Venkatesh Yerram

venky.y1997@gmail.com | +1 704-345-0538 | LinkedIn | TryHackMe | LetsDefend

SUMMARY:

Security Analyst with over 5 year of experience in cybersecurity frameworks, tools & incident response Architected secure solutions for insurance companies, developed intricate breach simulations.

PROFESSIONAL EXPERIENCE:

IT Security Intern | *UNCC* **Aug 2022 - May 2023**

- TA for Secure program and penetration testing collaborated with the professor to develop 10+ course materials.
- Tutored the concepts on Network Security (Traceroute, DNS, Routing), Risk Analysis, Cyber defense, and OWASP Top 10.
- Developed 10+ Semgrep scripts while conducting research and designed 4+ assignments to perform code reviews.

Information Security Analyst | iAssist Innovations labs **Apr 2020 - Dec 2021**

- Conducted vulnerability assessments including vulnerability scanning (using SAST/DAST tools) and penetration tests on 10+ applications following OWASP framework and provided mitigation techniques for 50+ vulnerabilities.
- Developed 10+ Rest APIs to manage microservices for applications resulting in reduction of code redundancy by 50%.
- Collaborated with stakeholders & 5 developer teams to remediate, prioritize fixes & guidance on secure coding practices.
- Secured the server architecture by introducing secure authentication capabilities (SSO, Token-Based, Two Factor, Multi Factor), access control technique, safely protected 10+ applications.
- Developed an adaptable insurance claim automation for 20 hospitals, adopted by 500+ hospitals with 0% code change.
- Implemented secure CI/CD pipelines, automated SAST solutions, and reduced deployment time by 80%.
- Conducted regular assessments of TCP/IP protocol stack solutions, identified areas for improvement, and implemented changes to enhance network performance and security.

Technical Analyst | *Manomay consultancy services* **Nov 2017 - Mar 2020**

- Developed backend and led the product development team resulting in project delivery within 50% of expected timeline.
- Designed and Developed ETL pipeline in python, launched application, configured, revamped the database, utilizing NoSQL database instead of SQL improving the query response time by 40%
- Aided in designing 5+ application architectures and implemented security measures for the applications.
- Managed security of cloud infrastructure by creating and maintaining firewalls, Routing, switching for 5+ apps

CYBERSECURITY PROJECTS AND LABS:

SOC Lab:

- Designed a virtual home lab network with 1 AD & 5 systems to test vulnerabilities and practice threat detection.
- Deployed ELK stack (SIEM), Snort(IDS/IPS), Hive, Cortex automation and MISP environment to simulate a small enterprise network.
- Simulated a breach on network with offensive & defensive tactics for adversary emulation & incident response practices.

Security Incident and Event Management with Splunk:

- Implemented Splunk search on 100,000 events to practice simple, complex filtering and advanced search syntax.
- Scheduled 20+ reports to detect errors within specified time frames, triggering email notifications for prompt action.
- Constructed informative dashboards and configured alerts with throttling & Slack integration for real-time notifications.

TECHNICAL KNOWLEDGE:

Programming Languages: Python, C#, Java/J2EE, SQL, Shell scripting, PowerShell.

Cybersecurity Frameworks: NIST, Cyber Kill Chain, MITRE ATT&CK, Pyramid of Pain, PCI-DSS, HIPPA.

Tools: Splunk, Nessus, Nmap**,** Burpsuite**,** Metasploit, Curl, Dirb, Gobuster, Sublist3r, Hydra, John-the-Ripper, Wireshark, Snort firewall, Autopsy, Registry Explorer, FTK, GitLab, Github

Cloud & Operating Systems: GCP, Azure, AWS Dynamo DB, AWS S3, Cloudwatch, Microsoft Windows, Linux, MacOS.

Certifications:

- SOC Level 1 & Offensive Pentesting – TryHackMe, CompTIA A+, CompTIA Security+ (Ongoing)

Education:

University of North Carolina at Charlotte: Master of Science in Cyber Security **Jan 2022 - May 2023**