



Ritika Verma

(669) 499-7975 | Cupertino, CA 95014

 ritika.tanwar7@gmail.com |  [linkedin.com/in/ritikaverma7/](https://www.linkedin.com/in/ritikaverma7/) |  github.com/RitikaVerma7 |  ritikaverma.tech

Dynamic cybersecurity professional with over 7.5 years of specialized experience in designing and leading security programs for critical infrastructures and high-stakes products. Skilled in **risk assessment, incident response, IAM, and cloud security**, with expertise in leveraging frameworks like **MITRE ATT&CK, OWASP Top 10, CIS, and NIST**. Currently advancing **offensive security skills** with OSWA certification, CTFs and pursuing a master's in information systems with a focus on **AI/ML security**. Known for embedding robust security measures in AI/ML tech stacks to secure critical infrastructure, I aim to drive innovations in securing AI environments and lead advancements in cyber defense.

EXPERIENCE

- Santa Clara University**
Prometheus Lab - Research Assistant

Santa Clara, California
July 2024 – Present

 - Spearheading comprehensive evaluations of market tools and AI/ML security methodologies, driving the development of an in-depth research paper
- Santa Clara University**
Generative AI - Teaching Assistant

Santa Clara, California
April 2024 – May 2024

 - Orchestrated course administration of a Generative AI, contributing to the enhancement of the educational experience for over 30 students.
- Box, Inc.**
AI / Natural Language Processing (NLP) Intern

Cupertino, California
Jan 2024 – June 2024

 - Developed and implemented a recurrent neural network (RNN) with LSTM architecture, achieving 94% precision in classification tasks, enhancing data extraction capabilities from textual content.
- SAP Labs**
Cyber Security Design Specialist

Bengaluru, Karnataka
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.
 - Implemented and tailored the MITRE ATT&CK framework within the product security lifecycle, significantly improving incident response efficiency by identifying and addressing data source gaps.
- SAP Ariba**
Security Consultant

Bengaluru, Karnataka
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.
 - Triaged approximately 150 incidents per day, reducing false positives by over 70% through policy tuning.
- SAP SuccessFactors**
Security Consultant

Bengaluru, Karnataka
May 2018 – April 2019

 - Conducted over 20 vendor risk assessments, updating the vendor onboarding program to align with industry compliance standards against ISO 27001, PCI DSS, SOC, SOC2 Security Standards.
- Accenture**
Security Analyst

Bengaluru, Karnataka
July 2014 – May 2018

 - Created and managed 10 out of 70 security standards for Securing Infrastructure, involving industry analysis and collaboration with affected business units, for ensuring adherence to the security controls.
 - Spearheaded compliance and governance effort for the team, regular updates to the tool and training the team for using the tool efficiently.

EDUCATION

- Santa Clara University, Leavey School of Business**
Master of Science in Information Systems
GPA: 3.9/4.0 (Dean's List: Spring 2024)

Santa Clara, CA
April 2025
- Visvesvaraya Technological University**
Bachelor of Engineering, Computer Science & Engineering

Bengaluru, Karnataka
June 2014

TECHNICAL SKILLS

Security Domain

- ❖ Infrastructure Security
- ❖ OWASP Top 10
- ❖ Incident Response
- ❖ DevSecOps
- ❖ Penetration Testing
- ❖ MITRE ATT&CK
- ❖ Cloud Security
- ❖ Vulnerability Management
- ❖ Risk Assessment
- ❖ Container Security
- ❖ Threat Modeling
- ❖ Compliance

Security Frameworks & Tools

- ❖ McAfee DLP
- ❖ PhishMe
- ❖ CIS Benchmark
- ❖ Splunk
- ❖ Rapid7
- ❖ PyTM
- ❖ Tanium
- ❖ Qualys
- ❖ Inspec
- ❖ Kali Linux
- ❖ NIST
- ❖ BurpSuite

AI / ML Tech Stack

- ❖ Generative AI
- ❖ LLM Evaluation
- ❖ Neural Networks
- ❖ Topic Modelling
- ❖ Natural Language Processing
- ❖ LangChain
- ❖ Deep Learning
- ❖ RAG

AI/ML Security Frameworks & Tools

- ❖ NIST Dioptra
- ❖ OpenLLMetry
- ❖ CleverHans
- ❖ SecML

PROFESSIONAL TRAININGS AND CERTIFICATIONS

- OSWA, Offensive Security WEB- 200 (ongoing) 2024
- Kubernetes, LinkedIn Learning 2024
- Deep Learning Specialization, DeepLearning.AI 2024
- Python Programming, Google 2023
- SANS GIAC 301 Information Security Fundamentals (GISF) 2017
- Administering Microsoft SQL Server 2012/2014 Databases 2016
- CompTIA Security+ 2015
- ISO LA 27001:2013 Lead Auditor 2014

PROJECTS

- **Cybersecurity Compliance and Remediation Automation** ([GitHub](#)) - Developed a local Retrieval-Augmented Generation (RAG), providing dynamic cybersecurity recommendations and detailed remediation plans for security vulnerabilities.
- **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.
- **Lease Recommendation Application Generator** ([GitHub](#)) - Engineered a custom application using OpenAI embeddings, resulting in a personalized relocation service platform for tailored suggestions.
- **Skincare Recommendation & Pricing System** ([GitHub](#)) - Developed a sophisticated ML-driven system for skincare recommendation and price forecasting, achieving 85% score for classification.

ADDITIONAL INFORMATION

Leadership Experience: President of AI Club at Santa Clara University; event organizer for internal corporate events; budget management.

Professional Memberships: Member of Women in Cybersecurity (WiCyS), NIST/ NICE Cybersecurity Career Ambassador

CTF Experience: Actively participates in Pacific Hacker's CTF challenges

Mentorship Experience: WiCyS mentor, Generative AI mentor, providing guidance to students AI/ML projects; mentor for Company's new joiners.

Community Involvement: Monthly contributor to a children's education center from 2018 to 2022.