Network Security Analyst

Job Number: NETWO006309
Position Status: Full Time
Union: Non-Union
Division: Corporate Services
Facility: Administration Building
City: Wyoming, ON

Number of Positions: 1
Hours of Work: 35 hours/week
Wage Rate: $42.92 - $51.10 per hour
Date Posted: Monday, July 20, 2026
Closing Date: Monday, August 3, 2026

About Us

The County of Lambton is located in Southwestern Ontario, nestled along Lake Huron and the St. Clair River, next to the state of Michigan and is home to a diverse and welcoming population of approximately 128,000 residents.

The Corporation of the County of Lambton is one of the area's largest employers with approximately 1,300 employees. The County's seven divisions deliver hundreds of services and programs to our residents, such as emergency medical services, provincial offences court, three long-term care homes, 25 library branches, three museums, an art gallery, archives, public works, public health services, social services, planning and building services.

We are committed to sustainability, economic growth, environmental stewardship and an enhanced quality of life through the provision of responsive and efficient services and collaborative efforts with our municipal and community partners.

About the Role

The Network Security Analyst is responsible for the security systems and infrastructure used to monitor the County's networks, devices, cloud services, and systems for cyber threats. The position monitors and responds to detected security events, analyzes alerts and supporting evidence, assesses risk and impact, contains and resolves incidents within delegated authority, and escalates complex or high-risk incidents to third-party security specialists and management. The Analyst recommends, implements, administers, and works with security software and service vendors to protect networks, systems, applications, identities, and endpoints. The Analyst coordinates vulnerability remediation and secure patching with the IT team; develops and delivers cyber security awareness and training programs; reports on the effectiveness of those programs; and maintains relationships with organizations such as the Canadian Centre for Cyber Security to identify emerging threats and support proactive protective action. The Analyst also performs network administration and provides operational backup to the Server Administrator and Cloud & Active Directory Administrator, including telephony support, when vacation coverage, incidents, projects, or priorities require additional resources.

Duties & Responsibilities

The Network Security Analyst assists the Corporate Manager, Information Technology and the Network Security and Infrastructure Supervisor, as applicable, with the following:

Cyber Security Operations:

• Administer, monitor, maintain, and continuously improve the security systems and services that protect and monitor County networks, endpoints, servers, identities, applications, cloud services, email, and data.

• Monitor security information and event management, endpoint detection and response, intrusion detection and prevention, firewall, identity, vulnerability, email security, cloud security, and related monitoring platforms for alerts, anomalous activity, and indicators of compromise.

• Triage and analyze security events; validate alerts; determine scope, severity, business impact, and required response; document investigative steps; and resolve or escalate incidents in accordance with approved procedures.

• Coordinate containment, eradication, recovery, evidence preservation, stakeholder communications, third-party specialist support, and post-incident review for cyber security incidents within assigned authority.

• Develop and maintain security monitoring use cases, alert rules, dashboards, response playbooks, escalation paths, contact lists, and incident records to improve detection quality and response consistency.

• Perform or coordinate vulnerability scanning, configuration assessment, exposure review, and remediation tracking across network, server, cloud, Active Directory, application, and endpoint environments.

• Work with the IT team and system owners to ensure operating systems, applications, firmware, network devices, and endpoints are maintained at supported and secure patch levels; identify exceptions and report unresolved risk.

• Recommend, test, implement, configure, and support security tools, controls, services, and architecture improvements based on risk, operational requirements, industry practices, and County policies.

• Work with security software and managed service vendors to investigate threats, tune services, resolve technical issues, manage support cases, review performance, and ensure security services meet contractual and operational requirements.

• Collect, analyze, retain, and report security metrics, trends, incidents, vulnerabilities, patch status, training results, control effectiveness, and material risks to the Network Security and Infrastructure Supervisor and Corporate Manager, Information Technology.

• Recommend, develop, coordinate, and deliver a cyber security awareness and training program for County staff and contracted partners, including role-based education, awareness communications, phishing simulations, remedial training, and measurement of program effectiveness.

• Monitor threat intelligence and security advisories from trusted vendors, peers, law enforcement, and organizations such as the Canadian Centre for Cyber Security; assess County exposure and coordinate proactive defensive action.

• Support security assessments, audits, penetration tests, tabletop exercises, disaster recovery tests, and compliance activities; track findings and assist responsible parties with timely remediation.

• Maintain current knowledge of cyber threats, attacker techniques, security technologies, privacy obligations, and recognized practices and frameworks; translate relevant changes into practical recommendations for the County.

• Assist in developing and maintaining cyber security policies, standards, procedures, technical baselines, incident response plans, and supporting documentation.

Network Administration:

• Plan, implement, configure, support, and maintain County network infrastructure, including routers, switches, firewalls, wireless access points, VPN services, load balancers, network access control, content filtering, uninterruptible power supplies, carrier services, and related components.

• Monitor and analyze LAN, WAN, wireless, internet, and cloud connectivity for availability, performance, utilization, traffic, and capacity; investigate issues and implement corrective or preventive improvements.

• Troubleshoot network incidents and service degradation, coordinate recovery with vendors and service providers, complete root-cause analysis, and recommend measures to reduce recurrence.

• Maintain secure network configurations, firmware and software levels, configuration backups, high-availability features, administrative access, certificates, and technical standards in accordance with change-management requirements.

• Support network architecture, lifecycle planning, product evaluation, technical specifications, procurement, implementation projects, budgeting, and vendor management activities.

• Maintain current network inventories, configurations, addressing records, carrier information, procedures, support information, and logical and physical topology diagrams.

• Support the County's Cisco VoIP and SIP telecommunications environment, including call services, voicemail, licensing, telephone devices, carrier circuits, moves and changes, troubleshooting, maintenance, patching, and documentation.

Infrastructure and Operational Backup:

• Provide backup support for physical and virtual servers, storage, backup and recovery systems, Windows and Linux server environments, and related monitoring and support tools under established procedures.

• Provide backup support for Azure and other cloud infrastructure, Microsoft 365, OneDrive, SharePoint, Intune, Active Directory, Entra ID, user and group administration, domain policies, and identity-related services under established procedures.

• Assist with infrastructure monitoring, incident and service request resolution, patching, recovery activities, capacity review, documentation, licensing, and vendor coordination across network, server, cloud, Active Directory, and telephony services.

• Maintain sufficient cross-training and current documentation to provide vacation relief and additional operational coverage when priorities dictate.

Documentation and Reporting:

• Maintain accurate security and network inventories, configurations, standards, procedures, diagrams, response records, knowledge-base articles, service records, and vendor support information.

• Record and resolve assigned incidents, alerts, problems, changes, and service requests in accordance with established priorities, procedures, and service-level expectations.

• Prepare clear technical and management reports, recommendations, presentations, and briefings concerning threats, incidents, risks, vulnerabilities, training, network performance, service levels, and improvement opportunities.

• Act as a cyber security and network resource to IT staff, departments, local municipalities, contracted partners, vendors, and users within the authority of the position.

General:

• Incumbents must keep up-to-date on all relevant legislation, collective bargaining agreements, County Policies and Procedures, and applicable technology standards, ensuring that these are implemented as prescribed

• Incumbents must possess the physical ability to meet the duties and responsibilities of the job description and/or the requirements identified within the position's Physical Demands Analysis

• Incumbents must be proficient in the documented operational procedures required to provide backup support to the Server Administrator, and Cloud & Active Directory Administrator, including telephony support, for vacation relief, incident response, project work, and additional coverage when priorities dictate.

These describe the general nature and level of work being performed by incumbents in this classification. They are not an exhaustive list of all job duties in the classification. Other duties may be assigned.

Supervision Requirements

Direct Supervision: None

Indirect Supervision: None

Functional Authority: Provides direction, consultative services and advice on cyber security, network security, network infrastructure, and telecommunications matters to the Corporation, the IT department, contractors, County end users, local municipalities, and contracted partners within the authority of the position. May provide technical direction to IT staff and service providers during incident response, remediation, network changes, and service restoration.

What We're Looking For

Minimum Formal Education

• Completion of post-secondary education in Cyber Security, Computer Science, Computer Engineering, Network Engineering, Information Technology, or a related field.

• A recognized cyber security certification such as CompTIA Security+, ISC2 Systems Security Certified Practitioner (SSCP), ISC2 Certified Information Systems Security Professional (CISSP), GIAC Security Essentials (GSEC), GIAC Certified Incident Handler (GCIH), or Microsoft Certified: Security Operations Analyst Associate (SC-200) is preferred or must be obtained within a period approved by the County.

• A current Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP Enterprise), or equivalent enterprise networking certification is considered an asset.

• Related certifications in Microsoft Azure, Microsoft 365, Active Directory, cloud security, incident response, vulnerability management, digital forensics, privacy, or IT service management are considered assets.

Experience

• Minimum of five years of relevant experience in cyber security operations, network security, network administration, systems administration, or a combination of these areas within a complex, multi-site environment.

• Hands-on experience monitoring, triaging, investigating, documenting, containing, resolving, and escalating cyber security alerts and incidents using security information and event management, endpoint detection and response, managed detection and response, intrusion detection and prevention, firewall, identity, email, cloud, and vulnerability-management technologies.

• Experience coordinating vulnerability remediation, secure patching, configuration hardening, risk and impact analysis, incident recovery, root-cause analysis, and follow-up actions with technical teams and third-party specialists.

• Strong working knowledge of enterprise network technologies, including switches, routers, firewalls, wireless networks, VPNs, network access control, content filtering, load balancing, DNS, DHCP, TCP/IP, IPv4/IPv6, VLANs, routing, quality of service, and VoIP/SIP.

• Experience configuring, supporting, monitoring, and troubleshooting LAN, WAN, wireless, internet, cloud-connected, and remote-access networks.

• Working knowledge of Windows and Linux servers, virtualization, storage, backup and recovery, Active Directory, Entra ID, Azure, Microsoft 365, Intune, endpoint management, and identity and access management.

• Knowledge of recognized security practices and frameworks such as the CIS Controls, NIST Cybersecurity Framework, and ISO/IEC 27001, together with applicable security, privacy, and records-management obligations.

• Experience developing and delivering cyber security awareness, role-based training, phishing simulations, communications, and program-effectiveness reporting is preferred.

• Experience preparing security metrics, management reports, technical documentation, response playbooks, standards, procedures, diagrams, and recommendations.

• Experience with PowerShell, Python, APIs, query languages, or other scripting and automation technologies used for investigation, reporting, and infrastructure administration is an asset.

• Excellent analytical, judgement, problem-solving, organizational, project-management, oral, written, consultative, coordination, and interpersonal skills, including the ability to communicate technical risk clearly to non-technical audiences, senior management, and County Council when requested.

Other:

• Weekend on-call work is a requirement for this position.

• A valid Ontario Driver’s licence and use of a vehicle are required.

Why Join Us?

Join a team dedicated to your professional growth and well-being. The County of Lambton offers a diverse, inclusive workplace featuring a competitive compensation plan, including group health insurance benefits for eligible staff and the OMERS pension plan, one of Canada's largest defined benefit pension plans, which is available to all staff.

We prioritize our people through robust wellness programs, career development opportunities across multiple divisions, and a collaborative environment where your work truly makes a difference in the community.

How to Apply

Applications are accepted online until 11:59pm on Monday, August 3, 2026. Please visit www.lambtononline.ca/jobs and select job posting NETWO006309 - Network Security Analyst to apply.