

Protégez votre organisation contre les cybermenaces

6 trillions \$

En coût direct, indirect et revenus pour les cybercriminels en 2021. Équivalent au PIB de la 3^{ème} plus grande économie mondiale.

(WEF Global Risk Report 2020)

42%

des Canadiens victimes de cyberattaque, hameçonnage, fraude, logiciels malveillants, piratage de compte en ligne.

(StatCan, Septembre 2020)

4 fois +

de cyberattaques depuis le début de la pandémie. Une statistique inquiétante et en constante augmentation.

(FBI, 2020)

«Le paysage des menaces a changé, mais surtout, la pandémie a créé un environnement d'anxiété et d'incertitude que les cybercriminels exploitent. Aujourd'hui plus que jamais, la cybersécurité est un problème qu'aucune organisation ne peut ignorer.»

Jacques Latour, Chef de la sécurité de l'ACEI



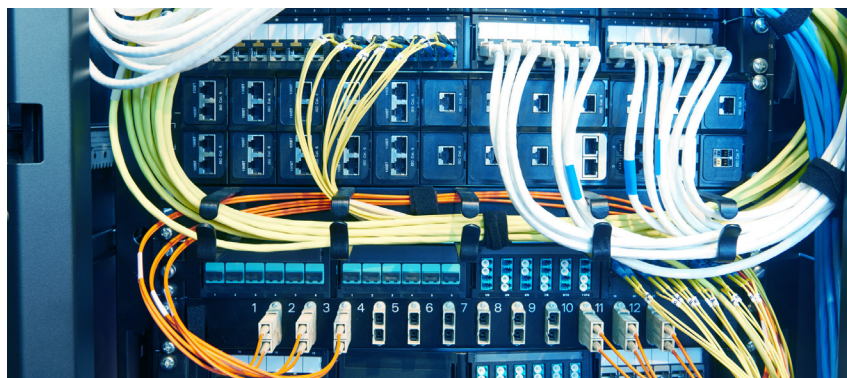
Subir une cyber-attaque, c'est s'exposer à des multiples risques.

- ◆ Perte de données personnelles et confidentielles
- ◆ Perte financière (rançon, investigation, prévention).
- ◆ Perte de temps (arrêt des activités et opérations quotidiennes).

Il est désormais crucial de réviser la sécurité de votre organisation afin de prendre toutes les précautions possibles.

Ensemble, mettons en place une bonne hygiène en sécurité pour votre organisation.

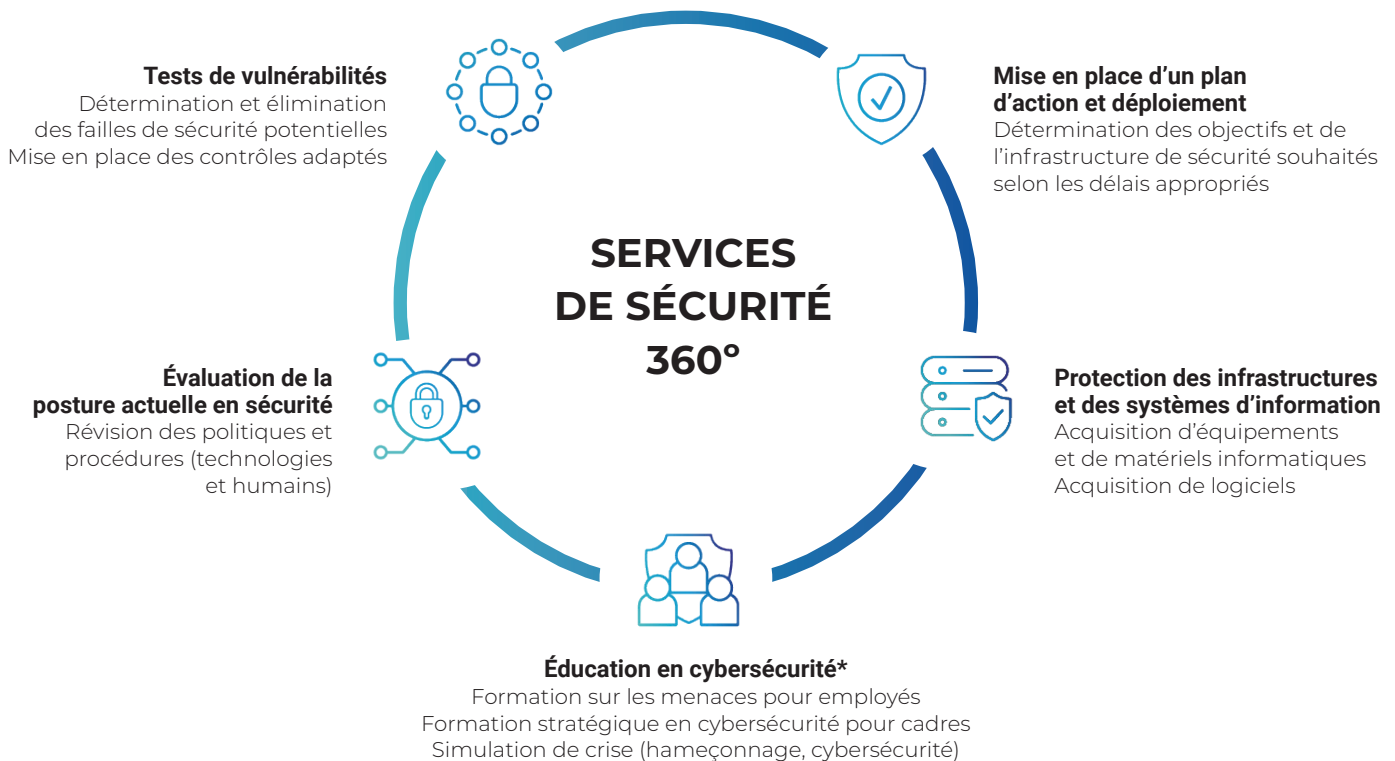
- ◆ Prévention des fraudes
- ◆ Protection de la réputation de votre organisation.
- ◆ Protection des vols de données personnelles et confidentielles des employés, des étudiants, des parents, des partenaires et des fournisseurs.



Profitez de notre offre de service 360° adaptée et surtout abordable.

Notre objectif : démocratiser la sécurité.

Division Sécurité International (DSI), composé de 13 membres fondateurs, met à votre disposition un grand éventail de spécialistes chevronnés provenant de tous les secteurs de la sécurité afin de vous offrir des solutions 360° optimisées. Notre expertise comprend la cybersécurité, la protection des personnes et des données, ainsi que la sécurité physique.



* Formateur accrédité par EC-Council et PECB en Cybersécurité et Conformité ISO

Offre de services

Phase 1 – Définir le contexte actuel de sécurité et documenter les besoins incluant les actifs de protection physique, informationnel et technologies

Poursuite de l'analyse des besoins

- ◆ Prise d'inventaire des actifs (Humains, Physiques, Procédures, Technologiques, Infrastructures et Partenariats).
- ◆ Documentation des relations existantes entre les processus et les technologies (Data Flow).
- ◆ Analyser les "flow" et production d'une architecture fonctionnelle (High level).
- ◆ Discuter et promulguer les recommandations applicables avec le premier responsable.
- ◆ Documenter et enregistrer les décisions et les orientations retenues.
- ◆ Documenter la posture de sécurité actuelle avec une analyse d'écart par rapport à la cible établie.