ABISHEAK SANKAR SUBRAMANIAN

+91 7339198016
abiedupersonal.99@gmail.com
linkedin.com/in/abisheak-sankar-subramanian

PROFESSIONAL SUMMARY

Cloud-focused SOC Analyst with a year of hands-on experience in Security Operations, detection engineering, and cloud security monitoring. Skilled in managing SIEM platforms (Splunk, Wazuh), triaging alerts, fine-tuning detection rules, and investigating incidents. Proficient in scripting (Python) and automation to support threat detection and reporting. Familiar with AWS, Azure and GCP security best practices, IAM risk identification, and DevSecOps pipelines. Adept at using tools like Zeek, Wireshark, and TheHive. Strong foundation in MITRE ATT&CK, NIST CSF, and threat intel ingestion.

EXPERIENCE

SECURITY ANALYST INTERN| SOC Level 1 (Training-Based) | Remote
April 2024 – Present

TUTELR INFOSEC Bangalore, India

- Monitored alerts using Wazuh and Splunk, triaging incidents and escalating based on severity.
- Investigated cloud security events from AWS/GCP CloudTrail, WAFs, and Kubernetes audit logs.
- Wrote Python scripts for log enrichment and alert notifications.
- Assisted in developing and updating detection rules aligned with MITRE ATT&CK.
- Supported DevOps teams in identifying IAM, storage, and network misconfigurations.
- Participated in daily reporting and false-positive trend analysis.

SOFTWARE DEVELOPER INTERN
December 2019 to January 2020

TECHCITI TECHNOLOGIES PRIVATE LIMITED | Bangalore, India

- Collaborated with senior developers in designing and implementing features for software applications, contributing to project milestones.
- Actively participated in code reviews, ensuring adherence to best practices and maintaining code quality.
- Conducted research and implemented innovative tools or frameworks to optimise application performance and efficiency.

SOFTWARE DEVELOPER INTERN
November 2018 to December 2018

REFINEMENT SOFTWARE SOLUTIONS PVT LTD | Coimbatore, India

- Assisted in the testing and debugging process, ensuring the delivery of high-quality, bug-free software to clients.
- Contributed to the creation of technical documentation, providing valuable insights for future software development projects.
- Demonstrated strong problem-solving and analytical skills while working on complex coding challenges, delivering efficient and scalable solutions.

EDUCATION

MSc Information Security
Royal Holloway, University of London, Surrey | 2023
Classification: - **Merit**
Dissertation - Survey on Machine Learning Techniques for Malware Detection

Bachelor of Engineering in Computer Science
Sri Ramakrishna Institute of Technology, Coimbatore | 2021
Graduated with **CGPA- 7.2**
Dissertation - Brain Tumor Detection and Classification using Deep Learning Techniques based on MRI Images

CERTIFICATION

CompTIA A+
Issued by CompTIA | [December, 2023]
Validated skills in hardware, networking, mobile devices, and IT troubleshooting.

Cloud Computing
Issued by NPTEL | [February, 2020]
Covered cloud service models, virtualisation, scalability, cloud storage, and security essentials.

SKILLS

- **SIEM & Monitoring**: Splunk, Wazuh, Zeek, Wireshark, NetworkMiner, Brim
- **Cloud Platforms**: AWS, Azure, GCP, Kubernetes
- **Security Tools**: Snort, Autopsy, Redline, KAPE, Volatility, Velociraptor, TheHive Project
- **Scripting**: Python, Bash (Basic Familiarity)
- **Frameworks**: MITRE ATT&CK, NIST CSF, SEF
- **DevOps**: Jenkins, GitHub Actions (Basic Familiarity)
- **Languages**: C, C++, Java, Python, HTML
- **Others**: MS Office, Data Visualization, Feature Engineering

PROJECT HIGHLIGHT

- **Threat Detection Lab (THM Based)**: Simulated and detected attack scenarios; created custom detection logic.
- **Cloud Security Assessment**: Identified IAM and network misconfigurations on AWS, Azure and GCP sandboxes.

SOFT SKILLS

- Proactive Incident Triage | Documentation | Team Collaboration
- Detail-Oriented | Swift Learner | Strong Analytical Thinking