IDENTIFICATION

Department	Position Title	
Aurora College	Cyber Security Analyst	
Position Number	**Community**	**Division/Region**
91-17555	Yellowknife	Corporate Services & Administration Division

PURPOSE OF THE POSITION

The Cyber Security Analyst is responsible for the development and implementation of security policies, procedures and standards for the Aurora College information, and technology networks and systems; monitoring and evaluating internal and external threats as they arise within the campuses, Community Learning Centres (CLCs), and the Aurora Research Institute (ARI) offices.

SCOPE

Reporting to the Manager, Information Systems and Technology (IS&T), the incumbent will be reviewing Aurora College information and technology networks and systems, identifying potential vulnerabilities, implementing mitigating actions to protect it from unauthorized access, and documenting detections. This responsibility extends to all Aurora College campuses, Community Learning Centres (CLCs), the Aurora Research Institute (ARI) offices, and the National Research and Educational Network (NREN) where applicable.

The incumbent is required to exercise professional judgment in determining how best to meet work priorities and objectives. The quality and reliability of the College's information systems is critical. As the campus, associated CLCs, and ARI offices are fully networked environments, failure to provide security and monitoring services will have a direct impact on the ability of the College to provide services to staff and students.

The incumbent will implement and manage security systems, including Security Information and Event Management (SIEM), intrusion detection and prevention (IDS/IPS), vulnerability management, and log management systems to protect Aurora College's network and server infrastructure. Additionally, they will collaborate with contractors and external partners, including the Government of the Northwest Territories (GNWT) and the NREN, to improve Aurora College's security posture, as well as that of the NREN. The position is guided by the Aurora College Strategic and Business Plans, the Code of Ethics, the Aurora College Act, the

Education Act, GNWT policies, regulations, legislation and guidelines, and the UNW Collective Agreement.

JOB RESPONSIBILITIES

1. **Coordinate and conduct threat detection and analysis for college campuses, associated CLCs, and ARI offices to ensure the protection of data, maintenance of operational continuity, safeguarding of research and intellectual property, and preventing unauthorized access to the College's networks and systems.**

- Monitor security event logs and alerts from various sources, including intrusion detection/prevention systems, firewalls, and antivirus solutions.
- Employ monitoring tools, such as Security Information and Event Management (SIEM) systems, to collect and analyze logs from various sources, including network devices, servers, and applications.
- Define and implement detection rules within the SIEM to identify specific indicators of compromise or abnormal behaviors.
- Monitor for unusual or suspicious activities that may indicate security threats, such as unauthorized access attempts, unusual data transfers, or patterns indicative of malware.
- Analyze network traffic patterns to identify unusual or malicious activities. Look for signs of lateral movement, data exfiltration, or communication with known malicious entities.
- Review and analyze logs from various sources, including firewalls, intrusion detection/prevention systems, and authentication logs.
- Prioritize and classify identified incidents based on severity and potential impact.
- Quickly assess the scope of an incident, its potential impact on the College, and the necessary response actions.
- Collaborate with incident response team, system administrators, and other relevant stakeholders to investigate and respond to identified incidents.
- Conduct post-incident analysis to understand the root cause of security incidents and identify areas for improvement in detection and response capabilities.
- Update detection rules and procedures based on lessons learned from incidents.
- Maintain detailed records of incidents, investigations, and response activities.
- Provide regular reports to management and relevant stakeholders on the state of cyber security threats, incidents, and the effectiveness of the College's defense mechanisms.

2. **Coordinate and conduct vulnerability assessments to identify weaknesses, flaws, and potential security risks within the College's systems, networks, and applications with the goal of proactively addressing vulnerabilities before they can be exploited by malicious actors.**

- Perform regular vulnerability assessments using industry-standard tools.
- Define the scope of the vulnerability assessment, including the systems, networks, and applications to be assessed.
- Identify the assets that are critical to the College and prioritize them based on their importance to business operations and continuity.
- Ensure a thorough understanding of the College's IT infrastructure and compile an inventory of all assets within the defined scope of the vulnerability assessment, including servers, workstations, network devices, databases, and applications.

- Utilize automated vulnerability scanning tools to identify known vulnerabilities in the target systems.
- Schedule regular scans to ensure ongoing visibility into the security posture of the College.
- Analyze the results of vulnerability scans to identify vulnerabilities, misconfigurations, and security weaknesses.
- Evaluate the impact and likelihood of each identified vulnerability, considering factors such as the sensitivity of the affected data, potential business impact, and the ease with which an attacker could exploit the vulnerability.
- Prioritize vulnerabilities based on severity, potential impact on the College, and the likelihood of exploitation.
- Document all identified vulnerabilities, including their details, severity, and recommended remediation actions.
- Provide clear and concise reports for technical and non-technical stakeholders.
- Collaborate with system administrators and network engineers to validate and remediate identified vulnerabilities, ensuring timely patching and configuration changes, considering factors such as the criticality of systems, potential business impact, and available resources for remediation.
- After remediation efforts, re-scan systems to validate that vulnerabilities have been successfully addressed.
- Confirm that security patches have been applied, configurations have been corrected, and security controls are effective.
- Implement continuous monitoring practices to regularly assess the security posture and identify new vulnerabilities that may emerge over time.
- Stay informed about software updates, patches, and emerging threats to adapt vulnerability assessment practices accordingly.
- Use insights gained from vulnerability assessments to enhance security policies, procedures, and preventive measures.

3. **Coordinate and conduct incident response focused on the detection, response, and recovery from a security incident with the goal of minimizing the impact of the incident, identifying the root cause, and implementing measures to prevent future occurrences.**

- Develop and maintain the College's incident response plan (IRP) including roles and responsibilities, communication procedures, categories and severity levels, and a step-by-step guide for responding to different types of incidents.
- Conduct regular tabletop exercises to familiarize the incident response team with the procedures and enhance their response capabilities.
- Lead incident response efforts, coordinating with cross-functional teams to contain, eradicate, and recover from security incidents.
- Quickly assess the initial impact, scope, and severity of the incident. Classify the incident based on predefined categories and severity levels.
- Activate the incident response team according to the roles and responsibilities outlined in the incident response plan.
- Ensure that all necessary stakeholders, both technical and non-technical, are informed and engaged in the response effort.

- Take immediate steps to isolate affected systems or networks to prevent further spread of the incident.
- Implement containment measures to minimize the impact and prevent the escalation of the incident.
- Maintain transparent and regular communication with key stakeholders, including management, legal, IT team, and external parties if necessary.
- Provide status updates, incident summaries, and recommendations for ongoing actions.
- Preserve evidence related to the incident for forensic analysis and thorough investigation into the root cause of the incident. This may include collecting logs and other relevant data.
- Document all aspects of the incident response, including actions taken, findings, and outcomes.
- Comply with legal and regulatory requirements related to incident reporting and notification.
- Conduct a comprehensive post-incident review to analyze the effectiveness of the response efforts and identify lessons learned, areas for improvement, and updates to the incident response plan.
- Use insights gained from the incident response to continuously improve the College's security posture.

4. **Enable effective security architecture at the College by designing and implementing a security framework to safeguard the institution's information systems, networks, and data.**

- Define security objectives and requirements through collaboration with key stakeholders, including IT team, academic programs, and administrative staff, to understand their security requirements and objectives.
- Work closely with IT team members to integrate security into the design and implementation of new systems and applications.
- Conduct security reviews of proposed changes to systems, ensuring that security controls are effectively implemented.
- Design and implement network security measures, including firewalls, intrusion detection/prevention systems, and secure network segmentation.
- Ensure the use of encryption for sensitive data in transit.
- Implement and manage endpoint security solutions to protect computers, servers, and other devices.
- Develop and implement IAM strategies to ensure that only authorized individuals have access to sensitive systems and data.
- Implement strong authentication mechanisms, such as multi-factor authentication (MFA).
- Regularly review and update the security architecture to adapt to emerging threats and technologies.
- Engage in continuous learning and professional development to stay current with best practices for security architecture.

5. **Lead security awareness and training initiatives to build a security-conscious culture at the College, reducing the risk of security incidents caused by human error, and fostering a more resilient cyber security posture.**

- Conduct an assessment to identify the specific security knowledge gaps and training needs within the College.
- Develop and deliver engaging security awareness training sessions for employees at all levels.
- Monitor training completion rates and work with leaders to ensure employees complete required training.
- Establish a regular schedule for security training sessions to reinforce key concepts and keep employees informed about evolving threats.
- Conduct simulated phishing exercises to help employees recognize and respond to phishing attempts.
- Provide immediate feedback to participants, reinforcing good security practices and educating them about common phishing tactics.
- Create and distribute security-related communications to keep the College informed about emerging threats and best practices.

6. **Contribute to the development and maintenance of security policies and monitoring compliance to build and maintain a strong security foundation, mitigate risks, and ensure that the College complies with relevant legal and regulatory requirements.**

- Collaborate with stakeholders to develop comprehensive security policies and procedures that align with College goals, industry best practices, and regulatory requirements.
- Regularly review and update security policies to reflect changes in the threat landscape, technology, and business processes.
- Ensure that policies remain relevant and effective in addressing emerging cyber security challenges.
- Communicate security policies to all relevant stakeholders, including employees, contractors, and third-party vendors.
- Work with IT and business units to enforce security policies consistently across the College.
- Conduct periodic compliance assessments and audits to verify adherence to security policies and standards.
- Continuously assess the effectiveness of security policies and compliance measures. Identify areas for improvement and work on enhancing the overall security posture of the College.

7. **Participate in and represent Aurora College and the Northwest Territories in the NREN Cybersecurity Analyst Working Group**.

- Collaborate with other NREN partners to ensure the security event monitoring processes are improved and contribute to the development of shared best practices for those processes.
- Contribute to the development and implementation of initiatives assigned to the Cybersecurity Analyst Working Group including metrics, and common operational procedures, and
- Implement and manage systems supporting NREN and national cyber initiatives including SIEM and IDS, as well as other initiatives that become available.

8. **Performs other related duties as required.**

- Attends conferences, seminars and instructional courses and maintains an ongoing study of professional and industry literature to ensure current knowledge of changing cyber security industry trends and emerging technologies.
- Provides briefing notes for Manager, Vice President, Education and Training, and President when required.
- Prepares reports.
- Serves on committees.

REQUIREMENTS AND SKILLS

- Knowledge of cyber security principles, technologies, frameworks, standards, and best practices
- Knowledge and proficiency with Information Security Management Systems, control frameworks and risk assessment methodologies from standards such as NIST and CIS.
- Knowledge of security, threat, and risk assessments through evaluating baseline security controls prior to onboarding new applications and cloud services.
- Knowledge of systems security administration, incident monitoring, detection and response, digital forensic investigations, disaster recovery, and intrusion prevention.
- Knowledge of security practices, tools and technologies, including risk management and control audits, monitoring and investigative tools, intrusion detection and prevention systems, firewalls, antivirus solutions, etc.
- Knowledge of computer systems, network designs and architectures.
- Experience with common network protocols and cryptography technologies.
- Priority setting and organizational skills, including the ability to manage multiple projects efficiently and effectively using project management tools and methods.
- Ability to research and analyze data from various sources to make security recommendations.
- Ability to work with colleagues across the organization at all levels of management and with vendors, third-party contractors and consultants to negotiate, influence, and gain trust.
- Ability to anticipate, assess, and quickly adapt to changing priorities, maintain resilience in uncertainty and effectively work in a changing environment.
- Ability to remain calm and focused during times of crisis.
- Written and verbal communication skills, including the ability to prepare briefing materials for the executive audience.
- Industry certifications such as CISSP, CISM, GIAC, SANS or equivalent would be considered an asset.
- Ability to commit to actively upholding and consistently practicing personal diversity, inclusion and cultural awareness, as well as safety and sensitivity approaches in the workplace.

WORKING CONDITIONS

Physical Demands

No unusual demands.

Environmental Conditions
No unusual demands.

Sensory Demands
No unusual demands.

Mental Demands
Significant mental demands may occur from intermittent high-stress security incidents.

Typically, the above qualifications would be attained by:

A relevant degree with 3 years of experience in a relevant field.

Equivalent combinations of education and experience will be considered.

ADDITIONAL REQUIREMENTS

Position Security (check one)

☐ No criminal records check required
☒ Position of Trust – criminal records check required
☐ Highly sensitive position – requires verification of identity and a criminal records check

French language (check one if applicable)

☐ French required (must identify required level below)
Level required for this Designated Position is:
ORAL EXPRESSION AND COMPREHENSION
Basic (B) ☐ Intermediate (I) ☐ Advanced (A) ☐
READING COMPREHENSION:
Basic (B) ☐ Intermediate (I) ☐ Advanced (A) ☐
WRITING SKILLS:
Basic (B) ☐ Intermediate (I) ☐ Advanced (A) ☐
☐ French preferred

Indigenous language: Select language

☐ Required
☐ Preferred