Devarajan P M

Security Analyst

+91 8330857529 | devarajanpm79@gmail.com | https://www.linkedin.com/in/devarajan-p-m/ | https://www.github.com/devarajan-here | Devarajan P M | Cybersecurity Professional | India, Kerala, Thrissur

PROFESSIONAL SUMMARY

Aspiring Security Analyst with hands-on experience in incident response, alert triage, and SIEM log analysis. Skilled in threat detection, escalation, and case management workflows, with a strong foundation in network security and threat intelligence. Familiar with ServiceNow for incident tracking and process automation. Eager to contribute to enhancing organizational security posture through proactive monitoring, timely escalation, and continuous process improvement.

SKILLS

- SIEM & SOC: Splunk, QRadar, Wazuh, Log Analysis, Alert Triage, Correlation Rules, Phishing Investigation, Incident Triage, Incident Escalation
- Security Domains: Threat Intel, MITRE ATT&CK, Cyber Kill Chain, Vulnerability Analysis, Email Security, DLP, ISO 27001
- Cloud & Systems: AWS Security/Networking, Linux, Windows Event Logs, Active Directory
- Programming & Tools: Python, SQL, Wireshark, VMs, Basic Pentest Tools

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst Intern
bblewrap

India (Remote) | 06/2024 – 12/2024

- Performed SIEM log analysis and event correlation (Splunk/QRadar) to detect incidents; increased incident detection by 15%.
- Tuned correlation rules and evaluated controls to reduce false positives by 10% and improve analyst efficiency.
- Identified and remediated critical vulnerabilities in the Manappuram Finance MADU application, improving application security posture.

Cybersecurity Engineer
Finpro Technologies

India (Remote) | 01/2025

- Supported ISO 27001-aligned GRC initiatives: contributed to risk assessments, control mapping, and policy documentation.
- Authored procedures and compliance artifacts aligning operations with best practices.
- Delivered pre-sales cybersecurity demos, translating technical capabilities to client requirements.
- Supported incident handling workflows, ensuring timely escalation and closure of cases in line with SOC playbooks.

CERTIFICATIONS

- **CompTIA Security+**
- *CompTIA | 08/2025*
- (Credential ID: COMP001022645550)
- **Generative AI Fundamentals**
- *GeeksforGeeks | Course Completed*

- **Google Cybersecurity Professional**
- *Coursera | 03/2024*
- **Ethical Hacking Associate**
- *RedTeam | Course Completed*
- **Ethical Hacking Essentials**
- *EC-Council | Course Completed*

EDUCATION

B.Tech, Computer Science, APJAKTU - SNMIMT (First Class),

2020–2024

Plus Two in Computer Science - MES P Vemballur High School,

2018–2020

Class X - T.H.S Kodungallur,

2017–2018

PROJECTS

- **AI Phishing Email Automation**: Tines, Sublime Security, VirusTotal, URLScan, GPT-4 (opt), 2025. Built a no-code workflow to ingest emails, enrich IOCs, classify, route attachment/non-attachment paths, and auto-notify SOC via Slack/Email; cut manual triage ~80%.

- **Malware Analyzer**: Implemented URL/embedded content analysis with link scanning, basic signature checks, and risk scoring.

ADDITIONAL EXPERIENCE & LEARNING

- **Home Lab:** VMs with Splunk and Wazuh; simulated attacks/defense; Windows Event Log parsing; phishing investigation.
- **TryHackMe**: Cybersecurity Analyst path (SIEM, endpoint protection, phishing analysis).
- **LetsDefend:** SOC workflows, MITRE ATT&CK mapping, alert analysis.
- **Stock Market Data Analyzer**: Built a tool to track and analyze stock market trends using APIs and custom algorithms, providing insights on price movements and corporate announcements for informed decision-making.
- **Interview Assistant Website** – Developed a web-based platform leveraging AI to generate interview questions, analyze answers, and offer real-time feedback to improve job readiness.