Le Darknet : Ce qu'il sait sur vous et que vous ne savez pas.

Merci d'avoir assisté à notre webinaire "**Le Darknet : Ce qu'il sait sur vous et que vous ne savez pas.**"

Comme promis, nous vous partageons ci-dessous un document regroupant un résumé des questions posées, les réponses détaillées de nos experts, ainsi qu'une **offre exclusive** réservée aux participants. Ce document a été conçu pour vous accompagner dans votre réflexion sur les dangers du darknet.

Questions et réponses

1. Pourquoi avoir besoin de SecureDNS si mon pare-feu a déjà une protection DNS incluse ?

Utiliser la protection DNS intégrée dans un pare-feu est un début, mais plus suffisant aujourd'hui pour se protéger contre les menaces émergentes. Une approche dédiée à la protection DNS est essentielle ! L'avantage avec SecureDNS, c'est qu'on combine plus de **42 sources d'intelligence sur les menaces en une solution**, provenant des principaux fabricants de pare-feu et d'antivirus.

Le **DNS est privilégié dans la majorité des attaques**, soit pendant leur cycle d'exécution, soit comme point d'entrée lorsque l'utilisateur clique sur un lien malveillant à travers l'hameçonnage.
Il faut savoir que 90% des logiciels malveillants, comme les ransomwares, voleurs d'informations et autres, dépendent du DNS pour fonctionner, et 70% des nouveaux domaines sont créés à des fins malveillantes.

Les attaquants exploitent les noms de domaine plutôt que les adresses IP pour contourner les défenses classiques, en changeant rapidement d'IP et en générant de nouveaux domaines par algorithme. SecureDNS bloque ces nouveaux domaines pendant 24 heures, le temps de les analyser.

2. Pouvez-vous comparer votre solution à des protections DNS connues sur le marché ?

SecureDNS, comme les autres protections DNS, vise à bloquer l'accès aux domaines malveillants. Cependant, Secutec utilise une stratégie multifournisseurs, intégrant les technologies et renseignements des leaders en cybersécurité. Cette approche a déjà démontré que SecureDNS détecte et bloque plus de risques que d'autres solutions bien connues.

Un autre avantage est que tous nos services sont centralisés sur **un seul portail, gérés 24/7 par Secutec**, avec des alertes SOC pour vous avertir en cas de risque élevé.
De plus, votre EDR peut contribuer à enrichir les événements SecureDNS afin de mieux contextualiser les risques. Cela fonctionne dans les deux sens.

Questions et réponses (suite)

3. J'utilise des services gratuits sur internet comme haveibeenpwned, pour vérifier les fuites d'identifiants.

Ces outils reposent sur des bases de données anciennes et gratuites, ignorant de nombreuses fuites récentes. De plus, ce n'est pas une surveillance en temps réel.
Il est essentiel d'être informé dès la publication d'informations sensibles afin de réduire le risque qu'un attaquant exploite un accès et s'authentifie dans votre système d'information.

Secutec exploite des sources payantes, accède à des bases de données privées et surveille les marchés noirs ainsi que les communautés de hackers afin de détecter un maximum de données compromises sur le Darknet.
Nous assurons une surveillance 24/7 des fuites de données et vous alertons via notre portail centralisé, où vous pouvez gérer ces risques.

Selon une étude, près de 80 % des brèches de données ont été facilitées par des identifiants compromis. L'équipe de réponse à l'incident chez Secutec a pu conclure à plusieurs reprises que certains incidents auraient pu être évités si une surveillance professionnelle avait été en place sur le Darknet.

4. Quel est le coût de SecureDNS et du Darknet monitoring ?

La surveillance continue du Darknet consiste en **deux services** :

Surveillance des fuites de données d'identification de votre organisation et des parties tierces qui se connectent à votre environnement (fournisseurs TI, plateformes, Veeam, VMware, O365, etc.).
Surveillance complète du Darknet : recherches approfondies et continues sur toutes les informations sensibles liées à votre organisation et à vos employés, notamment les marchés noirs, communautés de hackers, chats Telegram, et autres.

Le coût est basé sur le nombre de domaines et d'employés à surveiller. Pour un prix sur mesure, veuillez contacter un représentant chez Prival.

SecureDNS protège tout votre réseau de système d'information. Cependant, la licence est basée uniquement sur le nombre d'employés connectés.

Cela inclut :

- Soutien technique
- Un agent Windows, Mac, Linux, pour protéger les employés travaillant à l'extérieur du réseau.
- Possibilité d'enrichissement avec votre EDR.

Tous nos services sont gérés **24/7** avec alertes SOC.

Notre Offre

Protégez votre entreprise avec notre offre de sécurité gratuite!

1. **SecureDNS** : Bloquez l'accès à des sites dangereux comme ceux utilisés pour le hameçonnage. En quelques minutes, protégez vos employés et votre environnement. Activez votre **essai gratuit de 30 jours dès maintenant !**
2. **Scan gratuit des actifs exposés** : Identifiez les risques potentiels avant qu'ils ne soient exploités ou mis en vente sur le Darknet. Faites un **scan gratuit de vos actifs exposés à internet.**
3. **Analyse préliminaire du Darknet** : Vérifiez gratuitement si des informations sensibles concernant votre entreprise ou vos employés circulent déjà sur le Darknet.

Agissez dès aujourd'hui pour sécuriser vos données !

Planifiez un créneau avec notre équipe pour profiter de l'offre ou pour poser vos questions.

Prenez rendez vous !

outlook.office.com/book/PrivalXSecutecOffreexclusive@prival.ca