Anurag Dadhich
Cybersecurity Analyst
India | +91 9549550096 | anuragdadhich78@gmail.com | Portfolio

Summary

SOC Automation & Security Operations Analyst with expertise in ITIL-based procedures, monitoring, and incident response in round-the-clock settings. Competent in creating dashboards and reports for data visualization, integrating REST APIs, and creating Python-based automations. Practical experience with SIEM principles (logs, alerts, incidents), Workflows for incident management and SOAR playbooks.

Core Skills

SIEM: Splunk, IBM QRadar, Microsoft Sentinel
EDR/XDR: Microsoft Defender, Cortex XDR
Vulnerability Management: Nessus, Qualys, Metasploit
Networking: Cisco Routers, Checkpoint Firewall, VPNs
Programming: Python, Bash, SQL
Security Practices: Incident Response, Threat Hunting, Malware Analysis

Experience

Security Analyst L1 – COMNET Innovations (Dec 2024–Aug 2025)

- Monitored and analyzed security events using Azure Sentinel, identifying and responding to potential threats in real-time.
- Built and tuned Kusto Query Language (KQL) queries to improve detection accuracy and reduce false positives.
- Investigated security incidents such as phishing, malware, suspicious logins, and lateral movement across hybrid environments (Azure + on-prem).
- Created and managed analytics rules, workbooks, and playbooks in Azure
- Collaborated with Tier 2/3 teams to escalate high-severity incidents and improve threat detection.

Education

PG Diploma in Cyber Security & Forensics (PG-DCSF) – C-DAC Trivandrum (Feb 2025 – Aug 2025)
B.Tech in Computer Science & Engineering – JECRC (2020 – 2024) | CGPA: 7.8

Projects | GitHub

- **Incident Response Framework:** Automated alert classification & response using Microsoft Sentinel.
- **Threat Hunting:** Detected anomalies using KQL and SPL queries and IOC correlation.
- **Malware Analysis:** Conducted static and dynamic analysis with PEStudio, Detect It Easy, and Cuckoo Sandbox.
- **Phishing Investigation:** Implemented real-time phishing detection using open-source threat Intel platforms.

Certifications

- CCNA | CyberOps Associate | Cybersecurity Essentials (Cisco)
- Microsoft Azure Fundamentals (SC-900, AZ-900)
- Practical Cybersecurity & Threat Intelligence (EC-Council)
- Ethical Hacking (Udemy)

Achievements

- Participated in **HTB CTF** and **Advent of Cyber**.
- Rooted vulnerable machines on **VulnHub** and solved advanced challenges.