAP Labs Bengaluru, Karnataka
Cyber Security Design Specialist – Security Engineering July 2021 – April 2022

- Enhanced EDR solutions by aligning with product security incident response requirements, resulting in a 20% reduction in mean-time-to-response (MTTR) and stronger product resilience against threats.
- Integrated MITRE ATT&CK framework into the product security lifecycle, improving incident response efficiency by 30%.

SAP Ariba Bengaluru, Karnataka
Security Consultant – Security Operations April 2019 – July 2021

- Operationalized Endpoint Data Loss Prevention (DLP) for 1000+ users, including on-boarding/off-boarding, incident analysis, and investigation to prevent sensitive data disclosure outside the company.
- Managed IAM processes for 3400+ users, ensuring authorized access to the company's production environment.

SAP SuccessFactors Bengaluru, Karnataka
Security Consultant – Compliance Office May 2018 – April 2019

- Conducted 20+ vendor risk assessments, enhancing the vendor onboarding program's alignment with ISO 27001, PCI DSS, and SOC standards.

Accenture Bengaluru, Karnataka
Security Analyst – Security Architecture July 2014 – May 2018

- Developed 10 of 70 security standards for securing infrastructure, collaborating with business units to ensure adherence to controls.

EDUCATION

Santa Clara University, Leavey School of Business Santa Clara, CA
Master of Science in Information Systems April 2025
GPA: 3.9/4.0 (Dean's List)

Visvesvaraya Technological University Bengaluru, Karnataka
Bachelor of Engineering, Computer Science & Engineering June 2014

TECHNICAL SKILLS

- **Security Domain:** Infrastructure Security, Cloud Security, Container Security , DevSecOps , Penetration Testing , Vulnerability Management , Threat Modeling , Detection and Response (XDR), Governance, Risk and Compliance (GRC)
- **AI / ML Development:** Generative AI , Deep Learning , Natural Language Processing (NLP) , RAG , LangChain , LangGraph, LlamaIndex, DSPy , spaCy , RLHF , TensorFlow , PyTorch, Scikit-learn
- **AI/ML Security Frameworks & Tools:** NIST Dioptra , OpenLLMetry , CleverHans , LLM Evaluation , MITRE ATLAS , Shapley Value, OWASP LLM Top 10 , NIST AI RMF

PROFESSIONAL TRAININGS AND CERTIFICATIONS

- OSWA, Offensive Security WEB- 200 – *In Progress*
- Kubernetes, LinkedIn Learning - 2024
- Deep Learning Specialization, DeepLearning.AI - 2024
- Python Programming, Google - 2023
- SANS GIAC 301 Information Security Fundamentals (GISF) - 2017
- CompTIA Security+ - 2015
- ISO LA 27001:2013 Lead Auditor - 2014

PROJECTS

- **Offensive Security AI Agent** (*GitHub*) – Building an AI powered security agent to detect and triage vulnerabilities in configuration files, automating threat detection and response.
- **Mood-Sensitive News AI Agent** (*GitHub*) - Built a personalized chatbot using DSPy framework that filters and delivers news based on user mood, leveraging sentiment analysis and embedding-based relevance ranking.
- **Cybersecurity Compliance and Remediation Automation** (*GitHub)* - Built a Retrieval-Augmented Generation (RAG) system for dynamic security recommendations and vulnerability tracking.
- **Chatbot - RAG with Evaluation** (*GitHub*) **-** Created and evaluated (using LLM evaluation, Llama Index) a Retrieval-Augmented Generation (RAG) powered chatbot designed to answer questions related to auto insurance policies.

LEADERSHIP AND MEMBERSHIPS

- President, AI Club, Santa Clara University
- Member, Women in Cybersecurity (WiCyS), NIST/NICE Cybersecurity Career Ambassador
- WiCyS Mentor, Generative AI Teaching Assistant, and NLP Mentor
- Active participant in cybersecurity CTFs and hackathons