MONISHA M R

+91 9148105876 ◇ monishamr27@gmail.com ◇ linkedin.com/in/monisha-m-r ◇ GitHub ◇ Portfolio

OBJECTIVE

Seeking to join a dynamic SOC team where I can apply my knowledge of network protocols, SIEM tools, and incident response processes to detect, analyze, and contain cyber threats in real time.

EDUCATION

Dayananda Sagar College of Engineering, Bengaluru 2021 - 2025
Bachelor of Engineering in Electronics and Telecommunication, **CGPA: 8.88**

TECHNICAL SKILLS

- **Networking & Security:** TCP/IP, DNS, DHCP, Firewalls, VPN, IDS/IPS
- **SOC Processes:** Monitoring, Log Analysis, Incident Playbooks, Reporting
- **Frameworks:** MITRE ATT&CK, Cyber Kill Chain
- **Tools:** Splunk, Microsoft Defender, Any.run, Barracuda, Zscaler, ServiceNow, Code42, Nessus, AWS

INTERNSHIP & TRAINING

Brand Monitoring Intern – Digital Risk Protection Sept 2025 – Present
Mitigata^{TM} – Full-Stack Cyber Resilience

- Monitored brand impersonation, phishing domains, fake mobile apps, and malicious redirects across web and social media platforms.
- Performed OSINT-based investigations using Google Dorking, WHOIS lookups, URL analyzers, and SSL certificate analysis.
- Identified suspicious domains using IP reputation checks, SSL metadata, and URL redirection behaviour analysis.
- Investigated phishing websites and collected Indicators of Compromise (IOCs) such as URLs, IP addresses, and metadata for threat analysis.
- Prepared incident reports for escalation and takedown requests with screenshots, technical evidence, and risk summaries.

Security Analyst Trainee May 2025 – Jul 2025
SOC Experts Bengaluru, India

- Monitored and analyzed simulated alerts in **Splunk** to detect and respond to security incidents.
- Investigated phishing and malware threats using **Barracuda Email Gateway** and **Any.run sandbox**.
- Applied **Code42 DLP** for data exfiltration prevention and conducted vulnerability assessments using **Nessus**.
- Gained exposure to cloud security monitoring concepts in AWS environments.
- Gained knowledge of various cyberattack types, including malware, brute-force attacks, and other common threat techniques.

PROJECTS

Phishing Email Simulation using SET 2025

- Simulated phishing attacks using the **Social Engineering Toolkit (SET)** in Kali Linux within a controlled lab setup.
- Crafted phishing emails with spoofed senders and malicious links to study delivery methods and detection points.
- Identified phishing indicators such as suspicious headers, attachments, and redirect links.
- Analyzed detection methods of security tools to prevent phishing attacks.

System Hacking using Kali Linux and Metasploit Framework 2025

- Conducted system hacking simulation on a Windows 7 VM using **Kali Linux** and **Metasploit Framework**.
- Performed **Nmap scanning** to identify open ports and fingerprint the target operating system.
- Exploited the **MS17-010 (EternalBlue)** vulnerability to gain unauthorized access.
- Demonstrated understanding of the **penetration testing lifecycle** - reconnaissance, exploitation, and post-exploitation.

CERTIFICATIONS

- Certified Ethical Hacking Fundamentals – Coursera, 2025