



NETWORK SECURITY ANALYST INFORMATION TECHNOLOGY WASHINGTON, DC [HEADQUARTERS]

The Information Technology Department provides technology and telecommunications services to all AFL-CIO departments and staff in an effort to facilitate the goals and objectives of the Federation. In addition, the Information Technology Department provides technical leadership to Affiliated Unions, State Federations, Central Labor Councils and other constituency groups.

The network security analyst is responsible for leading computer network defense, auditing the network for vulnerabilities, conceptualizing and developing solutions for security issues, and investigating security breaches.

DESCRIPTION OF DUTIES:

Program Development and Implementation

- Leads and conducts all network monitoring and intrusion detection analysis using various Computer Network Defense (CND) tools, such as Intrusion Detection/Prevention Systems (IDS/IPS), Firewalls, Host Based Security System (HBSS), etc.
- Correlates network activity across networks to identify trends of unauthorized use.
- Reviews alerts and data from sensors and documents formal, technical incident reports.
- Researches emerging threats and vulnerabilities to aid in the identification of network incidents.
- Provides network subscribers with incident response support, including mitigating actions to contain activity and facilitating forensics analysis when necessary.
- Creates business continuity/disaster recovery plans, to include conducting disaster recovery tests, publishing test results, and making changes necessary to address deficiencies.
- Prepares an annual security upgrade plan with the Director, participates in the preparation of the annual security budget, and leads the implementation and project management of security upgrades.
- Prepares and gives briefings on security threats, security tools, and security defense measures.
- Acts as a resource and advisor to affiliated bodies (state federations, central labor councils, affiliated unions) on security threats and defensive measures and best practices.
- Participates in planning of, and response to, periodic penetration testing.
- Works with the network admin and help-desk team to provide support and guidance.

Reporting

- Keeps the Department Director and Deputy Director fully informed on a regular basis on issues affecting federation systems.
- Prepares periodic reports for officers as requested on the state of security preparedness and

potential vulnerabilities.

- Conducts briefings for staff and affiliated organizations about security tools and preparedness and best practices.
- Prepares and submits regular and ad hoc reports, especially on security status, on departmental activities as required.

Other

- Performs other duties as assigned.

QUALIFICATIONS:

Education & Experience

- Bachelor's degree in computer science, information security or a related field.
- Over eight years of work experience in information security, specifically in a network security analyst role.
- Certified Information System Security Professional (CISSP) desired.
- Certified Information Security Manager (CISM) desired.
- GIAC Certified Incident Handler desired.

Skills

- Extensive technical expertise in analyzing threat event data, evaluating malicious activity, documenting unusual files and data, and identifying tactics, techniques and procedures used by attackers.
- Strong decision-making capabilities, with a proven ability to weigh the relative costs and benefits of potential actions and identify the most appropriate one.
- Demonstrated ability to effectively influence others to modify their opinions, plans, or behaviors.
- An understanding of business needs and commitment to delivering high-quality, prompt, and efficient service to the business.
- An understanding of organizational mission, values, and goals and consistent application of this knowledge.
- Demonstrated ability to work with a diverse group of users on a professional level.
- Demonstrated ability to analyze problems and develop timely solutions.
- Demonstrated ability to provide input for strategic planning.
- Demonstrated ability to work well as a member of a team.
- Demonstrated communications skills, oral and written.
- Ability to work extended or irregular hours as needed.

Apply here: <http://aflcio.hirecentric.com/jobs/>

Equal Opportunity Employer