Cyber Analyst - Network

Position Summary

The Cyber Analyst – Network is a member of the Cyber Analysis and Context team, which develops and manages cyber security initiatives for the protection of the entire North American power grid. This person will provide technical support to these initiatives, as well as subject matter expertise for cyber security incident investigations. This person will also support ongoing risk assessment activities for grid-critical infrastructure. The Cyber Analyst will assist with security outreach and readiness reviews with NERC-registered critical infrastructure asset owners and operators. This role reports to the Manager, Cybersecurity Analysis and Context (CAC) Team within the Electricity Information Sharing and Analysis Center (E-ISAC).

The successful candidate should be familiar with the relationships between the electricity industry in North America and federal agencies, including the Department of Energy, the Department of Homeland Security, the Department of Defense, the Federal Energy Regulatory Commission, and the Federal Bureau of Investigation.

Ability to travel within North America is required. The position is located in Washington, D.C. An active security clearance is required.

Duties and Responsibilities

- Provide cyber security technical analysis, advice and expertise to electric industry members and government officials during critical infrastructure incidents.
- Provide expertise regarding critical infrastructure cyber security measures.
- Provide possible-impact assessment of network compromise campaigns.
- Collaborate with subject matter experts to identify opportunities to improve the cyber security protection of North American electric grid assets.
- Co-author reports on cyber security threats and mitigation strategies to protect North American electric grid assets.
- Co-develop cyber security training materials and programs.
- Participate and collaborate in North America-wide grid security exercises.
- Provide subject matter expertise to assist the NERC Critical Infrastructure Protection Committee and the Electricity Subsector Coordinating Council, as requested.

Qualifications
The successful candidate will have:

- A Bachelor’s Degree in a related technical field and related technical experience. An additional 4 years of experience may be substituted in lieu of a degree.
- Knowledge and skills to understand network design and analyze of router, firewall, VPN/remote access and other perimeter defense systems’ traffic and logs.
- Demonstrate the knowledge and skills to understand and analyze network traffic to detect abnormal traffic and identify possible threats and common attack indicators.
- Successfully demonstrate proficiency in the following tasks:
  - Describe in detail effective network defense principles to detect and/or mitigate different network attacks
  - Thorough understanding and analysis of DNS traffic. Identify legitimate and possibly malicious DNS traffic.
  - Demonstrate the ability to analyze network traffic to identify normal and application traffic. This includes the ability to discern malicious traffic from false positives.
  - Demonstrate the ability to detect encrypted intrusions on the network
  - Demonstrate the ability to dissect and analyze IP packet headers for normal and abnormal values
  - Deep packet inspection.
  - Packet dissection and analysis of HTTP and SMTP.
  - Thorough understanding of how fragmentation and fragmentation-based attacks work
  - Proficient in traffic analysis using Wireshark, Silk and other network traffic analysis tools
- Ability to provide insight into network activity analysis and possible detection and mitigation options
- Demonstrated proficiency in:
  - Critical thinking
  - Trend analysis, math and fact-based analytical experience
  - Report generation and peer reviewing
  - Presenting and defending analysis reports
  - Ability to pivot from a position when new evidence negates previous assessment
  - Incident response experience: from discovery to lessons learned
  - Tutorial Development - Lesson Plan, public speaking, engagement, travel
  - Use of cyber threat intelligence platforms and technologies
- Active Secret Security Clearance; if not currently held, selected candidate must be able to obtain and maintain a favorably adjudicated background investigation for continued employment
- Familiarity with past and current threat actors and associated tactics and tools
- Ability to understand and learn technical specifications, system requirements and other application design information as needed

Preferred Additional Qualifications
• Successfully passed one or more of the following or equivalent course:
  o Security +, Network +
  o GCIA
  o GCIH
  o GCTI

• **Network Analyst Level**
  o Ability to provide insight into campaigns that involve network compromises; ability to collaborate in determining the impact to the electric industry

• **Senior Network Analyst**
  o Ability to provide specific, detailed and unique insight into campaigns that involve network compromises; ability to collaborate in determining the impact and prevalence of campaign against the electric industry
  o Successfully passed the following or equivalent course:
    ▪ OSCE
    ▪ GNFA
    ▪ CISSP
    ▪ CISM
    ▪ CPP
  o Master’s degree in a related discipline

**Other**

• Background check will be conducted prior to employment
• In compliance with federal law, all persons hired will be required to verify identity and eligibility to work in the United States and to complete the required employment eligibility verification document form upon hire
• Travel necessary: Passport required for North American travel
• This position has been classified as exempt
• Job is located in Washington, DC

Qualified candidates should submit their resume and salary history in electronic format to hr@nerc.net.