GoSecure

fr.gosecure.net

GoSecure
APERÇU DES SOLUTIONS

GoSecure

VOTRE CONSEILLER DE CONFIANCE

GoSecure est un leader et un innovateur reconnu en matière de cybersécurité, pionnier dans l'intégration de la détection des menaces au niveau des terminaux, du réseau et de la messagerie dans un seul service de détection et réponse gérées. Depuis plus de 10 ans, GoSecure aide ses clients à mieux comprendre leurs lacunes en matière de sécurité ainsi qu'à améliorer le risque organisationnel et la maturité de la sécurité. Tout ça grâce à des solutions de détection et réponse gérées et à des services conseils fournis par l'une des équipes les plus fiables, compétentes et expérimentées du secteur.

DÉFENDEZ VOTRE ORGANISATION GRÂCE AUX SOLUTIONS DE CYBERSÉCURITÉ DE GOSECURE

Se préparer, identifier et répondre aux menaces de plus en plus sophistiquées que représentent les rançongiciels, l'hameçonnage, l'ingénierie sociale ainsi que toutes autres attaques, constitue un défi quotidien pour les équipes de sécurité. Une atténuation rapide et efficace peut faire la différence entre une journée de travail ordinaire et des dommages catastrophiques pour une organisation. Notre gamme complète de solutions gérées et de solutions logicielles de GoSecure Titan ainsi que les services professionnels spécialisés permet de se protéger contre les risques potentiels, mais également d'en détecter davantage par rapport aux offres traditionnelles. De plus, grâce aux services gérés, les équipes bénéficient du soutien dont elles ont besoin pour atténuer les menaces plus rapidement et pour se rétablir avec un impact sur l'organisation aussi faible que possible.

Le service de détection et de réponses gérées (MDR) de GoSecure Titan offre un temps de réponse de 15 minutes entre la détection et l'atténuation, ce qui permet une action rapide contre les attaques avancées d'aujourd'hui. Les solutions de sécurité gérées de GoSecure Titan associent une technologie de sécurité de pointe à des professionnels hautement qualifiés qui deviennent une extension de l'équipe de sécurité interne, dans l'optique d'atténuer les menaces avant même qu'elles ne puissent compromettre les données sensibles ou les opérations commerciales, ce qui permet de maximiser des ressources précieuses.

Les solutions logicielles de GoSecure Titan permettent de bloquer les menaces afin qu'elles ne parviennent jamais dans l'environnement de l'organisation. La combinaison de la sécurité du courrier électronique avec celle du Web, ainsi que l'analyse en mémoire, offre une protection complète afin de contrer les attaques et arrêter le contenu malveillant avant qu'il n'atteigne les utilisateurs.

GoSecure Titan

Les services professionnels de GoSecure offrent des solutions complètes d'évaluation et de tests de haut niveau pour aider les organisations à évaluer leur posture, leurs risques ainsi que leurs failles en matière de cybersécurité. Les experts de GoSecure peuvent évaluer la capacité d'une organisation à se protéger, se défendre et répondre aux menaces, tout en travaillant de pair avec les ressources internes afin de s'assurer que les améliorations recommandées soient réalisables et pratiques. Les services professionnels de GoSecure fournissent donc des solutions concrètes pour se protéger contre les brèches de sécurité.

GoSecure

GoSecure TITAN

Bénéficiez de l'avantage de la détection et réponse gérées grâce à l'assistance fournie par des chasseurs de menaces qualifiés qui deviennent un prolongement de votre équipe de sécurité interne.

Service de détection et réponse gérées de GoSecure Titan | Faites confiance à votre sécurité

Le service de détection et réponse gérées (MDR) de GoSecure Titan identifie, bloque et signale les brèches de sécurité potentielles. Ce service est accompagné des chasseurs de menaces expérimentés du centre de réponse avancée (ARC) de GoSecure qui réagissent rapidement afin d'aider à remédier aux problèmes, mais également à les résoudre. Avec un temps de réponse de 15 minutes entre la détection et l'atténuation, ce service est l'un des meilleurs de sa catégorie.

- Des offres groupées et flexibles fournissent aux organisations la couverture dont elles ont besoin pour se défendre contre les intrusions. De plus, celles-ci garantissent le soutien de professionnels expérimentés de la sécurité qui deviennent un prolongement de l'équipe de sécurité interne.
- Le portail MDR de GoSecure Titan centralise les données sur la santé de la sécurité des clients, fournissant des tableaux et des graphiques faciles à comprendre concernant les données relatives au réseau, aux terminaux et aux événements, ainsi que des rapports et des billets centralisés dans une seule interface.

« La tranquillité d'esprit que m'apporte la grande visibilité et le contrôle m'aident à mieux dormir la nuit, sans oublier, la certitude que nos 6 500 systèmes sont sécurisés. » - Benjamin Corll, Vice-Président de la cybersécurité et de la protection des données/Directeur de la sécurité informatique chez Coats Group, PLC.

Détection et réponse pour les terminaux de GoSecure Titan | Protégez vos terminaux

Les terminaux constituent un point d'exposition en constante augmentation pour les organisations et peuvent être compromis en tout temps soit 24 heures sur 24, 7 jours sur 7, et ce, 365 jours par année. **Les outils de détection et réponse sur les terminaux (EDR) de GoSecure Titan** automatisent les activités de surveillance et d'atténuation pour bloquer les menaces avant qu'elles ne se propagent. Lorsqu'ils sont combinés aux services MDR de GoSecure Titan, vous bénéficiez du soutien d'analystes experts qui traitent les menaces potentielles comme un prolongement de l'équipe de sécurité interne.

- Cette solution automatise l'identification et le confinement des activités suspectes, tout en bloquant les menaces potentiellement malveillantes telles que les attaques par des logiciels malveillants sans fichier, et offre une visibilité sur les terminaux pour la collecte et l'analyse des données.
- Permet de supprimer ou de bloquer les menaces potentielles dès les premiers stades d'une attaque, grâce à des outils d'analyse et d'investigation qui prédisent la nature de la menace et aident à identifier les causes sous-jacentes.

Le service de détection et réponse sur les boîtes de messagerie de GoSecure Titan | Protection des boîtes de messagerie

Le service de détection et réponse sur les boîtes de messagerie (IDR) de GoSecure Titan est une solution en un simple clic, permettant aux utilisateurs d'envoyer tout courriel suspect en vue d'une évaluation et d'une réponse professionnelles, ce qui permet aux organisations d'économiser en temps et en ressources, tout en se protégeant contre les intrusions.

- Se déploie facilement dans la boîte de réception des ordinateurs de bureau, des sites Web et des téléphones mobiles d'Office 365, ce qui simplifie le processus de soumission des courriels suspects, tout en offrant une expérience utilisateur transparente avec une assistance 24/7 et une analyse des soumissions par les experts de GoSecure.
- Combine l'analyse automatisée et l'analyse humaine qualifiée des experts de GoSecure lors de l'examen des propositions, et renvoie un statut facilement compréhensible, généralement quelques minutes après la proposition.
- Offre une réponse immédiate aux incidents liés aux menaces, y compris la suppression globale de messages veillants.

Détection et réponse des menaces internes de GoSecure Titan | Dissuader les menaces internes

Les menaces émergent de plus en plus d'une activité accidentelle, négligente ou malveillante au sein des organisations où les défenses traditionnelles de cybersécurité ne sont pas préparées à les combattre. **La détection et réponse des menaces internes (ITDR) de GoSecure Titan** peut contribuer à surveiller, détecter, dissuader et répondre à ces menaces souvent négligées.

- L'ITDR de GoSecure Titan permet aux organisations de définir des politiques les protégeant contre l'exposition accidentelle, tout en surveillant les comportements suspects, le tout, en identifiant les menaces pour une enquête plus approfondie et en recueillant des preuves légales si nécessaire.
- Plus de 50 ensembles de règles peuvent être déployés sur les terminaux afin de gérer l'accès, déclencher des alertes, limiter automatiquement l'accès et veiller à ce que des mesures soient prises rapidement lorsqu'une menace est détectée.

Antivirus de nouvelle génération de GoSecure Titan | Arrêter les brèches de sécurité

L'antivirus de nouvelle génération (NGAV) de GoSecure Titan transcende les outils traditionnels pour aider à protéger les organisations contre les menaces modernes telles que les rançongiciels et les attaques sans fichier. Soutenu par les chasseurs de menaces expérimentés de GoSecure, le centre de réponse avancée (ARC) surveille et bloque les brèches de sécurité potentielles dans les navigateurs, la messagerie, les lecteurs de documents, etc. Le ARC analyse également la mémoire à la recherche d'activités malveillantes telles que les attaques sans fichier, en signalant les activités en fonction des règles définies par l'organisation.

- Une surveillance automatisée continue et une assistance gérée 24 heures sur 24 et 7 jours sur 7 assurent une protection continue des organisations. Le centre de réponse avancée (ARC) de GoSecure détermine la gravité des menaces identifiées et réagit en conséquence pour contenir, atténuer et résoudre les problèmes, souvent avant même que l'organisation ne se rende compte de l'existence d'un problème.
- S'intègre de manière fluide aux technologies et systèmes d'exploitation existants, tels que Windows, Mac et Linux, et ce, sans altérer les performances.

« Lorsque j'ai posé des questions concernant la machine potentiellement infectée, GoSecure m'a répondu : « Nous avons préféré vous protéger en priorité, avant même de vous dire que vous aviez un problème ». C'est cet événement spécifique qui nous a fait signer dès le lendemain. » - Scott Howell, Directeur général des services technologiques et informatiques chez McInnes Cooper.

Détection et réponse sur les réseaux de GoSecure Titan | Protégez vos réseaux

Obtenir une visibilité sur les réseaux infonuagiques (cloud), virtuels et sur site est essentiel pour se défendre contre les intrusions, mais nécessite des ressources importantes, notamment pour répondre aux alertes correspondantes et enquêter sur les menaces potentielles. **La détection et réponse sur les réseaux de GoSecure Titan (NDR)** offre une visibilité complète du réseau ainsi que l'assistance des analystes qualifiés de GoSecure afin d'aider à se protéger contre les menaces.

- Centralise la surveillance et la production de rapports sur les activités du réseau, y compris les catégories de menaces, la cartographie des événements et les adresses IP d'origine et de destination, afin de bloquer les brèches de sécurité avant que celles-ci ne se propagent.
- Offre une analyse automatisée à partir du système de détection des intrusions dans les journaux, ainsi qu'une chasse aux menaces grâce à une analyse comportementale en temps réel du système de détection d'intrusion réseau (NIDS), qui combine des renseignements sur les menaces provenant de tiers avec un ensemble de normes développées par GoSecure.

GoSecure Titan SOLUTIONS DE SÉCURITÉ GÉRÉES

Gestion des pare-feu de GoSecure Titan | Optimisez votre périmètre

Le **service de gestion des pare-feu de GoSecure Titan** aide les organisations à relever le défi de la surveillance et de la gestion de leur infrastructure de pare-feu. Le centre de réponse avancée (ARC) de GoSecure offre une couverture mondiale pour les pare-feu fonctionnant de manière optimale 24 heures sur 24, 7 jours sur 7, 365 jours par an.

- La gestion des pare-feu de GoSecure prend en charge les principaux fournisseurs de l'industrie avec une surveillance complète 24 heures sur 24 et 7 jours sur 7 de tous les systèmes pour les problèmes de performance et/ou de disponibilité.
- La gestion des incidents, des changements et des urgences est prise en charge par les professionnels qualifiés du ARC de GoSecure, ce qui permet de décharger les équipes de sécurité internes et de garantir que les environnements de toute taille sont maintenus à un niveau d'efficacité optimal, mais également que les problèmes sont traités rapidement.

Les systèmes de gestion des informations et des événements de sécurité (SIEM) de GoSecure Titan | Améliorer la réponse aux alertes

Les systèmes de gestion des informations et des événements (SIEM) de GoSecure Titan offrent un soutien aux organisations qui souhaitent bénéficier de la collecte et de l'analyse des données de sécurité dans un emplacement central, mais qui ne disposent pas nécessairement des ressources requises pour traiter chaque alerte. Deux forfaits offrent des options de support flexibles pour les organisations en fonction de leurs besoins, de leur budget et de leur modèle commercial.

- **La gestion SIEM Essentials de GoSecure Titan** offre une formule de base pour la maintenance, la révision annuelle du service, la production régulière de rapport, une console en libre-service, ainsi qu'un support sur la demande de la solution gérée.
- **La gestion SIEM Entreprise de GoSecure Titan** s'appuie sur le forfait Essentials avec une surveillance après les heures de travail pour les cas d'utilisation à haut risque, des demandes de changement régulières, des examens de sécurité mensuels et un « runbook » client personnalisé qui détermine les actions qui seront prises par l'équipe de GoSecure afin de soutenir l'équipe de sécurité interne.

Gestion des vulnérabilités en tant que service de GoSecure Titan | Maintenez vos défenses

La **gestion des vulnérabilités en tant que service (VMaaS) de GoSecure Titan** aide les organisations à se défendre contre le paysage des menaces en constante évolution en maintenant les systèmes d'exploitation et les applications à jour et en conformité. L'assistance des experts de GoSecure est disponible 24 heures sur 24, combinée à des outils d'analyse, de déploiement et de balayage qui permettent aux équipes de sécurité de gagner du temps et d'améliorer la posture de sécurité.

- La solution VMaas de GoSecure est conçue pour identifier les actifs et l'exposition grâce à un balayage, pour hiérarchiser les menaces à l'aide d'une analyse contextuelle et pour répondre aux problèmes en mettant à jour les systèmes et les applications.
- Les experts de GoSecure gèrent le processus d'application des correctifs pour les systèmes d'exploitation et les applications, offrent des rapports de conformité complets et développent des pratiques de remédiation basées sur les besoins ainsi que sur de la sécurité de l'organisation, améliorant de ce fait la posture de sécurité et offrant un retour sur investissement immédiat.

GoSecure Titan SOLUTIONS LOGICIELLES

Passerelle de messagerie sécurisée de GoSecure Titan | Bloquez les attaques par courrier

La **passerelle de messagerie sécurisée de GoSecure Titan** offre une protection contre les menaces par courrier électronique générée par les virus, les pourriels ainsi que les rançongiciels. Elle offre également une protection contre les menaces d'origine sociale, notamment l'hameçonnage, la compromission de courriers professionnels et la prise de contrôle des comptes.

- Une solution hébergée qui peut être mise à disposition immédiatement, sans avoir à installer de matériel ou de logiciel.
- Technologie robuste et dynamique de filtrage de l'hameçonnage et de pourriel (« spam »), combinée aux technologies de protection avancée contre les logiciels malveillants et l'échantillonnage de logiciels malveillants afin d'identifier et de bloquer rapidement et efficacement les attaques avant qu'elles n'atteignent l'utilisateur.

Passerelle web sécurisée GoSecure Titan | Bloquer les menaces issues du Web

La **passerelle web sécurisée GoSecure Titan** fournit une défense en temps réel contre les logiciels malveillants ainsi qu'une classification des URLs en utilisant une combinaison de renseignements automatisés et humains sur les menaces, soutenues par GoSecure Titan Labs.

- Des fonctions de contrôle puissantes et une défense contre les logiciels malveillants en temps réel permettent de se défendre contre l'exposition aux réseaux zombies (« botnets »), aux virus, aux logiciels malveillants et autres.
- Des rapports complets ainsi qu'une surveillance en temps réel facilitent la gestion, avec une productivité accrue des utilisateurs, une faible latence et des taux de faux positifs réduits.

Responder PRO de GoSecure Titan | Enquêter sur les menaces

Responder PRO de GoSecure Titan offre des capacités d'analyse d'investigation (« forensics ») de la mémoire et d'analyse comportementale. Responder PRO de GoSecure Titan passe au travers du large éventail de mesures anti-forensic employées par les cybercriminels d'aujourd'hui afin de découvrir des artefacts essentiels pour la réponse aux incidents et la chasse aux menaces.

- Exploite le moteur comportemental propriétaire, l'ADN numérique « Digital DNA », afin de développer un système de notation de l'impact qui facilite l'analyse de logiciels malveillants et aide à identifier d'autres indicateurs de menace.
- Recherche et identifie les artefacts numériques essentiels tels que les mots de passe, les clés de cryptage, les historiques de recherche sur Internet ainsi que d'autres données d'investigation (« forensic ») situées dans la mémoire, et établit des rapports à leur sujet.
- L'interface intuitive s'intègre en douceur aux outils et processus existants pour rationaliser votre flux de travail d'investigation et produire des résultats rapides

GoSecure SERVICES PROFESSIONNELS

Améliorez la maturité en matière de cybersécurité, élevez la posture de sécurité, répondez et réglez les problèmes plus efficacement.

Services de GoSecure liés à la préparation en cas de brèches de sécurité | Faites face aux cyberattaques

Les services de GoSecure de préparation face aux brèches de sécurité testent et perfectionnent les capacités de réponse aux incidents des organisations et les aident à se défendre contre les cyberattaques.

- **L'évaluation de la préparation en cas de brèches de sécurité (BRA) de GoSecure** offre une évaluation complète du niveau de préparation aux incidents, que ce soit au niveau de la continuité des affaires, de la réponse aux incidents ou de la reprise après sinistre. L'objectif est de veiller à ce que les personnes, les processus, les outils et les politiques soient prêts et utilisables en cas de brèche de sécurité.
- **Les exercices de simulation de GoSecure** sont des exercices faits sur mesure et réalistes qui testent les outils, les processus, les politiques et les personnes en mettant l'accent sur la résolution de problèmes en groupe, dans une situation sous pression. Les communications, la documentation et l'engagement interfonctionnel sont également évalués tout au long de la simulation.

Évaluation de la cybersécurité de GoSecure | Déterminez votre niveau de maturité

Obtener une compréhension complète des risques et des écarts dans votre posture de sécurité grâce à l' **évaluation de cybersécurité de GoSecure (CSA)**. Le CSA fournit des informations précises et pertinentes sur votre maturité en matière de cybersécurité et formule des recommandations prioritaires adaptées en fonction de votre contexte d'affaires et de celui d'organisations de taille, de type et de secteur d'activité similaires. Choisissez entre nos deux formules.

- **Le CSA Enterprise** comprend plusieurs phases qui évaluent les aspects critiques de votre technologie, de vos environnements, de vos politiques et de vos procédures, dans le but d'apporter des améliorations globales en matière de sécurité.
- **Le CSA Essentials** est une évaluation plus rationalisée et simplifiée qui permet de cibler les informations les plus importantes, conçues de manière à élaborer une feuille de route et des améliorations en matière de sécurité qui traitent des risques les plus exploités selon un secteur donné.

Services de piratage éthique de GoSecure | Testez vos défenses

Faites confiance aux **tests d'intrusion de GoSecure** pour vous aider à identifier l'impact que des attaquants puissent avoir sur votre organisation. L'équipe de GoSecure certifiée Offensive Security Certified Professional (OSCP) travaille avec ses clients afin de cibler leurs besoins en matière de sécurité selon leur modèle de menace, leur industrie ainsi que leurs infrastructures technologiques.

- GoSecure fournit des programmes qui identifieront où et comment les adversaires peuvent cibler une organisation, y compris les réseaux externes, internes et sans fil, les applications Web, les applications et les appareils mobiles, les terminaux et les attaques d'ingénierie sociale telles que l'hameçonnage ou l'intrusion physique.
- GoSecure peut également effectuer une revue de la sécurité du code source d'applications, ainsi que des tests d'appareils industriels /embarqués /IOT /SCADA.

Services de réponse aux incidents de GoSecure | Mieux répondre et vous rétablir plus rapidement

Une organisation peut être victime d'une cyberattaque à tout moment. Les programmes de réponse aux incidents de GoSecure préparent les organisations à contenir et résoudre les brèches de sécurité, tout en les aidant à se rétablir plus rapidement; l'objectif étant de minimiser l'impact opérationnel, financier et réputationnel. GoSecure propose à la fois des programmes de réponse aux incidents sous contrat provisionnel et des services de réponse aux incidents d'urgence. Ces services comprennent des conseils en matière de reprise des affaires et la surveillance du Dark Web par notre équipe de chasseurs de menace (threat hunters).

Services stratégiques de GoSecure Red & Purple Team | Améliorez vos défenses

Les services stratégiques « Red & Purple Team » peuvent contribuer à améliorer la posture de sécurité, à renforcer les défenses de cybersécurité et à mieux préparer votre équipe de sécurité interne pour qu'elle soit prête à répondre aux attaques réelles.

- Les mandats stratégiques **« Red Team »** combinent plusieurs techniques d'attaque disponibles et effectuées par des professionnels de la sécurité expérimentés afin de tester les capacités internes d'une organisation.
- Les mandats stratégiques **« Purple Team »** adoptent une approche consistant à 'tester, remédier, tester à nouveau et répéter' pour améliorer rapidement la posture de sécurité des organisations, et ce, grâce à un engagement à long terme, en collaboration avec les équipes internes.

Services de confidentialité et de conformité de GoSecure | Protégez les données confidentielles

GoSecure aide régulièrement les organisations de tous types à comprendre, adopter et maintenir des cadres et des normes de conformité, tout en les soutenant et les accompagnant dans la protection de leurs données confidentielles.

- Les experts de **GoSecure en services de confidentialité** s'assurent d'appliquer les normes de confidentialité reconnues mondialement afin d'offrir des solutions complètes pour garantir la sécurité des informations personnelles et veiller à ce que les organisations soient préparées à se protéger contre les brèches de données.
- Les services de **GoSecure concernant la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)** sont disponibles pour les organisations qui ont besoin d'aide avec leur questionnaire d'auto-évaluation (SAQ). Au Canada, GoSecure est un évaluateur de sécurité qualifié (QSA) qui peut compléter et signer un rapport de conformité (ROC).

Évaluation de la compromission de la sécurité (SCA) de GoSecure | Identifiez les menaces

Le **service d'évaluation de la compromission de la sécurité (SCA) de GoSecure** peut vous aider à identifier les menaces cachées que l'automatisation seule ne peut pas détecter. Le SCA offre 60 jours de notre service de plateforme Titan de détection et réponse gérées (MDR) et suit une approche de type hybride qui combine des balayages de logiciels malveillants automatisés et une chasse à la menace active. Cette combinaison offre un avantage par rapport à la simple automatisation qui peut repérer les menaces susceptibles d'atteindre et d'affecter les données sensibles et qui pourraient potentiellement compromettre les opérations actuelles ou futures de votre organisation. Le SCA inclura également une analyse du trafic réseau, les résultats de la détection et réponse sur les terminaux, et plus encore.

GoSecure

Coordonnées

Tel: 855-893-5428
Urgence 24/7: 888-287-5858

sales@gosecure.net

fr.gosecure.net