United States Court of Appeals
for the Seventh Circuit
219 South Dearborn Street
Chicago, Illinois 60604

2024-5
2/26/2024

POSITION VACANCY

Position: Cybersecurity Specialist

Position Type: Full-time, temporary (funding dependent)

Salary Range: CL-27/28 – $64,781-$126,233 per annum in Chicago

Closing Date: Open until filled; applications received by March 18, 2024 will receive first consideration.

Position Overview:

The Circuit Executive's Office, located in the Everett McKinley Dirksen U.S. Courthouse in Chicago, Illinois, provides policy development, administrative, and technical and staff support to the Chief Judge of the Circuit and Judicial Council of the Seventh Circuit; the United States Court of Appeals for the Seventh Circuit; and the district and bankruptcy courts, probation and pretrial offices, and federal defender services within the Seventh Circuit.

The Cybersecurity Specialist is part of a cybersecurity team, under the guidance of the Circuit Internet Security Officer (CISO), that proactively and reactively defends the circuit and the court units within from cyber threats leveraging analytic techniques, internal defense measures, and appropriate response actions to mitigate threats and maintain operational security and functionality of judicial systems and the judicial process.

Position Duties and Responsibilities:

- Use cyber defense tools for continual monitoring and analysis of system activity to identify suspicious and malicious activity.
- Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
- Work with court units within the circuit to provide incident response to any possible attacks/intrusions, anomalous activities, and misuse activities, and distinguish these incidents and events from benign activities.

- Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
- Notify CISO of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.
- Provide expert technical support to circuit-wide cyber defense technicians to resolve cyber defense incidents, track them, and document them from initial detection through final resolution.
- Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, and direct system remediation) tasks to court unit Incident Response Teams (IRTs).
- Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
- Perform technical and non-technical (i.e., people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable remediation.
- Create and employ methodologies, templates, guidelines, checklists, procedures, and other documents to establish repeatable processes across the circuit's information technology security services.
- Oversee and document all technical remediations from beginning to end.
- Travel within the circuit (Illinois, Indiana, and Wisconsin) as required.
- Perform occasional off-hour work.
- Perform other duties as assigned.

Qualification Requirements:

Applicants must possess (1) an undergraduate degree in Cybersecurity, Computer Science, Information Security, Computer Forensics, or a similar field of study from an accredited college or university; (2) excellent problem solving skills; (3) an understanding of cybersecurity principles, including threat modeling, risk assessment, and security controls; and (4) knowledge of security tools, such as firewalls, intrusion detection/prevention systems, and anti-virus software, and experience in managing and maintaining them.

Qualified applicants must also possess outstanding written and oral communication skills; strong interpersonal and analytical skills; and the ability to work amicably and professionally as part of a team.

As a condition of employment, the selected candidate must successfully complete a background investigation with periodic updates every five years thereafter.

Preferred Qualifications:

An advanced degree in Cybersecurity, Computer Science, Information Security, Computer Forensics or a similar field of study from an accredited college or university. Experience with configuring, maintaining, and using Websense, Tenable Security Center/Nessus, and Splunk. Prior experience working with computer networks, endpoints and network management tools, including the understanding of principles, practices, and techniques of data communication and network management. Federal court experience and/or experience working with court-related computer systems.

Benefits:

Benefits include eleven paid holidays, paid vacation and sick leave, participation in the Federal Employees Retirement System (FERS), Thrift Savings Plan (401k), Benefits also include optional participation in the Federal Employees Health Benefits Program (FEHB), Federal Employees Group Life Insurance Program (FEGLI), Flexible Benefits Program, and Dental and Vision Insurance. Limited telework options are available. Information can be found on the court's website under Human Resources at: www.ca7.uscourts.gov.

Application:

Consideration will only be given to those individuals who apply through the court's online applicant tracking system and provide a resume and cover letter. Visit our applicant tracking system at: https://www.governmentjobs.com/careers/uscourtsilnd/7thcircuitcoa.

Due to the anticipated large response to this announcement, only those interviewed will be notified of the selection outcome. The court reserves the right to modify the conditions of this job announcement or to withdraw the announcement without written notice to applicants. Travel expenses for interviews cannot be reimbursed.

Please note that this position is covered by the Fair Chance Act and requires that applicants provide criminal history information prior to receiving any conditional offer of employment. All information provided by applicants is subject to verification and background investigation. Applicants are advised that false statements or omission of information on any application materials may be grounds for non-selection, withdrawal of an offer of employment or dismissal after being employed.

Pursuant to the Immigration and Reform Act of 1986, selection is contingent upon providing proof of being legally eligible to work in and for the United States. Employees are required to use Electronic Fund Transfer (EFT) for payroll deposit.

THIS OFFICE IS AN EQUAL OPPORTUNITY EMPLOYER