Judicial Council of Georgia

Administrative Office of the Courts
JOB ANNOUNCEMENT

Security Analyst I

Recruitment Period:	Open Until Filled. Submit Resume and Cover Letter		
Number of Positions:	1 (One) position	**FLSA Status:**	Exempt
Hiring Salary:	$55,001 - $65,001(USD)	**Position Location:**	Fulton County, GA

Job Summary

A Security Analyst will have proven their skills in Information Security, Information Systems, Packet Analysis, and Data Loss Prevention.

The Security Analyst provides support for complex computer network exploitation and defense techniques to include deterring, identifying, and investigating computer and network intrusions; providing incident response and remediation support; identifying vulnerabilities; developing secure network designs and protection strategies, and audits of information security infrastructure. The Analyst will provide technical support for continuous monitoring and the prevention of computer/network exploitation. The Analyst will provide technical support for forensics services and will research and maintain proficiency in open source and commercial computer exploitation tools, attack techniques, procedures, and trends.

Acting under limited supervision of a senior team member, this position examines information to help identify risks and threats then recommends and helps implement strategies to stop those threats from adversely affecting the Agency's network or property. In this role, you will work under a senior team member to develop your skills and learn more about the tools and techniques used to be more effective in your job.

Candidate must reside within 50 miles of the State Capitol of Georgia.

To be successful in this role a candidate must possess excellent customer service, observation, written and verbal communication skills, and acute attention to detail. The candidate must be able to effectively solve problems with limited direction. The candidate must demonstrate proficiency managing systems and preventing threats.

Job Responsibilities and Performance Standards

- Actively monitors and supports internal and external infrastructure systems (Incident & Problem Management), liaising with colleagues as necessary
- Compiles comprehensive audit reports identifying potential risks/threats
- Reports on Key Performance Indicators (KPIs) in relation to governance, compliance, and regulation; ensures thorough and accurate reporting to relevant stakeholders
- Advises and supports IT with defining specific information security controls and policies
- Leads the security awareness program and ensure all staff achieve regular completions
- Assists with security assessments in relation to projects and change management
- Maintain the threat and information risk register and recommend the appropriate remediation
- Develop general and detailed documentation describing system specifications and operating instructions
- Ensure infrastructure, applications, and data security/privacy controls are maintained in compliance with department and regulatory policies
- Participate as a member of the Service Desk support team resolving client-side issues as and when needed
- Develop appropriate project related documentation/business cases. Implement projects in accordance with policy ensuring the identified goals and objectives are delivered on time and within budget
- Procure IT related resources in line with company policy and ensure accurate record of assets is maintained
- Support business continuity processes (backups, replication, etc.) through continued documenting and testing of infrastructure environment
- Help staff with use of the company systems, providing training where necessary
- Responds to internal and external inquiries and requests for security support while providing direct assistance and issue resolution to security incidents and threats across the agency's infrastructure.
- Collaborates with other I.T. staff to develop and improve the creation and maintenance of supporting documentation.
- Monitors and utilizes an enterprise helpdesk ticketing system to effectively communicate with other team members and clients.
- As assigned, directly assists, or supports other I.T. projects and initiatives.
- Fosters innovation by continuing to familiarize themselves with new trends, technologies, and best practices relevant to their role.

Minimum Skills, Training, and Experience

- **CompTIA Security+, CASP+, CySA+** certification or equivalent
- Certified networking credential (**CompTIA Network+, Cisco CCNA**) or equivalent
- **1 or more years of experience** managing an endpoint security solution
- **Strong problem-solving abilities**
- Familiarity with common **I.T. protocols, technologies, and systems**
- Thorough understanding of **Microsoft Windows 10/11** and **Microsoft Office** applications
- Experience with an enterprise directory (e.g., **Azure Active Directory**)
- **Excellent interpersonal and customer service skills**
- **Possess the ability to communicate complex and technical concepts to a non-technical, general audience**
- Strong **hands-on information security skills** and experience
- Superior **organization** and **follow-up skills**
- Understanding of the **Incident Response Phases**
- Proven **capability to consult** on large enterprise information security matters
- Must be comfortable **acting as a liaison** between Information Security, Legal, HR, and Audit teams during security incidents
- In depth understanding of **operating systems, network/system architecture, protocols, and enterprise services,** and **enterprise architecture design**
- Capability to quickly **parse data**
- Understanding of **threats, vulnerabilities,** and **exploits**
- Previous experience in Information Technology or Information Security with a **track record of successful accomplishments**
- Previous experience developing and/or deploying **mitigation techniques** for **defending networks**

Preferred Qualifications

- A 2 or 4-year undergraduate degree from an accredited college or university
- Experience with cloud or IaaS solutions (e.g., AWS, Azure, Office 365, GCC)
- Experience with mobile device management (MDM)
- Experience with other operating systems, like GNU/Linux, OSX
- Proven experience designing, implementing, and managing innovative solutions to complex security and infrastructure environments
- Experience responding to information security incidents
- Expertise performing packet analysis

To Apply:
Send your resume and cover letter, in **.pdf** format, to resume@georgiacourts.gov.

Subject line must include: **Security Analyst I, IT Division**

Additional Information:
Due to the volume of applications received, we are unable to provide information on application status by phone or email. All qualified applicants will be considered but may not necessarily receive an interview. Selected applicants will be contacted by the hiring manager to complete next steps in the hiring process.

Applicants who require accommodations for the interview process should contact resume@georgiacourts.gov or call 404-463-0638. The JC/AOC will attempt to meet reasonable accommodation requests whenever possible.