Sr. Specialist Cybersecurity

Magna Powertrain of America Inc.

Aurora, Ontario, Canada

Temps plein · Poste permanent · Publié le 18 septembre 2026

Workday peut présenter l’annonce dans une autre langue selon la préférence d’affichage.

À propos de Magna

Magna offre du soutien, des ressources et des perspectives de carrière aux membres de ses équipes internationales. Le travail porte sur des technologies automobiles de pointe et s’inscrit dans un environnement dynamique où les responsabilités sont variées et les parcours professionnels peuvent évoluer.

À propos du groupe

Magna Powertrain cherche à rendre la mobilité plus intelligente, plus propre et plus légère grâce aux systèmes de transmission. Fournisseur mondial, le groupe assure la conception, le développement, les essais et la production de systèmes complets. Il met l’accent sur l’innovation, la qualité, la sécurité et l’environnement.

Responsabilités du poste

Résumé du position

Chez Magna Powertrain, la cybersécurité est une priorité absolue. La protection de nos données, internes et externes, contre les menaces est primordiale pour notre succès. Le spécialiste principal - Groupe Cybersécurité assure le leadership, l'application opérationnelle et le suivi de toutes les politiques de cybersécurité au niveau du Groupe, en étroite collaboration avec la sécurité de l'information de l'entreprise, l'informatique et d'autres fonctions connexes.

Le rôle de la Sr. Spécialiste - La cybersécurité de groupe consiste à s'assurer que toutes les exigences et tous les protocoles de cybersécurité sont mis en œuvre efficacement dans tous les emplacements.

Essentiel et responsabilités

tre le leader de la cybersécurité dans le groupe motopropulseur Magna (MPT) pour surveiller les indicateurs clés de performance en matière de sécurité et de conformité, analyser les résultats et prendre des mesures correctives pour combler les lacunes et améliorer la sécurité de l’organisation.

Fournir des conseils et des conseils d'experts aux différentes unités commerciales dans les domaines de l'informatique et de l'OT en ce qui concerne les opérations et les processus de sécurité.

Fournir un soutien pour la correction des constatations de l’audit de TI, collaborer avec les intervenants pour combler les lacunes identifiées, surveiller les mesures correctives et assurer la clôture en temps opportun des problèmes d’audit.

Évaluer les risques pour les actifs et les services, et décrire les options et les échéanciers d’atténuation.

Effectuer des évaluations des risques liés à l’IA pour identifier, évaluer et atténuer les menaces potentielles associées aux systèmes et technologies d’intelligence artificielle, en veillant à la conformité aux normes organisationnelles

Effectuer des activités de surveillance des risques de groupe et aider les divisions à tenir les registres des risques de la division respectifs, en veillant à ce que la documentation soit exacte et à ce que les risques identifiés soient mis à jour en temps opportun.

Coordonner les efforts de sécurité OT en appliquant des contrôles pour protéger les actifs critiques et donner des conseils sur la création, la mise à jour, les tests et la formation des plans de reprise après sinistre et de continuité des activités

Soutenir et améliorer continuellement le Système de Gestion de la Sécurité de l'Information (ISMS) pour assurer une protection efficace des actifs organisationnels et le respect des normes pertinentes.

Concevoir et consolider des processus de sécurité normalisés et les procédures associées à mettre en œuvre dans toutes les divisions MPT

Créer des campagnes de sensibilisation en partenariat avec Corporate Information Security et fournir une formation

Ce qui précède est destiné à décrire le contenu général et les exigences pour l'exécution de ce poste. Il ne doit pas être interprété comme un énoncé exhaustif des fonctions, des responsabilités ou des exigences.

Qualifications

Licence ès sciences en informatique, sécurité informatique, systèmes d'information ou preuve équivalente de connaissances de base.

Connaissance approfondie de divers cadres / réglementations tels que ISO 27001/2, TISAX, NIST 800-53, NIST Cybersecurity Framework, GDPR, SOX, ITIL, COBIT, COSO ou similaire.

Plus de 8 ans d'expérience en informatique et en sécurité.

Certifications accréditées un plus, tels que: CISA, CISSP, OSCP, CEH (Certified Ethical Hacker)

Précédent SOC / NOC expérience un plus

Principaux r ves comportementaux pour le succ s

Bien organisé et structuré; Capable de démontrer de solides compétences en communication et de partager constamment ses connaissances avec ses collègues, y compris en maintenant une documentation claire et approfondie; montre son auto-entraînement et sa motivation en prenant des initiatives proactives, en établissant des normes élevées pour la réussite personnelle et en cherchant continuellement des opportunités pour améliorer la performance et contribuer au succès de l'équipe.

Expertise technique / fonctionnelle: Capable de démontrer la maîtrise des compétences techniques / fonctionnelles nécessaires pour effectuer son propre travail; maintenir une connaissance de pointe des progrès dans le domaine; publier régulièrement ou présenter sur des questions de pointe; mener des recherches de pointe ou un travail similaire ayant un impact à l'échelle de l'organisation; jouer un rôle clé dans les progrès de la profession.

Flexibilité et réalisation du changement : Capacité à faire face positivement aux changements qui affectent les exigences du poste; s'adapter aux priorités changeantes en réponse aux besoins des clients internes et externes; reconnaître rapidement les situations / conditions où le changement est nécessaire; travailler à clarifier les situations où les informations, les instructions ou les objectifs sont ambigus; soutenir le changement organisationnel.

Résolution et analyse de problèmes : Capacité de recueillir des données appropriées et de diagnostiquer la cause d'un problème avant d'agir; causes distinctes des symptômes; appliquer les leçons apprises d'autres personnes qui ont rencontré des problèmes ou des défis similaires; anticiper les problèmes et élaborer des plans d'urgence pour les résoudre; élaborer et évaluer des plans d'action alternatifs.

Créativité et innovation : Capacité à générer des idées créatives pour résoudre des problèmes et améliorer les méthodes de travail; appliquer de nouvelles approches aux situations; appliquer de manière indépendante

l'expertise professionnelle de manière unique ou innovante; collaborer avec les membres de l'équipe pour réfléchir aux approches créatives; repenser les situations pour créer de nouvelles opportunités ou surmonter les obstacles.

Environnement de travail

Hybride

Environnement de bureau

10% de voyages

Normes Magna

Suivez le Code de conduite et d’éthique de Magna et les politiques de conformité connexes.

Soutient et adhère aux politiques, procédures et directives opérationnelles relatives au système de gestion de la qualité établi (IATF 16949).

Pratiquer et maintenir l’intégrité tout en respectant la Charte et la Constitution de Magna.

Piloter le développement de nouvelles technologies pour améliorer la qualité, l’efficacité et réduire les coûts.

Se conformer aux politiques et procédures de sécurité pour s'assurer que les tâches de soi sont exécutées de manière sécuritaire.

Responsabilités en matière de santé et de sécurité

Comprendre les politiques et procédures environnementales, de santé et de sécurité applicables sur le lieu de travail.

Signalez immédiatement les conditions dangereuses.

Signalez immédiatement les blessures, accidents, maladies, quasi-accidents, dommages matériels.

Respectez les règles de sécurité.

Se conformer aux exigences relatives à l'utilisation ou à l'utilisation de machines ou d'équipements.

Respecter les exigences relatives aux équipements de protection individuelle (EPI) (PPE).

Créer un environnement de travail positif en démontrant et en partageant des connaissances fonctionnelles / techniques.

Développer et maintenir une relation de travail réactive et coopérative avec les clients internes et externes.

Traitez tout le monde avec dignité, confiance et respect.

Accomplir les tâches et responsabilités supplémentaires qui lui sont assignées.

Respecter les politiques de Magna en matière d’information et de protection des données.

Ce qui précède est destiné à décrire le contenu général et les exigences pour l'exécution de ce poste. Il ne doit pas être interprété comme un énoncé exhaustif des fonctions, des responsabilités ou des exigences.

Cette description de poste reflète les éléments de base d'un poste. Il peut y avoir des exigences supplémentaires basées sur les lois et règlements locaux qui pourraient être jointes en tant qu'additif.

Égalité d’accès et confidentialité

Magna valorise la diversité et offre l’égalité d’accès à l’emploi. Les décisions tiennent compte de l’expérience, des qualifications et des exigences du poste sans distinction, notamment, de couleur, d’origine, d’ascendance, de religion ou de convictions, de sexe ou de genre, d’orientation sexuelle, d’âge, de citoyenneté, d’état matrimonial ni de handicap. L’entreprise protège les renseignements personnels. Pour respecter le RGPD et les lois locales sur les données personnelles, elle déconseille de soumettre les candidatures par courriel.

Divulgation de la présélection assistée par l’IA

Magna peut utiliser l’intelligence artificielle pour aider à présélectionner les candidatures dans Workday. L’outil repère les qualifications et l’expérience liées au poste afin d’appuyer un processus équitable, cohérent et efficace.

L’IA appuie les recruteurs. Le gestionnaire et l’équipe d’embauche prennent la décision finale. Les outils ne communiquent aucune donnée de candidature à l’extérieur. Les renseignements demeurent dans les systèmes sécurisés de Magna et sont traités selon ses politiques de confidentialité et de protection des données.

La législation applicable peut donner aux candidats le droit de demander comment l’IA a contribué à la prise de décision.

L’équipe d’attraction des talents répond aux questions sur ce processus.