SUNITHA B

Cyber Security Analyst L1

Email : sunithabmca@gmail.com
Mobile : 8660272148
Linked in : https://www.linkedin.com/in/sunitha-b-cybersecurity

CAREER OBJECTIVE

Dedicated Cloud Security professional with internship experience in securing cloud infrastructures, implementing IAM policies, and monitoring security threats. Proficient in AWS/Azure security tools, compliance frameworks, and incident response. Looking for a challenging role where I can enhance cloud security measures and contribute to the organization's cybersecurity resilience.

EDUCATION

MCA
Visvesvaraya Technological University
Bapuji Institute of Engineering and Technology College -Davnagere
Graduated;2024

SKILLS

Technical Knowledge:

- **SIEM tools :** Splunk ES
- **Firewall :** Palo Alto
- **EDR :** CrowdStrike
- **Proxy :** Cloudflare
- **ESA :** MS 365 Defender
- **Ticketing Tools :** JIRA
- **Malware Tool :** KASM , AnyRun
- **Cloud :** AWS -IAM,EC2,S3,Lambda,Security tools like-Guard duty,Security Hub,Detactive,CloudTrail, Config,KMS,Inspector,Shield, Azure

LANGUAGES KNOWN

- Kannada
- English
- Telugu
- Hindi

TECHNICAL SKILLS

- Good understanding of OSI Model, IP addresses and classes of IP Address.
- Understanding of recent common attacks, their attack vectors and their mitigation plans.
- Good knowledge of security concepts (CIA Triad, Cyber attack, Cyber Kill Chain (CKC) & MITRE Framework etc.)
- Knowledge on Malware and different type of attacks such as DOS, DDOS, DNS Poisoning.
- Understanding of common network services (web, mail, FTP, etc.) network vulnerabilities, and network attack patterns.
- Hands on experience with some Open-source Threat-Intel Tools.
- Knowledge on Servers like DNS, DHCP, Proxy server, Active Directory etc.
- Ability to maintain server, LAN, and WAN architecture.
- Keep up to date with latest trends of cyber security incidents.
- Understanding of Identity Acces Management(IAM)Principles.

SOC ANALYST SKILLS

- Monitoring Security alerts generated by SEIM.
- Knowledge on creating Reports, Dashboards and Alert.
- Analysing SEIM alerts by following runbooks and using varioustools.
- Well verse knowledge on generating tickets for validating incidents.
- Well known knowledge about Malware like Virus, Worms, Trojans, Ransomware, Botnets, Spyware etc.

CERTIFICATES

- Foundations of Operationalizing MITRE ATT&CK
- Intro to Splunk
- Splunk Scheduling Reorts & Alerts
- Network Defence Fundamentals : Training for IT Begginers
- Nmap for Ethical Hackers
- Introduction to Splunk Real User Monitoring.
- AWS Cloud Security

AREA OF INTERESTS

- Threat Detection and Response
- Cloud Security,Forensics
- Network Security Security
- Automation and Orchestration
- Threat Intelligence
- Cloud Security Posture
- IAM
- Malware Analysis

PERSONAL INFORMATION

Name	: SUNITHA B
Gender	: FEMALE
Date of Birth	: 28-Mar-2001
Fathers' name	: BASAVARAJA K
Mother's name	: CHANDRAMMA
Citizenship	: India
Address	: Chitradurga -577 501,Karnataka.
Hobbies	: Reading Security Blogs, Cycling.

I hereby declare that the above information is true to the best of my knowledge and belief.

(SUNITHA B)