ÉVALUATION PRÉPARATOIRE EN CAS D'INCIDENT DE GOSECURE 2024

[Permet un examen complet des capacités de réponse et prépare les organisations à se défendre contre les attaques]

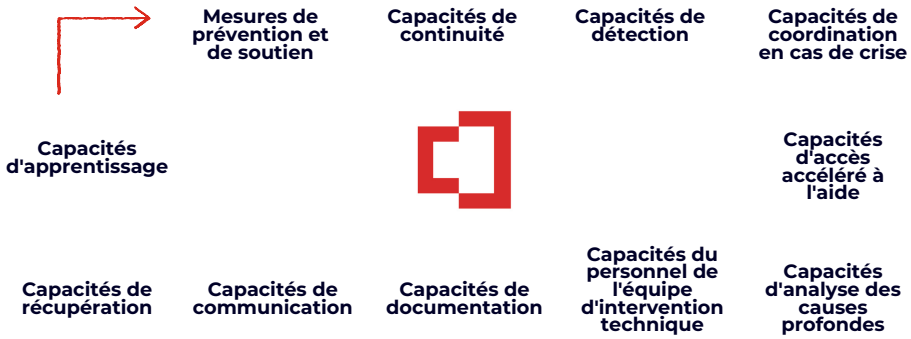
Dans une enquête récente, 81 % des organisations ont déclaré avoir été victimes d'un certain type de brèche de données au cours des 12 mois précédents*. Les organisations sont préoccupées par les menaces croissantes provenant des rançongiciels, des logiciels malveillants, des initiés malveillants et plus encore.

GoSecure propose deux services de préparation à la brèche pour aider les organisations à évaluer leur personnel, leurs processus, leurs politiques et leurs outils positionnés pour répondre en cas d'incident ou de crise majeure.

ÉVALUATION PRÉPARATOIRE EN CAS D'INCIDENT DE GOSECURE

L'évaluation préparatoire en cas d'incident (BRA) de GoSecure offre une évaluation complète de l'état de préparation aux incidents garantissant que les personnes, les processus, les outils, les politiques, les plans, les playbooks et les runbooks sont prêts lorsqu'une brèche se produit.

11 concepts essentiels d'une évaluation préparatoire en cas d'incident de GoSecure



Sur la base de ces concepts essentiels, l'équipe compétente et expérimentée de GoSecure a mis au point un cadre exclusif d'évaluation préparatoire en cas d'incident. Enraciné dans les meilleures pratiques industrielles internationalement reconnues en matière de réponse aux incidents, de gestion de crise et de gestion des infrastructures critiques, ce cadre examine en profondeur la capacité d'une organisation à se préparer, à se défendre et à répondre à un incident ou à une crise - puis à apprendre à s'améliorer pour l'avenir.

Les experts de GoSecure interrogent le personnel et rassemblent la documentation disponible pour évaluer les processus, les politiques, les outils et les plans de l'organisation consacrés aux incidents, à la continuité des activités et à la reprise après sinistre. Les clients reçoivent un rapport détaillé comprenant leur score de maturité par rapport à un profil cible.

3 PILIERS POUR SE PRÉPARER

Les services d'évaluation prépratoire en cas d'incident de GoSecure adoptent une approche holistique pour comprendre l'état de préparation d'une organisation à répondre à un incident.

GoSecure évaluera :

- La continuité des affaires
- Réponse aux incidents
- La reprise après une attaque

Les experts de GoSecure pensent que pour déterminer si une organisation est prête, il faut évaluer l'ensemble du programme de réponse - et toutes les personnes, les processus, les politiques et la technologie impliqués.

GoSecure adopte l'approche des 3 piliers de la préparation car une brèche n'a pas été entièrement traitée tant que l'organisation n'a pas repris ses activités habituelles.

* *Osterman Research Survey Report*

[CONTACTEZ-NOUS : +1 (855) 893-5428]

COMPRENDRE LA POSTURE DE MATURITÉ

Les participants à GoSecure BRA obtiennent un profil détaillé avec des scores pour chacun des 11 concepts critiques sur une échelle de 0 à 5 (de « Aucun » à « Optimisation »). Le modèle CMMI (Capability Maturity Model Integration) utilisé pour la notation est internationalement reconnu et facile à comprendre à tous les niveaux d'une organisation.

Les organisations identifieront un objectif pour chaque aspect de leur préparation à la brèche dans le cadre de l'évaluation.

Cela peut aider les équipes à :

- Évaluer l'état actuel
- Vérifier si les efforts d'amélioration ont eu un impact
- justifier une allocation plus importante de ressources dans un domaine susceptible d'être amélioré.

EXERCICES SUR TABLE DE GOSECURE

La clé pour minimiser, contenir et récupérer rapidement d'une attaque par rançongiciel ou autre est la préparation. Comment une organisation peut-elle évaluer la capacité de son personnel, de ses processus, de ses politiques et de ses outils en place sous la pression d'un incident majeur réel ? Les exercices sur table de GoSecure permettent d'évaluer les capacités de réponse et de récupération dans un environnement sûr mais réaliste.

Que sont les exercices sur table de GoSecure (TTE) ?

- Il s'agit d'incidents ou de crises majeurs conçus sur mesure où les participants clés (IT/Sécurité, direction, opérations, RH, marketing, etc.) s'engagent dans un jeu de rôle pour tester la capacité de l'organisation à réagir et à se rétablir, ainsi qu'à tirer des leçons de l'événement.

Qui devrait participer à un TTE ?

- GoSecure recommande le TTE aux clients qui ont terminé un BRA et qui souhaitent tester les améliorations associées.
- 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 cyber-assurance.

Comment GoSecure conçoit-il le TTE ?

- Chaque scénario d'incident est adapté à l'industrie du client, à la géographie, à la technologie, au personnel, etc. - GoSecure rassemble les documents disponibles tels que le plan de réponse aux incidents, le plan de continuité des activités et le plan de reprise après sinistre. Il interroge également l'équipe informatique afin de déterminer les meilleures faiblesses et failles à exploiter lors de l'exercice et de mettre les participants au défi.

Quels résultats une organisation peut-elle attendre d'un TTE ?

- L'approche de GoSecure comprend des discussions facilitées tout au long de l'exercice et une session sur les leçons à tirer lorsque l'incident théorique est résolu.
- Après la session, les clients reçoivent un rapport contenant des recommandations d'amélioration, ainsi que le procès-verbal et l'enregistrement de la session.

[CONTACTEZ-NOUS : +1 (855) 893-5428]

GoSecure est un leader et un innovateur reconnu en matière de cybersécurité, pionnier de l'intégration de la détection des menaces au niveau des points d'extrémité, du réseau et de la messagerie électronique en un seul service géré de détection et de réponse étendues (MXDR). La plateforme GoSecure TitanMC offre une détection prédictive multi-vectorielle, une prévention et une réponse pour contrer les cybermenaces modernes. GoSecure TitanMC MXDR offre une réponse rapide et des services d'atténuation active qui touchent directement le réseau et les points de terminaison des clients. Depuis plus de 20 ans, GoSecure aide ses clients à mieux comprendre leurs lacunes en matière de sécurité et à améliorer leurs risques organisationnels et leur maturité en matière de sécurité grâce aux solutions MXDR et aux services professionnels fournis par l'une des équipes les plus fiables et les plus compétentes de l'industrie. Pour en savoir plus, visitez le site :

www.gosecure.ai/fr

Votre allié pour consolider, évoluer et prospérer

GoSecure