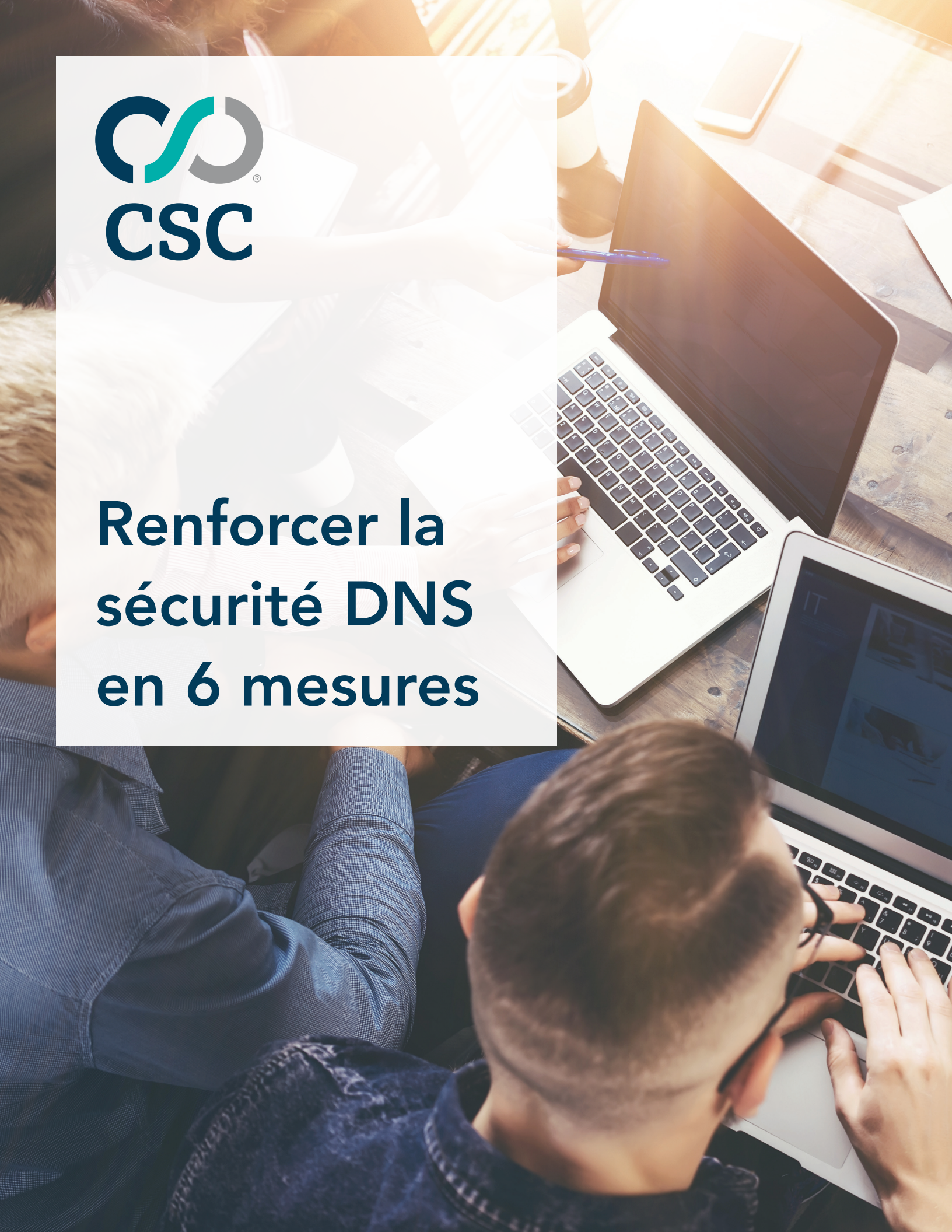

Renforcer la sécurité DNS en 6 mesures

Renforcer la sécurité DNS en 6 mesures

Le système de noms de domaine (DNS) a pris de l'importance dès les débuts d'Internet, lorsque qu'aucune menace ne pesait encore sur le Web. À cette époque, les premiers utilisateurs d'Internet étaient majoritairement des employés des services publics ou d'organisations éducatives. La confiance était tenue pour acquise et la question de la sécurité ne se posait pas. Comme la communauté en ligne était encore restreinte et Internet rarement utilisé, peu de gens comprenaient l'importance des serveurs DNS qui, de ce fait, n'étaient pas protégés.

Faites une avance rapide jusqu'à aujourd'hui, et vous comprendrez aisément les problèmes que cette absence de protection a engendrés. Les cyberattaques récentes mettent en lumière les techniques spécifiques utilisées par les individus malveillants pour intercepter et manipuler le trafic Web légitime d'une entreprise, récolter des informations comme les identifiants ou les adresses e-mail, et commettre d'autres activités hostiles, comme le hameçonnage (« phishing »). Dans certains cas, des certificats numériques gratuits, qui requièrent une validation de faible niveau, sont émis pour rendre les tentatives d'escroquerie (les « scams ») plus crédibles, ce qui amplifie le problème pour les marques comme pour leurs clients. Les clients craignent que leurs données personnelles soient accessibles et volées par des criminels. Ce type de failles de sécurité impacte donc la réputation et le chiffre d'affaires d'entreprises dans le monde entier. À cela, s'ajoute l'augmentation exponentielle des attaques DDoS, qui ciblent souvent les serveurs DNS pour nuire aux activités en ligne des entreprises.

Pour celles-ci, l'équation est simple : une panne de DNS signifie une panne de site Web ou aucune présence en ligne. En cas de dysfonctionnement du DNS, les clients qui veulent consulter un site Web ne pourront tout simplement pas y accéder. Parallèlement, les employés de l'entreprise ne pourront ni envoyer, ni recevoir d'e-mail. Si une entreprise utilise la téléphonie VoIP pour ses appels, l'accès est interrompu. En cas de panne de serveurs DNS, les entreprises devront utiliser les lignes fixes et les téléphones mobiles pour appeler leurs clients. Enfin, la capacité des télétravailleurs d'accéder aux systèmes via le réseau VPN disparaît, ce qui prive l'entreprise de ressources précieuses au moment précis où elle a besoin de son personnel au complet.

Comprenant l'importance de disposer d'une infrastructure DNS robuste et sécurisée, et d'une bonne gestion des noms de domaine et des certificats numériques, CSC a choisi de s'associer à Neustar® – qui exploite les réseaux DNS les plus étendus et les plus sécurisés au monde depuis plus de 20 ans – et recommande 6 mesures pour renforcer la sécurité DNS.

**Ce document s'inspire de la publication « Five Ways Neustar Strengthens DNS Security » de Neustar.*

1 Atténuer les attaques DDoS avec une protection multicouche

La puissance des attaques DDoS volumétriques a explosé, avec des attaques qui dépassent désormais 1 térabit/seconde (Tbits/s). Certaines des attaques les plus puissantes jamais enregistrées visaient des systèmes DNS.

De nombreux types d'attaques DDoS ciblent le DNS

L'attaque DNS par amplification n'est qu'une méthode parmi d'autres. Les attaquants exploitent la multitude de serveurs DNS ouverts sur Internet, qui peuvent être utilisés pour répondre à n'importe quelle petite interrogation en usurpant l'adresse IP de la cible. La cible reçoit alors un plus grand volume de réponses DNS qui submergent rapidement ses capacités. L'objectif : bloquer les requêtes DNS légitimes en épuisant les capacités du réseau.

Un autre type d'attaque commun est l'attaque DNS Flood, dirigée contre des serveurs DNS qui hébergent un ou des sites Web spécifiques. Cette attaque tente d'épuiser les ressources du serveur, comme la mémoire ou l'unité centrale de traitement (CPU), avec un barrage de requêtes UDP (user diagram protocol) générées en exécutant des scripts sur un réseau botnet de machines.

Protection anti-DDoS multicouche

Pour vous défendre contre tous types d'attaque DNS, utilisez une solution qui propose plusieurs couches de protection anti-DDoS.

Les nœuds DNS doivent être dotés d'un équipement de mitigation de DDoS afin de surveiller en continu tout trafic inhabituel issu d'une géolocalisation suspecte dans des volumes anormaux. Dans de nombreux cas, la mitigation se fait localement.

En cas d'attaque très puissante, le trafic malveillant doit être automatiquement redirigé vers un réseau de mitigation, à savoir une infrastructure complètement distincte conçue dans ce but. Cela permet de limiter les dommages potentiels aux adresses IP des serveurs de noms de domaine ciblés. Une fois l'impact isolé, une équipe de sécurité 24h/24, 7j/7 peut mettre en œuvre des contre-mesures agressives.

2 Isoler les serveurs de noms via la segmentation

Dans toute l'industrie, un DNS hautement évolutif est devenu un service dans le Cloud avec des centaines de milliers de clients, chacun disposant de plusieurs noms de domaine, regroupés sur des réseaux uniques et partageant un serveur de noms.

Cette évolution augmente le risque d'être impacté par une attaque visant une autre entreprise. Si vous utilisez un prestataire de services DNS tiers, la plupart des attaques sur son réseau ne vous seront pas destinées, mais cibleront le serveur de noms de ce prestataire.

Isoler l'impact d'une attaque DDoS : la bonne stratégie

Faites le choix d'un prestataire qui organise son réseau DNS en segments, chacun disposant d'une annonce de serveur de noms partagée par un petit groupe de clients uniquement. En diminuant le nombre de clients partageant les noms d'hôte et les adresses IP, vous réduisez les risques d'un effet de contagion.

Pour mieux comprendre, prenons l'analogie suivante : imaginez que vous soyez dans une salle immense avec 10 000 personnes et que quelqu'un se mette à crier si fort que personne ne peut entendre le conférencier parler. Maintenant, imaginez le même scénario, mais avec une vingtaine de personnes seulement. Le cri n'affectera que ces 20 personnes.

Si on considère que l'individu qui hurle est une attaque DDoS, lorsqu'il commence à crier (l'attaque), la segmentation du serveur de noms et la stratégie de mitigation de DDoS transfèrent immédiatement les personnes présentes vers une zone insonorisée, en protégeant celles-ci et en tentant de faire taire l'individu qui crie, avant de faire revenir tout le monde. On comprend donc qu'avec seulement 20 personnes, le cri a affecté une audience réduite, qu'il a été facile de déplacer pendant l'attaque.

Être protégé, que vous ou quelqu'un d'autre soyez visé

Cette approche permet aux annonces de serveurs de noms individuelles de se déplacer du réseau DNS vers le réseau de mitigation de DDoS sans retarder davantage la résolution des requêtes. Votre prestataire de services DNS doit être capable de fournir des mesures de mitigation immédiates efficaces aux équipements attaqués ET d'empêcher tout impact collatéral pour les clients qui sont encore sur le réseau DNS.

En cas d'utilisation de services DNS dans le Cloud, être sur une annonce de serveur de noms segmentée est une manière efficace de protéger votre trafic DNS.

3 Utiliser une résolution non-open source

Les serveurs DNS de résolution, c'est-à-dire les serveurs qui répondent aux interrogations de nom de domaine, permettent de garantir que les utilisateurs sont dirigés vers les bons sites. Le programme le plus populaire pour gérer le DNS est le Berkeley Internet Name Domain (BIND). Développé en 1983 à l'université de Berkeley, en Californie, BIND reste le programme utilisé par la majorité des implémentations de serveurs de noms. Aujourd'hui totalement dans le domaine public, le code source de BIND est en open source, et peut donc être librement analysé et exploité par les cybercriminels.

Éviter les menaces pesant sur les serveurs de résolution

CSC a choisi de s'associer à Neustar parce que l'entreprise a résolu ce problème il y a plusieurs années. Les spécialistes Neustar ont développé un code propriétaire et demandé à des auditeurs de sécurité externes d'identifier les vulnérabilités potentielles. Ils ont ainsi découvert qu'aucun attaquant ne pouvait l'exploiter à distance, que ce soit pour dérober des privilèges restreints ou pour entraver la résolution du répertoire.

En plus de prendre en charge les RFC (requests for comments) DNS standard, ils ont amélioré leurs programmes de résolution afin d'étendre les capacités DNS tout en fournissant une redondance et une sécurité supplémentaires. La plupart des implémentations de serveurs DNS hérités n'ont jamais atteint ce niveau de sécurité.

4 Déployer DNSSEC (DNS Security Extension)

Lorsqu'ils aident les utilisateurs d'Internet à trouver les sites souhaités, les serveurs DNS s'interrogent les uns les autres. Pour aller plus vite, les serveurs mettent en cache les résultats de recherche pour une durée spécifiée. En cas de requêtes pour le même nom avant l'expiration du délai d'enregistrement de la ressource, un serveur donnera la réponse en cache au lieu d'interroger une autre machine.

L'empoisonnement de cache DNS permet les attaques par pharming

Si cette technique améliore l'efficacité, elle est également favorable à l'empoisonnement du cache. Celui-ci survient lorsqu'un serveur DNS compromis par des criminels fournit une fausse réponse à une requête DNS. L'utilisateur atterrit alors sur des sites frauduleux qui lui demandent des informations personnelles ou, plus simplement, activent un malware.

Comment est-ce possible ? Souvent, les serveurs DNS ne vérifient pas si les réponses qu'ils reçoivent des autres serveurs sont liées à la requête initiale. Un serveur mettra en cache des informations erronées et les transmettra aux autres serveurs qui sont des clients DNS de la machine compromise.

La clé de la protection est DNSSEC

DNSSEC est un ensemble d'extensions de sécurité qui authentifient les réponses DNS. Son secret est une série de combinaisons de clés publiques et privées permettant de signer les données. Ce protocole fonctionne en fournissant une clé publique qui permet au serveur de résolution de l'utilisateur de confirmer que la réponse DNS correspond à la version chiffrée. Toutes les transactions sont signées : les cybercriminels ne peuvent donc pas simplement imiter les paquets de données.

En termes plus simples, DNSSEC sécurise le processus de résolution DNS en le protégeant contre l'empoisonnement de cache, les attaques par pharming et les autres menaces sérieuses. Assurez-vous de le déployer.

Adoption DNSSEC

Ces dernières années, dans nos Rapports de cybersécurité CSC, nous avons mentionné à quel point le niveau d'adoption de DNSSEC était singulièrement bas, avec un taux variant de 0 % à 5 % parmi les entreprises les plus importantes de divers secteurs d'activité.

5 Augmenter la résilience avec un réseau DNS privé

La sécurité de votre réseau est équivalente à celle de son maillon le plus faible. Et si vous pouviez renforcer votre stratégie de sécurité en éliminant les maillons faibles ? En réduisant la dépendance aux connexions publiques à Internet, le réseau privé supprime essentiellement la section médiane, soit la plus dangereuse, de la transaction DNS sur laquelle se concentre la vaste majorité des attaques DDoS et des tentatives d'empoisonnement de cache DNS. Demandez à votre prestataire s'il fournit ce service en option.

Un réseau privé présente trois avantages clés :

Une latence réduite

Dans certains cas, même si le DNS fonctionne sans problème, d'autres problèmes affectant la connexion Internet peuvent diminuer les performances du DNS et altérer l'expérience utilisateur. Le réseau privé garantit une expérience en ligne rapide et efficace parce que le trafic DNS évite les réseaux Internet habituels.

Une sécurité renforcée

Les attaques DDoS actuelles – intensifiées par l'Internet des objets (IoT) – qui interrompent l'accès à Internet sont condamnées à disparaître. Un réseau privé pour la résolution DNS au sein des réseaux du prestataire minimise la surface d'attaque face aux tentatives de type DDoS et d'empoisonnement de cache.

Une fiabilité améliorée

En cas d'attaque DDoS ou de panne massive, les requêtes continueront d'être résolues au sein du réseau privé sur lesquels le DNS est déployé. Cette résilience garantit une expérience Internet supérieure pour les utilisateurs qui consultent des sites Web et d'autres actifs en ligne sensibles.

6 Identifier les failles de sécurité de vos actifs numériques sensibles

Les entreprises doivent pouvoir être capables d'identifier leurs noms de domaine critiques, et de les surveiller en continu pour s'assurer qu'ils sont protégés par des mécanismes de sécurité adéquats.

Nous avons remarqué qu'aucune solution n'aidait les entreprises en ce sens, et nous avons donc développé CSC Security Center℠, une plateforme intelligente qui identifie les menaces autour des domaines critiques et au sein de l'infrastructure DNS qui les héberge, et alerte les entreprises des zones à risque.

Cette approche unique change la manière dont sont sécurisés les noms de domaine et le DNS, et aide les entreprises à mieux repérer leurs failles de sécurité. CSC Security Center aide notamment les clients à :

- Identifier les domaines critiques qui ont besoin d'une garantie de disponibilité de 100 %.
- Identifier tous les prestataires de services DNS actuels et évaluer les risques de sécurité au niveau fournisseur.
- Identifier toute fonctionnalité de sécurité manquante, qui augmente le risque d'empoisonnement de cache, de piratage de nom de domaine ou de DNS, de domain-shadowing, d'attaque DDoS et de phishing.

Demandez plus d'informations sur la manière dont CSC Security Center et nos services DNS peuvent vous aider à atténuer les cybermenaces.

CSC soutient les entreprises qui font d'importants investissements dans la sécurité en identifiant les failles de sécurité dans leurs actifs immatériels tels que les noms de domaine, le DNS et les certificats numériques. Les solutions de sécurité CSC protègent les entreprises des cybermenaces qui pèsent sur leurs actifs numériques, et les aident à éviter les pertes de revenus, les atteintes à la réputation de leur marque ou les pénalités financières pouvant résulter d'une non-conformité aux réglementations de type RGPD. Outre les actifs numériques, les solutions CSC permettent de sécuriser les marques en ligne face aux sites Web contrefaits, à la fraude et aux violations des droits de propriété intellectuelle. Les solutions CSC surveillent et contrent ce type d'attaques, et offrent des services de conseil et d'action en contrefaçon. Plus d'infos sur cscdigitalbrand.services.

cscdigitalbrand.services