www.gosecure.ai/fr/

GoSecure

VUE D'ENSEMBLE DES SERVICES

GoSecure

GoSecure est un leader et un innovateur reconnu en matière de cybersécurité, pionnier de l'intégration de la détection des menaces au niveau des terminaux, 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 cyber-menaces modernes. MXDR GoSecure TitanMC offre un temps de réponse optimal de la détection des menaces à l'atténuation, offrant une réponse rapide et des services d'atténuation active qui touchent directement le réseau et les terminaux 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.

VOTRE ALLIÉ DE CONFIANCE

DÉFENDEZ VOTRE ORGANISATION AVEC LES SERVICES DE CYBERSÉCURITÉ DE **GOSECURE**

Les équipes de sécurité sont confrontées au défi de se préparer, d'identifier et de répondre aux menaces de plus en plus sophistiquées posées par les rançongiciels, le hameçonnage, l'ingénierie sociale et d'autres cyberattaques. Des mesures d'atténuation rapides et efficaces peuvent faire la différence entre un jour comme les autres au bureau et des dommages catastrophiques durables pour votre organisation. La protection contre l'accélération des cybermenaces nécessite une approche de sécurité à plusieurs niveaux.

C'est pourquoi nous avons constitué un portefeuille d'offres complémentaires. Lorsque chacun de nos trois piliers, la **détection et réponse gérées et étendues GoSecure TitanMC**, **Plateforme GoSecure TitanMC** et **services de sécurité professionnels de GoSecure** sont inclus dans une approche globale de la cybersécurité, la valeur et l'efficacité des solutions sont amplifiées et les résultats sont perceptibles.

La pierre angulaire de la **détection et réponse gérées et étendues GoSecure TitanMC** est sa protection éprouvée et la réponse rapide fournies par ses composantes de services.

Avec un temps de réponse de la détection à l'atténuation parmi les meilleurs du marché, vous serez prêt pour les attaques avancées et disposerez d'options d'assistance gérées par les chasseurs de menaces expérimentés de l'équipe GoSecure.

Ses services s'étendent à notre support géré par des experts pour aider avec des activités de sécurité importantes comme les pare-feu, la gestion des vulnérabilités et la **Surveillance des événements liés aux informations de sécurité gérée GoSecure TitanMC.**

Grâce à des alertes précoces, la **Plateforme GoSecure TitanMC** bloque de nombreuses attaques avant qu'elles n'aient un impact sur une organisation. La Plateforme GoSecure TitanMC est plus qu'une plateforme MXDR, plus qu'une plateforme d'opérations de sécurité. C'est une plateforme unique qui peut équilibrer la consolidation, la transparence et l'actionnabilité, permettant aux professionnels de la cybersécurité de toute votre organisation de rester au-dessus du lot, de contrôler, d'agir et de prospérer.

Grâce aux **Services de sécurité professionnels GoSecure**, votre organisation peut tester, évaluer et améliorer sa position de sécurité. Identifiez les risques et les lacunes, optimisez vos outils de sécurité, testez votre personnel, vos processus et votre technologie - obtenez une vue d'ensemble ou concentrez-vous sur un domaine de préoccupation spécifique. GoSecure aide votre organisation à apprendre et à se développer avec chaque engagement.

DÉTECTION ET RÉPONSE GÉRÉES ET ÉTENDUES (MXDR)

GoSecure TITAN

[Détecter et atténuer plus rapidement]

Les organisations cherchent à mieux connaître l'état de leur infrastructure et les événements liés à leurs technologies, et les professionnels de la sécurité partagent une même préoccupation : protéger leur organisation contre les attaques.

Construite sur une architecture XDR ouverte, notre solution MXDR est conçue pour soutenir les investissements existants en permettant le choix des différents éléments de la configuration et pour aider votre organisation dans ses efforts de consolidation.

MXDR GoSecure TitanMC identifie, bloque et signale les brèches potentielles, souvent avant même que l'organisation ne se rende compte qu'il y a un problème - soutenu par les chasseurs de menaces expérimentés du Centre des opérations de sécurité (SOC) qui réagissent rapidement pour aider à remédier aux problèmes avec un temps de réponse le plus rapide de sa catégorie, entre la détection et l'atténuation.

MXDR GoSecure TitanMC offre :

- Protection contre les menaces avancées
- La possibilité d'en faire plus avec vos investissements
- Des humains au service de l'entreprise
- Une base à laquelle vous pouvez faire confiance et sur laquelle vous pouvez vous appuyer

GoSecure TITAN

DÉTECTION ET RÉPONSE SUR LES TERMINAUX GOSECURE TITAN (EDR)

[Défendez vos terminaux]

La solution EDR GoSecure TitanMC combine une visibilité de pointe avec une analyse multi-observationnelle pour détecter les menaces plus efficacement et réagir plus rapidement.

Alors que les antivirus traditionnels ont réussi à stopper les attaques connues, les adversaires utilisent désormais de nouvelles techniques pour contourner ces défenses. Avec l'obscurcissement, le chiffrement et les logiciels malveillants sans fichier qui opèrent en mémoire, ces menaces échappent aux technologies de sécurité traditionnelles.

Notre solution agit comme un bouclier unifié, offrant une défense multicouche qui détecte non seulement les vulnérabilités connues, mais identifie également de manière préventive les menaces émergentes et les atténue avant qu'elles ne causent des dommages.

La **détection et réponse sur les terminaux GoSecure TitanMC** offre :

- Détection en mémoire
- Analyse prédictive
- Atténuation automatique
- Réactivité

GESTION DES VULNÉRABILITÉS EN TANT QUE SERVICE GOSECURE TITAN (VMAAS)

[Entretenez vos défenses]

Avec 60 % des brèches impliquant des vulnérabilités connues non corrigées, VMaaS GoSecure TitanMC est conçu pour identifier les actifs et l'exposition grâce à l'analyse, hiérarchiser les menaces à l'aide de l'analyse contextuelle et réagir en mettant à jour les systèmes et les applications pour renforcer la résistance aux attaques, raccourcir les délais de remédiation et maintenir la conformité.

De nombreuses organisations manquent de ressources, de temps et d'expertise pour gérer efficacement les vulnérabilités et passent souvent leur temps à patcher les mauvaises vulnérabilités.

Le service VMaaS GoSecure TitanMC associe une technologie de pointe à une analyse experte pour offrir une rapidité, une précision, une cohérence et une fiabilité inégalées au programme de gestion des vulnérabilités personnalisé de l'entreprise, ce qui la rend plus sûre tout en lui faisant gagner du temps et de l'argent.

VMaaS GoSecure TitanMC c'est :

- Un gain de temps opérationnel
- Une réduction proactive des cyberrisques
- Un retour sur investissement immédiat
- De la visibilité, des rapports et des mesures en temps réel
- Un maintien de la conformité

SURVEILLANCE DES ÉVÉNEMENTS LIÉS AUX INFORMATIONS DE SÉCURITÉ GÉRÉE GOSECURE TITAN (SIEM)

[Améliorer la réponse aux alertes]

Le SIEM géré GoSecure TitanMC se concentre sur l'éradication des comportements malveillants et la limitation de la fatigue des alertes. Il offre une intelligence de sécurité avancée, un traitement complet des incidents, une conformité simplifiée, une évolutivité, une intégration des renseignements sur les menaces et des opérations de sécurité optimisées. Grâce à notre solution de pointe, nous permettons aux organisations de protéger activement leurs actifs précieux et de maintenir une posture de sécurité solide face à l'évolution des cybermenaces.

GoSecure combine les meilleurs outils de sa catégorie avec des renseignements exclusifs sur les menaces, élaborés au fil de nombreuses années d'expérience opérationnelle, afin d'aider les clients à façonner une plateforme qui leur fournit les renseignements dont ils ont besoin, avec moins de faux positifs.

SIEM géré GoSecure TitanMC c'est :

- Un traitement des incidents en temps réel
- Une visibilité complète
- Un soutien à la conformité et à la réglementation
- Personnalisable et évolutif
- Une protection complète

DÉFENSE DU PÉRIMÈTRE GÉRÉE GOSECURE TITAN (MPD)

[Optimisez votre périmètre]

La surveillance et la gestion continues de vos défenses périmétriques constituent la première ligne de défense du réseau de toute organisation.

Les responsables de la sécurité des réseaux y consacrent plus de temps qu'à toute autre activité. Et il est facile de se tromper, en particulier pour les administrateurs informatiques qui font double emploi avec le personnel de sécurité informatique de leur organisation.

L'équipe de sécurité réseau de GoSecure fournit l'expertise nécessaire pour identifier et mettre en œuvre de meilleurs contrôles du périmètre, garantissant que les systèmes tournés vers l'extérieur sont protégés.

La **défense du périmètre gérée GoSecure TitanMC** offre :

- Une meilleure sécurité 24x7
- Une maintenance plus facile
- Un déploiement plus rapide
- Des dépenses réduites

GoSecure TITAN

DÉTECTION ET RÉPONSE DES BOÎTES DE MESSAGERIE GOSECURE TITAN (IDR)

[Protégez votre boîte de réception]

Les employés font désormais partie de la solution, et non du problème. Les équipes de sécurité sont débordées par l'un des principaux vecteurs de menace dans le contexte actuel : le hameçonnage.

Les enquêtes sur les courriels suspects menées par les filtres de sécurité automatisés et l'examen des soumissions des employés consomment du temps et des ressources que certaines équipes n'ont pas à leur disposition. La plupart des organisations continuent de proposer des formations de sensibilisation aux employés et d'affiner les programmes de sécurité de la messagerie, mais n'ont pas été en mesure d'empêcher les menaces opportunistes et ciblées par le biais de la messagerie de se transformer en brèches de sécurité potentielles.

IDR GoSecure TitanMC permet à chaque utilisateur de tester tout courriel suspect. Ils peuvent enfin cesser de s'inquiéter de manquer des menaces, de perdre du temps à se demander ce qu'il faut faire ou de s'inquiéter de crier au loup trop souvent. D'un simple clic, les employés deviennent désormais une force unie contre le hameçonnage.

IDR GoSecure TitanMC c'est :

- Une défense contre le hameçonnage et les logiciels malveillants
- Intégration et facilité de la boîte de réception
- Compatibilité avec Office 365
- Contrôle d'équipe personnalisable

PASSERELLE DE MESSAGERIE SÉCURISÉE GOSECURE TITAN (SEG)

[Optimisez votre périmètre]

La passerelle de messagerie sécurisée GoSecure TitanMC (SEG) protège les entreprises contre les diverses menaces liées à la messagerie électronique tout en renforçant la sécurité des communications électroniques.

Fonctionnant comme un filtre entre le trafic de messagerie interne et externe, elle empêche les courriels malveillants ou indésirables d'atteindre les boîtes de réception des destinataires.

Le SEG garantit la sécurité, l'intégrité et la confidentialité des communications par courrier électronique, jouant ainsi un rôle essentiel dans la protection contre les menaces susceptibles de compromettre la sécurité des données, de nuire à la réputation ou d'entraîner des pertes financières.

Partie intégrante de la stratégie de cybersécurité d'une organisation, les passerelles de messagerie sécurisée complètent des solutions telles que la détection et la réponse au niveau du terminal (EDR), les systèmes de détection d'intrusion, les pare-feux et les logiciels antivirus.

SEG GoSecure TitanMC offre :

- Une sécurité renforcée de la messagerie
- Des capacités de filtrage
- Protection des données

IDENTITY GOSECURE TITAN

[Contrôlez vos opérations]

Conçu pour générer des alertes basées sur des techniques offensives spécifiques du monde réel, Identity GoSecure TitanMC est une suite de technologies qui fournit des détections et des alertes en tant que service.

Les organisations utilisent Identity GoSecure TitanMC pour fournir des alertes de haute qualité (peu de faux négatifs et de faux positifs) à leur personnel opérationnel interne sans avoir besoin de construire et de maintenir des analyses complexes basées sur la science des données. Ses détections sont classées selon la technique MITRE ATT&CK, ce qui facilite le déclenchement de procédures de réponse/runbooks au sein du centre d'opérations du client.

Il est optimisé pour détecter les attaques les plus critiques liées à l'identité, ce qui lui confère une grande valeur en termes de sécurité.

En mettant en œuvre **Identity GoSecure TitanMC**, les organisations vont :

- Amélioreront leur capacité à détecter les menaces
- Réagir rapidement aux menaces liées à l'identité
- Réduire le risque de brèches de données, d'accès non autorisés et d'autres incidents de sécurité pouvant découler d'identités d'utilisateurs compromises.

MODÉLISATEUR DE MENACES GOSECURE TITAN

[Atténuer les menaces]

Le modélisateur de menaces GoSecure TitanMC est un outil sophistiqué qui fusionne la modélisation traditionnelle des menaces et MITRE ATT&CK, offrant une vue holistique du contexte des menaces d'une organisation.

Cette intégration va au-delà de la simple identification des lacunes de contrôle ; elle évalue la maturité du programme de sécurité en incorporant les résultats de l'évaluation de la sécurité, en contextualisant les contrôles de sécurité sur la base des menaces identifiées.

En mettant en correspondance les contrôles techniques avec les techniques MITRE ATT&CK, l'outil donne la priorité à l'élimination des menaces et renforce la sécurité. Il évalue également la maturité du programme en intégrant les évaluations de sécurité et en alignant les contrôles sur les technologies déployées et les menaces connues, garantissant ainsi des défenses ciblées et efficaces.

Modélisateur de menaces GoSecure TitanMC offre :

- Une représentation complète du contexte des menaces
- Des informations sur la couverture des contrôles
- Évaluation de la confiance et de la maturité du programme de sécurité
- Des scores significatifs et des contrôles contextualisés

PLATEFORME

GoSecure TITAN

[Au-delà d'une plateforme opérationnelle : un écosystème de sécurité complet]

La plateforme GoSecure TitanMC consolide les données de sécurité critiques, offre une visibilité inégalée et fournit une protection éprouvée avec des vues personnalisées.

Grâce à des alertes précoces, la plateforme GoSecure TitanMC bloque de nombreuses attaques avant qu'elles n'aient un impact sur l'organisation. En combinaison avec la fondation de détection et réponse gérées et étendues GoSecure TitanMC (MXDR), les organisations cherchent à mieux connaître l'état de leur infrastructure et les événements liés à leurs technologies, et les professionnels de la sécurité partagent une même préoccupation : protéger leur organisation contre les attaques.

GoSecure TitanMC est plus qu'une plateforme MXDR, plus qu'une plateforme d'opérations de sécurité. C'est une plateforme unique qui peut équilibrer la consolidation, la transparence et l'actionnabilité, permettant aux professionnels de la cybersécurité de l'ensemble de votre organisation de rester au-dessus du lot, d'avoir le contrôle, d'agir et de prospérer.

La plateforme GoSecure TitanMC c'est :

- Votre centre de sécurité centralisé
- Simple et évolutive
- Reprendre le contrôle
- Rester au-dessus du lot

SERVICES DE SÉCURITÉ PROFESSIONNELS

SERVICES DE RÉPONSE AUX INCIDENTS DE GOSECURE

[Répondre et récupérer plus rapidement]

Une cyberattaque peut survenir à tout moment dans une organisation. Les programmes de réponse aux incidents de GoSecure préparent les organisations à contenir, résoudre et récupérer des brèches plus rapidement, en minimisant l'impact opérationnel, financier et sur la réputation. GoSecure offre à la fois des programmes de rétention et des services de réponse aux incidents d'urgence basés sur le NIST SP 800-61r2 et les meilleures pratiques de SANS.

- **Service de retenue de la réponse aux incidents (IRR)** - Lorsqu'une brèche se produit, les organisations ayant un Service de retenue de la réponse aux incidents GoSecure en place ont un accès prioritaire à des professionnels expérimentés pour aider à contenir et à résoudre rapidement le problème. Les clients IRR bénéficient d'une équipe qui connaît déjà les systèmes, les processus et les personnes de votre organisation grâce à la feuille de route de réponse élaborée au cours du processus d'intégration.
- **Analyses digitales de type forensics et la réponse aux incidents (DF&IR)** - Composés d'experts en sécurité ayant des années d'expérience en matière de réponse et d'investigation, ils aident à minimiser l'exposition et facilitent l'atténuation et le nettoyage rapides. Que vous ayez besoin d'une enquête complète ou simplement d'une autre paire d'yeux, GoSecure peut répondre à vos besoins avec un Service d'analyses digitales de type forensics et la réponse aux incidents (DF&IR).

ÉVALUATION DE LA MATURITÉ DE LA SÉCURITÉ DE GOSECURE (SMA)

[Comprendre et améliorer votre posture de sécurité]

Obtenez une compréhension complète de la posture de sécurité, des risques et des lacunes avec une Évaluation de la maturité de la sécurité GoSecure - fournissant des informations exploitables sur la posture de cybersécurité et fournissant des recommandations pratiques basées sur la taille de votre organisation, l'industrie, etc.

- **Améliorer votre stratégie d'information** - Si vous avez une stratégie de sécurité de l'information existante, votre organisation bénéficiera d'une évaluation de sa position de cybersécurité actuelle, ainsi que de l'opportunité de déterminer si vous tirez le meilleur parti de vos outils de sécurité actuels. Nos experts peuvent recommander des configurations mises à jour, trouver des lacunes ou aider à identifier les domaines d'investissement.
- **Feuille de route stratégique pour la sécurité** - Des feuilles de route sur mesure sont élaborées à partir de l'analyse de votre position en matière de sécurité, présentant des informations vitales et des recommandations alignées sur vos risques. Cette feuille de route, équipée de tableaux de bord et de connexions de conformité, permet de prendre des mesures proactives pour une sécurité accrue. Idéale pour les nouveaux programmes ou les nouveaux venus dans une organisation, elle établit des bases de référence pour les éléments de sécurité essentiels et propose des suggestions d'amélioration ciblées pour les configurations et les investissements.

SERVICES DE CONFIDENTIALITÉ ET DE CONFORMITÉ GOSECURE

[Améliorer la protection des données]

Les Services de confidentialité et de conformité de GoSecure évaluent et améliorent les pratiques de protection des données et de la vie privée afin d'atteindre les objectifs de conformité.

- Un examen complet des pratiques de **protection de la vie privée et une évaluation des pratiques de protection de la vie privée** fournis par les experts de confiance en matière de protection de la vie privée et de sécurité de GoSecure évalueront les programmes actuels de protection de la vie privée en place, évalueront le contexte réglementaire qui s'applique à une organisation et aideront à améliorer la conformité avec les normes régionales, nationales et internationales en matière de protection des données.
- GoSecure est un évaluateur de sécurité qualifié au Canada et peut effectuer une **Évaluation complète aboutissant à un rapport de conformité (ROC)**, ainsi qu'aider les organisations qui ont besoin d'aide avec le questionnaire d'auto-évaluation (SAQ).

SERVICES DE PIRATAGE ÉTHIQUE DE GOSECURE

[Tester vos défenses]

Comptez sur les tests de pénétration de GoSecure pour vous aider à identifier l'impact que les attaquants peuvent avoir sur une organisation. L'équipe de professionnels certifiés en sécurité offensive (OSCP) de GoSecure peut proposer des missions basées sur votre modèle de menace, y compris l'industrie et la pile technologique.

- Notre équipe délivre des engagements qui identifieront où et comment les adversaires peuvent cibler votre organisation, y compris les réseaux internes et externes, les applications web, les applications mobiles, les réseaux sans fil, les terminaux et les appareils mobiles, la sécurité physique et les attaques d'ingénierie sociale / hameçonnage, etc.
- GoSecure possède également les compétences spécialisées pour aider à la **révision du code**, aux **tests SAP**, aux **tests de pénétration du cloud** et aux **tests de dispositifs embarqués/IOT/SCADA/industriels**, à la **radiofréquence** et à d'autres engagements personnalisés.
- Les engagements stratégiques de **GoSecure Red Team** combinent plusieurs techniques d'attaque disponibles avec des professionnels de la sécurité expérimentés pour tester les capacités de réaction et de détection internes d'une organisation.
- Les engagements stratégiques **GoSecure Purple Team** adoptent une approche « tester, corriger, tester à nouveau, répéter » afin d'améliorer rapidement la posture de sécurité des organisations par le biais d'un engagement collaboratif à long terme avec les équipes internes.
- Les engagements de **chasse aux menaces en collaboration** peuvent être proposés après un service Red ou Purple Team ou en tant que service autonome. Ces services personnalisés aideront à améliorer les compétences de l'équipe interne en matière de chasse aux menaces en travaillant avec les experts de GoSecure sur un scénario de chasse aux menaces dans le monde réel.

OPÉRATIONS DE SÉCURITÉ DE MICROSOFT (SECOPS)

Votre allié pour consolider, évoluer et prospérer

[Évaluer, recommander, déployer et configurer les outils et composants de sécurité Microsoft]

L'objectif de cette mission est de fortifier l'écosystème numérique de l'organisation en abordant les considérations clés de sécurité à travers diverses dimensions. GoSecure vise à identifier et à rectifier les vulnérabilités potentielles, les mauvaises configurations et les faiblesses au sein de l'environnement M365 afin d'atténuer le risque d'exploitation par des acteurs malveillants.

Cette évaluation examinera de près l'efficacité des contrôles de gestion des identités et des accès, en garantissant des mécanismes d'authentification et d'autorisation robustes. En outre, l'évaluation se concentre sur l'amélioration de la gouvernance et de la protection des données, en examinant minutieusement les mécanismes de classification, d'étiquetage et de sauvegarde des données afin de sécuriser les informations sensibles. L'évaluation s'étend à la sécurité du courrier électronique, en évaluant les configurations de protection contre le hameçonnage, le courrier indésirable et les menaces liées aux logiciels malveillants. Grâce à des évaluations complètes des vulnérabilités, à la modélisation des menaces et à des simulations de réponse aux incidents, nous visons à traiter de manière proactive les menaces potentielles spécifiques à l'utilisation de M365 par l'organisation.

En outre, notre évaluation comprend une évaluation des programmes de sensibilisation et de formation des utilisateurs, fournissant des recommandations exploitables et une feuille de route pour l'amélioration de la sécurité. L'objectif global est d'assurer la conformité avec les normes de l'industrie, de favoriser l'amélioration continue et de renforcer la résilience de l'organisation face à l'évolution des cybermenaces.

SERVICES DE SÉCURITÉ PROFESSIONNELS

ÉVALUATION DE LA PRÉPARATION EN CAS DE BRÈCHES DE SÉCURITÉ DE GOSECURE (BRA)

[Se préparer aux cyberattaques]

Les services d'évaluation de la préparation en cas de brèches de sécurité de GoSecure testent et affinent les capacités de réponse aux incidents et préparent les organisations à réagir lorsqu'une brèche se produit.

- **L'évaluation de la préparation en cas de brèches de sécurité de GoSecure (BRA)** offre une évaluation complète de la préparation aux incidents, de la continuité des activités à la réponse aux incidents et à la reprise après sinistre, garantissant que les personnes, les processus, les outils et les politiques sont prêts lorsqu'une brèche se produit.
- **Les exercices sur table GoSecure** sont des exercices personnalisés et réels qui testent les outils, les processus, les politiques et les personnes, en mettant l'accent sur la résolution de problèmes en groupe et sous pression. Les communications, la documentation et l'engagement interfonctionnel sont également évalués tout au long des exercices.

ÉVALUATION DE LA COMPROMISSION DE LA SÉCURITÉ DE GOSECURE (SCA)

[Trouver les menaces]

Une évaluation de la compromission de la sécurité (SCA) de GoSecure peut aider à trouver les menaces cachées que l'automatisation seule peut ne pas détecter.

- Le SCA combine 60 jours de **Détection et de réponse étendues gérées GoSecure TitanMC (MXDR)** avec une chasse aux menaces humaine qualifiée et expérimentée, ce qui offre un avantage par rapport à l'automatisation pure qui peut trouver des menaces qui pourraient potentiellement compromettre les opérations actuelles ou futures.
- Le SCA peut identifier les risques potentiels pour vos réseaux, vos terminaux et plus encore. Votre organisation recevra un rapport complet expliquant en détail nos conclusions.

ÉVALUATION DE LA GOUVERNANCE DE L'INTELLIGENCE ARTIFICIELLE (IA)

[Veiller à ce que les outils d'IA soient responsables, sûrs et éthiques]

L'évaluation de la gouvernance de l'IA de GoSecure offre des avantages commerciaux significatifs en améliorant l'efficacité opérationnelle et le positionnement stratégique. Elle rationalise les politiques d'IA, la gestion des données et traite les risques liés à l'IA.

- Indépendant de la réglementation, il s'adapte aux lois émergentes avec flexibilité. Les pratiques éthiques d'IA favorisent la confiance, la crédibilité et la confiance des parties prenantes, positionnant l'organisation comme un leader de l'IA responsable, promouvant l'innovation et attirant les investisseurs.
- Cette évaluation garantit la durabilité à long terme en mettant à jour les cadres de l'IA pour s'aligner sur les nouvelles législations, les meilleures pratiques de l'industrie et les attentes de la société.

SERVICES DE CONSEIL EN CYBERSÉCURITÉ PERSONNALISÉS DE GOSECURE

[Faites travailler nos experts pour vous]

Notre équipe couvre toutes les disciplines de la sécurité afin de fournir des conseils et des recommandations proactifs pour améliorer la posture de sécurité en fonction des besoins de votre organisation.

- Les engagements des **services de conseil en cybersécurité personnalisés de GoSecure** sont conçus pour répondre aux besoins spécifiques de votre organisation et optimiser vos programmes de cybersécurité. Nous aidons les organisations qui veulent se concentrer sur la construction de solutions proactives à certains des plus grands défis de la cybersécurité aujourd'hui - de la façon de se défendre contre les brèches aux plans de récupération après une attaque.
- Nos engagements peuvent inclure, mais ne sont pas limités à, des exercices sur table personnalisés, des exercices offensifs immersifs et des tests personnalisés, la simulation et l'émulation de menaces, des ateliers et des séances d'information sur les renseignements sur les menaces, des examens de la stratégie en matière de technologie et d'architecture, des examens de la conformité et de la politique / du programme en matière de risques de tierces parties.

www.gosecure.ai/fr/

GoSecure TITAN

INFORMATION DE CONTACT

Tél: 855-893-5428
Urgences 24/7: 888-287-5858

sales@gosecure.ai

www.gosecure.ai/fr/
www.gosecure.ai/fr/detection-et-reponse-gerees-et-etendues-de-gosecure-titanmc/