

Director of Security Intelligence and Operations Center

Position Information:

Title: Director II, Info Technology

Business Title: Director of Security Intelligence and Operations Center

Location: Manhattan

Reports To: IT Chief Information Security Officer

Type: Full-time; 12 months; Supervisory; Exempt

Term: 1 year

Hours of work: 8am – 5pm

Occasional overnight travel

Job Responsibilities:

85% Manage Security Intelligence and Operations Center Team (SIOC)

- Spearhead SIOC's growth and evolution, actively improving our cyber incident response capability
- Respond to cybersecurity incidents, especially as an escalation point for high-priority or highly complex incidents
- Drive development and continuous updating of standard operating procedures (playbooks) and documentation for SIOC domains, including use of automation and integrations where possible.
- Manage the recruitment, development, and performance of SIOC personnel.
- Develop and maintain key performance indicators, key risk indicators, and other measurements of the effectiveness of SIOC programs
- Collaborate with the K-State IT leadership team to provide cross-functional support and guidance.
- Develop and maintain open, productive working relationships with internal departments, regulatory agencies, law enforcement agencies, security and technology vendors.
- Prepare and present accurate and timely information in response to audits.
- Train, mentor, and guide other team members (across both the SIOC and other IT teams) on cyber incident response practices, tooling, and capabilities.

10% Support Cloud Center of Excellence (CCoE) to support K-State's cloud-first infrastructure initiative

- Work within CCoE to present and review metrics for CCoE security progress.
- Document, communicate and encourage best security practices for securing and monitoring cloud service across the enterprise.

5% other duties as assigned

Organizational Information

The IT organization of Kansas State University is responsible for the life cycle planning of cloud and identity access services through the phases of strategize, architect, select, deploy, operate, evolve, and retire. The SIOC Manager is a highly visible and vital role. The role develops, oversees, and prioritizes actions during the detection, analysis, and containment of an incident. This role is also responsible for conveying the special requirements of high severity incidents to the rest of the university.

Qualifications

Required

Minimum Qualifications:

Bachelor's degree

Five - Ten years of relevant experience

Preferred

10 or more years in IT and business/industry

Ability to identify ways to improve effectiveness of work methods, procedures, distribution of work assignments, management controls, information and documentation systems, and similar functions

Excellent troubleshooting skills and the ability to logically think through problem situations

Excellent verbal and written communication skills

Expert communicator to influence acceptance of new methods, work procedures, organizational relationships, etc., that affect the basic content and character of operations, relationships with other groups, and overall mission goals

Expert knowledge of analytical and evaluative methods, supplemented by a practical knowledge of accounting theory, concepts, and practices, and of auditing techniques

Knowledge of Kansas State University structure, missions, programs, and organizational relationships

Masters' degree + 3 years of experience institution (preferred in computer science, information systems, business administration or related field)

Solid understanding of Network technologies, Application security, and infrastructure architecture

Three to five years of leadership responsibility in managing multiple, large, cross-functional projects and influencing senior-level management and key stakeholders

Able to work effectively and produce consistent results with a minimum of supervision.

High level of personal integrity and the ability to handle confidential matters with proper judgment.

Must have a high sense of urgency.

Ability to lead a team under pressure.

NIST CSF knowledge and understanding.

Ability to represent Kansas State University, as an analytical expert, within and outside the university, and to resolve different and entrenched viewpoints.