

Job Title: Cybersecurity Analyst  
Location: Bangalore  
Job Type: Full-Time  
Experience Level: Mid-Level (2-5 years)

**About the Role:**

We are seeking a detail-oriented and proactive Cybersecurity Analyst to join our growing security team. You will play a critical role in protecting our organization's digital assets and infrastructure from internal and external threats. The ideal candidate is passionate about cybersecurity, highly analytical, and capable of staying ahead of ever-evolving cyber threats.

**Key Responsibilities:**

Monitor networks and systems for security breaches, threats, or unauthorized activity.

Analyze security incidents to determine their root cause and propose corrective actions.

Implement and manage security tools such as firewalls, antivirus software, and intrusion detection systems (IDS/IPS).

Conduct regular vulnerability assessments and penetration testing.

Respond to and investigate security alerts, incidents, and anomalies in real-time.

Work closely with IT and development teams to ensure secure infrastructure and software deployment.

Maintain up-to-date knowledge of the latest cybersecurity trends, technologies, and regulations.

Create and maintain documentation, including incident reports, risk assessments, and security procedures.

Educate and train staff on cybersecurity best practices.

**Qualifications:**

Bachelor's degree in Computer Science, Cybersecurity, Information Technology, or a related field.

2+ years of experience in cybersecurity or a related IT security role.

Strong understanding of network protocols, system architecture, and security principles.

Experience with SIEM tools (e.g., Splunk, QRadar), firewalls, and endpoint protection systems.

Familiarity with standards and frameworks such as NIST, ISO 27001, and MITRE ATT&CK.

Relevant certifications such as CompTIA Security+, CEH, CISSP, or GIAC are a plus.

Strong analytical, problem-solving, and communication skills.

**Preferred Skills:**

Knowledge of scripting languages (Python, Bash) for automation.

Experience with cloud security (AWS, Azure, GCP).

Familiarity with threat intelligence platforms and malware analysis.