

SENIOR INFORMATION SECURITY ANALYST

>[Click Here for Further Information](#)<

Exciting Career Opportunity!

BENEFITS OF WORKING FOR AOC

- ◆ The state of Washington offers a comprehensive benefits package, including health, dental, life and long-term disability insurance
- ◆ Vacation leave
- ◆ Sick leave
- ◆ Shared leave
- ◆ Family – Medical leave
- ◆ Military and Civil leave
- ◆ Eleven paid holidays per year
- ◆ A state retirement plan
- ◆ Deferred Compensation Program
- ◆ Membership in the Public Employees' Retirement System
- ◆ Opportunities to participate in a Medical Flexible Spending Arrangement and Dependent Care Assistance Programs

WHERE IS AOC LOCATED?

The Administrative Office of the Courts is located in Olympia, Washington, on Interstate 5 between Seattle, Washington and Portland, Oregon. Olympia and the surrounding Thurston County area offer numerous social, recreational, educational, and cultural opportunities. Natural features include Puget Sound, the Olympic National Park to the west, and Mt. Rainier to the east. Mount St. Helens and the Pacific Ocean beaches are within a two hour drive of the city.

SALARY: \$69,648 TO \$91,332 per year DOQ

LOCATION: Olympia, Washington

OPENS: August 18, 2016

CLOSES: August 26, 2016

POSITION PROFILE

The Senior Information Security Analyst (SISA) is responsible for conducting application vulnerability assessments, performing comprehensive risk analysis, and producing detailed reports and recommendations. The position works closely with AOC project managers and technical leads for application development, procurement, and integration. The SISA also serves as a member of the Enterprise Incident Response Team.

Extensive experience and high degree of technical proficiency with web application penetration tools and exploitation techniques. Experience creating detailed network diagrams, threat models, and presentations illustrating vulnerabilities and critical control points.

DUTIES AND RESPONSIBILITIES

Performs and analyzes vulnerability scans and penetration testing for locally developed and agency procured web enabled applications.

Develops detailed risk analysis reports describing assessed vulnerabilities, risk levels, and recommended security controls.

Collaborates with AOC project managers and technical leads throughout the application development and deployment lifecycle, providing expertise and

The Administrative Office of the Courts (AOC) is a department of the Washington State Supreme Court. Established by state statute in 1957, the mission of the AOC is to advance the efficient and effective operation of the Washington State judicial system.

The AOC carries out its mission through formulation of policy and legislative initiatives, court technology development, educational programs, and program support for 428 Washington judges and their staff. The AOC draws its employees from a wide range of professions including legal, information technology, research, education, and judicial administration.

The agency is administered by an executive team that is committed to maintaining a dedicated and diverse workforce that provides the highest quality of customer service and continuously develops strategies for improving the performance and effectiveness of the court system in Washington.

AGENCY-WIDE VALUES & COMPETENCIES

Agency Values

- Integrity
- Honesty
- Accountability
- Teamwork
- Trust
- Respect
- Customer Service
- Communication

Behavioral Competencies

- Influencing
- Problem solving
- Planning/organizing
- Consulting
- Relationship building
- Tact/diplomacy

recommendations to integrate effective security controls.

Interacts with "Network Operations" team to understand network topology and develop library of network diagrams for use with assessments and security operations.

Performs network traffic analysis to identify potentially malicious activity.

Performs malware analysis on suspicious information systems.

Assists in development of configuration management standards and procedures.

Assists in the efforts to establish and maintain security hardened workstation and server configurations.

Assists in troubleshooting conflicts resulting from recommended security controls and configurations.

Assists Information Security Officer with establishment and maintenance of the Information Security SharePoint site.

Assists in development of the Enterprise Incident Response Team, and serves as a member.

Knowledge –

- Expert knowledge of web application security standards and best practices (W3C, OWASP, SANS, Microsoft, etc.)
- Expert knowledge in hardening computer configurations (Microsoft Security Templates, DISA STIGs, etc.)
- Expert knowledge in 'Cloud Computing' technologies and secure implementations
- In-depth knowledge in MS Internet Information Server (IIS) configuration and management
- In-depth knowledge in IT configuration and change management procedures
- In-depth knowledge of incident response structure and operations
- Basic knowledge of project management terms, methodologies, and goals

Skills 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.

- Configuring and effectively operating web application penetration tools (e.g. Burp Suite Pro, Zed Attack Proxy (ZAP), etc.)
- Creating 'Threat Models', using Visio or 'Microsoft Threat Modeling Tool'
- SharePoint site administration
- Creating professional looking MS PowerPoint presentations
- Creating, configuring, and utilizing virtual computing systems
- Applying OWASP standards to web application assessments

Behavioral – Has excellent interpersonal skills, and enjoys collaborating and solving problems as part of a focused team effort. Is a strong presenter, effectively sharing details and concepts to diverse groups. Has well developed problem solving skills, concentrating on root cause, rather than symptoms. Is a self-starter, and retains focus in busy environments. Ability to build rapport and work in close collaboration with both technical and non-technical staff.

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)

See next page for further qualifications and application instructions.

The AOC is committed to the practice of equal employment opportunity and non-discrimination for all persons without regard to race, creed, color, national origin, sex, marital status, sexual orientation, age, honorably discharged veteran or military status, or the presence of any sensory, mental, or physical disability or the use of a trained dog guide or service animal by a person with a disability. Persons of disability needing assistance in the application process, or those needing this announcement in an alternative format, please contact Colleen Clark, AOC Human Resource Office, at (360) 704-4143 or fax (360) 586-4409, or via email to Employment@courts.wa.gov.

SPECIAL NOTE:

All employees hired by the Administrative Office of the Courts are required to be fingerprinted for a criminal history background check with continued employment with the AOC contingent upon the results of this background check.

Application materials will be screened for the purposes of determining who will be selected for an interview.

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)

Minimum required:
COMTIA Security+ **or** Certified Information Systems Security Professional (CISSP)

THE PREFERRED CANDIDATE WILL HAVE

Other security-related industry certifications are a plus.

Special: Advanced competency with the following tools or products:

- ◆ Microsoft IIS
- ◆ Linux Command Line
- ◆ 'Regular Expressions' (RegEx)
- ◆ VMware

APPLICATION PROCEDURE

To be Considered for this Position, Please Submit:

- A **cover letter** specifying how you meet the qualifications of the position (no more than two pages);
- A chronological **resume** describing your prior job experience to include employers, dates of employment (by total months/years), description of duties, and education; and
- A completed AOC **Application for Employment** (found at www.courts.wa.gov/employ).

Failure to submit the required materials listed above may eliminate your application from consideration.

Submission by email is preferred: Employment@courts.wa.gov; or you can fax to (360) 586-4409; or send by mail to Administrative Office of the Courts, PO Box 41170, Olympia, WA 98504-1170