# Vedant Bhalerao

**Cell:** +1 227-275-1300 | **Email:** vedantbhalerao315@gmail.com | **LinkedIn**: linkedin.com/in/vedantb31/ | **Website:** vedantbhalerao.com | Willing to Relocate

## EDUCATION

**University of Maryland, College Park, MD, United States** *May 2027 (Expected)*
Master of Engineering in Cybersecurity
*Relevant Coursework – Hacking of C programs and Unix Binaries, Security Tools for Information Security, Cloud Security.*

**Vellore Institute of Technology, Vellore, Tamil Nadu, India** *May 2025*
Bachelor of Technology in Computer Science and Engineering with **Specialization in Information Security**, **CGPA: 9.13/10**
*Relevant Coursework – Cryptography and Network Security, Information Security Management, Data Privacy, Malware Analysis, Web Application Security, Penetration Testing and Vulnerability Analysis, Digital Forensics.*

## TECHNICAL SKILLS

**Programming Languages –** Python (Automation & Scripting), Java, C/C++, Bash, PowerShell
**Tools** – Burp Suite, OWASP ZAP, Metasploit, Wireshark, Nmap, Nessus, OpenSSL, Microsoft Office Suite (Word, Excel, PowerPoint)
**Cloud & DevOps** – AWS (EC2, IAM, S3, VPC, CloudTrail, Lambda), Azure, GCP, Docker, Kubernetes, Git, Linux, Windows Server
**Security Frameworks** – NIST CSF, OWASP Top 10, MITRE ATT&CK, CIS Benchmarks, ISO 27001
**Interests** – Risk Assessment, Secure Software Development, Cloud Security, DevSecOps, Threat Modeling, Vulnerability Management, Red Teaming

## WORK EXPERIENCE

**Security Software Developer Intern, IoTian Technologies Pvt. Ltd, Pune, India** *Jan 2025 – June 2025*
- Conducted **secure code reviews and remediation** using **Python and C/C++**, identifying and fixing **20+ application and access-control flaws**, reducing exposure to **OWASP Top 10** vulnerabilities impacting confidentiality and integrity.
- Performed threat modeling and application security testing across multiple feature releases, evaluating **security architecture, authorization flows, and cryptographic usage** to detect risks early in the SDLC.
- Supported **on-premises to AWS migration** by configuring and validating workloads across **EC2, VPC, S3, IAM, Lambda, DynamoDB**, ensuring secure access control and reliable cloud operation.

**Information Security Intern, Larsen & Toubro Financial Services Pvt. Ltd, Mumbai, India** *Aug 2023 – Oct 2023*
- Conducted and reported **CIS Benchmark** compliance assessments for **100+ RHEL 7 and RHEL 8** systems across **UAT and Production environments**, supporting remediation efforts and reducing configuration-based security risks.
- Collaborated with a VAPT team to perform **penetration testing** on LTFS customer web applications and internal mobile platforms, uncovering vulnerabilities including IDOR, authentication bypass, and improper input validation, leading to a **30% reduction** in exploitable attack surface.
- Created developer-friendly **Proof of Concept (PoC)** reports in **Jira** for **web, API, and mobile application** vulnerabilities, clearly documenting reproduction steps, impact, and remediation guidance to enable efficient fixes by development teams.

## CERTIFICATION

- Certified Ethical Hacker (CEH v12)
- AWS Cloud Practitioner
- QRadar SIEM Foundation
- Google Cloud Computing
- CompTIA Security+ (Pursuing)

## PROJECTS

**Cloud-Based Security Operations Center Development, AWS**
- Architected a cloud-native SOC using Security Onion with integrated CloudTrail, GuardDuty, and VPC Flow Logs for real-time detection of **10+ simulated attack scenarios**.
- Implemented least-privilege IAM, VPC segmentation, KMS encryption, and hardened access policies to strengthen monitoring security and ensure high availability.
- Built automated alerting and response workflows **reducing manual investigation time by over 30%**.

**AI-Enabled Incident Response Automation, Azure**
- Deployed and configured Microsoft Sentinel (SIEM) on Azure Cloud, implementing custom KQL analytics rules and automation playbooks to strengthen real-time threat detection and incident response.
- Integrated AI-driven incident response automation using LLM's within the SIEM framework, enabling intelligent triage, analysis, and **cutting false positives during simulations**.
- Enhanced overall security posture by enforcing role-based access controls, optimizing AI performance for contextual insights, and streamlining response workflows through automated incident handling.

## ACTIVITIES

- Ranked in **Top 1%** on TryHackMe.
- Publish **technical blogs** on Cyber Security and Penetration Testing on Medium, contributing to the global security community. – medium.com
- Solved **100+ CTF and exploit lab challenges** focused on real world vulnerability classes and attack techniques.