Guide rapide
CSC Security Center

Avec des cyberattaques quotidiennes en recrudescence, il est plus important que jamais que les responsables chargés de protéger la présence en ligne de la marque choisissent les bons partenaires et les outils adaptés.

Les actifs numériques constituent une vulnérabilité exploitée par les cybercriminels et les hackers. Il n'est donc pas suffisant de choisir des services de gestion de base et de vous contenter de revoir votre approche chaque année.

Pour garder une longueur d'avance sur les cybercriminels et pour accompagner les titulaires de marques au fur et à mesure que leurs modèles d'activité évoluent, CSC a développé CSC Security Center[SM], qui supprime la complexité et rend le contrôle à nos clients.

Quels sont les risques et en quoi CSC Security Center peut-il m'aider ?

À l'aide de plusieurs sources de données et d'un algorithme complexe, testé dans certaines des plus importantes entreprises du monde entier, CSC Security Center est capable d'identifier et de surveiller les actifs numériques essentiels à votre activité et d'assurer une évaluation du risque en continu. Cette approche vous permet de détecter et de contrer instantanément les cyberattaques potentielles sur vos actifs sous surveillance.

Risques	Conséquences	Impact	Solution CSC
Comptabilité et gestion déficientes	Expiration des noms de domaine critiques et des certificats numériques SSL (Secure Sockets Layer)	Absence de résolution du site web, dysfonctionnement de la messagerie, du réseau VPN ou de la téléphonie VoIP ; perte de la confiance des usagers et vulnérabilité potentielle face aux logiciels malveillants et aux attaques par rançongiciel	Effectuer un audit et consolider les noms de domaine, les services DNS et les certificats SSL
Prestataires tiers	Ingénierie sociale, phishing ou attaques DDoS	Aucun contrôle sur la résolution du site web, la messagerie, le réseau VPN ou la téléphonie VoIP et possibilité que les cybercriminels clonent les sites et dérobent des e-mails	Priorité à la sécurité ; nous investissons massivement dans la technologie et le personnel
Accessibilité des actifs	Ingénierie sociale, attaques de phishing	Aucun contrôle sur la résolution du site web, la messagerie, le réseau VPN ou la téléphonie VoIP et possibilité que les cybercriminels clonent les sites et dérobent des e-mails	Sécuriser l'accès au système de gestion via la validation IP, l'authentification à deux facteurs et la gestion des identités fédérées
Menaces externes	Incapacité à limiter les attaques DDoS et de phishing	Absence de résolution du site web, dysfonctionnement de la messagerie, du réseau VPN et de la téléphonie VoIP ; peut agir comme « rideau de fumée » pour dissimuler une seconde attaque	Sécuriser les actifs contre les menaces connues à l'aide de MultiLock, de la mitigation des attaques DDoS, de l'authentification des e-mails et des services anti-phishing.
Une approche statique	Domaines critiques et risques non identifiés	Aucun contrôle sur la résolution du site web, la messagerie, le réseau VPN ou la téléphonie VoIP et possibilité que les cybercriminels clonent les sites et dérobent des e-mails	CSC Security Center