SERVICES DE CYBERSÉCURITÉ

Test d'intrusion et analyse de vulnérabilité

OFFRE SPÉCIALE AUX SOCIÉTÉS MEMBRES DE L'ACCVM

Les tests d'intrusion et l'analyse de vulnérabilité sont deux parties d'un service global. Un test d'intrusion recherche les lacunes dans les pare-feu de réseau (Internet) extérieurs, sites Web et connexions avec des fournisseurs par lesquelles des logiciels malveillants peuvent s'introduire et s'attaquer à votre réseau. Une analyse de vulnérabilité interne s'applique à l'intérieur des pare-feu de votre entreprise pour repérer les vulnérabilités réelles et potentielles dans votre réseau (pare-feu, routeur(s), commutateur(s), serveur(s), poste(s) de travail, imprimante(s), etc.). Ce processus combiné dure généralement de 3 à 4 jours selon l'infrastructure et il est généralement recommandé de l'exécuter pendant les fins de semaine.

TEST D'INTRUSION :

- Conçu pour évaluer l'état de votre sécurité extérieure avant que des cyberattaquants le fassent.
- Les outils simulent des scénarios d'attaque en condition réelle pour découvrir et exploiter les lacunes de sécurité qui pourraient se solder par des vols de données, le dévoilement d'authentifiants, d'éléments de propriété intellectuelle, de renseignements permettant d'identifier des personnes, de renseignements personnels et de renseignements sur la santé protégés, des demandes de rançons informatiques et d'autres événements commerciaux préjudiciables.
- En découvrant les vulnérabilités de la sécurité, un test d'intrusion vous aide à déterminer le meilleur moyen d'atténuer le risque et de protéger vos données commerciales vitales contre des cyberattaques actuelles et futures.

ANALYSE DE VULNÉRABILITÉ :

L'objectif de l'analyse de vulnérabilité est de :

- Tester l'infrastructure interne et les différents types d'appareils clients en fonction des actes malveillants possibles.
- Empêcher les atteintes à la sécurité de l'intérieur de votre réseau.
- Conduite parallèlement à l'évaluation du niveau de sécurité du réseau interne.
- Vous donne une meilleure compréhension de votre infrastructure réseau ainsi que de votre sécurité à chaque niveau, une fois terminée.
- Procédez à l'analyse de tous les serveurs internes, appareils clients et du réseau à chaque emplacement. (Avant de lancer une analyse, une liste des emplacements et de tous les appareils raccordés au réseau interne sera nécessaire.)

PAR CES TESTS, L'ENTREPRISE PEUT DÉCELER :

- Les vulnérabilités de sa sécurité avant toute attaque informatique
- Les lacunes de conformité dans la sécurité des informations
- Le taux de réponse de l'équipe de sécurité informatique (interne ou en impartition)
  - Le temps qu'il faut à l'équipe pour comprendre qu'une effraction a eu lieu et le temps qu'il faut pour y remédier
- L'effet d'une violation de données ou d'une cyberattaque possible dans le monde réel
- Des orientations de correctifs applicables

À PROPOS DE CANDEAL SOLUTIONS

CanDeal Solutions offre une gamme de solutions technologiques de premier ordre à ses clients institutionnels, allant de la veille de cybersécurité à la recherche et analytique des données du marché. CanDeal Solutions appartient à six grandes banques canadiennes et au Groupe TMX. CanDeal est réglementée par des membres des Autorités canadiennes en valeurs mobilières et par l'OCRCVM et participe à un audit annuel sur la réglementation et la technologie.

RENSEIGNEMENTS

WWW.CANDEALSOLUTIONS.COM | 1.866.422.6332 | IIAC_CYBERSECURITYSERVICES@CANDEALSOLUTIONS.COM

CANDEAL SOLUTIONS