



Administrative Office of the Courts

Senior Information Security Analyst

Primary Purpose

The Senior Information Security Analyst (SISA) is responsible for conducting comprehensive vulnerability assessments, developing detailed reports, and planning and coordinating remediation operations. This position provides direction and technical support for configuration and patch management operations, and the establishment and maintenance of secure baseline configurations for all AOC information systems. Additionally, the SISA is instrumental in developing procedures for, and serves as a member of, the Enterprise Incident Response Team.

Distinguishing Characteristics

Extensive experience and high degree of technical proficiency with enterprise vulnerability scanners, network access controls, configuration management tools, and associated processes. Experience managing and leading incident response actions, and establishing and monitoring secure information system baselines.

Duties and Responsibilities

- Performs and analyzes vulnerability scans for all enterprise systems
 - Performs network discovery scans, and maintains an up-to-date listing of authorized AOC information systems
 - Establishes methods to improve efficiency of automated vulnerability patching
 - Creates and customizes scripted application and security update installations
 - Assists in development of configuration management standards and procedures
 - Leads efforts to establish and maintain security hardened workstation and server configurations
 - Assists in troubleshooting conflicts resulting from security updates
 - Collaborates with "Network Operations" to assure accuracy of network diagrams
 - Assists Information Security Officer with network and application security assessments
 - Leads efforts to develop the Incident Response Team, and serves as a member
 - Performs network traffic analysis to identify potentially malicious activity
 - Performs malware analysis on suspicious information systems
-

Key Competencies

Knowledge –

- Expert knowledge in enterprise vulnerability scanner operations and analysis
- Expert knowledge in hardening computer configurations (Microsoft Security Templates, DISA STIGs, etc.)
- Expert knowledge in configuration and change management procedures
- Expert knowledge of Microsoft and other major vendor patch deployment tools
- In-depth knowledge in troubleshooting Microsoft operating systems and application conflicts
- In-depth knowledge of incident response structure and operations

Skill and Ability – Capacity to perform a function. Examples include operating equipment, utilizing certain software, applying occupational standards (such as accounting principles), negotiating agreements, developing operational or strategic plans, planning and conducting training sessions, analyzing data, oral/written communication.

- Operating vulnerability scanners (e.g. Tenable Nessus and/or eEye Retina)
- Conducting vulnerability scanner analysis and developing remediation plans
- Conducting setup and using Microsoft WSUS tool
- Creating and troubleshooting policies for ForeScout CounterAct appliance
- Developing customized security baselines for Microsoft operating systems
- Conducting network “discovery” scans for an enterprise environment
- Using network tools to monitor and enforce configuration management policies
- Scanning for malware or other unauthorized applications
- Maintaining an inventory of authorized software and services
- Scanning for unauthorized or “rogue” computers or access points
- Using application penetration tools (e.g. Burp Suite Pro and ZAP)

Behavioral – Has strong leadership attributes, enjoys teaching and mentoring, and works very effectively with small groups. Has well developed problem solving skills, concentrating on root cause, rather than symptoms. Is a self-starter, retains focus in busy environments. Ability to build rapport and work in close collaboration with other IT technical professionals.

Qualifications and Credentials

REQUIRED

- Training and experience using enterprise grade vulnerability scanners
- Training and experience configuring and using automated security patch solutions
- Experience as a member of an enterprise incident response team

Experience

- Five (5) years as a network security manager or senior analyst for an enterprise
- Three (3) years as a member of an enterprise incident response team
- Five (5) years configuring security baseline settings for Microsoft workstation and server operating systems, in an medium to large enterprise environment
- Five (5) years of experience maintaining security standards for a government agency or organization (state or federal)

Education

Bachelor degree in computer science or information assurance required

- Relevant experience may substitute year for year for education

Certifications, Memberships, Licensure or Permit (Current Certified)

Minimum required:

- COMTIA Security+ **or** Certified Information Systems Security Professional (CISSP)

Salary Range: 70

- Workweek may fluctuate depending on workload or agency need.
 - Travel (including overnight) may be required to meet job responsibilities.
 - This position is exempt from the Fair Labor Standards Act (FLSA).
-

Established: 12/14