Toronto District School Board

No.: CUPE C-25-1009UE
POSTED: January 15, 2025
DEADLINE: 4:30 p.m. January 23, 2025

Analyst I, Cyber Threat and Vulnerability Management

1 – Permanent Position

Information Technology Services

CUPE Local 4400 Unit C - Grade O (12 Month)
$47.73 – $56.27 per hour

The Toronto District School Board adheres to equitable hiring, employment and promotion practices.

Reporting to the Senior Analyst, IT Security Threat Management, the Analyst I, Cyber Threat and Vulnerability Management will assist the Senior Analyst to ensure that the Cyber Threat and Vulnerability Management functions are managed and carried out.

The Analyst 1, Cyber Threat and Vulnerability Management will ensure that the Cyber Threat and Vulnerability are managed in accordance with the TDSB security and risk tolerance including the functions to ensure safety and security of the users along with availability, confidentiality and integrity of the technology assets including the data contained within.

Summary of Duties:

- Perform Cyber Threat and Vulnerability management tasks in accordance with established programs and directed by the Senior Analyst;
- Conduct regular review of Indicators of Attack (IoAs) and Indicators of Compromise (IoCs) derived from all available sources (e.g., SIEM, NGFW, Logs from Systems and Security Tools) to assess the real and material threats and vulnerabilities;
- Perform ethical hacking activities on the direction of management, as well as perform programming, and related scripting duties;
- Tune the SIEM to recognize real and actionable threats from security information and events collected;
- Create playbooks to automate the response for actionable threats and link them to risk objects;
- Optimize the collection, processing, and analysing parameters to improve the efficiency of the SIEM;
- Create and evolve new/existing rules in the SIEM to accommodate new and evolving threats;
- Collaborate/Support with/to other IT units to assess, neutralize and reconcile threats and vulnerabilities, and report deviation;
- Perform proactive threat hunting in a systemic and iterative manner throughout the environment to detect and isolate threats;
- Perform threat-based risk assessments on systems and services and effectiveness of controls;
- Assess discovered/identified/obtained through subscribed feeds threat/vulnerability impact and recommend appropriate actions to reduce exposure and ensuring risks remains within the tolerance levels;
- Review, develop and report on appropriate metrics for the Threat/Vulnerability Management solutions, performance, exception and compliance and ensure continuous improvements of such metrics and its affects;
- Track and report threat and vulnerability mitigation efforts;
- Develop and document guidelines, processes and procedures for review and approval and implement approved procedures to secure IT environment;
- Liaise between departments to develop and implement approved security standards and guidelines;

- Raise awareness of good security practices to all levels of the organization and perform security awareness and learning duties as directed;
- Analyze and define training requirements in security matters related to Cyber Threat and Vulnerability management for staff;
- Analyze and help define appropriate controls to manage Cyber risks for approval;
- Identify controls that require changing/adding based on the changes to the IT environment;
- Maintain broad awareness of threat and vulnerability trends including changes to legislations and regulatory frameworks;
- Advise on security practices for all IT projects as required;
- Other related duties as assigned.

Qualifications:

- University Degree in Computer Science or related field with three years progressive working experience in IT security/threat management within an Information Technology environment or an equivalent combination of education and experience;
- Training and/or technical certification in Global Information Assurance in the following areas: Security Essentials, Information Security Fundamentals, Threat Hunting, Penetration Testing, Intrusion Analysis, Forensic Analysis, Perimeter Defense, Enterprise Defense, System and Network Auditing;
- Experience in monitoring threat landscape, mapping potential applicable threats, and ethical hacking methodologies and tolls;
- Experience with application security, and programming/scripting skills using Python, PowerShell, and other programming languages;
- Experience in vulnerability assessment of end points, switches, routers, gateways, servers, storage, storage area networks, firewalls, applications, web services, cloud services, etc.;
- Experience using Splunk SIEM technologies (Splunk enterprise security administration and management), O365 Security technologies, end-point detection and Response (EDR) technologies;
- Experience with Azure technologies, and security products;
- Experience with Google Cloud, and security technologies including email security;
- Maintain currency of knowledge on current and emerging security trends, including but not limited to cloud based services, IoT, etc.;
- Demonstrated ability to understand the implications of legislation, insurances and regulatory frameworks;
- Understanding of IT information, process, system, technology architectures and models;
- Good oral, written, interpersonal and organizational skills;
- Strong analytical, reasoning and problem solving skills;
- Demonstrated ability to handle matters requiring high levels of diplomacy, sensitivity and confidentiality;
- Proven ability to work under pressure and consistently meeting deadlines; and
- Project management and time management skills.

Asset:

- CISSP certification
- Ethical hacking certifications (e.g., OSCP, CEH), Splunk SIEM certifications, and Azure security technology certifications

Special Requirements:

- Must provide own vehicle for Board business to travel to designated sites.
- Ability to stand/walk for extended periods; and
- Ability to lift boxes and cooking equipment (e.g. pots and pans) and supplies etc (up to 50 pounds).

Location: 1 Civic Centre Court (Wheelchair Accessible) (Hybrid Work Eligible)

Hours: 35 Hours per week

Work Year: 12 Months

Please note:

Applications **must** be submitted:

1. In résumé form with a covering letter to: Application.Submission@tdsb.on.ca
2. With competition # **CUPE C-25-1009UE** in the subject line
3. Apply no later than 4:30 pm on **January 23, 2025.**

Only applicants selected for an interview will be contacted. Applications will not be acknowledged in writing.

We strive to meet the accommodation needs of persons with disabilities. Applicants are encouraged to make their needs for accommodation known in advance during the hiring process.

The TDSB follows a hybrid work structure where some employees may be able to work remotely at times, based on operational requirements. Please refer to Policy P103, Flexible Working Arrangements for more information.