Title: Cyber Threat Analyst

Experience: 4 – 10 years of relevant industry experience (or combination of education and experience)

Education: Bachelor's degree in computer science, information systems, information security, or related field

Applicable Certifications: GCTI, GCFA, GNFA, GMON, GCED, GREM, GSNA, GCIH, GSEC

Overview: The Cyber Threat Analyst will be a critical contributor to the organization's security team. This position will provide targeted threat information and analysis, and will be actively involved in incident response and threat hunting activities. The ideal candidate will have a thorough understanding of information security, cyber threats, cyber threat actors, and monitoring and detection.

Responsibilities:

- Hunting, tracking, and analyzing advanced persistent threats (APTs)
- Conducting research, collecting & analyzing data and evaluating intelligence; identifying patterns and trends and developing appropriate strategies
- Recognizing critical security incidents and escalating as needed
- Providing guidance to leadership on strategies and plans of action to eradicate threats – act as cyber threat subject matter expert
- Providing actionable intelligence to detection operations that proactively monitor systems for potential threats.
- Developing plans and procedures for continuous monitoring and detection operations.
- Providing actionable intelligence to investigate security incidents and conduct data analysis based on findings.
- Writing and presenting routine reports regarding findings. Advising team on responsible sharing of reporting information to trusted partners.
- Informing team members who conduct cyber threat emulation operations by providing context and realism.

Requirements:

- Excellent data analysis skills and ability to identify patterns and trends
- Experience with intrusion detection
- Knowledge of Unix/Linux and SIEM tools such as Splunk
- Deep understanding and knowledge of networking, including TCP/IP, DNS, HTTP, SMTP
- Experience working in cyber security or information assurance, ideally as part of a SOC or NOC
- Ability to work individually and as part of a team
- Ability to think creatively and come up with innovative solutions
- May need to have or be able to obtain a security clearance

- Must be driven and motivated with excellent organization skills
- Excellent written and verbal communication skills. Should be comfortable with public speaking and presenting findings to others, including leadership.