Legislative Assembly Service
SASKATCHEWAN

Security Analyst - (Permanent, Full-Time, onsite)

Position Summary

Reporting to the Manager ITS, the position is responsible for monitoring, analyzing and responding to security threats and vulnerabilities to mitigate security risks and protect enterprise IT systems and data. The position is key in designing and implementing security measures to protect the LAS's computer networks and information architecture. This includes conducting vulnerability scans, penetration test, operating and monitoring network and intrusion detection/prevention systems. The position also recommends security solution and advises on systems and application-level security configuration to mitigate security risks as required.

Primary Responsibilities

- Monitor networks, systems, and applications for suspicious activity, security breaches, potential vulnerabilities and collaborate with security service providers to respond to threats in real time. Use security tools and software to identify and analyze security threats.
- Implement and maintain security controls such as firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint security, and automated threat detection tools to protect infrastructure and assets.
- Conduct risk assessments and vulnerability scans on systems and infrastructure, identifying and prioritizing risks, and recommending appropriate safeguards.
- Investigate and respond to security incidents and vulnerabilities, coordinating mitigation actions in accordance with the organization's incident response plan. This includes collaborating with security service providers to investigate the incident and coordinating an effective response to mitigate damage and prevent future occurrences.
- Develop and enforce security policies, procedures, and user awareness training to ensure staff understand their role in maintaining a secure environment.
- Plan and execute incident response and disaster recovery activities, working with ITS leadership and security service providers to protect data and restore operations quickly after cybersecurity events.
- Assist technical support staff with implementing security safeguards, such as patching, anti-malware, secure configuration, and access controls.
- In collaboration with security service providers to operate and monitor security software and tools; ensuring they are updated, functional, and aligned with current threat landscapes.
- Work with IT analysts to integrate security into system development and operations, ensuring secure design and deployment of applications and infrastructure.
- Document and review security policies, procedures, system configurations, and test results, maintaining audit-ready records.
- Perform security audits and compliance reviews, reporting findings and developing corrective action plans where needed.
- Prepare detailed reports on security incidents, vulnerabilities, and security measures for the review of management and other stakeholders.
- Analyze network traffic, intrusion attempts, and system alerts for anomalies, trends, and potential breaches.
- Confer with clients to identify and document system requirements, including physical and technical security risks.

- Report security risks and provide recommendations to the Director and Manager of ITS to guide strategic decisions.
- Develop scripts, tools, and procedures to automate monitoring, scanning, and reporting activities for improved efficiency.
- Stay current on evolving threats, vulnerabilities, and best practices in cybersecurity to inform ongoing risk management.

Job Knowledge

Knowledge is typically obtained through a bachelor's degree in Cybersecurity, Information Security, or a related field, combined with three or more years of progressively responsible experience in cybersecurity roles involving system monitoring, risk assessment, incident response, and the implementation of security protocols—preferably in a public sector or enterprise-level IT environment.
Certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or Certified Ethical Hacker (CEH) are preferred and may support ongoing professional development and credibility in the role.

In-depth knowledge of:

- Security principles and technologies, including identity and access management (IAM), encryption protocols, endpoint protection, and intrusion detection and prevention systems (IDS/IPS).
- Risk assessment methodologies, penetration testing, vulnerability management, and incident response strategies aligned with frameworks such as NIST, ISO 27001, and CIS Controls.
- Security information and event management (SIEM) systems, malware detection and remediation tools, and log analysis techniques to monitor and protect organizational assets.

Working knowledge of:

- IT network infrastructure components, including their integration into secure system architecture.
- Secure coding practices and basic scripting to automate security tasks and improve threat detection capabilities.
- Change management processes and IT service management tools, particularly as they relate to maintaining a secure and compliant operational environment.

Demonstrated ability to proactively identify and respond to evolving security threats, educate users on cybersecurity practices, implement and maintain layered security controls, and collaborate with IT teams to embed security throughout infrastructure and software lifecycles. The role demands strong analytical thinking, discretion, and sound judgment in protecting sensitive systems and data within the Legislative Assembly environment.

Employees of the Legislative Assembly Service are required to provide non-partisan confidential service to all Members of the Legislative Assembly.

A Criminal Record Check is required for this position.