TECHNICIENNE OU TECHNICIEN EN INFORMATIQUE, CLASSE PRINCIPALE
EXPERTE OU EXPERT EN CYBERSÉCURITÉ

EXIGENCES TECHNIQUES PARTICULIÈRES

SCCM/Intune

- Participer à l'emballage (packaging) et au déploiement des applications ainsi qu'aux activités mensuelles de gestion des correctifs;
- Collaborer aux initiatives de correction des vulnérabilités et d'amélioration de la conformité des postes de travail;
- Analyser les échecs de déploiement et travailler avec les analystes pour identifier et résoudre les problèmes;
- Participer aux activités de gestion des changements et aux essais des modifications apportées aux environnements de postes de travail;
- Documenter les résultats des déploiements, les mesures correctives et les processus opérationnels.

SharePoint

- Administrer, maintenir et optimiser l'environnement SharePoint Online et ses sites;
- Gérer l'architecture de l'information, les permissions, les groupes de sécurité et les contrôles d'accès;
- Assurer la gouvernance documentaire, incluant les bibliothèques, métadonnées, versions et règles de conservation;
- Veiller à la conformité, à la protection des renseignements et à l'application des politiques de gouvernance avec Microsoft Purview;
- Accompagner les utilisateurs et collaborer avec les équipes de sécurité, d'infrastructure et de conformité afin d'assurer une gestion efficace et sécuritaire de l'information.

Cybersécurité

- Connaissance des principes, méthodes et bonnes pratiques reconnues en matière de cybersécurité, notamment en matière de prévention, de détection et de réponse aux incidents;
- Connaissance des systèmes d'exploitation de serveurs Microsoft Windows et de leur sécurisation;
- Connaissance des systèmes d'exploitation Linux et des mécanismes de sécurité qui leur sont associés;
- Connaissance des concepts d'administration et de sécurité des environnements Microsoft Active Directory, notamment la gestion des utilisateurs, des groupes, des politiques de sécurité et des contrôles d'accès;
- Connaissance des principes de segmentation et de sécurisation des réseaux, notamment les pares-feux, les réseaux VLAN, les VPN et les contrôles d'accès réseau;

- Connaissance des méthodes et outils de surveillance de la sécurité des réseaux, des systèmes et des postes de travail, notamment la collecte et l'analyse de journaux d'événements;
- Connaissance des principes de fonctionnement des systèmes de détection et de prévention des intrusions et des systèmes de gestion des événements et des informations de sécurité (SIEM);
- Connaissance des mécanismes de protection des postes de travail et des serveurs, notamment les solutions antivirus, antimalware et EDR;
- Connaissance des principes de gestion des vulnérabilités, notamment l'identification, l'évaluation, la priorisation et le suivi des vulnérabilités et des correctifs de sécurité;
- Connaissance des principes de gestion des identités et des accès, notamment l'authentification multi facteur (MFA), le principe du moindre privilège et la gestion des comptes privilégiés;
- Connaissance des méthodes reconnues de gestion et de réponse aux incidents de cybersécurité, incluant la détection, l'analyse, la documentation, la mitigation et le rétablissement des services;
- Connaissance des principes de sécurité des environnements infonuagiques et des services Microsoft 365;
- Connaissance des principes de sécurité liés aux réseaux sans fil et aux appareils mobiles;
- Connaissance des méthodes de sensibilisation et de prévention en matière de cybersécurité, notamment en ce qui concerne l'hameçonnage, l'ingénierie sociale et les bonnes pratiques de gestion des mots de passe;
- Connaissance des principes de journalisation, de conservation et d'analyse des traces et des événements de sécurité;
- Atout : connaissance des outils d'analyse de vulnérabilités et de sécurité, notamment Microsoft Defender;
- Atout : connaissance des environnements infonuagiques, notamment Microsoft Azure et Microsoft Entra ID;
- Atout : connaissance des techniques d'analyse et de traitement des courriels malveillants, de l'hameçonnage et des logiciels malveillants.