OFFRE D'EMPLOI

POSTE TEMPORAIRE AVEC POSSIBILITÉ DE RÉGULARISATION : EP2627-045
ANALYSTE SPÉCIALISÉ(E) EN INFORMATIQUE, PROFIL CYBERSÉCURITÉ
Service des technologies de l'information
Du lundi au vendredi de 8h30 à 16h30 (35h par semaine)

Tu as envie d'intégrer une équipe **passionnée** qui met son savoir-faire au service de la **réussite** des élèves?
Tu as envie de rencontrer des personnes **engagées** et **bienveillantes** qui s'**entraident** et qui **collaborent** pour servir une des causes les plus nobles qui soient, celle de l'**éducation**?

Tu as envie de découvrir le **milieu scolaire** et toute sa richesse?

Ça tombe bien! Nos nombreux établissements représentent un immense terrain de jeux dans lequel évoluent près de 55 000 élèves et près de 11 500 employés. Si tu te joins à nous, crois-nous, ton **expertise** permettra de faire la différence dans le parcours des élèves lavallois de **TA** collectivité!

Joins-toi au **CSS de Laval** pour avoir un **impact positif** sur les décideurs de demain!

TA MISSION

Sous l'autorité du coordonnateur de l'équipe de sécurité informatique, tu joueras un rôle clé afin d'assurer la sécurité des environnements technologiques du CSS de Laval. Tu surveilleras et analyseras les menaces, en participant à la gestion des incidents et en faisant évoluer les outils et pratiques de cybersécurité. En collaboration avec les équipes TI, tu mettras à profit ton expertise pour renforcer la protection des systèmes et des données.

TES RESPONSABILITÉS AU QUOTIDIEN :

- Agir à titre d'experte ou d'expert en cybersécurité et exercer un rôle-conseil auprès du personnel d'encadrement, des équipes techniques et des responsables de projets;
- Maintenir une vision globale de la posture de sécurité de l'organisation, notamment en matière d'identités et d'accès, d'appareils, d'infrastructures, de services infonuagiques, de données, de messagerie et d'applications;
- Planifier, coordonner et assurer la mise en œuvre, l'évolution, l'intégration et l'optimisation des solutions de cybersécurité;
- Assurer la prise en charge et l'amélioration des activités d'analyse, de détection, d'investigation, de réponse aux incidents et de chasse aux menaces;
- Assurer l'évolution et l'amélioration continue de Microsoft Sentinel et de Microsoft Defender XDR, notamment des sources de données, des règles de détection, des requêtes KQL, des tableaux de bord et des mécanismes de corrélation;
- Concevoir et améliorer l'automatisation des activités de cybersécurité au moyen de scripts, de playbooks, d'API et de flux de travail;
- Prendre en charge l'analyse des incidents complexes, établir des diagnostics, recommander les mesures de mitigation appropriées et coordonner les interventions avec les équipes concernées;
- Évaluer les besoins de sécurité liés aux projets, aux services et aux changements technologiques, puis réaliser des analyses de risques, des évaluations de sécurité, des preuves de concept et des travaux de validation;
- Participer à la définition et à l'amélioration des mécanismes de sécurité du courriel, des services Web, des environnements infonuagiques et des services de protection périmétrique;
- Contribuer à la définition des orientations, des normes, des procédures et des contrôles de sécurité, puis veiller à leur mise en œuvre et à leur amélioration continue;
- Produire des analyses, des rapports, des indicateurs et des recommandations permettant au personnel d'encadrement de comprendre les risques et de prendre des décisions éclairées;
- Assurer une veille technologique sur les menaces, les vulnérabilités, les outils de cybersécurité et les nouvelles technologies, notamment l'intelligence artificielle, puis proposer des améliorations adaptées à l'environnement;
- Concevoir et maintenir la documentation technique nécessaire à l'exploitation sécuritaire des ressources informationnelles et au transfert des connaissances;

- Collaborer avec les différentes équipes du Service des technologies de l'information ainsi qu'avec les partenaires internes et externes dans le cadre des activités et des projets de cybersécurité;
- Effectuer toute autre tâche connexe.

Si tu souhaites avoir plus d'informations sur le poste, tu peux te référer à la page 10 du plan de classification du personnel professionnel en cliquant ici.

TON PARCOURS PROFESSIONNEL

Diplôme universitaire terminal de premier cycle dans un champ de spécialisation approprié à l'emploi, notamment en informatique ou en génie informatique **ainsi** qu'une certification de spécialisation délivrée par une autorité compétente et reconnue notamment dans le domaine des ressources informationnelles.

POUR BIEN RÉUSSIR DANS CE POSTE, TU DEVRAS:

- **Être disponible, selon une rotation établie, pour assurer la surveillance et la gestion des alertes en dehors des heures normales de travail et intervenir, au besoin, lors d'incidents majeurs, avec compensation conformément aux modalités applicables;**
- Posséder une expérience démontrée en cybersécurité, notamment dans les opérations de sécurité, l'analyse des incidents ou l'amélioration de solutions de protection;
- Être capable de comprendre un environnement technologique complexe dans son ensemble, d'établir des liens entre différentes sources d'information et d'anticiper les risques;
- Posséder une très bonne connaissance de Microsoft Sentinel et de Microsoft Defender XDR, notamment pour l'analyse des incidents, la corrélation des événements, les règles de détection et la chasse aux menaces;
- Posséder une bonne maîtrise de KQL afin de rechercher, de corréler et d'interpréter les données de sécurité ainsi que de développer des détections et des rapports;
- Posséder une expérience en scripting ou en automatisation, notamment avec PowerShell, Azure Logic Apps ou Power Automate;
- Être à l'aise avec les structures JSON utilisées dans les API, les configurations et les automatisations;
- Posséder une bonne connaissance de Microsoft Entra ID;
- Être capable d'analyser des situations complexes, d'établir un diagnostic, d'évaluer les risques et de recommander des solutions adaptées au contexte organisationnel;
- Faire preuve de leadership technique, d'autonomie, de jugement, de rigueur, de curiosité et d'initiative;
- Savoir gérer les priorités et prendre des décisions judicieuses lors de situations complexes ou d'incidents majeurs;
- Posséder d'excellentes aptitudes en communication et être capable de vulgariser les enjeux techniques, de produire une documentation claire et de formuler des recommandations structurées;
- Avoir une connaissance de Microsoft Purview constitue un atout;
- Avoir une connaissance des mécanismes de sécurité du courriel, notamment SPF, DKIM et DMARC, constitue un atout;
- Avoir une connaissance des services de sécurité Cloudflare constitue un atout;
- Avoir une connaissance des risques et des mécanismes de sécurité associés à l'intelligence artificielle constitue un atout.

TON SALAIRE Échelle salariale de **57 492 $ à 105 469 $** selon les qualifications et l'expérience. Selon l'entente nationale régissant les professionnels non enseignants.

TON LIEU DE TRAVAIL **Service des technologies de l'information (centre administratif)**
955 boulevard Saint-Martin, Ouest
Laval, Québec, H7S 1M5

DATE EFFECTIVE : Dès la nomination

DATE LIMITE POUR POSTULER : 6 octobre 2026 à 16h00

CE QUE NOUS AVONS À OFFRIR

- Vingt (20) jours de vacances annuelles incomparables *(au prorata du nombre de mois travaillé);* ***Imagine tous les voyages et les aventures à venir!***
- Dix-neuf (19) jours chômés et payés par année scolaire, incluant la période des fêtes;
- Conciliation travail-vie personnelle;
- Assurances collectives et régime de retraite à prestation déterminée (RREGOP); ***Imagine tes projets de retraite!***
- Programme de perfectionnement en continu;
- Possibilités d'avancement; ***Imagine tes possibilités d'avenir!***
- Stationnement à proximité et sans frais;
- Possibilité de télétravail conformément au cadre de référence établi;
- Autres avantages (Insertion professionnelle, programme d'aide aux employés, rabais corporatifs).

**Veuillez noter que certains avantages s'appliquent seulement sous certaines conditions*

CE DÉFI TE PARLE?

Postule maintenant en cliquant ici et contribue à la relève de demain.

Le Centre de services scolaire de Laval applique un programme d'accès à l'égalité en emploi. Tu peux voir nos réalisations en ce sens en cliquant ici.

Veuillez prendre note que le Centre de services scolaire de Laval est visé par des obligations en matière de laïcité, conformément à la Loi sur la laïcité de l'État. La loi prévoit notamment que le port d'un signe religieux est interdit aux membres du personnel scolaire dans l'exercice de leurs fonctions. Les personnes qui postulent au Centre de services scolaire de Laval s'engagent à respecter et à se conformer aux obligations prévues par la loi.