Udhayakumar m

**SOC Analyst**

Phone NO: 8098731040

Email: [udhayakumarm1999@gmail.com](mailto:udhayakumarm1999@gmail.com)

LinkedIn: <https://www.linkedin.com/in/udhayakumar-m-97a028268/>

Portfolio: <https://udhayakumar2212.github.io/portfolio/>

Rajapalayam

**Summary**

Dedicated and detail-oriented SOC Analyst with 3 years of experience in cyber threat detection, analysis, and incident response. Skilled in SIEM solutions (Sentinel), threat intelligence, and network security monitoring. Proven ability to triage, investigate, and mitigate cybersecurity incidents. Adept at working in 24/7 SOC environments, collaborating with cross-functional teams, and implementing security best practices. Seeking to leverage my expertise to strengthen an organization’s cyber defence strategy.

**Roles & Responsibility**

* Monitored and analyzed security events using Sentinel, responding to over 500 security alerts monthly.
* Investigated phishing campaigns, malware infections, and insider threats, reducing security risks by 30%.
* Performed log analysis and threat hunting using SIEM tools, identifying zero-day vulnerabilities.
* Developed custom detection rules in Sentinel to enhance threat visibility and improve SOC efficiency.
* Collaborated with IT and security teams to implement security policies and incident response playbooks.
* Extensive experience in designing and implementing Email Security Appliances and Exchange Online Protection controls like domain or IP reputation filtering, Anti-Virus, Anti Malware, Anti Phishing, Content Filtering, URL Filtering.
* In-depth knowledge of email security protocols and best practices, including SPF, DKIM, and DMARC.
* Specialized in securing email infrastructure from threats.
* Worked in Hybrid Email Infrastructure for 6.5 lakh mailboxes.
* Continuous learning and professional development in cybersecurity.

**Technical Skills**

* Security Tools: Microsoft Sentinel
* Threat Intelligence: MITRE ATT&CK
* Endpoint Security: EDR/XDR solutions (Microsoft Defender)
* Network Security: IDS/IPS, Firewalls, VPN, Proxy
* Incident Response: Malware analysis, forensic investigation, log analysis
* Scripting & Automation: KQL, Python
* Compliance & Frameworks: NIST 800-53, ISO 27001, CIS Controls, GDPR
* CISCO Email Security Appliance Management
* Networking Fundamental
* Networking Traffic Monitoring

**Experience**

2020- Till Now **Tata Consultancy Services**

SOC Analyst

**Education**

April 2019 **Bachelor of Science Information Technology**

The American College, Madurai