Protégez-vous des brèches de sécurité

Assurez-vous d'avoir une organisation sécurisée

LA DEMANDE POUR LES PROFESSIONNELS DE LA SÉCURITÉ DE L'INFORMATION AUGMENTERA DE 31% ENTRE 2019 ET 2029,

ce qui est beaucoup plus rapide que la moyenne pour toutes autres professions[1], incluant celles liées aux autres technologies de l'information. À mesure que la demande augmente, l'acquisition d'une expertise qualifiée pour aider les équipes déjà susceptibles d'être surchargées de travail et de manquer de personnel à mettre fin aux brèches de sécurité sera une priorité. Il est temps de se PRÉPARER.

Paysage des menaces: comptes d'utilisateurs

- **Détournement de session**
- **Hameçonnage**
- **Utilisateurs internes malveillants**

PRÉPARATION

Évaluez vos capacités de détection et réponse face aux menaces. Quel est votre niveau de préparation pour mettre fin à une brèche de sécurité ou répondre à un événement?

LES TROIS PILIERS D'UN BON PROGRAMME DE PRÉPARATION AUX BRÈCHES SONT LES SUIVANTS:

1. Plans de réponse aux incidents
2. Plans de reprise après sinistre
3. Plans de continuité des affaires

LES PRINCIPALES RAISONS D'OBTENIR UNE PERSPECTIVE DE SÉCURITÉ EXTERNE

La plupart des équipes de sécurité TI passent leur temps à identifier des menaces de sécurité, mais cela leur laisse moins de temps pour collecter des informations sur les incidents et les résoudre[1]. Le fait d'avoir des politiques et des procédures détaillées pour protéger les données, ainsi que la validation régulière de ces pratiques, aideront les organisations à mieux protéger leurs actifs.

LES TESTS D'INTRUSION

sont conçus pour identifier et évaluer les risques de sécurité dans plusieurs domaines – réseaux internes ou externes, applications Web, etc. Les équipes informatiques TI internes auront la possibilité de déployer leurs efforts de manière stratégique, en fonction des divers paramètres disponibles et seront mieux préparées pour l'application de correctifs.

Les tests d'intrusion peuvent vous aider à sécuriser vos mots de passe d'entreprise!

Encore aujourd'hui, l'équipe de testeurs de GoSecure identifie **1 utilisateur sur 4** avec un mot de passe « All-Star » (c.-à-d. Password123, nom-de-l'entreprise123).[2]

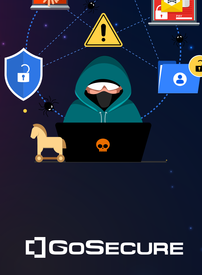
RÉPONSE

CHOISISSEZ VOTRE ÉQUIPE!

Nos services « Red | Blue | Purple Teams » effectuent des exercices pour déterminer dans quelle mesure vous êtes exposé aux attaques et comment améliorer la posture de sécurité de votre organisation. Les exercices de « Purple Team » sont les plus novateurs et permettront de tester et d'améliorer rapidement les « use case » de sécurité.

Paysage des menaces: infrastructure de données

- **Rançongiciels**
- **Logiciels malveillants**
- **Menaces persistantes avancées**
- **Robots et cheval de troie (« Botnet » et « Trojans »)**



SE PRÉPARER

fr.gosecure.net/advisory-services

GoSecure

[1] – 2019 Osterman Research Inc. [2] – Cybersecurity Perceptions vs Reality [1] – Bureau of Labor Statistics, United States