AFL-CIO

AMERICA'S UNIONS

NETWORK SECURITY ADMINISTRATOR
INFORMATION TECHNOLOGY
WASHINGTON, D.C. [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 administrator is responsible for coordinating with management and IT department staff on computer network defense, auditing the network for vulnerabilities, investigating security breaches, and working with the network engineer on "workflow" and reporting.

DESCRIPTION OF DUTIES:

Network Security, Network Management, and Helpdesk Support

- Manages and maintains email system(s) in a load-balanced hybrid physical/virtual server, VMware DAG, utilizing a Network Appliance storage network.
- Serves as lead to Gmail, AT&T Managed Threat Detection and Response, and CrowdStrike, for testing and managing failed user accounts.
- Manages and maintains GSuite applications.
- Works with Network Engineer to manage and maintain Cisco Meraki infrastructure.
- Manages and tests Endpoint Protection Software, including documenting and creating staff documentation, mapping and updating network infrastructure.
- Develops and deploys PC upgrades, and updates and creates network maps.
- Provides second level and advanced support of email products and configuration, including personal contacts, calendar shares across desktop and mobile environments.
- Enforces account policy making efficient use of CALs.
- Manages patch management, evaluates patches, and ensures the patching of systems that cannot be automatically patched.
- Manages user access, account creation and security and reviews user and group accounts for proper levels of access.
- Ensures that systems are secure, including, changing passwords, and disabling and deleting accounts when users leave or change responsibilities.
- Monitors mailbox databases for growth and trends.
- Configures and deploys applications and desktop images via GPO, TrackIt, and BMC Software.
- Keeps the Network Engineer and Manager of Office Automation, Networking and Electronic Communications fully informed on a regular basis on issues affecting departmental systems.
- Prepares and submits regular and ad hoc reports, especially on security status, on departmental activities as required.
- Performs other duties as assigned.

Reporting

- Keeps the Department Director and Deputy Director fully informed on a regular basis on issues affecting federation systems.
- Conducts briefings for staff about security tools and preparedness and best practices.

- Prepares and submits regular and ad hoc reports on security status as required.

Other
- Performs other duties as assigned.

QUALIFICATIONS:

Education & Experience
- BS Degree in Software Engineering preferred.
- BS Degree in Computer Science or Information Systems or AS Degree in Computer Science with Certified Advance Analyst in CrowdStrike required.
- Mastery of a discipline, such as G-Suite, CrowdStrike, and AT&T Managed Threat Detection and Response.
- Microsoft Certified Systems Engineer/Exchange or similar credentials required.
- Security credentials are a plus.
- SCCM certification is a plus.

Skills
- Technical expertise in analyzing threat event data, evaluating malicious activity, documenting unusual files and data, and identifying tactics, techniques and procedures used by attackers.
- At least eight years' demonstrated experience in network and systems monitoring tools.
- At least five years' demonstrated experience with VMware and Storage Area Network.
- At least five years' demonstrated experience with multiple desktop products including software and hardware.
- At least five years' demonstrated experience with administering a medium to large scale G-Suite environment.
- Demonstrated experience with Network Management software.
- Demonstrated experience in documenting Systems configurations and procedures as well as preparing written instructions for internal users.
- Experience or at least training in Server (physical/virtual) configuration.
- Experience in Internet and TCP/IP configuration and troubleshooting.
- Microsoft Windows Deployment Toolkit experience is a plus.
- Microsoft Windows Group Policy Administration experience is a plus.
- Ability to communicate with outside vendors, consultants and internal users to quickly diagnose and solve PC problems.
- Ability to work with a diverse group of users on a professional level.
- Ability to analyze problems and develop timely solutions.
- Ability to provide input for strategic planning.
- Ability to work independently, well as a member of a team.
- Demonstrated communications skills, oral and written.
- Ability to work extended or irregular hours as needed.

Starting salary is $96,323

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

Equal Opportunity Employer