SAHIL VAKKANI

+91 7775850473| https://www.linkedin.com/in/sahil-vakkani-0b1722192/ |sgvakkani1130@gmail.com

EDUCATION

Maharashtra Institute of Technology - World Peace University **Pune, India**
Bachelor of Technology – Computer Science & Engineering - CGPA: 9.24/10 May 2019 - June 2023
Coursework: Cybersecurity, Operating Systems, Networking, Data structures and Algorithms, Object-Oriented Programming, Big Data Analytics, Artificial Intelligence, and Internet of Things (IoT).

SKILLS

Technical Skills: Static and Dynamic Analysis, Reverse-Engineering, VAPT, Reconnaissance
Tools: Microsoft SysInternal tools, Oly-Debugger, WIRESHARK, Packet Trace, DNSpy, x32dbg.
Languages: Java, Python, XML, C, C++, HTML, CSS, JavaScript, SQL.
Soft Skills: Leadership, Communication, Teamwork, Curiosity, Decision making, Critical Thinking, Problem Solving.

WORK EXPERIENCE

LTIMindtree **Pune, India**
Malware Researcher **August 2023-Present**

- Monitored and responded to security events/incidents for clients in a **24 by 7 environment**.
- Identify and use tools and techniques to conduct **static** and **dynamic analysis** of malware, including building a lab environment
- Deep working knowledge of **networking concepts** and **protocols**, **OS hardening**, and **cloud security fundamentals.**
- Worked closely with security teams to strengthen overall cybersecurity posture and **reduce security risks.**
- Monitored and removed various **types of malware** infection including **Spyware**, **Ransomware**, **Adware**, **Trojan viruses,** Potentially Unwanted application (**PUA**)from client machines.
- Accomplished **100% accuracy** in evaluating and classifying samples given by clients, guaranteeing accurate analysis, and upholding high standards of quality.
- Performed **root cause analysis** of security breaches and recommended **corrective** and **preventive** actions.
- Understanding regulations, risk assessment, and organizational security policies.

Olyphaunt Solutions **Pune, India**
IOT Engineer **July 2022- September 2022**

- Worked on **a smart room monitoring device** to track temperature, oxygen, CO_2, and additional health parameters, transmitting real-time data to a centralized dashboard at specified intervals.
- Implemented **secure MQTTs communication** protocol, ensuring encrypted data transmission by coding, and configuring secure channels for IoT devices.

ACADEMIC PROJECTS

SIEM-Based Log Analysis & Incident Response Simulation **Machine Learning Project**

- Performed SOC-style log monitoring using Splunk by configuring custom correlation rules, detecting abnormal login attempts, and generating incident reports with mitigation recommendations.
- Create correlation rules and alert triggers
- Analyzed Windows event logs and developed dashboards to track failed authentication anomalies and lateral movement indicators using SPL queries.

File Integrity Monitoring & Malware Indicator Detection

- Implemented file integrity monitoring in Wazuh to detect unauthorized system file modifications and automated alert response workflows.

ACCOMPLISHMENTS

Employee of the Month (x2) – Awarded for 100% accuracy in high-priority malware classifications, creating documentation on new malware campaigns, and leading knowledge-sharing sessions to enhance team skills.
Authored detailed write-ups on malware **campaigns** and contributed research that improved internal threat intelligence and automated classification processes.

CERTIFICATIONS

- **CompTIA Security +**
- **Python Programming (Udemy)**
- **Microsoft Power BI Desktop for Business Intelligence Management (Udemy)**
- **AWS Identity and Access Management (IAM) Foundations (Udemy)**