JOB DESCRIPTION:
Security Intern

Location:

Bangalore, India

Company:

CyberWarFare Labs

Company Description

CyberWarFare Labs (CWL) is UK based Ed-tech leader in cybersecurity with operations located in Bengaluru. We provide cutting-edge cybersecurity Education and immersive training services, enabling organizations to enhance their cyber capabilities. Our client-focused approach ensures tailored solutions in this ever-evolving field. We prioritize proactive defense with innovative solutions, backed by on-demand educational services.

Brief description

We are looking for a capable Security Engineer, who enjoys security work and possesses both deep and wide expertise in the security space.

You will make things more secure by protecting system boundaries, keeping computer systems and network devices hardened against attacks and securing highly sensitive data. Qualified candidates will have a background in Security or Systems Engineering.

Tasks
- Well versed with **Python, Bash, C & C++**
- Understanding of **Network Security**, Web Security, **Blue Teaming (SOC)** & **Reverse Engineering**, **Docker environments**
- Collaborate with Leads to define, design realistic cyber range labs
- Replicate **Tactics, Techniques & Procedures (TTPs)** in staging environments

- Manage / Develop & Test Cyber Range Labs
- Well versed with **AWS, Azure & Google** Cloud
- R&D in accordance with emerging cyber security threats
- Identify and correct bottlenecks and fix bugs
- Design and maintain vulnerable apps and systems.

Qualifications and requirements

- BS degree in Computer Science
- B.E /B.Tech /M.Tech degree from a recognized and accredited university/college
- Proven work experience as a Security Engineer or Information Security Engineer
- Experience in building and maintaining security systems
- Detailed technical knowledge of database and operating system security
- Hands on experience in security systems, including firewalls, intrusion detection systems, anti-virus software, authentication systems, log management, content filtering, etc
- Experience with network security and networking technologies and with system, security, and network monitoring tools
- Thorough understanding of the latest security principles, techniques, and protocols
- Familiarity with web related technologies (Web applications, Web Services, Service Oriented Architectures) and of network/web related protocols
- Problem solving skills and ability to work under pressure

Role and Responsibility

- Analyse security systems and seek improvements on a continuous basis
- Report possible threats or software issues
- Research weaknesses and find ways to counter them
- Find cost-effective solutions to cybersecurity problems
- Understand software, hardware and internet needs while adjusting them according to our business environment

- Develop best practices and security standards for the organisation
- Test company software, firmware and firewalls
- Assist fellow employees with cybersecurity, software, hardware or IT needs

Working conditions
- Works primarily on-site mode and prefers the timing of 10am to 6pm (Or according to college schedule) & Weekends will be off.
- You'll work as part of a team in a flexible work environment, learning and enhancing your expertise.

Reference No.

- SE-02