

KUSUMA M S

mskusuma56@gmail.com • +91-9008057635 • Karnataka, India
linkedin.com/in/kusumams

SUMMARY

A motivated and enthusiastic recent graduate seeking an opportunity to apply my technical skills and academic knowledge in a dynamic work environment. Eager to contribute to a progressive organization, learn from experienced professionals, and grow both personally and professionally. Ready to collaborate with a team that values innovation, hard work, and continuous development.

EDUCATION

Maharaja Institute of Technology Mysore

Bachelor of Engineering, Information Science and Engineering

- Overall CGPA: 8.82 out of 10

Marimallappa PU College

Pre-University Course, Physics, Chemistry, Mathematics and Biology

- Percentage: 91.5%

Christ The King Convent High School

- Percentage: 92.16%

TECHNICAL SKILLS

- Good understanding of the security concepts and networking concepts.
- Good understanding on various attacks such as Phishing, Spoofing, MITM, Brute force, DOS, DDOS, ARP Spoofing, SYN Flood, Ping of Death, etc.
- Good understanding on various malwares such as Virus, Worm, Trojan Horse, Ransomware, Adware, Spyware, Scareware etc.
- Knowledge on the architecture and key components of Splunk Enterprise Security.
- Knowledge on architecture and key components of IBM QRadar.
- Foundational knowledge of incident response plans, including frameworks like NIST 800-61.
- Understanding of key concepts in security analysis, such as True Positives, False Positives, False Negatives, and True Negatives, and their relevance in minimizing security risks.
- Investigating on the reputation of IP addresses, suspicious URL's, files with the help of IBM X-Force, CISCO TALOS, VIRUSTOTAL.
- Basic knowledge on SOC Workflow and roles and responsibilities of L1/L2 Security Analyst in SOC.
- Familiar with the workings of DNS and DHCP, including their roles in network communication.
- Knowledge of common ports and protocols and the significance of event IDs, logon types in system logs, with an understanding of their role in network monitoring and troubleshooting.
- Knowledge on analysing the email via SPF, DKIM, DMARC protocols to detect and prevent email spoofing and phishing attacks, ensuring secure email communication.
- Basic knowledge on CIA TRIAD and AAA's.
- Good knowledge on Cyber Kill Chain.

- Familiar with the MITRE ATT&CK framework, with a understanding of its structure and how it is used to identify and analyze adversarial tactics and techniques in cybersecurity.
- Knowledge on firewalls, IDS/IPS,VPN, Antivirus.

ANALYSIS TOOLS

- IBM X-Force Exchange
- CISCO TALOS
- VIRUSTOTAL
- CVE MITRE

TOOLS

- SPLUNK

PERSONAL SKILLS

- Time Management
- Communication Skills.
- Team Work and Work Ethics.

EXTRACURRICULAR ACTIVITIES

Member of EWB Club.

Attended various events ,seminars,workshops.

Participation in Hackathon.

Participated in Hack-4-Mysore in MITM-by UNSTOP Organisation.

Won prizes at inter college dance competitions

ADDITIONAL INFORMATION

Certifications

JAVA,C/C++

Languages

English (*Fluent*), Kannada (*Native*),Telugu (*Elementary*)

Interests

Dancing, plantation, fashion, Listening to music

Work Eligibility

India citizenship by birth;

Eligible to work in India

DECLARATION

I hereby Declare that all the details mentioned above are accurate to the best of my familiarity and Confidence.

KUSUMA M S