Le CIS

Par Patrick Sentinel – 29a.ca

Le CIS : Votre ninja personnel contre les cyberméchants !

Dans le monde merveilleux de la cybersécurité, où les hackers mal intentionnés pullulent comme des zombies dans un film de série B, il est essentiel d'avoir un guide pour survivre. Heureusement, le **CIS (Center for Internet Security)** est là pour vous aider à ne pas finir comme la première victime d'un film d'horreur informatique.

CIS : Hein ?

Le *Center for Internet Security* est une organisation à but non lucratif qui délivre des recommandations et des *benchmarks* de sécurité pour vous éviter d'être la prochaine star d'un épisode de "Piratage Catastrophe". En gros, ils écrivent les règles du jeu pour que votre infrastructure ne se transforme pas en buffet à volonté pour les cybercriminels.

Les CIS Controls : Un programme d'entraînement de cyber-jedi

Le CIS propose une liste de **18 contrôles critiques**, qui sont l'équivalent des arts martiaux pour votre réseau. Voici quelques perles qui vous aideront à bloquer les méchants avant même qu'ils ne commencent à pianoter sur leur clavier maléfique :

1. **Inventaire des actifs et des logiciels**
    - Parce que si vous ne savez même pas ce qui tourne sur votre réseau, autant laisser les hackers s'installer avec un petit café.
2. **Protection des données**
    - Vos données sont comme des chiots mignons : il faut les protéger, sinon quelqu'un va les voler (et les revendre sur un marché douteux du *dark web*).
3. **Contrôle des accès**
    - Parce que laisser un employé junior accéder aux données sensibles, c'est comme confier les codes nucléaires à un gamin de 5 ans. Mauvaise idée.
4. **Monitoring et analyse des journaux**
    - Si un hacker pénètre votre système et que personne ne le remarque, a-t-il vraiment piraté votre réseau ? Spoiler : oui.

Les Benchmarks CIS : La bible du sysadmin en panique

En plus des contrôles, le CIS propose des benchmarks de configuration pour éviter que vos serveurs ne soient plus exposés qu'un touriste en short dans l'Arctique. Que ce soit pour *Windows*, *Linux*,

MacOS, ou même *Kubernetes* (pour les fans de containers qui aiment souffrir), ces guides vous disent exactement quoi désactiver, renforcer ou configurer pour que votre système soit aussi sécurisé qu'une base secrète de la CIA (ou presque).

Niveau 1 et Niveau 2 : Le mode facile vs. le mode hardcore

Le CIS Benchmark est divisé en **deux niveaux de configuration** :

- **Niveau 1** : C'est le mode "tranquille" qui vous permet de renforcer la sécurité sans trop briser votre système. Il comprend des recommandations basiques qui minimisent les risques sans perturber les opérations quotidiennes. Autrement dit, vous renforcez votre sécurité sans avoir un appel de panique de l'équipe IT à chaque déploiement.
- **Niveau 2** : Pour les vrais guerriers de la cybersécurité qui veulent un système aussi blindé qu'une forteresse numérique. Ce niveau pousse les restrictions à fond, ce qui peut parfois casser des applications ou rendre l'expérience utilisateur aussi fluide qu'une brique lancée dans un marre. Mais si vous voulez que votre système soit impénétrable, c'est le choix à faire.

Pourquoi appliquer le CIS ?

Si vous hésitez encore, voici quelques bonnes raisons d'adopter les recommandations du CIS :

- Vous dormirez mieux la nuit (ou du moins, vos alertes SIEM crieront un peu moins);
- Vos audits de conformité ressembleront moins à un tribunal où vous êtes l'accusé;
- Vous pourrez relaxer en réunion en disant : "Oui, nous suivons les benchmarks CIS, bien entendu" 😉;
- Vos utilisateurs vous en voudront peut-être d'avoir bloqué leur accès aux sites de streaming, mais au moins, votre réseau ne sera pas une passoire numérique.

Conclusion : Soyez le héros que votre SI mérite

Le CIS, c'est comme un coach personnel pour votre cybersécurité. Suivez ses conseils et vous pourrez affronter les hackers avec plus de confiance qu'un chevalier en armure numérique. Ignorez-le, et votre réseau risque de finir en passoire. Alors, à vous de jouer : mettez en place ces contrôles, appliquez ces benchmarks et devenez le ninja de la cybersécurité dont votre entreprise a besoin !