HARSHAND C

DOB:20/06/2000 **Nationality:** Indian **Gender:** Male **Phone number:** (+91) 9074012439

Email: harshandcpurameri@gmail.com **LinkedIn:** https://www.linkedin.com/in/harshand-c-89795a230

Address: Chalilpoyil house, purameri post, vadakara, kozhikode,kerala, Pin 673503

WORK EXPERIENCE

21/12/2022 – CURRENT

SOC ANALYST - MACOM EVOLV, Trissur, India

- Monitored and analyzed security alerts using SIEM and XDR platforms,investigating and responding to potential threats and incidents in real-time. -Conducted in-depth analysis of security events and alerts to identify,evaluate and mitigate potential threats. -Employed advanced data correlation techniques to combine information from multiple sources,including network traffic,endpoint logs,and user activities to provide a comprehensive view of security events. -Developed detailed reports,documenting findings and recommendations to improve security posture and prevent recurrence of similiar threats. -Experienced in using tools like Splunk,ELK Stack,XDR,Splunk,Sentinel. -Identified and implemented process improvements to enhance efficiency of SOC operations,including automation of repetitive tasks and refining of alert tuning. -Playbook based investigation & response - Incident Triage for securitys using multiple security tool,Provide near real-time analysis, investigation and, reporting security incidents for customers.

06/07/2022 - 12/12/2022

PYTHON DEVELOPER - Soften technologies kochi, kerala

-Experience with popular Python frameworks such as Django, Flask or Pyramid.Knowledge of data science and machine learning concepts and tools.
Contributions to open-source Python projects or active involvement in the Python community.

EDUCATION AND TRAINING

BACHELORS IN COMPUTER APPLICATION(BCA)- 05/07/2018 – 2/03/2021

Calicut University Nadapuram,Kerala, India

CERTIFICATIONS

Certified Ethical Hacker - CEH V13 (EC Council)

Python fulstack development - Soften Technologies 25/07/2021- 09/04/2022

ORGANISATIONAL SKILLS

--SIEM(Security Information and Event management System) -XRD(Extended Detection and Response)-Stellar Cyber - SIEM solutions (Sentinel,Defender) -Seqrite QuickHeal EPS -Kali Linux -Burpsuit,Frida,Nessus,Metasploit Framework -IPS (Intrusion prevention system) and IDS(Intrusion Detection System) -Detecting Different IOC(Indicator of Compromise)AND IOA(Indicator of Attacks)

LANGUAGES

English, Hindi, Malayalam, Tamil