Venkatesh Yerram

venkateshyerram6@gmail.com | +1 704-345-0538 | Charlotte, NC | LinkedIn | TryHackMe | LetsDefend | Portfolio

SUMMARY:

Security Analyst with over 5 years of experience in cybersecurity frameworks & tools, Incident Response, Malware Analysis. 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, Compliance, Incident management, 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 assessment including vulnerability scanning (using SAST/DAST tools) and penetration tests on 10+ applications following OWASP framework and provided remediation for 50+ vulnerabilities.
- Investigated and responded to security incidents including monitoring and triaging security alerts and alerts in a timely manner.
- 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 like Checkmarx, Semgrep and reduced deployment time by 80%.

Security Software Engineer | *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

PROJECTS AND LABS:

SOC Analyst Pathway Project | Let's Defend Platform:

- Analyzed over 65 Incident alerts varying from Malware, Web app based, Email exchanges, and Proxy to find root cause and figure out Indicators of compromise, root causes, suspicious activities and Threat Indicators.
- Triaged tickets by following established runbooks, playbooks and standard procedures to analyze alerts and deduce positive issues.
- Implemented effective response actions for true positive alerts and escalated security incidents to IR teams while promptly closing false positive alerts with detailed explanations along with attack vectors. And, escalate any true positive alerts

Security Incident Response 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.

Malware Analysis:

- Constructed a sandbox VM with Process Hacker, Process Monitor, Wireshark, and Regshot tools for malware analysis. Employed malware analysis platforms VirusTotal, Any.run, hybrid-analysis & FileScan to gather additional TTP's.
- Created a report after analyzing 7 different malware, to provide recommendations for improved application security.

TECHNICAL KNOWLEDGE:

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

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

Tools: SIEM - Splunk, SOAR, Nessus, Burp Suite, WireShark, Metasploit, Digital Forensic tools - FTK, Autopsy, Nmap, API testing tool - Postman, IDS/IPS, Endpoint Detection and Response (EDR)tools, Web Content Filtering, SAST/DAST tools, Network Intrusion Detection, Packet Analysis, Computer Forensics, Information Risk Management, Cyber Threat Intelligence, Malware Detection and Prevention, DLP, CTI, Checkmarx

Network Security: Network protocols and troubleshooting: TCP/IP, OSI, Routing, Switching, Proxies, WAF, DNS, Firewalls - policies, rules; topologies - LAN/WAN, traceroute, iperf, dig, cURL, ARP, tcpdump, nslookup,whois; securing network perimeter; PCAP analysis.

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+

Education:

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