PRINCE M VARGHESE

Cybersecurity Analyst | SOC Analyst (L1) | Security Operations | Threat Detection

Dubai, UAE | princemvarghese2001@gmail.com | linkedin.com/in/princemv-cybersec/ | Visa Status: **Visit Visa**

PROFESSIONAL SUMMARY

Proactive and detail-oriented Cybersecurity Analyst with hands-on exposure to penetration testing, system hardening, and incident monitoring. Certified Penetration Tester (CPT) with CEH v13 knowledge and a strong grasp of SOC operations, log analysis, and vulnerability remediation. Experienced in using industry tools such as Wireshark, Nmap, Nessus, Splunk, and Wazuh for detection and analysis. Currently based in Dubai and seeking a SOC Analyst / Security Support position to contribute to real-time threat monitoring and defensive security operations

Keywords: SOC Analyst, Cybersecurity Analyst, Incident Response, Threat Detection, Security Operations, SIEM, Network Security, Log Analysis, Threat Intelligence

WORK EXPERIENCE

Associate

ResourcePro, Bangalore, India — November 2023 to December 2024

- Achieved 100% accuracy across 1,000+ insurance documentation cases under stringent compliance and quality control parameters.
- Ensured adherence to client-specific data protection standards and internal security governance protocols.
- Partnered with cross-functional teams to meet aggressive SLAs while maintaining operational integrity.
- Safeguarded confidential client data in accordance with GDPR-equivalent privacy frameworks and access control policies.
- Identified and implemented workflow optimization initiatives that reduced turnaround time and enhanced productivity.
- Gained practical exposure to secure data handling, quality assurance, and compliance monitoring within a high-volume processing environment.
- Demonstrated rapid adaptability to new regulatory requirements, internal tools, and evolving client policies in a fast-paced operational setting.

Computer Lab Instructor

Koshys Institute of Management Studies, Bangalore, India — November 2022 to August 2023

- Administered and secured 50+ Windows and Linux lab systems, ensuring continuous availability and system integrity.
- Implemented endpoint hardening, access control policies, and regular patch management to mitigate vulnerabilities.
- Monitored network performance and system logs to identify and resolve security or configuration anomalies.
- Conducted vulnerability assessments on internal systems and applied remediation measures to reduce exposure.
- Assisted in configuring firewalls, routers, and network services, supporting a secure and stable infrastructure.
- Delivered technical instruction and lab support to 100+ students in networking, system administration, and cybersecurity fundamentals.
- Developed and supervised hands-on cybersecurity exercises, including ethical hacking and incident analysis simulations.

- Collaborated with faculty to align lab sessions with industry-relevant cybersecurity practices and emerging technologies.

EDUCATION

Bachelor of Computer Applications (BCA)
Koshys Institute of Management Studies, Bangalore, India **Graduated: 2022**

PROJECT EXPERIENCE

Security Operations & Penetration Testing Simulation to Red Team Hacker Academy (CPT)

- Performed internal vulnerability assessment and exploit simulation in a Windows-based lab.
- Monitored logs and network traffic for anomalies using Wireshark and Splunk.
- Executed privilege escalation and lateral-movement testing under controlled conditions.
- Produced CVSS-based incident and remediation reports aligned with MITRE ATT&CK mapping.

SKILLS

- **Security Operations & Monitoring**: SIEM (Wazuh, Splunk, QRadar to Familiar), Incident Response, Threat Detection, Alert Triage
- **Vulnerability & Penetration Testing:** Nmap, Nessus, Burp Suite, Metasploit, Wireshark
- **Network & System Security:** TCP/IP, DNS, Firewalls, Event Logs, System Hardening
- **Platforms:** Kali Linux, Windows Server, VMware, VirtualBox
- **Programming & Automation:** Python, Bash
- **Other Skills:** Technical Documentation, Report Writing, System Hardening, Self-Learning

CERTIFICATIONS

- **Fortinet Certified Fundamentals in Cybersecurity (NSE 1)** - Fortinet (2025)
- **Certified Penetration Tester (CPT)** - RedTeam Hacker Academy (2025)
- **Certified Ethical Hacker (CEH v13)** - EC-Council (Exam in Progress)
- **Cloud Computing** - Koshys Institute of Management Studies (2021)
- **Artificial Intelligence & Machine Learning** - Koshys Institute of Management Studies(2021)
- **Ethical Hacking** - Koshys Institute of Management Studies(2021)

PROFESSIONAL DEVELOPMENT

- Built a personal SOC lab for log analysis and incident triage.
- Active participant in CTFs and Blue-Team labs (TryHackMe).
- Continuous learning on SIEM tuning, threat intelligence, and incident handling workflows.