Job Title: Network Security Engineer

Job Description
The Network Security Engineer has the responsibility to plan, implement, oversee and maintain networks and security-related projects.

Candidates must have the technical abilities to support the daily tasks of a network operations and security operations center, while possessing the ability to design and engineer secure and reliable wide area networks. In other words, while this role will focus on network security, the ideal candidate will also have the technical skills, and desire, to support network operations.

Additionally, the ideal candidate possesses the business competencies and interest to play an integral role in developing an effective managed security service platform. While intimate knowledge and experience with the NERC standards, specifically Critical Infrastructure Protection (CIP), is not required, the role is for performing security activities in support of our clients' CIP compliance programs—therefore the ability to work within existing compliance and security frameworks is a must.

Since all of our clients are part of the Bulk Electric System (BES), the ideal candidate has experience working with industrial control systems, preferably direct experience with Supervisory Control and Data Acquisition (SCADA) systems in power system environments.

Objectives of this Role
- Improve the security posture and reliability of our clients' networks and infrastructure
- Support the security operations team by assisting in network-related security investigations and incident response
- Support the network operations team by quickly identifying and troubleshooting operational issues
- Work within the requirements of CIP to generate evidence and maintain compliance
- Play a key role in the development and implementation of GridSME's MSSP division, GridSecurity

Essential Duties:

- Design and engineer critical networks
- Select and implement security tools, policies, and procedures in conjunction with the rest of the security team
- Design and implement monitoring, configuration management, reporting and alerting functions for automating the environment

- Use network security tools (e.g. IDS, IPS, netflow, etc.) to identify potential security incidents and support incident response efforts
- Assist with security hardware and software vendor evaluation, recommendation, and negotiations

Supporting Duties:

- Configure and install various network devices and services (e.g., routers, switches, firewalls, load balancers, VPN, QoS)
- Perform network maintenance and system upgrades including service packs, patches, hot fixes and security configurations
- Monitor performance and ensure system availability and reliability
- Monitor system resource utilization, trending, and capacity planning
- Provide support and troubleshooting to resolve operational issues
- Define and document best practices and support procedures
- Maintain inventory and asset configuration documentation
- Interact with customers and staff at the technical level, as required

Desired Business Skills

- Strong leadership, project management, time management, and problem solving skills
- A penchant to identify and remediate inefficiencies in processes
- Ideation, critical thinking, and prioritization of resources to provide the most value to our clients
- Ability to adapt to a changing environment and make timely decisions
- An entrepreneurial spirit
- Ability to work with technical and non-technical business owners to get things done
- Work collaboratively within a team environment
- Excellent written and oral communication

Desired Technical Skills

- Experience in a multi-site network environment with routers, switches and firewalls is required
- In-depth experience with IDS/IPS, packet analysis, event correlation and forensics, and IDS/IPS rule sets and signature creation
- Detailed technical knowledge of security engineering, system and network security
- Strong understanding of networking fundamentals (i.e. architecture, protocols, etc.)
- Working knowledge of Linux and Windows Operating Systems
- Understanding of system hardening processes, tools, guidelines and benchmarks

- Design and implement monitoring, configuration management, reporting and alerting functions for automating the environment
- Experience selecting and implementing security tools, policies, and procedures in accordance with the client's business and compliance needs
- Perform network maintenance and system upgrades including service packs, patches, hot fixes and security configurations
- Experience working within established policies and procedures
- Experience defining and documenting policies and procedures

Desired Education:

- A bachelor's degree in Computer Science or IT-related discipline is preferred
- Additional/Bonus: CISSP, Network+, CCNP, CCIE, PCNSE

Experience:

- 5-8 years' relevant experience is desired