Cyber security Analyst

Job Description

We are seeking a motivated and detail-oriented **Entry Level Cybersecurity Analyst** to join our team. This role is designed for individuals who are passionate about cybersecurity, eager to learn and ready to begin their professional journey in safeguarding digital assets and information systems. The successful candidate will work closely with senior team members to monitor, detect and respond to security threats, while building foundational skills in cybersecurity operations.

Key Responsibilities

- Monitor and analyze security alerts from various tools and systems (e.g., SIEM, endpoint security, firewalls). *Wazuh* or *LogRhythm* is preferred.
- Assist in identifying, investigating, and escalating to Level 2 (L2) potential security incidents.
- Support in vulnerability assessments, penetration tests and patch management processes.
- Document security incidents, investigations and resolution steps.
- Contribute to maintaining and improving security policies, procedures, and awareness initiatives.
- Stay updated on current cybersecurity trends, threats, and best practices.
- Work with and incorporate Threat Intelligence tools like OpenCTI, Virus Total and DarkTrace into the environment.
- Provide basic support in compliance and audit-related activities.

Qualifications

- Recent graduate or final-year student in **Computer Science, Information Technology, Cybersecurity, or related field**.
- Basic understanding of networking concepts (TCP/IP, DNS, firewalls, etc.).
- Familiarity with operating systems (Windows, Linux) and common security tools.
- Knowledge of cybersecurity fundamentals such as malware, phishing, ransomware, and intrusion detection.
- Strong analytical, problem-solving, and communication skills.
- Willingness to learn, adapt, and grow within the cybersecurity field.

Preferred (but not required)

- Relevant certifications such as **Cyber Threat Management Analyst, Certified Ethical Hacking (CEH), CompTIA Security+, Network+, or Cisco CyberOps Associate**.
- Hands-on experience from labs such as TryHackMe, Lets Defend, Over-The-Wire and Capture the Flag (CTF) competitions or internships in a cybersecurity related field.
- Exposure to SIEM tools (Wazuh, LogRhythm, SPLUNK), endpoint protection platforms (Crowdstrike, DarkTrace) or vulnerability scanners (NESSUS - Tenable).