ADARSHA JK

8861878501 ⋄ Adarshjk20@gmail.com ⋄ Bangalore, Karnataka
⋄ linkedin.com/in/adarsha-jk-a91a31238

OBJECTIVE

A cybersecurity enthusiast with hands-on experience in cloud security, IAM, incident response, network security, and SIEM operations. Passionate about threat detection, security automation, and vulnerability assessments. Looking for an opportunity to apply my skills in SOC operations, access management, and cloud security to strengthen organizational defenses.

EDUCATION

Master of Computer Applications

Dayananda Sagar College of Arts Science and Commerce, Bangalore *Nov 2024*

CGPA: 7.9

TECHNICAL SKILLS

Operating System: Windows Server, Linux (Ubuntu, Kali Linux).

Programming/Scripting: Java, Bash, PowerShell, Html/CSS, JS.

Tools & Platforms: Wireshark, pfSense, Snort (IDPS), Nessus, Qualys (VMs), Splunk, AWS Security Tools.

INTERNSHIP PROJECTS

Cybersecurity Intern | Extion Infotech, *Remote* *2024 June - 2024 Sep*

- Access Management: Configured IAM roles, RBAC policies, and enforced the principle of least privilege to reduce attack surface.
- Cloud Security: Conducted cloud security assessments using AWS Security tools and Scout-Suite to detect misconfigurations.
- Network Security: Performed traffic analysis and network segmentation as part of a Zero Trust Architecture implementation.
- Security Operations: Assisted in incident response, investigating security logs, and mitigating security threats in cloud environments.

PROJECTS

Security Operations and Threat Response Simulation

- SOC Operations: Deployed and managed the ELK Stack (SIEM) for real-time log ingestion, threat analysis, and incident detection.
- Threat Hunting: Simulated brute force attacks and monitored Sysmon logs to detect suspicious behaviour in Windows/Linux environments.
- Incident Response: Configured alerts to identify RDP/SSH brute force attempts and recommended mitigation strategies.
- Threat Intelligence: Operated Mythic C2 server to analyse attacker tactics, techniques, and procedures (TTPs).

Detection Engineering and Automation

- Endpoint Security: Utilized Lima-Charlie (EDR) for real-time endpoint monitoring and threat detection.
- Rule Writing: Developed custom detection rules (YARA, Sigma) to identify malicious file executions.
- Security Automation: Integrated Tines (SOAR) to automate incident response workflows and reduce MTTR (Mean Time to Respond).

CERTIFICATIONS

- AWS Certified Cloud Practitioner (AWS Security Foundation)
- Internshala Ethical Hacking Certification
- Datacom Cybersecurity Job Simulation (Forage) – SOC and Incident Response Simulation

EXTRA – CURRICULAR ACTIVITES

- **Hands-on Labs:** Blue Team Lab Online, Hack The Box.