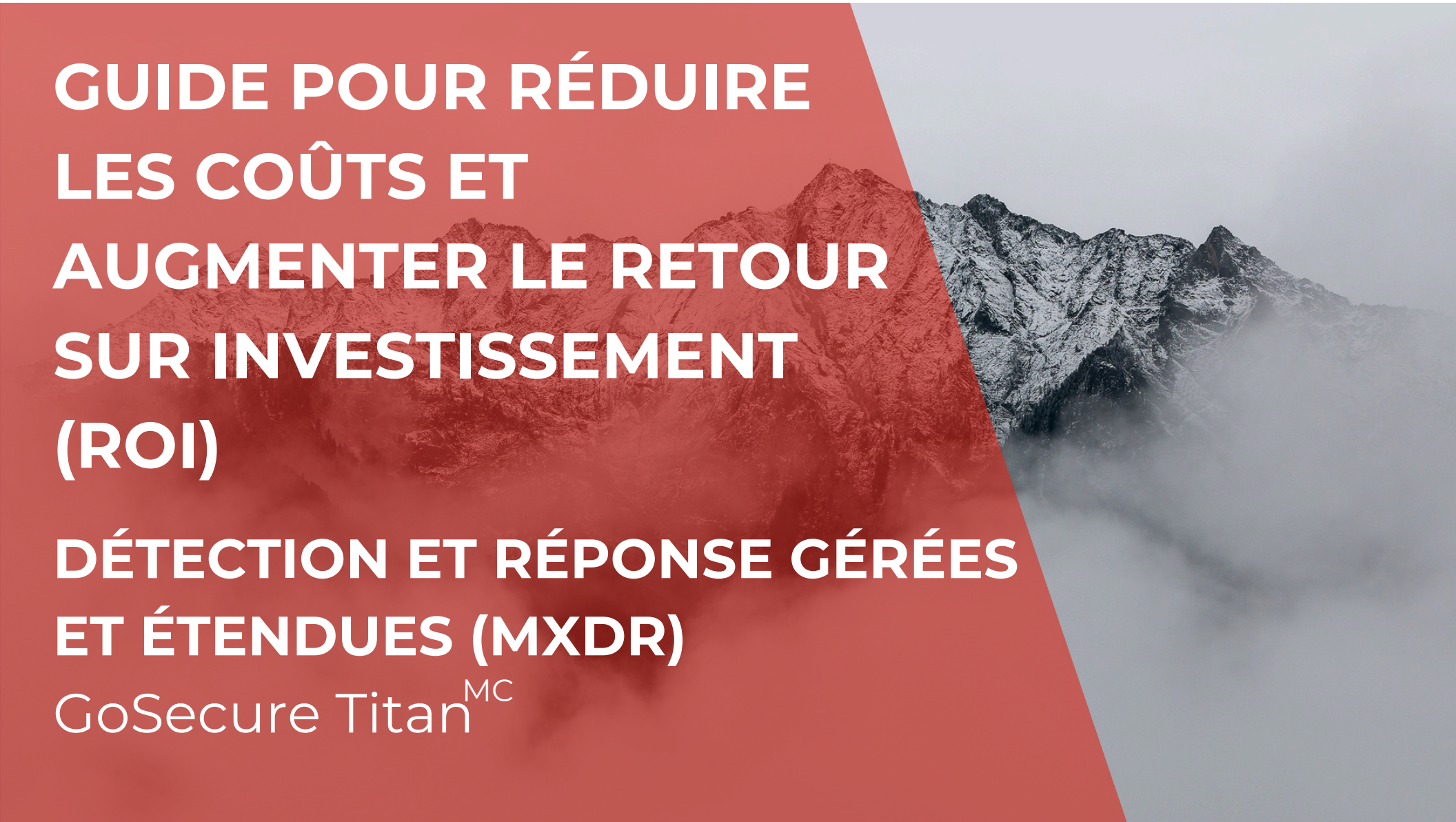
https://gosecure.ai/fr/detection-et-reponse-gerees-et-etendues-de-gosecure-titanmc-fondation/

GoSecure TITAN

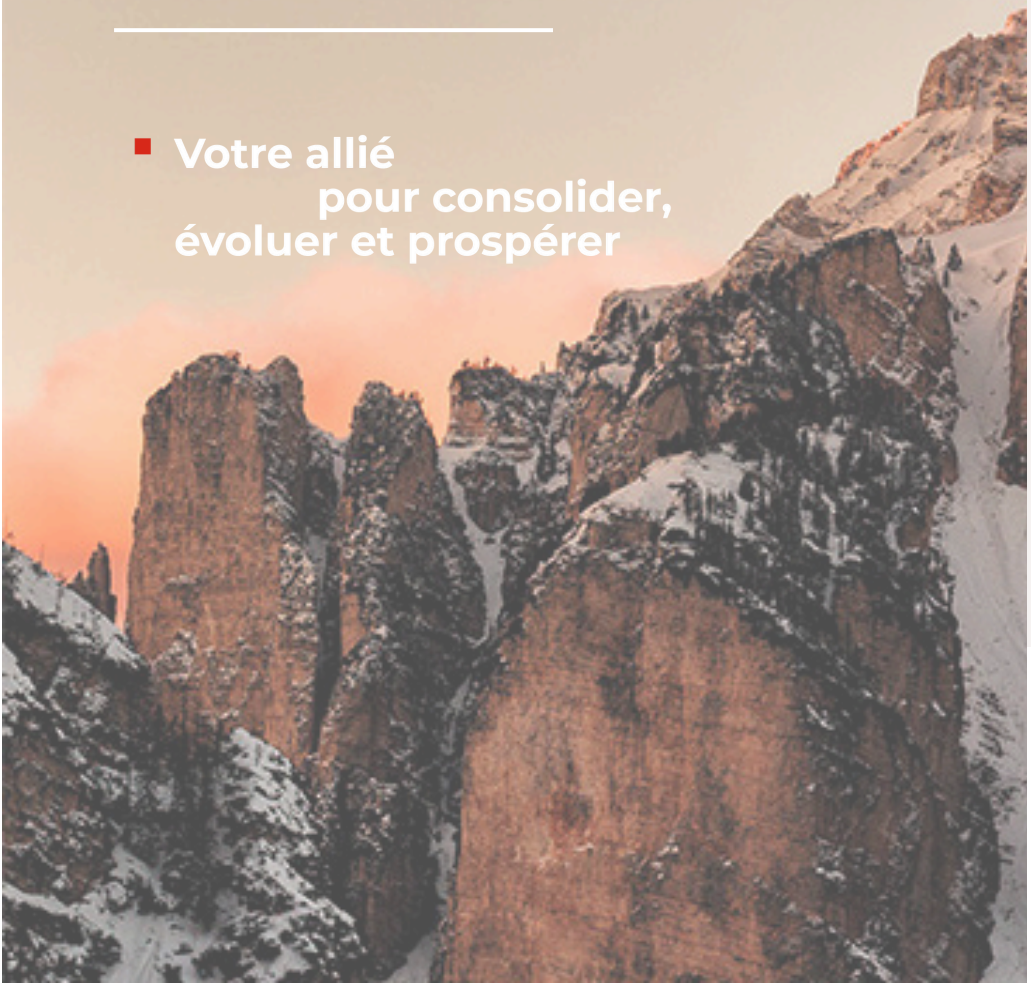
GUIDE POUR RÉDUIRE LES COÛTS ET AUGMENTER LE RETOUR SUR INVESTISSEMENT (ROI)

DÉTECTION ET RÉPONSE GÉRÉES ET ÉTENDUES (MXDR)

GoSecure Titan[MC]



DANS CE GUIDE **VOUS DÉCOUVREZ**



- Votre allié pour consolider, évoluer et prospérer

POURQUOI CONSOLIDER ?

LES BÉNÉFICES

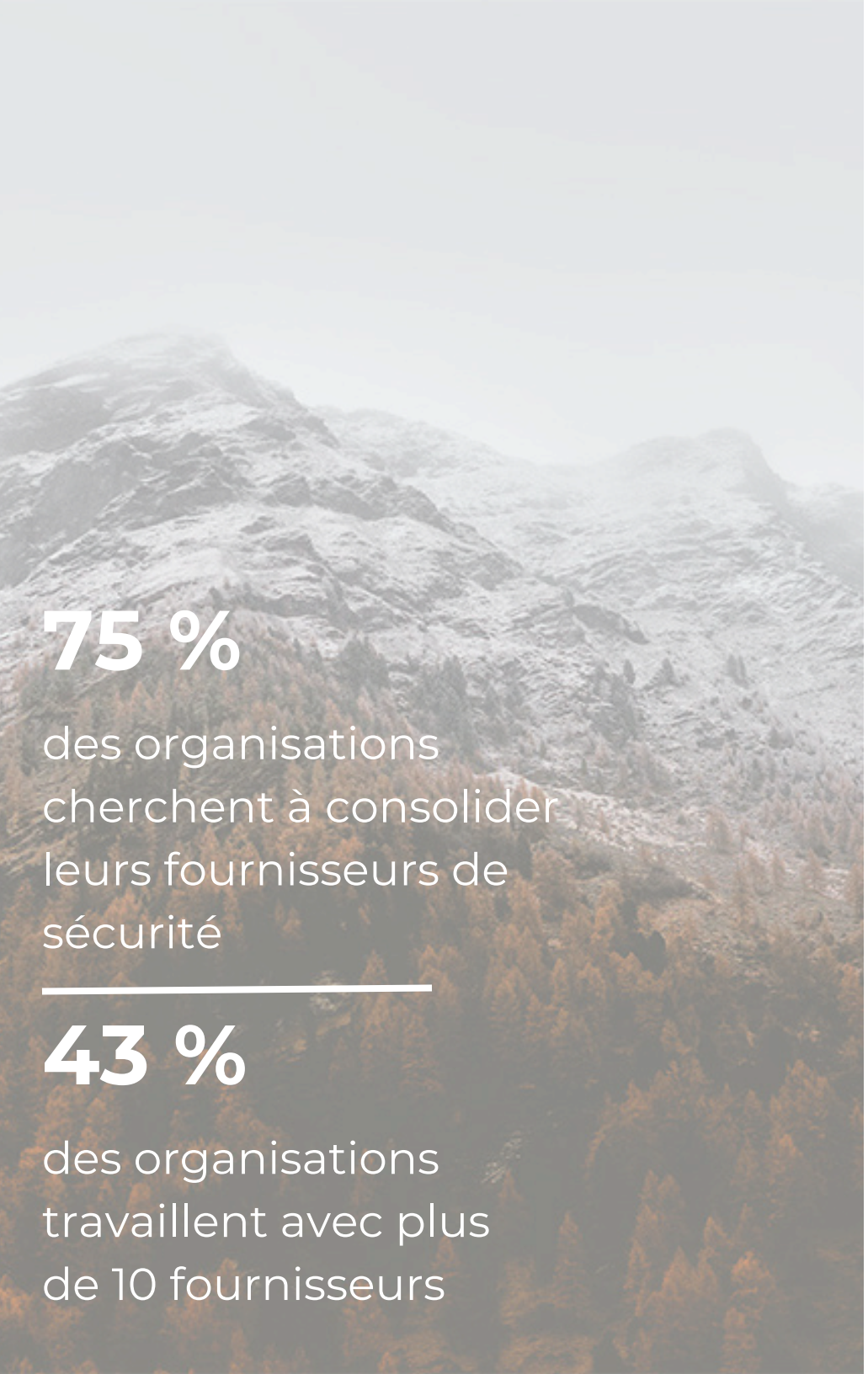
LES DÉFIS PERÇUS

LES PREMIÈRES ÉTAPES

POURQUOI ET COMMENT MXDR GOSECURE TITAN[MC] EST VOTRE ALLIÉ ULTIME

E-MAIL@GOSECURE.AI

WWW.GOSECURE.AI



CONSOLIDATION

Pourquoi ?

On ne saurait trop insister sur l'importance de mesures de cybersécurité solides. Alors que les organisations s'efforcent de protéger leurs données sensibles et leurs actifs numériques contre des menaces de plus en plus sophistiquées, la question de la meilleure façon de gérer leur infrastructure de cybersécurité devient primordiale.

Une étude récente de Gartner a révélé qu'en 2022, 75 % des organisations envisageront de consolider leurs fournisseurs de sécurité, soit une augmentation de près de 50 % par rapport à 2020. Cette statistique souligne que le secteur reconnaît de plus en plus la nécessité de rationaliser et d'optimiser les stratégies de cybersécurité.

En effet, de nombreuses entreprises sont aux prises avec une pléthore de fournisseurs de sécurité, 43 % d'entre elles reconnaissant travailler avec plus de dix fournisseurs. Cette prolifération de fournisseurs complique non seulement l'efficacité opérationnelle, mais pose également des problèmes en termes de gestion des coûts, d'évaluation des risques et de posture de sécurité globale.

Ces dernières années, le contexte économique mondial a connu des bouleversements importants : l'inflation galopante, la réduction des dépenses et la multiplication des licenciements ont incité les organisations à réévaluer leurs pratiques en matière de dépenses. La récente vague de licenciements dans tous les secteurs d'activité a mis en évidence et exacerbé la pénurie de compétences qui sévit actuellement. Les entreprises n'ont tout simplement pas la capacité de retenir des experts pour chaque solution de sécurité ou d'entretenir des relations avec de nombreux fournisseurs.

Dans ce guide, nous examinerons les nombreux avantages de la consolidation des solutions de cybersécurité, nous nous pencherons sur les obstacles perçus à la consolidation et nous explorerons les possibilités d'amélioration de la sécurité.

GoSecure

BÉNÉFICES

La consolidation des solutions de cybersécurité permet aux entreprises de mettre en place un dispositif de sécurité plus robuste et plus résistant, d'optimiser leurs investissements en matière de sécurité et de s'adapter plus efficacement à l'évolution des cybermenaces. En simplifiant la gestion, en réduisant les coûts, en renforçant la visibilité et en améliorant l'intégration, la consolidation permet aux organisations de garder une longueur d'avance dans un contexte de menaces de plus en plus complexe et difficile.

- **Votre allié pour consolider, évoluer et prospérer**

E-MAIL@GOSECURE.AI

WWW.GOSECURE.AI/FR/

> POSTURE DE SÉCURITÉ RENFORCÉE

En 2021, IBM a publié les résultats de sa sixième étude annuelle sur la résilience des organisations. L'étude révèle que 45 % des équipes de sécurité utilisent plus de 20 outils pour enquêter et répondre à un incident de cybersécurité.

La complexité et la fragmentation causées par l'utilisation de nombreux outils disparates provenant de divers fournisseurs entravent souvent les efforts de cybersécurité au lieu de les renforcer. Chaque outil fonctionne en vase clos, générant son propre ensemble d'alertes, de mesures et d'interprétations des événements de sécurité.

En conséquence, les équipes de sécurité se retrouvent submergées de données, perdant un temps précieux à passer d'une plateforme à l'autre et à tenter de réconcilier des informations contradictoires. Cette « fatigue des outils » ne détourne pas seulement l'attention des menaces de sécurité réelles, mais contribue également à ce que les initiés de l'industrie appellent le phénomène de « surcharge d'alertes ». Face à la multitude d'alertes et de notifications qui envahissent leurs écrans, les analystes de la sécurité ont du mal à hiérarchiser efficacement les incidents, ce qui conduit souvent à négliger ou à ignorer des menaces critiques.

La consolidation des fournisseurs de sécurité offre une solution à ce problème en fournissant une plateforme unifiée pour la gestion des opérations de sécurité. Avec toutes les données de sécurité centralisées et corrélées dans un seul tableau de bord, les organisations peuvent rationaliser leurs efforts de cybersécurité, améliorer les temps de réponse et favoriser une meilleure collaboration entre les équipes.

En simplifiant la complexité et en réduisant la lassitude à l'égard des outils, la consolidation des fournisseurs de sécurité renforce le dispositif de sécurité global de l'organisation et améliore la qualité de l'information.

RÉDUCTION DES COÛTS ET AMÉLIORATION DU RETOUR SUR INVESTISSEMENT

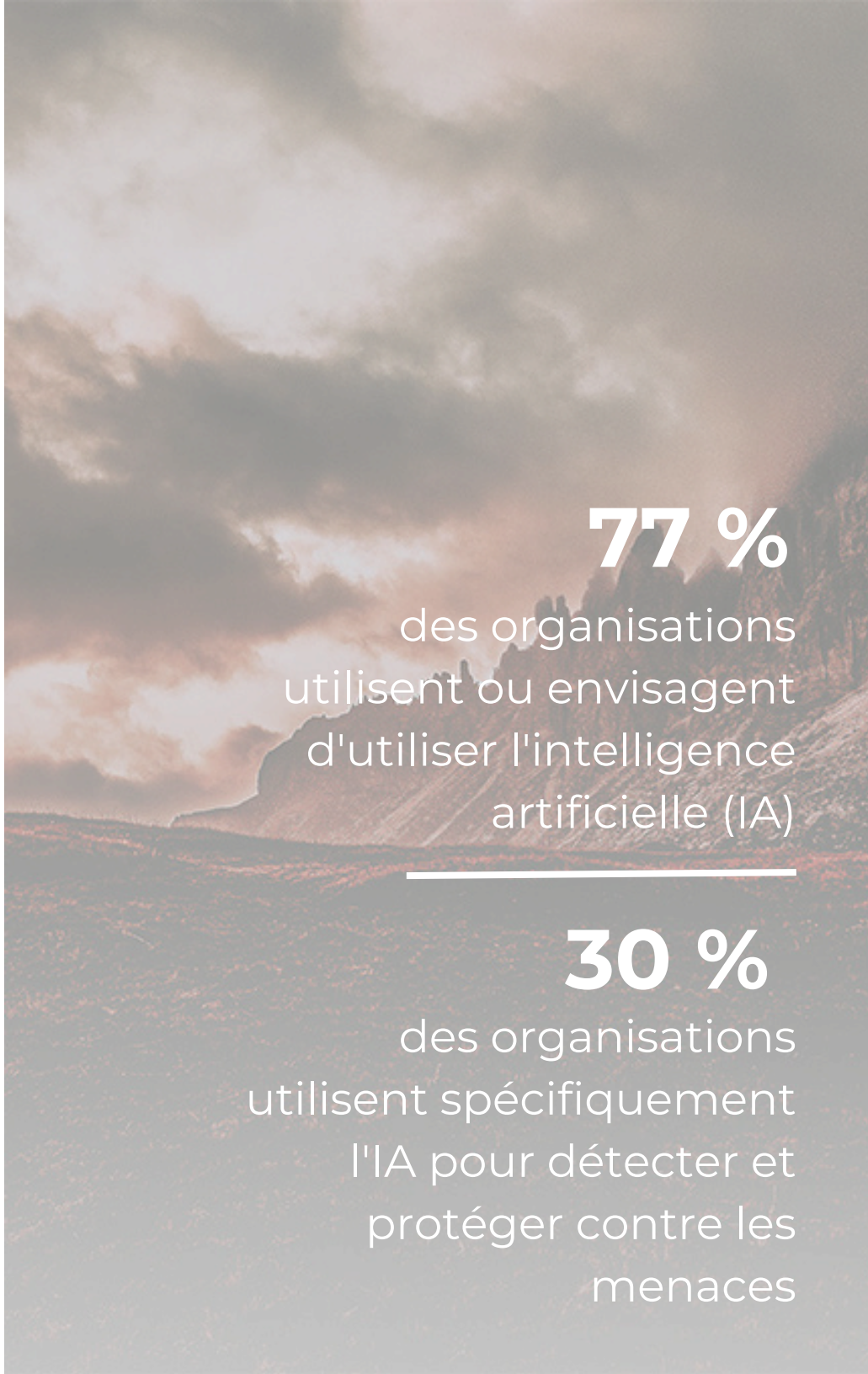
On le sait peu, mais en matière de cybersécurité, la simplicité fait souvent la force. Consolider le dispositif de sécurité de votre organisation ne consiste pas seulement à réduire la complexité, mais aussi à maximiser le retour sur investissement. L'un des moyens les plus simples d'économiser sur votre budget de sécurité est d'évaluer et d'éliminer les redondances dans vos solutions de sécurité.

En réduisant le nombre de fournisseurs et en rationalisant les services, les organisations peuvent souvent bénéficier de remises de consolidation de la part de leurs fournisseurs préférés. Ces économies peuvent alors être réorientées vers d'autres domaines au sein de l'organisation, tels que la formation du personnel ou les investissements dans les technologies de sécurité de pointe.

Prenons l'exemple d'IBM. Ses recherches indiquent que 77 % des organisations utilisent ou envisagent d'utiliser l'intelligence artificielle (IA) dans le cadre de leurs efforts de cybersécurité. L'IA a un large éventail d'applications, et près de 30 % des organisations l'utilisent spécifiquement pour la détection et la protection contre les menaces.

En consolidant les solutions de sécurité et en réaffectant les économies budgétaires, les organisations peuvent se permettre d'investir dans la formation de leurs équipes informatiques à l'IA, à l'apprentissage automatique et à d'autres technologies émergentes, améliorant ainsi leurs capacités de cyberdéfense sans s'exposer à des risques inutiles.

En outre, la consolidation peut permettre de gagner beaucoup de temps dans la détection et la réponse aux menaces. La gestion de plusieurs outils de sécurité provenant de différents fournisseurs nécessite souvent de passer d'une plateforme à l'autre, de transférer des données et de trier les faux positifs et les alertes redondantes. La consolidation de ces outils rationalise la gestion des données et permet d'accéder à une plateforme unique pour la surveillance des menaces et la réaction. Cette efficacité permet non seulement de gagner du temps, mais aussi d'accroître la productivité et la satisfaction des employés, ce qui, en fin de compte, améliore le retour sur investissement global du programme de sécurité de l'organisation.



[« Nous avions le choix entre embaucher une ou deux personnes et nous assurer que nous pouvions maintenir leurs compétences à jour - et nous assurer que nous les gardions avec nous. Nous pouvions aussi établir un partenariat avec un fournisseur de services de sécurité gérés comme GoSecure. Nous avons opté pour cette solution, afin d'avoir accès à des professionnels de la cybersécurité expérimentés et d'être sûrs d'être soutenus 24 heures sur 24, 7 jours sur 7 et 365 jours par an en cas d'urgence. »]

Frederick Pouliot
Directeur principal des technologies de l'information, Agri-Marché

AMÉLIORER L'EFFICACITÉ OPÉRATIONNELLE

L'efficacité et la productivité s'améliorent lorsque les organisations prennent l'initiative stratégique de réduire le nombre de leurs fournisseurs. Cette pratique libère une quantité importante de temps et de ressources, permettant aux équipes de réorienter leur attention des tâches administratives banales vers des initiatives plus stratégiques et axées sur la valeur.

En regroupant les fournisseurs, les organisations jettent les bases de relations plus profondes et plus significatives avec les vendeurs qu'elles ont choisis. Ces partenariats renforcés se traduisent souvent par des avantages tangibles allant au-delà du simple échange transactionnel de biens ou de services, notamment des prix préférentiels, l'accès à des ressources exclusives et une meilleure assistance à la clientèle.

Un écosystème de fournisseurs rationalisé offre aux organisations une meilleure visibilité et un meilleur contrôle de leur contexte opérationnel. En réduisant la complexité associée à la gestion de multiples fournisseurs, les entreprises ont une vision plus claire des performances de chaque solution. Cette transparence accrue permet d'identifier et de résoudre les problèmes de manière proactive, ce qui minimise le risque de vulnérabilités du système et de brèches de sécurité potentielles. En outre, la rationalisation des relations avec les fournisseurs facilite une communication et une collaboration plus efficaces, ce qui conduit à des processus d'intégration plus fluides et à des temps de réponse plus rapides aux défis émergents.

La consolidation simplifie les efforts de mise en conformité en offrant une approche plus cohérente et unifiée du respect des réglementations. Avec moins de fournisseurs à gérer, les organisations peuvent rationaliser leurs processus de conformité, en s'assurant qu'elles respectent les normes industrielles et les exigences réglementaires nécessaires. Cette attitude proactive permet non seulement de réduire le risque de pénalités pour non-conformité, mais aussi d'améliorer la réputation et la crédibilité de l'organisation au sein du secteur.

La consolidation stratégique des fournisseurs offre de nombreux avantages qui vont bien au-delà de l'efficacité opérationnelle. En favorisant des relations plus solides, en améliorant la visibilité et le contrôle et en simplifiant les efforts de conformité, les organisations se positionnent pour une réussite et une croissance à long terme dans un contexte commercial de plus en plus concurrentiel.

DÉFIS PERÇUS

GoSecure TITAN

Bien que les avantages de la consolidation soient évidents, certaines organisations peuvent encore considérer les inconvénients perçus comme une raison suffisante pour s'en écarter. Cependant, de nombreuses objections à la consolidation sont fondées sur des malentendus ou un manque de contexte, et deux préoccupations majeures sont souvent exprimées.

- **Votre allié pour consolider, évoluer et prospérer**

E-MAIL@GOSECURE.AI

WWW.GOSECURE.AI/FR/

SYNDROME FOMO DES SOLUTIONS « MEILLEURE DE LEUR CATÉGORIE »

L'une des réticences les plus courantes à l'égard de la consolidation de la cybersécurité tient à la crainte de passer à côté des solutions supposées les plus performantes. Les organisations consacrent souvent un temps considérable à la recherche et à l'évaluation de divers produits pour chaque besoin de sécurité spécifique, dans l'espoir de trouver la solution idéale. Cependant, elles peuvent découvrir que si un fournisseur excelle dans un domaine, il n'est pas à la hauteur dans d'autres. Ce dilemme peut susciter des doutes quant à la compatibilité entre la consolidation et la qualité.

Néanmoins, un nombre croissant de professionnels affirment aujourd'hui que les avantages de la consolidation dépassent de loin ceux de l'approche « meilleur de sa catégorie ». Les résultats récents d'une enquête de Gartner révèlent que **41 % des personnes interrogées considèrent l'amélioration de la position de risque de leur organisation comme le principal avantage de la consolidation des solutions de sécurité**. Cela souligne les améliorations significatives en matière de sécurité, d'efficacité opérationnelle et de visibilité de bout en bout qu'offre la consolidation.

Contrairement à la croyance selon laquelle les solutions individuelles sont supérieures, les experts affirment que l'effet cumulatif d'une approche consolidée garantit une sécurité beaucoup plus efficace. Plutôt que de s'appuyer sur des solutions disjointes, qui peuvent exceller isolément mais peinent à s'intégrer de manière transparente, une stratégie consolidée fournit un cadre cohésif qui permet de relever les défis de sécurité de manière globale. Par conséquent, il ne s'agit pas de disposer des meilleurs outils individuels, mais plutôt de les intégrer dans un écosystème de sécurité unifié et synergique.

PEUR DE SE RETROUVER COINCÉ AVEC UN SEUL FOURNISSEUR

L'une des principales préoccupations liées à la consolidation est la crainte d'être enfermé dans un fournisseur unique. De nombreuses organisations hésitent à consolider leur pile technologique, craignant que le fournisseur choisi ne soit pas à la hauteur ou ne tienne pas ses promesses. Cette appréhension provient du scénario potentiel d'être coincé avec une solution de qualité inférieure jusqu'à la fin du contrat ou de la période d'abonnement.

Pour dissiper les inquiétudes liées à la consolidation avec des fournisseurs de qualité médiocre, il est essentiel de procéder à des évaluations approfondies des partenaires potentiels. L'évaluation de différents fournisseurs permet de s'assurer que chaque candidat est en mesure de répondre à vos exigences en matière de produits, d'atténuer les vulnérabilités en matière de sécurité et de suivre le rythme des innovations du secteur. Voici quelques questions essentielles à se poser lors de l'évaluation des fournisseurs potentiels :

- **Approche de la sécurité :** Comprenez comment le fournisseur aborde la sécurité. Demandez-lui s'il fait appel à des fournisseurs tiers pour la gestion de la sécurité et si certaines de vos données résideront sur leurs systèmes. En outre, cherchez à savoir comment il a réagi aux menaces de sécurité dans le passé afin d'évaluer son efficacité à protéger les actifs de votre organisation.
- **Considérations relatives aux coûts :** Clarifiez tous les coûts associés aux services du fournisseur. Souvent, le prix initial n'inclut pas la maintenance, les frais d'abonnement supplémentaires, les ajouts de licences ou d'autres modules nécessaires. En comprenant bien les coûts potentiels, vous pouvez garantir le respect du budget et éviter les surprises dues à des frais cachés.
- **Compatibilité d'intégration :** Évaluez dans quelle mesure les outils du fournisseur s'intègrent aux systèmes existants de votre organisation. Si les fonctionnalités d'une solution peuvent être impressionnantes, l'intégration transparente avec votre infrastructure est cruciale. Opter pour un fournisseur dont les outils s'alignent parfaitement sur vos systèmes minimise le besoin de personnalisation et réduit les difficultés de mise en œuvre.
- **Flexibilité de la transition :** Anticipez vos besoins futurs et envisagez la facilité d'intégration ou de transition vers d'autres fournisseurs. Au fur et à mesure que les besoins de l'organisation évoluent, il devient primordial de pouvoir changer de fournisseur en douceur. En posant dès le départ des questions pertinentes sur les processus d'intégration et de désintoxication, vous pouvez garantir des transitions sans heurts à l'avenir.

Une fois ces obstacles surmontés, les entreprises peuvent s'engager en toute confiance sur la voie de la consolidation, en renforçant leur sécurité et leur efficacité opérationnelle.

GoSecure

PREMIÈRES ÉTAPES

Naviguer dans le labyrinthe de votre infrastructure de cybersécurité actuelle et de vos fournisseurs peut sembler impressionnant au départ.

Mais n'ayez crainte ! Nous sommes là pour vous guider en toute confiance dans votre parcours de consolidation. Alors que vous vous lancez dans cette entreprise, il est impératif d'acquérir une compréhension approfondie de tous les outils et solutions disponibles, tout en recueillant des informations sur les fournisseurs concernés.

Tout comme vous avez besoin d'une vision claire de votre système pour faire des choix éclairés en matière de sécurité, il est essentiel de plonger dans votre pile technologique existante pour identifier les domaines mûrs pour la consolidation. Cette analyse introspective jette les bases d'une stratégie de consolidation réussie, vous permettant d'optimiser efficacement votre infrastructure de cybersécurité.

E-MAIL@GOSECURE.AI

WWW.GOSECURE.AI/FR/

ÉVITER LA CONSOLIDATION PAR COUCHES

Une fois que vous avez fait l'inventaire de vos ressources existantes, l'étape suivante consiste à élaborer une stratégie intelligente de consolidation. Notre recommandation ? Concentrez-vous sur la consolidation des fonctions plutôt que sur celle des couches. Voici pourquoi : votre infrastructure intègre probablement plusieurs couches de sécurité, chacune servant de filet de sécurité pour identifier les vulnérabilités - une tactique communément appelée « défense en profondeur ». Par exemple, vous disposez peut-être d'une solution dédiée à la surveillance des terminaux et d'une autre pour gérer les menaces dans l'ensemble de votre écosystème.

Mais pourquoi éviter de consolider différentes couches ? Ce faisant, vous risquez d'affaiblir involontairement votre position en matière de sécurité en supprimant de précieuses redondances au sein de votre système. Le principe de la conception sécurisée repose sur la redondance pour atténuer le risque d'un « point de défaillance unique ».

Dans le contexte complexe des infrastructures hybrides d'aujourd'hui, l'adoption d'une approche de défense en profondeur n'est pas seulement prudente, elle est impérative.

CONSOLIDATION DES FONCTIONS

La consolidation des fonctions apparaît comme une stratégie fondamentale pour la résilience des organisations. En concentrant leurs efforts sur des domaines vitaux tels que la sécurité de l'infonuage, la gestion des vulnérabilités et la sécurité des applications, les organisations peuvent renforcer leurs défenses et rationaliser leurs opérations. Cette consolidation améliore non seulement la visibilité et la gestion des risques, mais favorise également une approche cohérente de la cybersécurité.

Un examen plus approfondi des différentes couches de la cybersécurité révèle d'autres possibilités d'optimisation. En identifiant les fonctions mûres pour la consolidation, telles que la détection et la réponse ou l'intégration de la veille sur les menaces et de la gestion des vulnérabilités, les organisations peuvent affiner leur posture de sécurité. En substance, la consolidation des fonctions permet aux organisations de naviguer dans le contexte évolutif des menaces avec agilité et résilience, en veillant à garder une longueur d'avance sur les risques potentiels tout en rationalisant leurs efforts en matière de cybersécurité.

TROUVER LES BONS OUTILS

Une fois que vous avez identifié les meilleures fonctions à consolider ou la façon dont vous souhaitez aborder la consolidation des fonctions à travers différentes couches, vous devez déterminer les offres et les outils les plus adaptés à votre organisation.

Si la sécurisation de votre migration vers l'infonuage est une priorité, voici quelques caractéristiques essentielles à rechercher dans les offres et solutions de consolidation :

Hiérarchisation des risques
La consolidation peut éviter la confusion causée par des flux de données multiples provenant de différentes solutions, mais vous devez également trouver un outil qui fournit le contexte nécessaire pour classer les signaux de risque dans l'ensemble de votre écosystème. Cela inclut des solutions qui permettent à votre équipe de déterminer quels ports indésirables sont ouverts sur vos actifs publics.

Automatisation de la conformité
Votre solution consolidée doit vous aider à vous conformer aux réglementations internes et externes en détectant et en comblant les lacunes. Les outils qui surveillent et appliquent les réglementations spécifiques à l'industrie tout en fonctionnant de manière transparente avec vos flux de travail pour assurer une conformité continue sont privilégiés.

Analyse de la sécurité
Le contexte des menaces est en constante évolution, c'est pourquoi l'analyse et le test continus des applications de votre infrastructure sont essentiels à votre stratégie de sécurité. Une offre de consolidation idéale devrait fournir à votre organisation des évaluations de sécurité en temps réel, des rapports détaillés pour une meilleure collaboration entre les équipes et des informations précieuses sur l'évolution des risques. Les meilleurs outils veilleront également à ce que votre équipe soit consciente des quatre principaux types de risques dans votre système : les risques connus, les risques connus inconnus, les risques connus inconnus et les risques inconnus inconnus.

En revanche, si votre priorité est d'étendre votre programme de détection et d'intervention par le biais de l'externalisation, voici quelques caractéristiques essentielles à rechercher :

Couverture complète
Lorsque vous consolidez votre programme de détection et de réponse, vous devez vous assurer que l'ensemble de votre surface d'attaque est sous contrôle. Cela signifie que vous avez besoin d'outils qui offrent une couverture complète de vos terminaux, de votre réseau, de vos utilisateurs et de votre infonuage afin d'éliminer les menaces dans l'ensemble de votre environnement.

Partenariat transparent
Une bonne offre de consolidation gérée doit être un véritable partenariat. Vous devez pouvoir compter sur une collaboration fluide avec des experts pour obtenir des réponses à tout moment et savoir exactement ce que l'équipe SOC externe voit.

Détection et réponse de bout en bout
Une offre consolidée de détection et de réponse doit aller au-delà de ces fonctions de base. Vous devez choisir une solution qui vous assiste tout au long du processus, avec une investigation numérique de bout en bout et une réponse complète aux incidents.

GoSecure

Une fois que vous avez identifié les outils et les progiciels de consolidation appropriés, vous pouvez les affecter aux domaines de votre organisation qui, selon vous, ont le plus besoin d'être consolidés. Il est judicieux de discuter de vos objectifs avec les fournisseurs potentiels afin qu'ils puissent vous aider à identifier les meilleures offres, voire à créer une solution personnalisée.

- **Votre allié pour consolider, évoluer et prospérer**

CONTACTEZ-NOUS

GoSecure

MXDR GOSECURE TITAN[MC]

L'ALLIÉ ULTIME DE VOTRE CONSOLIDATION

35 %

Les entreprises qui choisissent MXDR GoSecure Titan[MC] peuvent réaliser des économies allant jusqu'à 35 %.

DE 100 % À 300 %

Les organisations peuvent obtenir un retour sur investissement positif dès la première année de mise en œuvre d'une solution XDR ouverte.

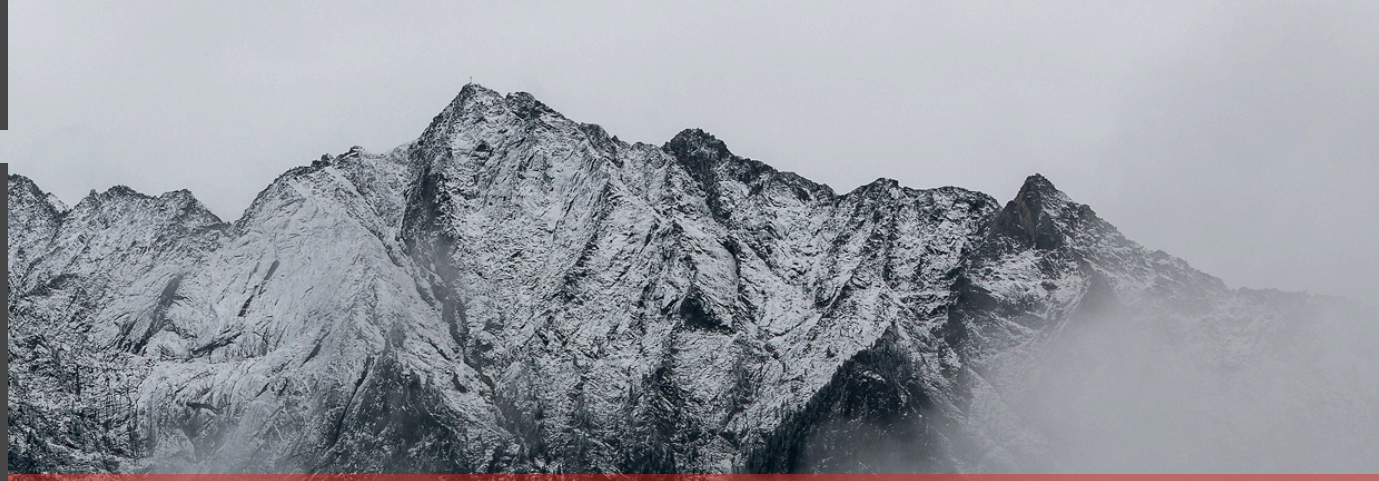
60 %

Réduction des incidents de sécurité jusqu'à 60 % suite à la mise en œuvre de MXDR GoSecure Titan[MC]

- **Votre allié pour consolider, évoluer et prospérer**

E-MAIL@GOSECURE.AI

WWW.GOSECURE.AI/FR/



MXDR GOSECURE TITAN[MC] S'INTÈGRE DE MANIÈRE TRANSPARENTE AUX OUTILS DE SÉCURITÉ EXISTANTS, OFFRANT UNE GESTION CENTRALISÉE SANS QU'IL SOIT NÉCESSAIRE DE LES REMPLACER.

En s'appuyant sur notre technologie ouverte XDR, MXDR GoSecure Titan[MC] offre une visibilité, une détection et des capacités de réponse inégalées, permettant aux entreprises de faire face efficacement à l'évolution des cyber-menaces. Avec une seule fenêtre et un écosystème très flexible, vous pouvez incorporer votre technologie actuelle, ce qui permet une ingestion et une gestion transparentes.

LES AVANTAGES DE LA TECHNOLOGIE OUVERTE XDR DU MXDR GOSECURE TITAN[MC]

- VISIBILITÉ ACCRUE DES MENACES
- AMÉLIORATION DE LA RÉPONSE AUX INCIDENTS
- EFFICACITÉ DES COÛTS
- PRODUCTIVITÉ DES EMPLOYÉS
- FLEXIBILITÉ ET ADAPTABILITÉ

DÉTECTION ET RÉPONSE GÉRÉES ET ÉTENDUES GOSECURE TITAN[MC] (MXDR)

UNE FONDATION EN LAQUELLE VOUS POUVEZ AVOIR CONFIANCE ET SUR LAQUELLE VOUS APPUYER

MXDR GoSecure Titan[MC], alimenté par notre technologie ouverte XDR, est une solution de cybersécurité complète qui répond efficacement aux défis et aux besoins des entreprises.

Avec sa détection avancée des menaces, ses actions de réponse automatisées, ses solutions économiques et ses améliorations de la productivité, MXDR GoSecure Titan[MC] permet aux organisations de renforcer leur posture de sécurité, d'atténuer les risques et de se protéger contre les menaces numériques croissantes.

EN SAVOIR PLUS

VOTRE ALLIÉ ULTIME

Choisissez GoSecure comme votre allié ultime avec un record éprouvé d'expertise, l'excellence de la recherche, et un engagement à répondre aux paysages en constante évolution des menaces pour les terminaux. Notre notoriété dans le monde de la cybersécurité témoigne de notre engagement à fournir des solutions innovantes et efficaces qui protègent les organisations dans un environnement numérique de plus en plus complexe.

PROTÉGEZ-VOUS

https://gosecure.ai/fr/detection-et-reponse-gerees-et-etendues-de-gosecure-titanmc-fondation/

GoSecure TITAN

INFORMATIONS DE CONTACT

Tel : (855) 893-5428
Urgence 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/