

Security Intern

Location: Bangalore, India

Company: CyberWarFare Labs

About Us:

CyberWarFare Labs is an Ed-Tech Cyber Security Focused Platform which is totally engrossed in solving the problem of Cybersecurity by providing real-time hands-on manner solutions to problems of B2C & B2B Audience.

Job Overview:

As a Security Intern at CyberWarFare Labs, you will play a pivotal role in enhancing our cybersecurity posture by conducting in-depth research and analysis of emerging threats, vulnerabilities, and attack methodologies. You will collaborate with cross-functional teams to develop cutting-edge security solutions and contribute to our mission of ensuring the highest level of protection for our clients.

Key Responsibilities:

1. Utilize ELK Stack for log collection, analysis, and threat detection using KQL.
2. Perform real-time monitoring and investigation of security events.
3. Conduct Blue and Red Team operations in on-premise environments.
4. Configure and manage cloud security settings across AWS, Azure, and GCP.
5. Replicate attack scenarios and create challenges in lab environments.
6. Research emerging threats, exploits, and develop PoCs.
7. Design and develop new security challenges based on recent attacks.
8. Maintain clear documentation of tools, methodologies, and findings.
9. Support threat detection improvements through hands-on experimentation.
10. Collaborate with cross-functional teams to enhance defensive capabilities.

Security Intern

Requirement:

- Bachelor's or Master's degree/Pursuing in Computer Science, Information Security, or a related field.
- Familiarity with security tools, techniques, and methodologies.
- Proficient in conducting **log analysis** and investigating security incidents across diverse IT environments.
- Skilled in **securing cloud-native workloads** and managing security across major cloud platforms including **AWS, Azure, and Google Cloud Platform (GCP)**.
- Conducted comprehensive research and analysis on **emerging threats, tactics, techniques, and procedures (TTPs)**, and **vulnerabilities**, enabling proactive detection, **threat hunting**, and effective **defense strategy development**.
- Basic knowledge of **MITRE ATT&CK framework, Digital Forensics and Incident Response (DFIR)** methodologies, **log analysis**, and **security analytics**.

GOOD TO HAVE : Proven hands-on experience in **threat detection, security operations, and incident response** within **Blue Team** environments.

Stipend Offered - 15k per month (10% TDS is cut which can be claimed while filing ITR) 13.5k in hand will be received

Job Location - 3rd Floor, Cyberwarfare Labs. HustleHub H1907,240, 19th Main Rd, 4th Sector, HSR Layout, Bengaluru, Karnataka 560102

Internship time period - 3 months

After 3 months, Full time position will be offered based on performance