CATHOLIC DISTRICT SCHOOL BOARD OF EASTERN ONTARIO

DEPARTMENT OF HUMAN RESOURCES

2755 Highway 43, Kemptville, Ontario K0G 1J0
phone: 613-258-7757 toll free: 1-800-443-4562
hr@cdsbeo.on.ca

NU-284 – BO2025

April 7, 2025

Position:	**ICT Security Operations Operator – Temporary Long-Term Occasional**
Location:	**Kemptville Board Office (with travel to CDSBEO Schools)**
Hours of work:	**35 hours per week**
Salary:	**$54,024 - $63,558** (annualized; to be prorated based on contract duration)
Effective:	**May 1, 2025 – August 31, 2025**

Job Summary

The Security Operations Operator is responsible for frontline IT security incident and alert management, assisting in monitoring, troubleshooting, and maintaining security infrastructure. This role will focus on Security Operations which will include technical security support, security alert and incident monitoring, incident and alert investigation and triage, automation, and incident response. It is an ideal junior-level position for those qualified security practitioners looking to build a career in IT security. Responsibilities include supporting endpoint security, scripting for automation, assisting in threat hunting, data and usage investigations, and implementing security incident response workflows.

Qualifications

- Post-secondary diploma in Information Technology, Cybersecurity.
- Minimum of two (2) years of work-related experience in IT support, security operations, or networking.
- Understanding of security operations, automation, and scripting for cybersecurity tasks.
- Familiarity with SIEM solutions and log analysis using KQL (Kusto Query Language) or similar query languages.
- Experience with scripting (PowerShell, Bash) and automation tools (Logic Apps, Power Automate, or similar).
- Knowledge of firewalls, VPNs, endpoint security, and cloud security practices.
- Strong troubleshooting and problem-solving skills.
- Excellent communication and customer service skills.
- Ability to work both independently and as part of a team.
- Must possess a valid driver's license and a reliable vehicle.

Interested applicants may submit a cover letter and resume no later than:

Monday, April 14, 2025 by 4:00pm

Please specify what position you are applying for.

e-mail: hr@cdsbeo.on.ca

We thank all applicants in advance for their interest; however, only those candidates selected for an interview will be contacted.

The CDSBEO adheres to equitable hiring, employment and promotion practices and is committed to an inclusive workforce. We encourage applications from Indigenous peoples, racialized people, persons with disabilities, people from gender diverse communities and/or people with intersectional identities, as well as others who may contribute to the further diversification of ideas.

The Catholic District School Board acknowledges that our schools are located on the unceded, traditional Algonquin territory of the Anishinaabe people as well as the land of the Mohawk territory of the Haudenosaunee/Rotinonhsho'n:ni people. We respect both the land and the people of this land including all Indigenous people who have walked in this place.

Pursuant to the Accessibility for Ontarians with Disabilities Act, (AODA), if applicants require accommodations at any time throughout the application process, please reach prior to the posting closing date so that appropriate arrangements can be made.

Chris Cummings
Chair of the Board

Laurie Corrigan
Director of Education

A. JOB IDENTIFICATION:

TITLE:	ICT SECURITY OPERATIONS OPERATOR
DEPARTMENT:	ICT (INFORMATION AND COMMUNICATION TECHNOLOGY)
IMMEDIATE SUPERVISOR:	COORDINATOR, ICT SECIRITY SYSTEMS AND NETWORK MANAGEMENT

B. JOB SUMMARY:

The Security Operations Operator is responsible for frontline IT security incident and alert management, assisting in monitoring, troubleshooting, and maintaining security infrastructure. This role will focus on Security Operations which will include technical security support, security alert and incident monitoring, incident and alert investigation and triage, automation, and incident response. It is an ideal junior-level position for those qualified security practitioners looking to build a career in IT security. Responsibilities include supporting endpoint security, scripting for automation, assisting in threat hunting, data and usage investigations, and implementing security incident response workflows.

C. Duties and Responsibilities:

Technical Support & Security Operations

- Configure, install, modify, and maintain security software.
- Diagnose and resolve hardware, software, and network security-related issues.
- Provide on-site and remote technical support, assisting end users with IT-related security concerns.
- Support identity management, Multi-Factor Authentication (MFA), and endpoint security tools.
- Assist in managing Microsoft 365 security and cloud-based security configurations.

Network & Security Monitoring

- Monitor security alerts and logs for suspicious activity, escalating incidents as needed.
- User and Data investigations as related to incidents and alerts as part of triage and response process.
- Assist in threat hunting using KQL (Kusto Query Language) or similar query languages in security information and event management (SIEM) tools.
- Support the implementation of security automation and orchestration workflows (e.g., Logic Apps, Playbooks, Power Automate, or other SOAR solutions).
- Assist in configuring and managing Virtual Local Area Networks (VLANs) and Virtual Private Network (VPN) connections.
- Work with security tools for monitoring, alert management, and incident response automation.

Security Automation & Incident Response

- Assist in developing and deploying security incident response automation using Logic Apps, PowerShell, or scripting.
- Work with IT security teams to develop automated responses to security threats, such as phishing detection, endpoint isolation, and user access controls.
- Help integrate security monitoring tools with automated workflows to improve response times and reduce manual tasks.
- Assist in writing and optimizing KQL queries for proactive threat detection and log analysis.
- Maintain security dashboards and reporting tools to track vulnerabilities and response efforts.

Preventative Maintenance & Troubleshooting

- Monitor IT helpdesk tickets, prioritize, and escalate security-related issues.
- Perform basic security audits, vulnerability monitoring, and patch management tasks.
- Assist in disaster recovery procedures and IT asset security management.
- Collaborate with senior IT staff on security incidents and troubleshooting tasks.

Other Responsibilities:

- Responsible for handling sensitive and confidential information possibly regarding other staff members with the utmost integrity and ensuring compliance with established protocols and proper usage policies to safeguard data and maintain confidentiality.
- Stay current with emerging cybersecurity threats, security automation technologies, and best practices.
- Assist in preparing security awareness training materials and documentation.

- Maintain documentation of security standards, policies, and automation workflows.
- Perform other duties as assigned that align with the role.

D. Qualifications:

- Post-secondary diploma in Information Technology, Cybersecurity.
- Minimum of two (2) years of work-related experience in IT support, security operations, or networking.
- Understanding of security operations, automation, and scripting for cybersecurity tasks.
- Familiarity with SIEM solutions and log analysis using KQL (Kusto Query Language) or similar query languages.
- Experience with scripting (PowerShell, Bash) and automation tools (Logic Apps, Power Automate, or similar).
- Knowledge of firewalls, VPNs, endpoint security, and cloud security practices.
- Strong troubleshooting and problem-solving skills.
- Excellent communication and customer service skills.
- Ability to work both independently and as part of a team.
- Must possess a valid driver's license and a reliable vehicle.