SERVICES DE PRÉPARATION AUX BRÈCHES DE SÉCURITÉ

Les services de préparation aux brèches de sécurité de GoSecure offrent un examen complet des capacités de réponse et préparent les organisations à se défendre contre les attaques.

TROIS (3) PILIERS DE PRÉPARATION

Les services de préparation aux brèches de sécurité de GoSecure adoptent une approche globale pour comprendre l'état de préparation d'une organisation en vue de répondre à un incident.

GoSecure évaluera:

- La continuité des activités;
- La réponse aux incidents;
- La reprise après sinistre.

Les experts de GoSecure estiment que pour déterminer le niveau de préparation d'une organisation, il faut évaluer l'ensemble du programme d'intervention ainsi que toutes les personnes, les processus, les politiques et les technologies impliqués.

GoSecure adopte une approche de préparation reposant sur trois piliers, car une brèche de sécurité n'est pas entièrement traitée tant que l'organisation n'a pas repris ses activités habituelles.

*Osterman Research Survey Report

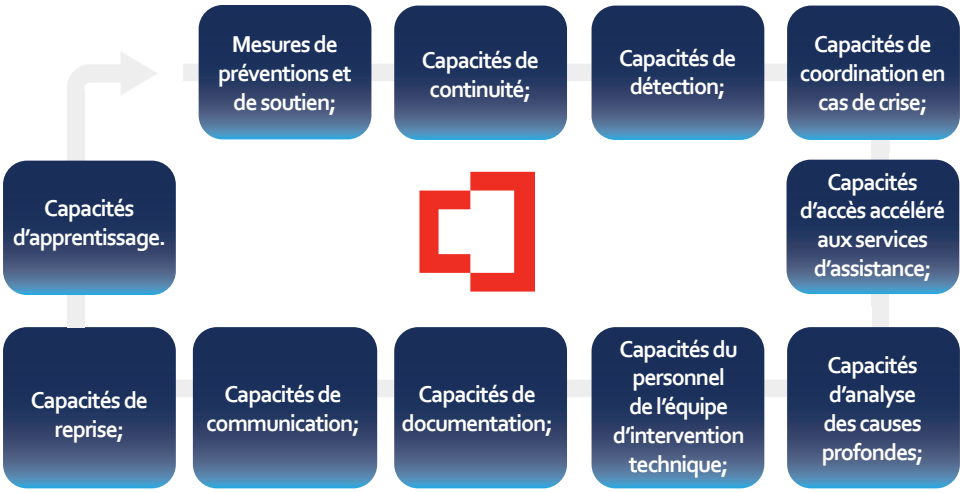
LA PRÉPARATION AUX CYBERATTAQUES

Dans une récente enquête, 81% des organisations ont déclaré avoir été victimes d'un certain type de brèche de données au cours des 12 derniers mois.* Les organisations sont préoccupées par les menaces croissantes que représentent les rançongiciels, les logiciels malveillants, les employés malveillants, etc.

ÉVALUATION DE LA PRÉPARATION AUX BRÈCHES DE SÉCURITÉ DE GOSECURE

L'évaluation de la préparation aux brèches de sécurité de GoSecure (BRA) offre une évaluation complète de la préparation aux incidents, en veillant à ce que les personnes, les processus, les outils, les politiques, les plans, les scénarios et les livres d'exécution soient prêts lorsqu'une brèche de sécurité se produit.

11 concepts essentiels de l'évaluation de la préparation aux brèches de sécurité de GoSecure



Se basant sur ces concepts essentiels, l'équipe qualifiée et chevronnée de GoSecure a mis au point un cadre exclusif d'évaluation de la préparation aux brèches de sécurité, composé de 75 éléments, qui examine en profondeur la capacité d'une organisation à se préparer, à se défendre et à intervenir en cas d'incident ou de crise, et ensuite apprendre à s'améliorer pour l'avenir.

Les experts de GoSecure interrogent le personnel et recueillent la documentation disponible pour évaluer les processus, les politiques, les outils et les plans de l'organisation dédiés aux incidents, à la continuité des activités et à la reprise après sinistre. Les clients reçoivent un rapport détaillé indiquant leur niveau et posture de maturité comparativement à un profil cible.

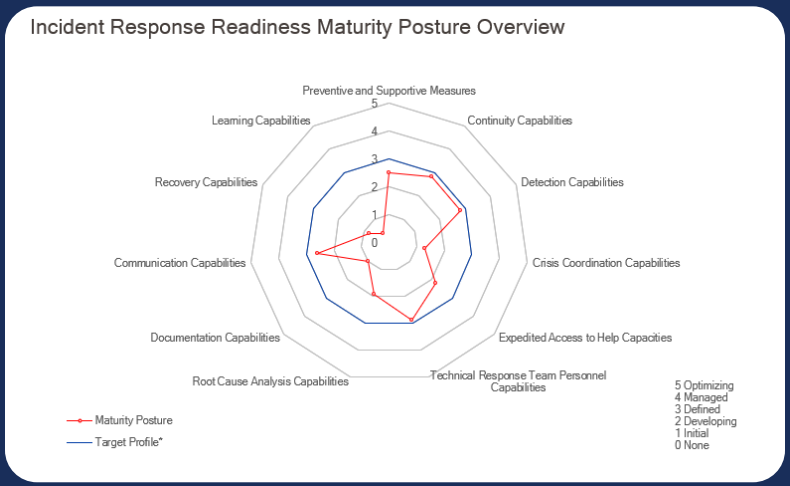
COMPRENDRE LA POSTURE DE MATURITÉ

Les participants au service BRA de GoSecure obtiennent un profil détaillé avec un niveau entre 0 et 5 (aucun à optimisation) pour chacun des 11 concepts critiques. Le Capability Maturity Model Integration (CMMI - intégration de modèle de maturité de la capacité) utilisé pour déterminer le niveau de maturité est reconnu internationalement et est facile à comprendre pour tous les niveaux d'une organisation.

Dans le cadre de l'évaluation, les organisations identifieront une cible pour chaque aspect de leur préparation aux brèches de sécurité.

Cela peut aider les équipes à:

- **Évaluer l'état actuel;**
- **Vérifier si les efforts d'amélioration ont eu un impact;**
- **Plaider en faveur d'une allocation plus importante de ressources dans un secteur qui pourrait être amélioré**



EXERCICE DE SIMULATION DE GOSECURE

La clé pour minimiser, contenir et se rétablir rapidement d'une attaque par rançongiciel ou autre type d'attaque est la préparation. Comment une organisation peut-elle évaluer la capacité de son personnel, de ses procédés, de ses politiques et de ses outils en place lorsqu'elle est soumise à la pression d'un incident majeur réel? Les exercices de simulation de GoSecure permettent d'évaluer les capacités de réponse et de reprise dans un environnement sûr, mais réaliste.

Que sont les exercices de simulation (TTE) de GoSecure?

- Des incidents majeurs ou des crises conçues sur mesure où les participants clés (informatique/sécurité, direction, opérations, RH, marketing, etc.) s'engagent dans des jeux de rôle pour valider la capacité de l'organisation à réagir et à se rétablir, ainsi qu'à tirer des leçons de l'événement.

Qui doit s'engager dans un TTE?

- GoSecure recommande le TTE pour les clients qui ont terminé une évaluation BRA et qui veulent valider les améliorations qui ont été instaurées.
- Les organisations qui souhaitent tester la communication, la collaboration et la prise de décision au sein d'une équipe dans le cadre d'un scénario réel d'incident majeur devraient envisager un TTE.
- De nombreuses organisations doivent effectuer un TTE annuel pour des raisons de conformité ou de cyberassurance.

Comment GoSecure élabore-t-il le TTE?

- Chaque scénario d'incident est personnalisé et adapté selon le secteur d'activité, la localisation, les technologies, le personnel, etc. du client.
- GoSecure recueillera les documents disponibles, tels que le plan d'intervention en cas d'incidents, le plan de continuité des affaires et le plan de reprise après sinistre, et interrogera l'équipe informatique pour déterminer les meilleures faiblesses et failles à exploiter au cours de l'exercice et ainsi mettre les participants au défi.

Quels sont les résultats d'un TTE auxquels une organisation peut s'attendre?

- L'approche de GoSecure comprend des discussions facilitées tout au long de l'exercice et une session de leçons apprises lorsque l'incident théorique est résolu.
- Après la séance, les clients reçoivent un rapport contenant des recommandations d'amélioration, ainsi qu'un compte rendu et un enregistrement de la séance.

GoSecure

APPRENDRE ENCORE PLUS
fr.gosecure.net/breach-readiness-services

CONTACTEZ-NOUS
fr.gosecure.net/sales-contact
1-855-893-5428

À PROPOS DE GOSECURE

GoSecure est un leader et un innovateur reconnu dans le domaine de la cybersécurité, pionniers de l'intégration de la détection des menaces au niveau des points de terminaux, du réseau et de la messagerie dans un service unique de détection et de réponses gérées. La plateforme Titan de GoSecure offre une détection, une prévention et une réponse prédictives multivecteurs pour contrer les cybermenaces d'aujourd'hui. Le service de détection et réponse gérée Titan est conçu pour détecter et répondre en moins de 15 minutes, offrant une réponse rapide et des services d'atténuation active qui touchent directement le réseau et les terminaux des clients. Depuis plus de 10 ans, GoSecure aide ses clients à mieux comprendre leurs lacunes en matière de sécurité et à améliorer leur risque organisationnel et leur maturité en matière de sécurité grâce à des solutions MDR et à des services professionnels fournis par l'une des équipes les plus fiables, compétentes et expérimentées du domaine. Pour en savoir plus, veuillez visiter: https://fr.gosecure.net.