CYBER SECURITY ANALYST 2

REGULAR FULL-TIME

As one of the fastest growing cities in Canada, the City of Surrey is a globally recognized leader building vibrant, sustainable communities through technology and innovation. City of Surrey employees are talented innovators, inspired by meaningful work and the opportunity to drive our city—and their careers—forward. **Build a City. Build a Future** at the City of Surrey.

EMPLOYMENT STATUS

Union – CUPE Local 402 – Regular Full-time

OVERVIEW

Grow your career where innovation meets impact. At the City of Surrey, we're building a connected, secure, and resilient digital future. As a Cyber Security Analyst 2, you'll play a key role in protecting the City's digital assets and supporting a culture of cyber awareness across departments.

SCOPE

Reporting to the Cyber Security Manager, this intermediate-level technical position provides consultative services, evaluates and mitigates cyber risks, and responds to security incidents. You'll help shape and enhance the organization's data security posture.

RESPONSIBILITIES

As a Cyber Security Analyst 2, you will:

- Conduct cyber security risk assessments and health checks.
- Monitor and enhance the organization's data security posture by analyzing access patterns, identifying sensitive data exposure, and recommending remediation strategies.
- Develop and deliver awareness campaigns, training materials, and presentations.
- Maintain the enterprise cyber security risk register and develop mitigation plans.
- Maintain and update firewall rules, VPN tunnels, and intrusion prevention systems.
- Configure antivirus policies and manage malware registration.
- Triage and tune Advanced Threat Detection (ATD) alerts.
- Conduct vulnerability scans and penetration testing for PCI and internet-facing systems.
- Respond to real or suspected cyber security incidents and perform forensic investigations.
- Provide guidance to junior staff and training to City employees.
- Perform other job-related duties as required.

QUALIFICATIONS

- Completion of a Bachelor's Degree in Computer Science/Information Systems or in a related IT field, plus 3 year of cyber security experience; OR a diploma in Computer Science/Information Systems or in a related IT field, plus 6 years of cyber security experience. An equivalent combination of education and experience may be considered.
- CISSP, GIAC, or equivalent security certification required.

KNOWLEDGE, SKILLS, AND ABILITIES

You bring:

- Strong knowledge of antivirus, IPS, firewalls, and cloud/email/web security.
- Familiarity with identity and access management, encryption, tokenization, and PCI compliance.
- Experience with threat modeling, incident management, and mobile/industrial controls security.
- Excellent communication skills and the ability to work collaboratively in a team environment.
- Analytical thinking and a proactive approach to problem-solving.

WORK ENVIRONMENT

This position operates in an office environment with occasional requirements for incident response or forensic activities.

OTHER INFORMATION

Pay Grade: 31
Hourly Rate: $55.86 (2024 Rates)

Pay Steps	Hourly Rates
Step 1	$55.86
Step 2 (6 months)	$58.40
Step 3 (18 months)	$60.82
Step 4 (30 months)	$63.35