CONTACT

☎ 9166228586

✉ rahulkharod1177@gmail.com

📍 Ahmedabad Gujrat

🌐 linkedin.com/in/rahul-kharod09

EDUCATION

RAJASTHAN TECHNICAL UNIVERSITY,KOTA

- B.Tech - Electronics Instumentaion & Control Engineering

SKILLS

- Sporact (SOAR), Service Now - Ticketing Tools
- SIEM (ESDL,Splunk), XDR and EDR (Trendmicro)
- Cloud One Workload Security (C1WS) – Cloud Security
- TM Cloud App Security – Email Security
- Security Tools: Firewall, IDS/IPS
- Log Analysis
- Risk Assessment and Mitigation
- Incident Management
- Phishing Email Analysis

LANGUAGES

- English
- Hindi

RAHUL

SECURITY ANALYST

CAREER OBJECTIVE

- To secure a position and be a part of progressive organization that gives scope to enhance my knowledge and skills, which can be used for the organizational growth and personal growth and contribute to the organization success.

WORK EXPERIENCE

EVENTUS SECURITY PVT LTD

SECURITY ANALYST L1

04th of Sep - 2023 -Present

- Monitor network traffic and security logs using SIEM tools (Cyberal, ESDL) to detect and respond to security incidents in real-time.
- Monitoring, maintaining, and troubleshooting of EDR and XDR services.
- Analyze logs from IDS, firewalls, and security appliances to identify potential threats and escalate incidents as needed.
- Investigate false positive alerts and collaborate with the team to fine-tune detection logic.
- Analyze security logs, telemetry data, and threat intelligence feeds (IOCs) to detect anomalous activities or compromises.
- Utilize OSINT tools (VirusTotal, Browserling, IBM X-Force) for threat verification and malware analysis tools for IOC extraction and sandboxing.
- Ensure timely investigation and remediation of security incidents as per SLA guidelines.
- Implement allow/block actions on IOCs based on client requirements and investigation outcomes.
- Maintain security documentation, including incident reports, analysis findings, and mitigation efforts for compliance.
- Deliver weekly/monthly reports to clients, enhancing their security posture.
- Monitor and manage security product licenses and infrastructure health on TM Vision One.
- Participate in client meetings with L2 analysts to discuss raised incidents and security improvements.
- Work in a 24x7 rotational shift environment, handling incident escalations.

CERTIFICATION

- TryHackMe SOC Level: 01
- TryHackMe SOC Level: 02
- SOC Experts Certified Security Analyst
- Trend Micro Certifications
- AttackIQ Foundations of Operationalizing MITRE ATT&CK