# Job Title: Cybersecurity Analyst

**Location:** [Remote/Hybrid/Onsite]

**Experience Level:** [Entry/Mid-level]

**Reports To:** [CISO / IT Security Manager]

## Job Summary

We are looking for a vigilant **Cybersecurity Analyst** to join our defense team. You will be responsible for protecting our network, systems, and data from unauthorized access and cyber threats. Your day-to-day will involve monitoring traffic, investigating breaches, and implementing "best-in-class" security protocols to stay ahead of bad actors.

## Key Responsibilities

- **Security Monitoring:** Monitor network traffic for unusual activity and potential security breaches using SIEM (Security Information and Event Management) tools.
- **Incident Response:** Lead the initial investigation into security alerts; contain and mitigate threats as they arise.
- **Vulnerability Assessment:** Conduct regular scans and audits of our systems to identify weaknesses before they can be exploited.
- **Policy Enforcement:** Assist in developing and maintaining corporate security policies (e.g., password rotations, access controls, and data encryption).
- **Reporting:** Create detailed reports on security findings and incident post-mortems for technical and non-technical stakeholders.
- **Security Awareness:** Educate staff on security best practices, such as recognizing phishing attempts and practicing good digital hygiene.

## Required Skills & Qualifications

- **Education:** Bachelor’s degree in Computer Science, Cyber Security, or a related field (or equivalent experience).
- **Technical Proficiency:** Hands-on experience with firewalls, VPNs, IDS/IPS, and endpoint protection.
- **Analytical Mindset:** Ability to correlate data from disparate sources to identify complex attack patterns.

- **Certifications (Preferred):** CompTIA Security+, CEH (Certified Ethical Hacker), or CISSP.
- **Soft Skills:** Strong communication skills—you'll need to explain a "SQL injection" to someone who thinks it's a medical procedure.

## Technical Environment

- **SIEM Tools:** [e.g., Splunk, IBM QRadar, Microsoft Sentinel]
- **Operating Systems:** Windows, Linux, and Cloud environments (AWS/Azure/GCP).
- **Scripting:** Basic proficiency in Python or PowerShell for automation is a major plus.

## Why Work With Us?

- [Benefit 1: Competitive salary and "no-burnout" on-call rotation]
- [Benefit 2: Stipend for continuous learning and certifications]
- [Benefit 3: Modern tech stack and a collaborative team culture]

**Would you like me to tailor this for a specific industry, such as Healthcare (HIPAA) or Finance (PCI-DSS)?**