Aperçu Des Capacités de Cybersécurité D'insight

Insight

Introduction

La cybersécurité est plus cruciale que jamais pour les entreprises de toutes tailles à mesure que la fréquence et la sophistication des cybermenaces augmentent. Les violations de la cybersécurité peuvent avoir des conséquences dévastatrices, y compris des pertes financières, des responsabilités légales, des dommages à la marque et une perte de confiance des clients.

Protéger votre entreprise contre les cybermenaces n'est pas seulement une question de conformité ou de meilleures pratiques ; c'est essentiel pour sécuriser vos opérations et garantir. La continuité de vos opérations.

Investir dans des mesures de cybersécurité robustes est un investissement dans la résilience et le succès futurs de votre entreprise. En mettant en œuvre des stratégies de cybersécurité efficaces, vous pouvez atténuer les risques, détecter et répondre aux menaces en temps opportun et construire une défense solide contre les cyberattaques.

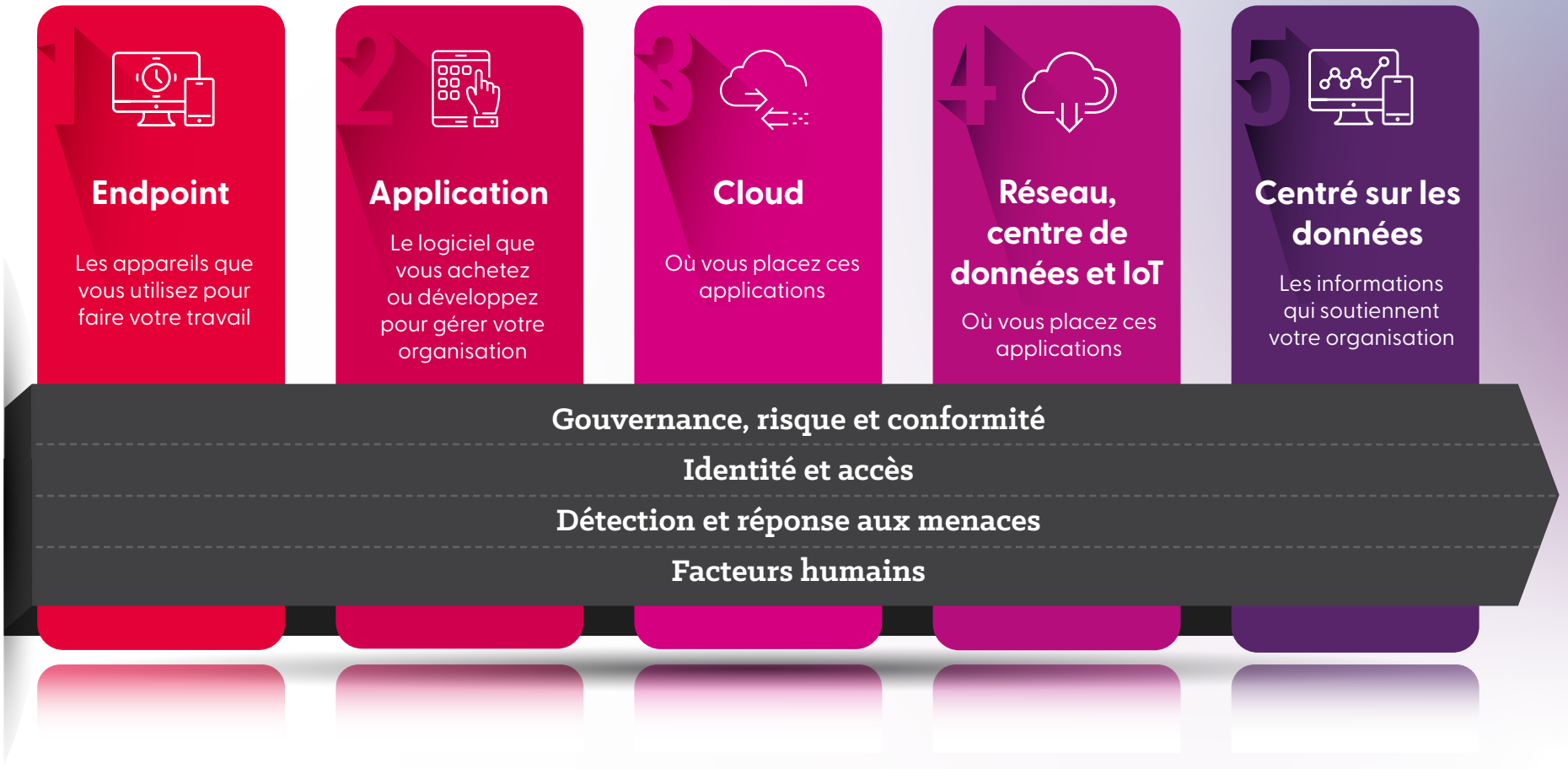
La cybersécurité n'est pas seulement une nécessité ; c'est un impératif stratégique pour les entreprises qui cherchent à prospérer dans un environnement sécurisé et résilient.

Chez Insight, nous comprenons la nécessité d'uneapproche complète de la sécurité.

L'approche d'Insight en matière de cybersécurité

La cybersécurité est compliquée et exige une approche tout-en-un de la part de vos utilisateurs finaux, de vos équipes de sécurité et de vos outils. C'est pourquoi nous adoptons une approche holistique de la cybersécurité à la fois dans les domaines de la technologie et de l'intégration, fournie par des méthodes répétables et des processus éprouvés qui donnent des résultats fructueux. Nos experts vous guideront de bout en bout, ce qui vous permettra d'améliorer l'efficacité et l'alignement stratégique.

Le modèle de sécurité holistique d'Insight



L'approche d'Insight en matière de cybersécurité

Nous possédons des compétences techniques complètes dans les cinq domaines de la technologie :

- Endpoints
- Applications
- Cloud
- Réseau, centre de données et IoT
- Centrées sur les données

mais en tant qu'intégrateur de solutions , nous comprenons que l'excellence technique dans ces domaines ne suffit pas. La sécurité a besoin d'être abordée de manière holistique, en s'assurant que tous les domaines de la sécurité sont intégrés et coordonnés. Nous y parvenons par l'application de :

- · Gouvernance, Risque et Conformité
- · Identité et accès
- · Détection et réponse aux menaces
- · Facteurs humainss

Les lacunes où les domaines technologiques se connectent sont souvent là où une valeur ajoutée peut être obtenue, contribuant à améliorer votre posture de sécurité globale de manière rentable.

Nous pouvons vous aider à :

- Renforcer la confiance en cybersécurité
- Identifier et atténuer les risques
- Réduisez la complexité en minimisant les chevauchements.
- Optimiser les opérations de sécurité
- Assurez-vous que les contrôles de sécurité ajoutent de la valeur et améliorent le retour sur investissement.

Piliers de la technologie

Endpoints

L'époque où un seul appareil était utilisé par un utilisateur dans une entreprise est révolue. Il est plus que probable que vos collaborateurs utilisent plusieurs appareils. Les terminaux jouent un rôle essentiel dans la cybersécurité pour les organisations, servant de points d'entrée pour les cybermenaces et les vulnérabilités. Les défis liés à la sécurisation des terminaux ont augmenté en raison de la prolifération des appareils, des environnements de travail à distance et de la sophistication croissante des cyberattaques ciblant les terminaux.

Les défis courants incluent la visibilité des terminaux, le management des vulnérabilités, la protection des données et le contrôle des applications. Ces appareils doivent être managés, leur posture de sécurité surveillée et mise à jour, et des défenses actives pour bloquer les malwares et les exploits doivent être déployées et maintenues. Nos solutions de sécurité des terminaux se concentrent sur le processus de sécurisation des terminaux tels que les ordinateurs portables, les ordinateurs de bureau, les serveurs et les appareils portables utilisés pour accéder aux réseaux et aux données de l'entreprise.

Nous pouvons vous aider à :

- Obtenez une visibilité sur votre parc de terminaux, au niveau des appareils et des applications.
- Détectez et répondez aux cybermenaces en temps réel.
- Protégez les données sensibles sur les appareils contre tout accès non autorisé.
- Empêchez les infections par malwares et les cyberattaques sur les terminaux.
- Obtenez une visibilité sur les activités des terminaux pour une surveillance efficace.
- Sécuriser les appareils pour les environnements de travail à distance..

Applications

Face à l'évolution constante des cybermenaces, les organisations sont confrontées à des défis considérables. La complexité croissante des applications modernes s'accompagne d'un nombre croissant d'adversaires interconnectés et d'intégrations tierces, ce qui élargit la zone d'attaque.

la surface. Les pirates informatiques et les cybercriminels développent en permanence de nouvelles techniques pour exploiter les failles des applications. Toutes les entreprises utilisent des applications qui nécessitent des correctifs pour rester au fait des vulnérabilités, tant sur les terminaux des utilisateurs que sur l'infrastructure des serveurs. De nombreuses organisations créeront également leurs propres applications, soit via un code faible/pas de code, soit via le développement traditionnel ou le DevOps. L'intégration de la sécurité et de la confidentialité dès la conception dans le cycle de vie du développement logiciel est essentielle pour ces organisations.

Chez Insight, notre équipe de consultants sécurité peut vous aider à réduire les risques liés à votre infrastructure d'applications. Nous vous aiderons à vous tenir à jour de la gestion des failles et des correctifs pour vos applications prêtes à l'emploi et nous vous fournirons des tests d'intrusion pour toutes les applications Web intégrées en interne.

Faites confiance à Insight pour relever les défis de sécurité de vos applications, en vous offrant une protection solide et une tranquillité d'esprit.

Nous pouvons vous aider à :

- Gérez votre parc d'applications pour rester au fait du cycle de vulnérabilité et de correctifs.
- Intégrez des contrôles de sécurité dans vos processus DevOps sans compromettre la vitesse de développement.
- Déplacement vers la gauche de la détection et de la correction des menaces, ce qui réduit le coût de la correction.

Cloud

Le Cloud computing offre une évolutivité et une efficacité inégalées, mais il présente également des défis de sécurité importants. Les entreprises doivent protéger leurs données sensibles contre les accès non autorisés, les brèches et les failles tout en respectant les réglementations et en protégeant leur réputation.

Vous devez adopter une démarche proactive et basée sur les risques, en collaborant avec vos fournisseurs de Cloud pour mettre en place une structure de sécurité solide.

Les spécialistes du Cloud et de la sécurité d'Insight ont des années d'expérience dans la création, la sécurisation et l'exploitation d'environnements multicloud pour des organisations de toutes tailles et de toutes complexités. Nous créerons un cadre de sécurité complet avec une surveillance proactive afin que vous puissiez vous concentrer sur la croissance, l'évolutivité et les innovations.

Nous pouvons vous aider à :

- Visualisez votre environnement multicloud.
- Sécurisez les charges de travail où qu'elles soient créées.
- Surveiller et maintenir la conformité aux cadres de sécurité.

Datacenter, réseau et IoT

Dans le monde interconnecté d'aujourd'hui, l'environnement numérique s'élargit rapidement, créant un réseau complexe de technologies qui a ouvert la voie à des cybermenaces accrues, des violations de données et des accès non autorisés. Il s'agit d'une approche multi-couches pour construire les défenses de sécurité et la résilience dans les entreprises actuelles. Une combinaison de pare-feu, de chiffrement, les contrôles d'accès et les audits de sécurité réguliers ne sont que le début. Pour être proactif dans l'identification et l'atténuation des risques potentiels, vous devez garder une longueur d'avance sur les menaces grâce à des systèmes de détection des menaces avancés et à une analyse spécialisée.

Nous nous engageons à vous conseiller pour résoudre vos problèmes de datacenter, de réseautage et de sécurité de l'IoT. Grâce à notre connaissance approfondie de l'activité, de la technologie et de la sécurité, nous créons la solution adaptée à votre entreprise – de la stratégie et la planification avec la conception à la mise en œuvre et aux services managés. Nos spécialistes de la sécurité peuvent vous aider à gérer la complexité de la technologie requise pour mettre en place et gérer des outils de protection de cybersécurité efficaces, en minimisant les chevauchements et en assurant une protection rentable de la cybersécurité.

Nous vous aidons à :

- Visibilité sur les architectures hybrides complexes
- Une meilleure continuité opérationnelle.
- Les contrôles de sécurité fonctionneront à la fois sur vos réseaux sur site et dans le Cloud.
- Protégez vos données de la source à la destination..

Centrées sur les données

Alors que les professionnels de la sécurité passent beaucoup de temps à sécuriser les applications et l'infrastructure, en fin de compte, presque tout ce que nous faisons se résume à sécuriser les données. Qu'il s'agisse des informations des collaborateurs, des commandes des clients, des chiffres de production ou de la propriété intellectuelle, ce sont les données qui circulent dans votre entreprise qui apportent probablement la plus grande valeur ajoutée à vos clients finaux et à votre entreprise.

Lorsque vous envisagez votre stratégie de sécurité globale, vous devez commencer par les données, et une approche centrée sur les données doit commencer par impliquer vos parties prenantes, et non la technologie.

Nous nous concentrons sur la protection des données elles-mêmes, plutôt que sur la sécurisation des systèmes ou des réseaux qui les stockent et les transmettent. Nous vous aidons à garder une longueur d'avance et à protéger efficacement l'actif le plus précieux de votre organisation : ses données.

Nous vous aidons à :

- Découverte des données sensibles et obsolètes de votre parc.
- Aider à classer les données pour s'assurer que le bon niveau de contrôle est appliqué.
- Conformité aux réglementations sur la protection des données.
- Auditabilité de l'utilisation des données

Domaines d'intégration

Gouvernance, Risque et Conformité

La gouvernance, les risques et la conformité sont des éléments essentiels de la cybersécurité pour les entreprises, englobant les politiques, les procédures et les mécanismes pour gérer les risques de cybersécurité et garantir la conformité aux exigences réglementaires telles que le RGPD et la NIS2. Les organisations sont confrontées à des défis dans la mise en place de structures de gouvernance efficaces, l'identification et l'évaluation des risques de cybersécurité et la mise en œuvre de contrôles robustes pour atténuer les menaces.

Des pratiques GRC efficaces établissent des rôles clairs, rationalisent les processus et atténuent les cyber-risques. Une démarche solide augmentera votre maturité en matière de cybersécurité, réduira vos responsabilités juridiques et financières, améliorera la confiance de vos clients et le respect de la conformité réglementaire. S'assurer que la sécurité répond aux besoins de l'entreprise, sans la contraindre. Utiliser des cadres pour évaluer le risque, calculer le coût de ce risque et déterminer où les contrôles doivent être placés pour obtenir le meilleur effet, tout en s'assurant que les contrôles que vous avez sélectionnés font leur travail efficacement.

Nous mettons notre expertise à votre disposition concernant :

- Évaluer les risques
- Définir les contrôles les plus efficaces
- Développer des politiques et des processus
- Experts intégrés à tous les niveaux de l'organisation jusqu'au niveau RSSI
- Embedded experts at all levels of the organisation up to CISO level

- **NIS / NIS2**
- **Acte EU AI**
- **Cyber Essentials/+**
- **NIST CSF**
- **DORA**
- **ISO27001**
- **CIS18**
- **PCI-DSS**

Identité et accès

Le management des identités et des accès est un aspect crucial de la cybersécurité pour les entreprises, englobant les processus et les technologies utilisés pour gérer et sécuriser les identités numériques et contrôler l'accès aux ressources. Les organisations sont confrontées à des défis pour garantir des pratiques de gestion des identités et des accès sécurisées et efficaces, telles que la gestion des identités des utilisateurs sur plusieurs systèmes, l'application des contrôles d'accès à moindre privilège et la prévention des accès non autorisés.

C'est là qu'une solution de gestion des identités et des accès déployée sur vos piliers de technologie fournit une cybersolution solide et complète.

Nous vous aidons en vous concentrant sur l'identification et l'atténuation des domaines de risque, puis nous vous aidons à créer des solutions rentables qui répondent aux exigences des politiques et processus de votre organisation. Profitez d'une sécurité renforcée, de risques réduits et d'une efficacité accrue grâce à la démarche d'Insight adaptée à votre entreprise.

Comment nous y parvenons ?

- Nous vous accompagnons sur la voie du Zero Trust
- Adopter une approche axée sur l'entreprise concernant l'accès aux données et aux applications
- S'assurer que les bonnes personnes ont accès à vos applications et données.

Détection et réponse aux menaces

La détection et la réponse aux menaces sont des éléments essentiels d'une stratégie de cybersécurité solide pour les entreprises. Les organisations sont confrontées à une myriade de défis pour identifier et atténuer les cybermenaces, notamment la nature évolutive des attaques, la complexité des environnements informatiques et la pénurie de professionnels de la cybersécurité qualifiés. Une détection efficace des menaces nécessite une surveillance en temps réel, une analyse des événements de sécurité et une réponse rapide aux incidents pour minimiser l'impact des violations de sécurité.

Les experts en sécurité d'Insight peuvent vous aider à adopter une approche multicouche des solutions de détection et de réponse aux menaces dans tous les domaines de la technologie de votre entreprise.

Nous créons des solutions à l'aide d'outils et de technologies de pointe, ainsi que du savoir-faire de nos consultants en sécurité, afin d'identifier et d'atténuer les risques avant qu'ils ne causent des dommages significatifs à votre entreprise. En utilisant des technologies telles que SIEM et XDR, complétées par des analystes de sécurité pour rassembler les grandes quantités de données générées par vos outils de sécurité afin de prendre des décisions intelligentes sur les menaces qui pèsent sur l'ensemble de votre parc informatique.

Nous pouvons vous aider à :

- Identifier les menaces plus tôt
- Réduire les risques sur l'ensemble de votre réseau
- Vous fournir des informations exploitables sur les menaces
- Automatiser la défense contre les menaces

Facteurs humains

Même si l'infrastructure, les outils et les contrôles de sécurité sont constamment améliorés et font l'objet d'investissements, des violations se produisent toujours, et il n'est pas facile de les identifier et de les résoudre. Il existe de nombreux contrôles de sécurité spécialisés pour différents types de menaces, des attaques sur les terminaux aux attaques sur les chaînes d'approvisionnement, mais lorsque vous examinez comment ces attaques se sont réellement produites, les trois principales raisons sont les suivantes :

- **Mot de passe**
- **Phishing**
- **Correctifs**

Les équipes informatiques peuvent utiliser la technologie pour réduire le risque de violations, mais les utilisateurs finaux joueront toujours un rôle dans le support de la sécurité d'une organisation. Les équipes IT se concentrent souvent sur la technologie,
et parfois sur le processus, et oublient l'aspect humain, alors que c'est lui qui peut déterminer l'échec ou la réussite d'un projet.

Donnez à vos collaborateurs les moyens de devenir une première ligne de défense impénétrable contre les cybermenaces avec Insight. En adoptant une approche centrée sur l'humain, nous pouvons vous aider à traiter les vulnérabilités de front, en renforçant votre posture de sécurité et en minimisant les risques.

Nous vous aiderons à :

- Améliorer la sensibilisation des utilisateurs finaux à la cybersécurité.
- Fournir une formation aux développeurs sur la manière de coder en gardant la sécurité à l'esprit.
- Assurez-vous que vos administrateurs disposent des compétences nécessaires pour détecter et répondre à une cyberattaque.
- Réduisez les risques d'attaques réussies.
- Réduisez les coûts en évitant les violations de données.

Sécurité managés

Les défis de sécurité sont incessants, les organisations étant confrontées à une augmentation des cybermenaces, des tentatives de piratage sophistiquées aux attaques par ransomware insidieuses. Les entreprises doivent faire face à des exigences de conformité réglementaires complexes, protéger les données sensibles et garder une longueur d'avance sur les risques de cybersécurité en constante évolution. Les solutions de sécurité fournissent de nombreuses alertes et alarmes, mais il est essentiel de savoir sur quelles alertes et alarmes réagir en cas d'urgence pour éviter de nuire davantage à votre entreprise.

Ces défis combinés créent le besoin de fournir des solutions de cybersécurité complètes et proactives pour protéger les entreprises des diverses menaces sophistiquées auxquelles elles sont confrontées au quotidien. La préparation et la résilience en matière de cybersécurité sont essentielles pour protéger la pérennité et le succès de toute entreprise moderne.

C'est là qu'Insight peut vous aider : notre équipe d'experts en sécurité expérimentés est disponible pour vous aider à améliorer votre cybersécurité grâce à une surveillance, une détection et une réaction proactives aux menaces avec un accès à des technologies de pointe.

- Détection et réponse des terminaux managés (MEDR) Couvrant les ordinateurs portables, les ordinateurs de bureau et les appareils mobiles.
- Détection et réponse étendues managées (MXDR) Réunissant des journaux et des flux provenant d'un large éventail de sources, il offre la capacité de détection la plus robuste pour votre environnement.

Combinant des technologies telles que l'IA, l'intelligence des menaces et l'analyse, notre équipe d'analystes experts en sécurité est capable de détecter et de réagir aux menaces pesant sur votre envCiroonmnemememennt tn eno tus e ymp psa rréveel. nons ?

Comment nous y parvenons ?

- Gestion proactive des menaces.
- Expertise en matière d'analyse de la sécurité et de réponse aux incidents.
- Accès à des technologies de sécurité avancées.
- Stratégie de sécurité et orientation de la feuille de route.
- Modèle évolutif et rentable.

Notre démarche

Nous vous aidons à élaborer une stratégie, à mettre en œuvre et à gérer des solutions de sécurité informatique évolutives.

Évaluation

- Hous aider à obtenir l'accréditation selon des cadres industriels tels que ISO27001 ou NIS2
- Examinez vos contrôles de sécurité existants et identifiez les risques résiduels
- Aidez à créer une feuille de route hiérarchisée pour atteindre le niveau de sécurité souhaité

Planification et conception

- Aider à traduire vos défis commerciaux en projets de sécurité
- Support et conseils pour sélectionner les fournisseurs, produits et services appropriés
- Ateliers de vision et conception technique

Construire et mettre en œuvre

- Toncrétisez vos projets – de la conception aux contrôles de sécurité entièrement construits et documentés
- Insight considère chaque projet dans le contexte de votre feuille de route globale
- Transfert à vos équipes internes pour le management ou la transition vers nos services managés

Centre des opérations de sécurité

- Les services de support services maintiennent vos contrôles de sécurité en parfait état de fonctionnement
- Services managés où Insight assume la responsabilité de vos contrôles de sécurité

Nos partenaires en matière de technologie de sécurité

La modernisation informatique est un effort d'équipe. Nous réunissons les capacités de + de 6 000 partenaires et éditeurs de logiciels, de matériel informatique et de cloud avec l'expertise approfondie de notre équipe au même endroit pour créer les meilleures solutions de leur catégorie qui accélèrent votre parcours de transformation.

Nous travaillons directement avec des entreprises technologiques de premier plan afin que vous puissiez bénéficier :

- Un point de contact unique pour accéder aux derniers produits et solutions technologiques.
- · Un écosystème d'équipes collaboratives et hautement qualifiées pour équiper et gérer votre environnement informatique.
- · Tarification compétitive et négociation rationalisée des contrats.
- · Des solutions indépendantes des partenaires adaptées à vos besoins spécifiques.
- · Partner-agnostic solutions tailored to your specific needs.

Microsoft · Cisco · aws · Google · paloalto NETWORKS · KnowBe4 · Barracuda · Check Point SOFTWARE TECHNOLOGIES LTD. · FORTINET

Pourquoi engager un partenariat avec Insight ?

La cybersécurité est compliquée et exige une approche tout-en-un de la part de vos utilisateurs finaux, de vos équipes de sécurité et de vos outils. C'est pourquoi nous avons mis au point des méthodes reproductibles et des processus éprouvés qui donnent des résultats satisfaisants. Nos experts vous guideront de bout en bout, ce qui vous permettra d'améliorer l'efficacité et l'alignement stratégique.

Nous avons :

+ de 20 ans de connaissances et d'expérience dans la transformation de la sécurité

Partenariats étroits avec les meilleurs fournisseurs

Une approche indépendante des solutions pour trouver les solutions les mieux adaptées à vos besoins.

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Cisco Partner

Advanced Security Architecture Specialized
SASE Specialized
XDR Specialized

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Identity and Access Management
Information Protection & Governance
Threat Protection

Gold Microsoft Partner
Microsoft
Azure Expert MSP

Microsoft Solutions Partner
Microsoft Cloud

Étapes suivantes

Contactez Insight pour améliorer votre stratégie de cybersécurité et vos opérations quotidiennes. Avec l'augmentation des menaces à la cybersécurité, la protection de votre entreprise est cruciale pour la continuité et le succès. Notre approche complète améliore la posture de cybersécurité, identifie et atténue les risques, rationalise les opérations, optimise les contrôles de sécurité, tout en maximisant les investissements. Faites confiance aux méthodes éprouvées et aux conseils d'experts d'Insight pour renforcer vos défenses de cybersécurité et stimuler la résilience et la croissance de votre entreprise.

- **fr.insight.com**
- **01 30 67 25 00**