TUSHAR CHANGAN

tusharchangan2001@gmail.com | +91-8587018151 | linkedin.com/in/tusharchangan/

Cybersecurity professional with 1+ years of experience in security operations, specializing in threat monitoring, incident response and log analysis. Proficient in Security Information and Event Management (SIEM) tools like Microsoft Sentinel and Splunk, with hands on experience in SOAR, EDR, WAF, Antivirus, and vulnerability assessment. Strong understanding of SOC workflows, playbooks, SLAs, and incident escalation. Skilled in using OSINT investigation, MITRE ATT&CK mapping, and ticketing platforms. Exposure to cloud security and basic malware analysis.

Education

Krishna Engineering College, AKTU **2019 - 2023**

- B.Tech, Computer Science and Engineering-CGPA: 8.36

Greenway Modern School, India **2017 - 2019**

- *CBSE (Class XII)- Aggregate:* 82.4%

Tools and Technologies

Microsoft Defender, CrowdStrike, Microsoft Sentinel, Splunk Enterprise, Abnormal Security, Palo Alto Networks, Vulnerability Assessment, Nessus, Cisco Talos, Virus Total, IP Lookup, Abuse IPDB, Mx Toolbox, WAF, EDR, SOAR, SIEM, Phishing email analysis, Malware Analysis, Log Analysis, Cloud Security, Security monitoring, Application security, Threat Analysis

Work Experience

TCS | Cyber Security Analyst **May'24 - Present**

- Investigated **over 200 security alerts weekly** using SIEM tools, integrating threat intelligence and detailed log analysis to identify and triage potential incidents.
- Collaborated with cross-functional teams to mitigate **critical vulnerabilities**, reducing average incident response time by **30%**.
- Conducted root cause analysis for **major security breaches**, producing detailed reports and recommending remediation steps that improved system resilience by **25%**.
- Streamlined incident escalation process by creating **detailed documentation for 10 common false positives,** reducing the volume **of Level 2 escalations by 15%** and enabling quicker resolution times.
- Prepared 10+ detailed **shift handover reports weekly** and participated in **15+ bridge calls monthly** to support real time incident response and ensured proper incident escalation and continuity.

Nagarro | Associate Software Engineer Intern **Mar'23 - Oct'23**

- Developed and deployed **5+ enterprise web applications** using ASP.NET MVC, C#, and Web API with SQL Server, serving **hundreds of end users** across departments.
- Ensured responsive and accessible UIs using Bootstrap, Angular CLI, and Angular Material, resulting in **40% improvement in user satisfaction scores** (based on internal surveys).
- Created and optimized **complex SQL queries, stored procedures, functions, and views**, improving database performance by **35%**.

Projects

Object Detection using Machine Learning

- Developed an object detection model using NumPy, OpenCV, and Anaconda to classify and display items based on trained dataset.
- Applied supervised learning for object classification.

The British Council Project

- Worked in a simulated 24/7 SOC environment to monitor, analyze, and respond to security incidents using Microsoft Sentinel, Splunk, CrowdStrike and Abnormal Security.
- Conducted threat hunting, log correlation, and incident documentation to enhance incident response.

Certificates

- NPTEL: Developing Soft Skills and Personality
- Microsoft Certified: Azure Fundamentals (AZ-900)
- TCS iON: IT Security Foundations