UNIFIED JUDICIAL SYSTEM
POSITION DESCRIPTION

COMPUTER SECURITY ANALYST

CLASS CODE: 99-31-54

POSITION PURPOSE

Implements, monitors, and maintains cybersecurity and data security measures across Unified Judicial System (UJS) networks, servers, workstations, applications, and cloud-integrated services to ensure the confidentiality, integrity, availability, and secure access of UJS systems and data.

DISTINGUISHING FEATURE

This position performs enterprise-level cybersecurity analysis and operations using established security controls. Responsibilities focus on continuous cybersecurity monitoring, threat detection, incident investigation, correction and prevention of system vulnerabilities. The position requires advanced technical judgment, ongoing risk assessment, and coordination with internal and external security stakeholders.

MAJOR RESPONSIBILITIES

Note: The duties listed are typical examples of work performed by positions in this job classification. Not all duties are included, nor is the list exclusive.

1. Identifies, audits, evaluates, assesses, and mitigates cybersecurity risks to the UJS to ensure continued operations.
    a. Monitors enterprise security tools, logs, alerts, and system events to identify threats, vulnerabilities, and anomalous activity.
    b. Investigates security incidents, documents findings, performs root-cause analysis, and implements corrective actions.
    c. Escalates security incidents and risks in accordance with procedures established by the CISO.
    d. Proactively identifies vulnerabilities and mitigates risks prior to exploitation.
2. Monitors, automates, and coordinates security patches and system hardening to ensure systems remain secure, compliant, and operationally stable.
    a. Monitors, tests, installs, and validates operating system and application security patches.
    b. Develops and maintains scripts to deploy updates, audit compliance, and reduce manual processes.
    c. Performs system configuration to reduce risk and meet the established security standards.
    d. Coordinates patching activities to minimize operational disruption while maintaining security compliance.

3. Maintains enterprise security platforms for endpoint protection, secure access, and authentication to ensure continuous threat visibility and controlled access.
    a. Administers endpoint protection, malware prevention, threat detection, and monitoring platforms.
    b. Manages secure file transfer services and access controls.
    c. Administers authentication and credential management systems, including password policies and multi-factor authentication solutions.
    d. Maintains monitoring systems to ensure consistent visibility across servers, workstations, and applications.
4. Investigates cybersecurity incidents and supports continuous security improvement efforts in collaboration with the CISO to reduce organizational risk.
    a. Analyzes and investigates cybersecurity incidents, assesses associated risks, and implements or supports containment and remediation actions in coordination with the CISO.
    b. Assists with forensic analysis and evidence collection, as appropriate.
    c. Participates in enterprise risk management and the continuous improvement of security controls.
    d. Identifies emerging risks and proactively recommends measures to reduce impact to UJS operations.
    e. Researches and evaluates emerging security technologies and provides recommendations based on risk, compatibility, and organizational need.
5. Assists with disaster recovery and backup processes to ensure system restoration following disasters, cybersecurity incidents, or system failures.
    a. Tests, maintains, and updates disaster recovery and business continuity procedures.
    b. Validates backup and recovery processes for servers and other critical systems.
6. Creates and maintains security documentation and compliance reporting.
    a. Develops and maintains documentation for security configurations, tools, system dependencies, desk books, procedures, and standards.
    b. Implements and maintains automated security and compliance reporting.
7. Provides guidance and training to staff on cybersecurity tools, processes, and best practices.
    a. Provides technical guidance to UJS staff on security-related matters.
    b. Assists and trains technical staff on cybersecurity tools, processes, and best practices.
8. Performs other work as assigned.

SUPERVISORY FUNCTIONS

This position does not have supervisory authority.

ESSENTIAL FUNCTIONS REQUIRE

In-state travel for project implementation and meetings; in-state and out-of-state travel for training; evaluating and understanding computer systems interactions, including hardware, software, and data storage capabilities; occasional work in nonstandard environments during system installations; extended periods of computer use; working outside normal business hours when required; operating computer hardware, systems, and technology standard office equipment; and attendance in accordance with applicable rules and policies.

The incumbent must effectively work with coworkers and the public; understand, evaluate, and analyze statistical data and draw reasonable and accurate conclusions from that data; manage stress appropriately; demonstrate organizational skills; meet deadlines; show initiative and motivation; and communicate complex technical and security concepts clearly, both verbally and in writing, to non-technical individuals.

PROBLEMS AND CHALLENGES

Challenges include maintaining secure and reliable operation of complex, interdependent systems in a constantly evolving threat environment; ensuring timely remediation of vulnerabilities; balancing operational availability with security requirements; and maintaining accurate and current documentation for enterprise infrastructure.

DECISION-MAKING AUTHORITY

The position exercises independent judgment in analyzing cybersecurity threats and incidents and in recommending data security measures, policies, procedures, and access controls. Decisions involving significant risk exposure, policy changes, or enterprise-wide impact are referred for review and approval and are made in consultation with leadership.

CONTACT WITH OTHERS and PURPOSE

Regular contact with the CISO to coordinate cybersecurity initiatives, report risks and incidents, and support enterprise security objectives; with BIT security staff to coordinate responses to identified vulnerabilities; with UJS IT staff to provide security guidance; and with vendors and external partners regarding security tools, updates, and security incidents.

WORKING CONDITIONS

The incumbent works in a typical office environment and may be required to work on-call or after hours to address critical security incidents or system vulnerabilities, as approved by a supervisor.

COMPETENCIES/QUALIFICATIONS FOR APPOINTMENT

Knowledge, Skills and Abilities:

Knowledge of:

- cybersecurity principles, risk management, and vulnerability mitigation;
- enterprise operating systems, patch management, and endpoint protection platforms;
- identity and access management technologies, including Active Directory, Group Policy, and multi-factor authentication;
- security information and even management (SIEM) tools and log analysis techniques;

- disaster recovery and business continuity concepts related to system security.

Skill in:

- analyzing security data and system configurations to identify risk and compliance gaps;
- developing automation or scripts to improve operational efficiency and consistency;
- creating clear technical documentation, reports, and compliance artifacts;
- monitoring systems and security tools to identify trends and anomalies.

Ability to:

- assess security risks and implement appropriate technical or administrative controls;
- communicate complex technical and security concepts to non-technical audiences;
- anticipate potential issues and proactively mitigate security or operational risks;
- support compliance, audit, and reporting requirements through accurate data and analysis.

Education:

Bachelor's degree from an accredited college or university in computer science, cybersecurity, information technology, or a related field.

Experience:

Two (2) years of experience performing cybersecurity, systems security, or data security functions in a network environment, or an equivalent combination of education and experience.