

Vedant Bhalerao

Cell: +1 227-275-1300 | Email: vedantbhalerao315@gmail.com | LinkedIn: <https://www.linkedin.com/in/vedantb31/> | 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, Java, C/C++, Bash, PowerShell

Security Tools – Nmap, Wireshark, Metasploit, Burp Suite, OpenSSL, QRadar SIEM, Microsoft Sentinel, CrowdStrike, Tenable Nessus

Fields of Interest – Cloud Security, DevSecOps, Application Security, Incident Response, Threat Modelling, Endpoint Security, Penetration Testing, Vulnerability Remediation, Code Reviews

Web Technologies – HTML5, JavaScript, Tailwind CSS, Node.js, React JS, MongoDB

Cloud, Systems & Tools – AWS (EC2, Lambda, S3, IAM, CloudTrail, VPC), Azure, Docker, Kubernetes, Linux (Ubuntu, Kali), Windows Server, Mac, Microsoft Office Suite (Excel, Word, PowerPoint, Power BI), Git

Security Frameworks and Standards – MITRE ATT&CK, NIST, CIS Benchmarks, ISO 27001, SOX, GDPR, SOC2, OWASP Top 10

WORK EXPERIENCE

Security Software Developer Intern, IoTian Technologies, Pune, India

Jan 2025 – June 2025

- Collaborated with cross-functional teams to design and enhance secure access control mechanisms in medical embedded software using Qt QML and C++, improving resilience against threats.
- Performed detailed code reviews of the medical embedded software to identify security flaws, enforce secure coding practices, and ensure compliance with internal and industry cybersecurity standards.
- Supported the implementation of secure cloud-based infrastructure for embedded systems on AWS, leveraging IAM, VPC, CloudTrail, Security Groups, and KMS, which ensured compliance and improved data protection.

Information Security Intern, Larsen & Toubro Financial Services, Mumbai, India

Aug 2023 – Oct 2023

- Collaborated with testers and developers to streamline vulnerability remediation using Tenable Nessus, reducing OWASP Top 10 risks.
- Delivered clear security assessment reports and CIS Benchmark reviews to stakeholders, enabling compliance improvements across RHEL systems.
- Worked in a team to conduct penetration testing on web and mobile applications, identifying and presenting high-impact vulnerabilities that reduced potential attack surface by 40%.

CERTIFICATIONS

Certified Ethical Hacker (CEH v12) | AWS Cloud Practitioner | QRadar SIEM Foundation | Google Cloud Computing | OSCP (Pursuing)

PROJECTS

Cloud-Based Security Operations Center Development, AWS

- Developed a cloud-based Security Operations Center (SOC) on AWS using Security Onion for real-time threat detection, log analysis, and incident response automation.
- Strengthened cloud security posture by implementing IAM-based access controls, optimizing system performance, and ensuring high availability of monitoring infrastructure.
- Integrated AWS CloudTrail and VPC Flow Logs to improve threat visibility, accelerate response workflows, and enable comprehensive audit and compliance tracking.

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 remediation of cybersecurity events across cloud environments.
- 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](https://medium.com/@vedantb31/)
- Placed in the Top 10 among 90 participants at the Cyberchaze CTF competition organized by Schneider Electric.