Tanvi Giri

Security Analyst

Proactive SOC Analyst with 2 years of hands-on experience in monitoring, detecting, and mitigating security threats. Skilled in analyzing alerts, identifying vulnerabilities, and implementing swift incident responses to safeguard critical systems. Adept at leveraging advanced security tools to ensure robust defense against evolving cyber threats.

✉ tanvigiri0@gmail.com   📱 9511649227   📍 Baner, Pune, India

WORK EXPERIENCE

Security Analyst

Security HQ

01/2023 - 01/2025

Roles and Responsibilities

- SOC Analyst with 2 years of hands-on experience in cybersecurity operations,specializing in real time threat detection and incident response.
- Monitor security offenses and alarms in the QRADAR SIEM tool in real time. Create incidents for true positive alerts, providing proper recommendations and escalating to clients through the ticketing tool.
- We monitor firewall traffic for any port scans, port sweep and suspicious activity,identifying anomalies triggered by Web attack signatures
- Analyze suspicious, phishing related emails and take necessary action using email gateways: Darktrace Antigena email, O365defender, and Mimecast consoles.
- Analyse threats and malware related offenses, correlating them with advanced tools such as Crowdstrike sentinelOne, and O365 Defender.
- Understanding of TCP/IP networking fundamentals: ports, protocols, and infrastructure details along with knowledge of the cyber threats, exploits and vulnerabilities.
- *Identified and fine-tuned false positive alerts and detection rules to enhance SOC efficiency and reduce alert fatigue.*
- Monitor security events and alerts using Azure Sentinel to detect and respond to suspicious activity across the enterprise.
- Good at maintaining all the quality parameters and procedures defined in the SLA.
- Worked on mapping security incidents to MITRE ATT&CK techniques to enhance threat detection and response.

EDUCATION

Bachelors of forensic science and cyber security

Peoples college of forensic science and cyber security (Aurangabad)

07/2018 - 03/2021 *Aurangabad, 431154*

Intermediate PCB

Shri Gajanan maharaj Jr college shegaon, maharashtra

07/2015 - 03/2017 *Shegaon maharashtra, 444203*

SKILLS

- Incident Response
- Monitoring SIEM: IBM Q-Radar Azure Sentinel (KQL Query)
- Endpoint Security: Crowd Strike, Sentinel One, MS Defender
- Email Gateway: Mimecast, proofpoint
- NDR: Darktrace Antigena
- Analysis Tools: Virus Total, Triage, IBM X-ForceExchange Censys, Sandboxing

CERTIFICATIONS

CEH EC Council and CCNA from Sysap Technologies,Pune (08/2022)

Various certificates achieved on Udemy Platform CompTIA Network+, CompTIA security+,Active Directory on Windows Server, Cyber security from beginner to expert etc

LANGUAGES

Marathi (Native)
Full Professional Proficiency

Hindi
Full Professional Proficiency

English
Full Professional Proficiency

INTERESTS

Singing   Travelling   Cooking