ISG Provider Lens®

Cybersécurité — Services et Solutions

Analyse du marché de la cybersécurité et comparaison de l'attractivité et des avantages concurrentiels des portefeuilles des prestataires

BROCHURE | JANVIER 2026 | AUSTRALIE, BRÉSIL, FRANCE, ALLEMAGNE, SUISSE, ROYAUME-UNI, ÉTATS-UNIS ET SECTEUR PUBLIC AMÉRICAIN

Table des Matières

Introduction

En 2026, le paysage de la cybersécurité devrait connaître une augmentation de la sophistication des menaces, un renforcement des exigences réglementaires et une transition rapide vers des modèles de défense basés sur le renseignement. Les entreprises de tous les secteurs sont soumises à une pression croissante pour sécuriser leurs architectures de plus en plus distribuées, protéger les données sensibles dans les environnements hybrides et répondre à la recrudescence des attaques basées sur l'IA. Parallèlement, les conseils d'administration et les régulateurs recherchent une cyber-résilience démontrable et une efficacité des contrôles vérifiable, ouvrant la voie à des programmes de sécurité intégrés aux programmes de transformation numérique.

Dans ce contexte, le marché se réorganise en domaines de compétences clairement définis. Alors que les services techniques de sécurité (TSS) garantissent l'intégrité de la configuration, la sécurité des implémentations et le renforcement continu, les services stratégiques de sécurité (SSS) gagnent en importance, les dirigeants accordant la priorité à la cybersécurité en matière de gouvernance, de gestion des risques et d'alignement architectural.

Les SOC de nouvelle génération et les services de détection et de réponse gérés (MDR) gagnent également en popularité, sous l'impulsion de la demande de surveillance des menaces 24 heures sur 24, 7 jours sur 7, d'analyses assistées par l'IA et de modèles de réponse basés sur les résultats. En outre, la gestion des vulnérabilités basée sur les risques renforce la sécurité préventive en hiérarchisant les expositions à l'aide d'informations sur le contexte de l'entreprise et les voies d'attaque. Enfin, le conseil en cryptographie post-quantique fait son entrée sur le marché, les organisations commençant à préparer des inventaires cryptographiques et des stratégies de transition afin de garantir la confidentialité des données à long terme.

Cette étude IPL couvre, entre autres, les domaines de compétences mentionnés et offre une vue d'ensemble de la manière dont les prestataires se différencient dans un environnement caractérisé par la rapidité, l'intelligence et la résilience.

Domaines d'intérêt clés pour la cybersécurité — Services et solutions 2026.

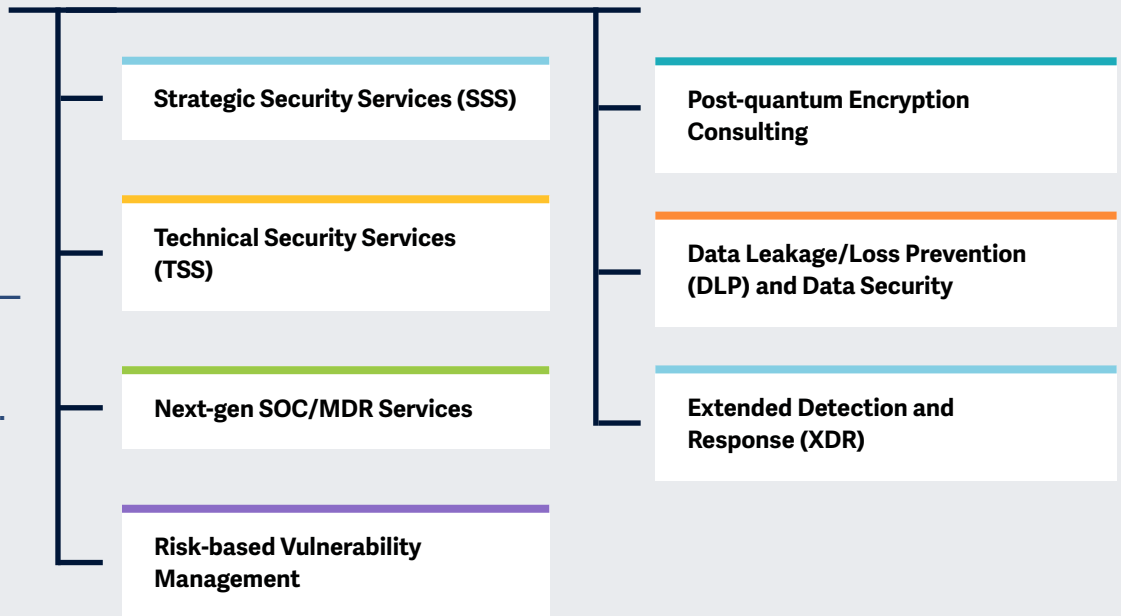


Illustration simplifiée Source: ISG 2026

L'étude ISG Provider Lens® Cybersécurité — Services et Solutions offre aux décideurs commerciaux et informatiques les éléments suivants :

- Une transparence sur les forces et les faiblesses des prestataires concernés.
- Un positionnement différencié des prestataires par segment en fonction de leurs atouts concurrentiels et de l'attractivité de leur portefeuille.
- Un focus sur différents marchés, notamment l'Australie, le Brésil, la France, l'Allemagne, la Suisse, le Royaume-Uni, les États-Unis et le secteur public américain.
- Des caractéristiques spécifiques à chaque pays : conseil en cryptographie post-quantique en Allemagne et aux États-Unis, analyse XDR et gestion des vulnérabilités basée sur les risques au Brésil, et analyse DLP en Allemagne.

Notre étude sert de base décisionnelle importante pour le positionnement, les relations clés et les considérations relatives à la mise sur le marché. Les conseillers ISG et les entreprises clientes utilisent également les informations contenues dans ces rapports pour évaluer leurs relations actuelles avec leurs prestataires et leurs engagements potentiels.

Définition

Ce quadrant évalue les prestataires qui fournissent des services de conseil en cybersécurité, en mettant l'accent sur la stratégie, la gouvernance, la gestion des risques et la transformation organisationnelle pour les environnements IT et OT. Ces prestataires évaluent la maturité, quantifient les risques, définissent des modèles opérationnels cibles et élaborent des stratégies, des politiques et des feuilles de route alignées sur les objectifs commerciaux et les exigences réglementaires. Leurs offres comprennent des audits, des évaluations, des programmes de sensibilisation à la sécurité, la planification de la continuité des activités, des exercices de simulation et des conseils sur le choix des technologies. Ces prestataires emploient également des consultants expérimentés qui guident les entreprises dans la conception de programmes, l'amélioration de la gouvernance et le développement des capacités, y compris des services de RSSI virtuel (vCISO) pour un leadership stratégique continu ou à la demande. Contrairement aux TSS, qui mettent l'accent sur l'intégration pratique, les prestataires SSS se concentrent sur le conseil plutôt que sur la surveillance opérationnelle ou la gestion de produits propriétaires.

Critères d'éligibilité

1. Fournir **des services de conseil en sécurité, indépendants des éditeurs**, couvrant l'évaluation de la maturité, l'élaboration de stratégies, la conception de politiques, les modèles de gouvernance et la création de feuilles de route.
2. Démontrer des capacités dans des domaines stratégiques tels que la quantification des risques, la préparation réglementaire, la sélection de solutions, la planification de la continuité des activités et le conseil en matière de cyber-risques au sens large.
3. **Appliquer des cadres reconnus** et se conformer aux normes (telles que ISO 27000, NIST CSF, CIS Controls) lors de l'orientation de programmes d'entreprise.
4. **Fournir au moins l'un** des services stratégiques de sécurité ci-dessus dans la région cible par l'intermédiaire de consultants **qualifiés et certifiés.**
5. Présenter **des preuves documentées d'engagements** qui ont amélioré la posture de sécurité, les structures de gouvernance, la conformité réglementaire ou la prise de décision basée sur les risques des clients.
6. Fournir **des méthodologies de conseil structurées**, des modèles ou des guides pour les évaluations, la planification stratégique ou la transformation organisationnelle.
7. Opérer en tant que **prestataires de services axés sur le conseil** plutôt que comme éditeurs, tout en autorisant l'utilisation de cadres ou d'outils propriétaires qui facilitent la prestation de services de conseil.
8. **Ne pas** se concentrer exclusivement sur des produits propriétaires.

Définition

Ce quadrant évalue les prestataires de services qui conçoivent, intègrent, mettent en œuvre et modernisent les technologies de sécurité IT et OT. Leurs services comprennent le déploiement et la configuration d'architectures de contrôle de sécurité pour la gestion des identités et des accès, le cloud et les centres de données, le SASE/SSE, les terminaux, les réseaux, les systèmes OT et de contrôle industriel (ICS) et les domaines connexes. Les prestataires utilisent des architectures de référence, des cadres d'automatisation et des accélérateurs propriétaires pour proposer des transformations axées sur l'ingénierie qui rationalisent la mise en œuvre et améliorent l'efficacité des contrôles. Ils entretiennent des partenariats solides avec des éditeurs de sécurité, détiennent des certifications spécialisées et prennent en charge des tâches tout au long du cycle de vie, telles que le renforcement, la configuration, l'application de correctifs et la gestion des appareils. Contrairement aux SSS, qui se concentrent sur le conseil et la gouvernance, les fournisseurs de TSS mettent l'accent sur l'exécution technique pratique. Ils ne proposent pas de surveillance basée sur un SOC ni d'opérations MDR, mais peuvent fournir des services de sécurité gérés traditionnels.

Critères d'éligibilité

1. Démontrer une expérience dans la conception, l'intégration et **la mise en œuvre** de technologies de sécurité IT et/ou OT, étayée par des certifications multi-éditeurs et des partenariats OEM.
2. Déployer **des accélérateurs, des ensembles d'outils propriétaires ou des architectures de référence** qui améliorent la qualité de la mise en œuvre, l'interopérabilité et le délai de rentabilisation.
3. Employer des ingénieurs et **des architectes certifiés**, compétents dans la configuration, la personnalisation et l'optimisation de solutions de sécurité dans les environnements cloud, réseaux, terminaux et OT.
4. Adopter une **approche structurée et méthodologique** pour intégrer des technologies de sécurité qui répondent aux exigences des clients, aux profils de risque et aux contraintes architecturales
5. Fournir **des services d'ingénierie du cycle de vie** tels que la gestion de la configuration, l'ajustement des politiques, l'application de correctifs, le renforcement des contrôles et la modernisation technologique.
6. Présenter **des études de cas** documentées démontrant des déploiements ou des transformations réussis de technologies de sécurité dans la région cible.
7. Opérer en tant **qu'intégrateurs** plutôt que comme des éditeurs de logiciels indépendants, en autorisant les accélérateurs propriétaires ou les outils développés en interne pour la livraison de services.
8. **Ne pas** se concentrer exclusivement sur des produits propriétaires.

Définition

Ce quadrant évalue les prestataires qui offrent des services de surveillance continue et de MDR par le biais de SOC. Leurs offres couvrent l'ensemble du cycle de vie des incidents, y compris la détection, le triage, l'investigation numérique, le confinement et la remédiation coordonnée. Les prestataires intègrent et exploitent des technologies de sécurité modernes, utilisent des informations sur les menaces et des analyses avancées, et fournissent une recherche de menaces automatisée et pilotée par des experts afin de renforcer la résilience des entreprises. Les services SOC/MDR de nouvelle génération combinent des opérations de sécurité gérées avec des analyses innovantes basées sur l'IA, un triage autonome et des capacités d'automatisation et d'orchestration (SOAR) afin de réduire les temps de réponse et d'améliorer la visibilité des menaces dans les environnements IT et OT. Ils prennent en charge les modèles co-gérés et ne se concentrent pas sur le conseil stratégique ou l'exécution de la mise en œuvre technologique, qui relèvent respectivement du champ d'application des SSS et des TSS.

Critères d'éligibilité

1. Fournir des services de surveillance, **de détection et d'intervention** 24 heures sur 24, 7 jours sur 7, via des SOC propriétaires, couvrant les environnements IT et/ou OT.
2. Fournir **des capacités spécifiques au MDR**, notamment l'analyse comportementale, l'intégration de renseignements sur les menaces tenant compte des modèles linguistiques à grande échelle (LLM), la recherche de menaces automatisée et dirigée par des humains, et l'ingénierie de détection avancée.
3. **Exploiter et gérer les outils** de gestion des informations et des événements de sécurité (SIEM), le SOAR, la détection et la réponse aux incidents au niveau des terminaux (EDR), la détection et la réponse au niveau du réseau (NDR) et d'autres technologies de sécurité pertinentes, avec le soutien d'accréditations OEM.
4. Démontrer une **approche** structurée **de réponse aux incidents** couvrant le triage, l'investigation numérique, le confinement, la coordination des mesures correctives et l'amélioration post-incident.
5. Utiliser des analyses **basées sur l'IA**, des agents de triage autonomes et des workflows SOAR pour accélérer la détection et réduire le temps moyen de réponse (MTTR).
6. Proposer **des modèles de services co-gérés** avec les équipes de l'entreprise, permettant une visibilité partagée, une collaboration entre analystes et des processus de réponse joints.
7. Présenter **des cas de référence** montrant des améliorations mesurables en matière de couverture de détection, d'efficacité de réponse ou de résilience opérationnelle dans la région cible.
8. **Ne pas** se concentrer exclusivement sur des produits propriétaires, mais gérer et exploiter les meilleurs outils de sécurité.

Définition

Ce quadrant évalue les prestataires qui offrent des services continus de gestion des vulnérabilités basée sur les risques dans les environnements informatiques, cloud, applicatifs et d'infrastructure numérique. Ces prestataires identifient, évaluent et hiérarchisent les vulnérabilités en fonction de leur exploitabilité, de leur exposition et de leur impact sur l'activité, plutôt que sur la seule base de leur gravité. Leurs services combinent la découverte automatisée, les tests de pénétration, les tests de sécurité des applications et l'analyse contextuelle des risques afin de faire face à des techniques d'attaque en constante évolution, notamment celles accélérées par l'IA générative, et à l'augmentation des activités de ransomware. La gestion des vulnérabilités basée sur les risques facilite la visibilité continue des actifs internes et exposés à Internet, permet de hiérarchiser les mesures correctives en fonction des voies d'attaque réelles et de la criticité pour l'entreprise, et aide les entreprises à réduire leur exposition dans des environnements technologiques en rapide évolution grâce à l'observabilité continue, l'évaluation, les nouveaux tests et le recalibrage des risques.

Critères d'éligibilité

1. Fournir **des services d'évaluation continue des vulnérabilités** qui hiérarchisent les résultats en fonction de leur exploitabilité, de leur exposition et de leur impact sur l'activité de l'entreprise, et non pas uniquement en fonction de mesures statiques de gravité.
2. Fournir **des services de test** pour les applications web et mobiles, les API, les réseaux internes, les environnements cloud (conteneurs), l'IoT et autres actifs exposés.
3. Appliquer **des méthodes de test reconnues** telles que les tests d'intrusion, les tests de sécurité dynamiques des applications (DAST), les tests de sécurité statiques des applications (SAST) , les tests de sécurité interactifs des applications (IAST) et les techniques connexes combinant des outils automatisés et une validation manuelle par des experts.
4. Aligner **les résultats et les rapports sur les vulnérabilités** avec les normes et cadres pertinents tels que ISO 27001, NIST SP 800-53, PCI DSS, SOC 2 et bien d'autres, les exigences réglementaires applicables et les exigences spécifiques au secteur d'activité.
5. Proposer **de nouveaux tests, un suivi des mesures correctives et une réévaluation continue des risques** afin de refléter les changements en matière d'exposition, de renseignements sur les menaces et de progrès en matière d'atténuation.
6. Employer **des professionnels de sécurité** tels que des hackers éthiques (CEH), des professionnels certifiés en sécurité offensive (OSCP) et des professionnels de la sécurité des systèmes d'information (CISSP), ainsi que des experts titulaires des certifications CompTIA PenTest+ ou GIAC, afin de garantir une qualité de service constante.

Définition

Ce quadrant évalue les prestataires de services de conseil qui aident les entreprises à se préparer et à mettre en œuvre la transition cryptographique nécessaire pour atténuer les risques liés à l'informatique quantique. Ces prestataires évaluent les dépendances cryptographiques dans les environnements IT, OT, IoT et de la chaîne d'approvisionnement numérique, y compris la gestion des stocks, l'identification des algorithmes vulnérables à l'informatique quantique et l'exposition aux menaces de collecte immédiate et de décryptage ultérieur. Ils élaborent des stratégies de cryptographie post-quantique (PQC) basées sur les risques, conçoivent des feuilles de route pour la migration et la cryptographie hybride, et fournissent des conseils sur l'adoption des nouvelles normes post-quantiques alignées sur celles du National Institute of Standards and Technology (NIST), du Federal Office for Information Security (BSI) et d'autres organismes de réglementation. Le conseil en PQC aborde les impacts sur la gestion des clés, les systèmes d'identité, les communications, les applications et les architectures d'infrastructure, permettant aux organisations de planifier des transformations cryptographiques conformes, évolutives et résilientes pour l'avenir.

Critères d'éligibilité

1. Réaliser **des évaluations des risques cryptographiques et quantiques,** y compris l'inventaire des actifs cryptographiques, des algorithmes et de l'utilisation des clés dans les environnements IT, OT, IoT, cloud, réseau et applicatifs.
2. Démontrer **des capacités de conseil en matière d'élaboration de stratégies PQC**, y compris des feuilles de route de migration par étapes, la planification de la cryptographie hybride et l'analyse des dépendances.
3. Fournir des services de conseil alignés sur **les normes et les directives émergentes** telles que NIST PQC, BSI TR-02102, l'Institut européen des normes de télécommunication (ETSI) et les mandats ISO/IEC pertinents.
4. Évaluer les **impacts sur la gestion des clés**, l'infrastructure à clé publique (PKI), les systèmes d'identité et d'accès, les communications sécurisées et les architectures d'applications.
5. Présenter des preuves **d'engagements clients**, de projets pilotes, de simulations ou de PoC **liés à la PQC** visant à réduire les risques liés au quantique.
6. Offrir des services de conseil indépendants des éditeurs tout en démontrant une connaissance des écosystèmes technologiques pertinents et des implémentations cryptographiques.
7. **Soutenir la conformité** aux mandats gouvernementaux et atteindre les objectifs des initiatives de transition cryptographique spécifiques à un secteur ou nationales.

Data Leakage/Loss Prevention (DLP) and Data Security

Définition

Ce quadrant évalue les éditeurs de logiciels indépendants (ISV) qui développent des solutions propriétaires de DLP et de sécurité des données fournies sous forme de logiciels sur site, de plateformes cloud ou de SaaS. Ces produits permettent la découverte, la classification et la surveillance des données sensibles sur les terminaux, les réseaux, les services cloud et les systèmes de stockage, et appliquent des contrôles basés sur des politiques pour empêcher tout accès non autorisé ou toute exfiltration. Les technologies DLP modernes intègrent de plus en plus le renforcement des appareils, le contrôle des applications et l'analyse comportementale afin d'empêcher l'utilisation abusive des données au niveau des terminaux et d'appliquer les politiques, même dans des environnements hors ligne ou non gérés. Elles fournissent une gouvernance centralisée, des rapports et une assistance en matière de conformité afin de protéger les données structurées et non structurées tout au long de leur cycle de vie. Dans un environnement informatique distribué présentant des risques accrus de violations internes et de flux de données, ces solutions constituent une protection essentielle pour protéger les actifs informationnels critiques et garantir des pratiques cohérentes en matière de traitement des données.

Critères d'éligibilité

1. Fournir un **produit DLP ou de sécurité des données propriétaire** (pas de moteurs DLP tiers intégrés).
2. **Prise en charge des architectures de base** telles que les environnements de terminaux, de réseau, de cloud et de stockage.
3. **Détecter, classer et protéger** les données structurées et non structurées au repos et en transit.
4. Offrir **des fonctions de gestion centralisée**, notamment des contrôles de politique, des rapports et des configurations.
5. **Permettre** la découverte des données, la surveillance en temps réel et les mesures d'application basées sur des politiques.
6. **Démontrer** des déploiements à l'échelle de l'entreprise et une adoption documentée par les clients.

Définition

Ce quadrant évalue les éditeurs de logiciels indépendants (ISV) qui développent des plateformes XDR propriétaires intégrant des capacités de télémétrie, d'analyse et de réponse sur les terminaux, les réseaux, les identités, les charges de travail cloud et les applications. Ces solutions corrèlent et contextualisent les données provenant de multiples contrôles de sécurité afin d'améliorer la précision de la détection, de réduire la fatigue liée aux alertes et de renforcer l'efficacité opérationnelle. Les plateformes XDR modernes unifient la visibilité des menaces dans une interface unique, appliquent des analyses comportementales et du ML, et automatisent les actions de réponse en fonction de la gravité et du contexte de l'entreprise. Elles fonctionnent comme des architectures cloud ou hybrides avec une couche de capteurs frontale définie et un moteur d'analyse et d'orchestration en back-end. Alors que les entreprises cherchent à consolider leurs outils et à améliorer la maturité de la détection, le XDR sert de base stratégique pour une défense coordonnée et axée sur le renseignement.

Critères d'éligibilité

1. Fournir une **plateforme XDR propriétaire** (sans dépendre de moteurs XDR tiers).
2. Inclure une **interface XDR définie** (intégration multi-capteurs) et un back-end XDR (analyse, corrélation et orchestration).
3. **Intégrer au moins trois** capteurs natifs ou étroitement couplés, par exemple EDR/plateforme de protection des terminaux (EPP), NDR, identité, messagerie électronique, protection des charges de travail mobiles ou cloud.
4. Offrir **une visibilité unifiée** sur les terminaux, les réseaux et les environnements cloud.
5. Démontrer sa **capacité à détecter et à bloquer les menaces sophistiquées telles** que les menaces persistantes avancées (APT), les ransomwares et les logiciels malveillants avancés.
6. **Utiliser les renseignements sur les menaces**, l'analyse comportementale et les corrélations télémétriques en temps réel.
7. Fournir des mesures de réponse **automatisées ou semi-automatisées** ayant un impact mesurable.

Quadrants par régions

Dans le cadre de cette étude ISG Provider Lens®, nous présentons les sept quadrants suivants sur la cybersécurité — Services et solutions 2026

Quadrant	Australie	Brésil	France	Allemagne	Suisse	Royaume-Uni	États-Unis	Secteur public américain
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	Grandes et moyennes entreprises	Grandes et moyennes entreprises	✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	Grandes et moyennes entreprises	Grandes et moyennes entreprises	✓
Next-gen SOC/MDR Services	✓	Grandes et moyennes entreprises	✓	Grandes et moyennes entreprises	Grandes et moyennes entreprises	Grandes et moyennes entreprises	Grandes et moyennes entreprises	✓
Risk-based Vulnerability Management		✓						
Post-quantum Encryption Consulting				✓			✓	
Data Leakage/Loss Prevention (DLP) and Data Security				✓				
Extended Detection and Response (XDR)		✓						

La phase de recherche se déroulera entre janvier et juin 2026, période pendant laquelle l'enquête, l'évaluation, l'analyse et la validation auront lieu. Les résultats seront publiés en juillet 2026.

Étapes	Début	Fin
Lancement de l'enquête	7 janvier 2026	
Phase d'enquête	7 janvier 2026	13 février 2026
Webinaire	12 janvier 2026	
Avant-première	Mai 2026	Juin 2026
Communiqué de presse et publication	Juillet 2026	

Veuillez vous référer à l'agenda de recherche **ISG Provider Lens® 2026** pour consulter et télécharger la liste des autres études menées par ISG Provider Lens®.

Accès au portail en ligne

Vous pouvez consulter/télécharger le questionnaire ici en utilisant les identifiants que vous avez déjà créés, ou vous référer aux instructions contenues dans l'e-mail d'invitation pour générer un nouveau mot de passe. Nous nous réjouissons de votre participation !

Guide d'achat

ISG Software Research, anciennement « Ventana Research », offre des informations sur le marché en évaluant les fournisseurs de technologies et les produits à travers ses guides d'achat. Les conclusions sont tirées de l'analyse basée sur la recherche des catégories de produits et d'expérience client, du classement et de l'évaluation des éditeurs de logiciels afin de faciliter la prise de décision et les processus de sélection en matière de technologie.

Dans le cadre du lancement de l'IPL Cybersecurity — Services and Solutions, nous souhaitons profiter de l'occasion pour attirer votre attention sur les recherches et les informations connexes qu'ISG Research publiera en 2026. Pour plus d'informations, consultez le calendrier de recherche du guide d'achat.

Avertissement concernant la production de recherches

ISG collecte des données dans le but de mener des recherches et de créer des profils de prestataires/éditeurs. Les profils et les données à l'appui sont utilisés par les conseillers ISG pour formuler des recommandations et informer leurs clients de l'expérience et des qualifications de tout prestataire/éditeur applicable pour l'externalisation des tâches identifiées par les clients. Ces données sont collectées dans le cadre du processus ISG FutureSource™ et du processus de qualification des prestataires candidats (CPQ). ISG peut choisir de n'utiliser ces données collectées que pour certains pays ou certaines régions à des fins de formation et d'information de ses conseillers, sans produire de rapports ISG Provider Lens®. Ces décisions seront prises en fonction du niveau et de l'exhaustivité des informations reçues directement des prestataires et de la disponibilité d'analystes expérimentés pour ces pays ou régions. Les informations soumises peuvent également être utilisées pour des projets de recherche individuels ou pour des notes d'information qui seront rédigées par les analystes principaux.

ISG Star of Excellence™ - Appel à candidatures

Star of Excellence™ est une reconnaissance indépendante de l'excellence de la prestation de services basée sur le concept de la voix du client. ISG a conçu le programme Star of Excellence pour recueillir les retours des clients sur la capacité des prestataires de services à démontrer les plus hauts standards d'excellence et d'orientation client.

L'enquête globale porte sur les services associés aux études IPL. Par conséquent, tous les analystes de l'EIG reçoivent en permanence des informations sur l'expérience des clients de tous les prestataires de services concernés. Ces informations viennent s'ajouter aux commentaires de première main des conseillers que l'IPL exploite dans le cadre de son approche de conseil axée sur les praticiens.

Les prestataires sont invités à proposer la participation de leurs clients. Une fois la candidature soumise, l'EIG envoie un courrier de confirmation aux deux parties. Il va de soi que l'EIG rend anonymes toutes les données relatives aux clients et qu'il ne les divulgue pas à des tiers.

Nous souhaitons que Star of Excellence™ soit reconnue comme la référence du secteur en matière de reconnaissance de l'excellence du service à la clientèle, ainsi qu'un baromètre fiable pour mesurer la satisfaction des clients. Pour vous assurer que les clients que vous avez sélectionnés soumettent leurs retours concernant votre prestation, veuillez utiliser la section « Nominate (for Providers) » sur le site web de Star of Excellence.

Nous avons mis en place une adresse électronique dédiée pour vos questions et commentaires. Cette boîte est consultée quotidiennement. Veuillez prévoir un délai de réponse pouvant aller jusqu'à 24 heures.

Voici l'adresse électronique :
star@cx.isg-one.com

ISG Star of Excellence

L'étude ISG Provider Lens® Cybersecurity — Services and Solutions analyse les fournisseurs de logiciels/fournisseurs de services pertinents en France, sur la base d'un processus de recherche et d'analyse à plusieurs phases, et positionne ces fournisseurs selon la méthodologie ISG Research.

Commanditaire de l'étude
Heiko Henkes

Auteurs Principaux:
Andrew Milroy, Benoit Scheuber, Bhuvaneshwari Mohan, Frank Heuer, João Mauro, Yash Jethani

Rédacteurs en Chef:
Monica K and Rafael Rigotti

Chef De Projet:
Shreemadhu Rai B

Information Services Group Inc. est seul responsable du contenu de ce rapport. Sauf mention contraire, tout le contenu, y compris les illustrations, la recherche, les conclusions, les affirmations et les positions contenues dans ce rapport ont été développées par, et sont la propriété exclusive de Information Services Group Inc.

La recherche et l'analyse présentées dans cette étude comprendront des données provenant du programme ISG Provider Lens™, des programmes de recherche ISG en cours, d'entretiens avec des conseillers ISG, de briefings avec des fournisseurs de services et d'analyses d'informations de marché publiquement disponibles provenant de sources multiples. L'ISG a conscience des délais et des développements possibles du marché entre la phase de recherche et la publication, en termes de fusions et d'acquisitions, et sait que les rapports de cette étude ne pourront refléter ces changements.

Toutes les références de revenus sont en dollars américains ($US), sauf indication contraire.

Contacts pour cette étude

Promoteur de l'étude

Heiko Henkes

Directeur et Analyste Principal

Frank Heuer

Analyste Principal – Allemagne, Suisse

Bhuvaneshwari Mohan

Analyste Principal – Royaume-Uni, Secteur Public Américain

Yash Jethani

Analyste Principal – États-Unis

Benoit Scheuber

Analyste Principal – France

Andrew Milroy

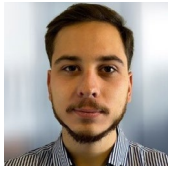
Analyste Principal – Australie

João Mauro

Analyste Principal – Brésil

Monica K

Analyste de Recherche



Rafael Rigotti

Analyste de Recherche

Rajesh Chillappagari

Analyste de données

Laxmi Sahebrao Kadve

Analyste de données

Shreemadhu Rai B

Chef de Projet

La participation de conseillers au programme ISG Provider Lens®

ISG Provider Lens® propose des évaluations de marché intégrant les connaissances pratiques, reflétant l'orientation régionale et la recherche indépendante. ISG veille à ce que des conseillers participent à chaque étude afin de couvrir les détails du marché appropriés, en fonction des gammes de services/tendances technologiques, de la présence des prestataires de services et du contexte de l'entreprise.

Dans chaque région, ISG dispose d'experts et de conseillers respectés qui connaissent les portefeuilles et les offres des prestataires, ainsi que les exigences des entreprises et les tendances du marché. En moyenne, trois conseillers consultants participent au processus d'examen de la qualité et de la cohérence de chaque étude.

Les conseillers consultants veillent à ce que chaque étude reflète l'expérience des conseillers ISG dans le domaine, ce qui complète les recherches primaires et secondaires menées par les analystes. Les conseillers ISG participent à chaque étude au sein du groupe de conseillers consultants et apportent leur contribution à différents niveaux en fonction de leur disponibilité et de leur expertise.

Les conseillers consultants :

- aident à définir et à valider les quadrants et les questionnaires,
- donnent des conseils sur l'inclusion des prestataires de services et participent aux réunions d'information,
- donnent leur point de vue sur les évaluations des prestataires de services et examinent les projets de rapports.

Conseillers de l'EIG pour cette étude

Doug
Saylors

Associé, Responsable de la Cybersécurité chez ISG

David
Gordon

Consultant Principal en Cybersécurité

Jason
Stading

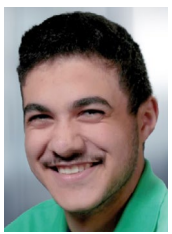
Consultant Directeur en Cybersécurité

Brendan
Prater

Responsable Conseil en Cybersécurité

Christophe
deBoisset

Responsable Conseil en Cybersécurité



Marco
Ezzy

Consultant en Cybersécurité

Entreprises invitées

Si votre entreprise figure sur cette page ou si vous estimez qu'elle devrait y figurer, veuillez contacter ISG afin de vous assurer que nous disposons des coordonnées de la ou des personnes à contacter pour participer activement à cette étude.

* Noté dans la précédente version de l'étude

8com
Absolute Software*
AC3*
Accenture*
Acronis*
Actar (Peers Group)
ActioNet*
Addvalue
Advens*
Agility Networks*
Airbus Protect*
Aizoon*
Akamai Technologies
All for One Group*
AlmavivA*
Almond*
Alten*
Amazon Web Services
Appdome
Apura Cyber Intelligence S/A
Arcon
Arctic Wolf Networks, Inc.
Asper*
Atos*
Aveniq*
Avertium*
Avivatec
Axians*
Axur
Azion
BDO
Bechtle/Apixit*
Berghem
BeyondTrust
BIP
Bitdefender
Blaze Information Security
Bluepex*
BlueVoyant*
Brainloop*
Bravo GRC
Brennan IT*
Bricon
Bridewell*
Broadcom*
BT*
CANCOM*
Capgemini*
Capita*
CDW*
Century Data
CGI*
Check Point Software*
CI&T*
Cipher*
Cirion Technologies*
Cisco*
Citrix
Claranet*
Claro empresas

Entreprises invitées

Si votre entreprise figure sur cette page ou si vous estimez qu'elle devrait y figurer, veuillez contacter ISG afin de vous assurer que nous disposons des coordonnées de la ou des personnes à contacter pour participer activement à cette étude.

* Noté dans la précédente version de l'étude

Clavis*
ClearSale
Cloud Target*
CloudFlare
Cognizant*
Combate a Fraude (Caf)
Compugraf
Computacenter*
Consort Group*
Controlware*
CoSoSys (Netwrix)*
C-Risk
Critical Start*
Crowdstrike*
CTM*
CyberArk
CyberProof*
CyberSecOp*
Cyderes*
Cyera
Cynet Security Ltd.
Darktrace
Data#3*
Datacom*
DATAGROUP*
dataRain
Data-Sec
deepwatch, Inc.
Defcon1
Delfia
Delinea
Deloitte*
Deutsche Telekom*
Devoteam*
Dfense
DIGITALL*
DriveLock*
DXC Technology*
EcoTrust*
Edge UOL*
e-Safer
ESET
E-TRUST
Expel, Inc
EY*
FastHelp
Fidelis Cybersecurity*
FireEye
Forcepoint*
ForgeRock (Ping Identity)
Formind*
Fortinet*
Fortra*
Fujitsu*
Future Segurança da Informação
GBS*

Entreprises invitées

Si votre entreprise figure sur cette page ou si vous estimez qu'elle devrait y figurer, veuillez contacter ISG afin de vous assurer que nous disposons des coordonnées de la ou des personnes à contacter pour participer activement à cette étude.

* Noté dans la précédente version de l'étude

GC Security
Genetec
Genpact
Getronics*
Gigamon
Globant*
glueckkanja*
GoCache*
Google*
GTT*
HackerOne
HackerSec
Hakai Offensive Security
Happiest Minds*
HCLTech*
Headmind Partners*
Hillstone Networks
HiSolutions*
Holiseum*
HPE Aruba Networking
HSC Brasil
HubOne (SysDream)*
Huge Networks*
IBLISS Digital Security*
IBM*
iC Consult*
ID Quantique
Imperva
inCloud Tecnologia
indevis*
Inetum*
InfoGuard*
Infosys*
Innova Solutions*
Insight*
Inspira*
Integrity360*
Interactive*
Interop
Intrinsec*
IonQ Quantum, Inc.
IPTRUST*
ISH Tecnologia*
iSPIN*
iT.eam*
It4us
Italtel*
ITC Secure*
I-tracing
ITS Group*
itWatch*
Kaspersky*
KnowBe4
KPMG*
Kroll*
KRYPTUS*

Entreprises invitées

Si votre entreprise figure sur cette page ou si vous estimez qu'elle devrait y figurer, veuillez contacter ISG afin de vous assurer que nous disposons des coordonnées de la ou des personnes à contacter pour participer activement à cette étude.

* Noté dans la précédente version de l'étude

Kudelski Security*
Kyndryl*
L8 Group
Leidos*
LevelBlue (Trustwave)*
Littlefish
Logical IT
Logicalis*
LRQA Nettitude*
LTIMindtree*
Lumen Technologies*
Macquarie Telecom Group*
ManageEngine*
Materna*
Matrix42*
McAfee
Mckinsey
Metsys*
Micro Focus
Microland*
Microsoft*
Mimecast*
MindPoint Group LLC
Minsait (Indra)
Modulo Security Solutions*
Mphasis*
MTF*
NAVA*
NCC Group*
NEC
NetBr
Netconn
Netfive
NetSecurity
Netskope*
NetSurion
Network Secure
Network Security Professionals, Inc.
Neverhack*
Nextios
Niji*
Nomios*
Nova8
Novacoast
Novared
Noventiq
Npo Sistemas
NRI*
NTSEC
NTT DATA*
Nv7
NXO*
Okta
One Identity
Ontinue (Open Systems)*
OpenText*
Oplium
Optiv*
Optus*
Opus Tech

Entreprises invitées

Si votre entreprise figure sur cette page ou si vous estimez qu'elle devrait y figurer, veuillez contacter ISG afin de vous assurer que nous disposons des coordonnées de la ou des personnes à contacter pour participer activement à cette étude.

* Noté dans la précédente version de l'étude

Oracle
Orange Cyberdefense*
ORBIT*
Ornisec*
OST Tecnologia
Palo Alto Networks*
pco*
Peers
Performanta*
Persistent Systems*
Post-Quantum
PQShield
Presidio*
PRIDE Security*
Proficio*
Proofpoint*
Protega Managed Cybersecurity
Protiviti/ICTS
PsiQuantum Corp.
PurpleSec*
PwC*
qbeyond
Qrypt
Quantinuum LLC
Quantum Xchange
QuEra Computing, Inc.
QuintessenceLabs
Quorum Cyber*
QuSecure
Rackspace Technology*
Radware
Rapid7
RCZ
Redbelt
ReliaQuest
Reply
Riedel Networks
Rpost
RSA Security
Safe Inc
Safeweb
SailPoint
Samsung
Scaltel
SCC*
Scunna*
SEC4U
Secureway
Secureworks*
Securiti
Security First
SecurityHQ*
SecurityScorecard
SEK (Security Ecossystem Knowledge)*
Sempre IT
Senhasegura
Sequretek*
Service IT*
Servix
Seti

Entreprises invitées

Si votre entreprise figure sur cette page ou si vous estimez qu'elle devrait y figurer, veuillez contacter ISG afin de vous assurer que nous disposons des coordonnées de la ou des personnes à contacter pour participer activement à cette étude.

* Noté dans la précédente version de l'étude

SFR*
Sigma Telecom
Skaylink
Skyhigh Security*
SLK Software*
Smarttech247*
SNS Security*
Softcat PLC*
Solo Iron*
Solo Networking
Solor
Sonda*
Sophos*
Sopra Steria*
Splunk
Squad*
Stefanini*
Strati
suresecure*
SVA*
Swisscom*
Symantec
Synetis*
Syntax*
Talion*
Tanium
Tata Communications*
TCS*
TDec Network Group*
Tech Mahindra*
Telefonica*
Telstra*
Teltec Solutions*
Tempest Security Intelligence
Tenable
Tenchi Security
terreActive*
Thales*
Think IT*
Tidalcyber
TIVIT*
Trellix*
Trend Micro*
Trigent
T-Systems*
UMB*
Under Protection*
Unisys*
United Security Providers*
Varonis*
Vectra*
Venturus
Verizon Business*
Vigilant
VIVO
VMware Carbon Black
Vodafone
Vortex Security*
Vortex TI
Vultus*

Si votre entreprise figure sur cette page ou si vous estimez qu'elle devrait y figurer, veuillez contacter ISG afin de vous assurer que nous disposons des coordonnées de la ou des personnes à contacter pour participer activement à cette étude.

* Noté dans la précédente version de l'étude

WatchGuard

Wavestone*

Wipro*

Wizard Group

WWT*

Xantaro*

XYPRO Technology Corp.

You IT

Zensar Technologies*

Zscaler*

ISG Provider Lens®

La série de recherche ISG Provider Lens® Quadrant est la seule évaluation des prestataires de services de ce type à combiner des recherches et des analyses de marché empiriques, fondées sur des données, avec l'expérience et les observations du monde réel de l'équipe internationale des experts consultants d'ISG. Les entreprises y trouveront une mine de données détaillées et d'analyses de marché pour les aider à sélectionner les partenaires de sourcing appropriés, tandis que les conseillers d'ISG utilisent les rapports pour valider leur propre connaissance du marché et faire des recommandations aux entreprises clientes d'ISG. La recherche couvre actuellement les fournisseurs qui offrent leurs services dans plusieurs pays du monde. Pour plus d'informations sur la recherche ISG Provider Lens, veuillez consulter cette page web.

ISG Research™

ISG Research™ fournit des services de recherche par abonnement, de conseil et d'événements exécutifs axés sur les tendances du marché et les technologies perturbatrices qui entraînent des changements dans l'informatique d'entreprise. ISG Research fournit des conseils qui aident les entreprises à accélérer leur croissance et à créer davantage de valeur.

ISG offre des recherches portant spécifiquement sur les fournisseurs aux gouvernements d'État et locaux (y compris les comtés, les villes) ainsi qu'aux établissements d'enseignement supérieur. Visitez le site : Secteur public.

Pour plus d'informations sur les abonnements à ISG Research, veuillez envoyer un courriel à contact@isg-one.com, appeler le +1.203.454.3900, ou visiter le site research.isg-one.com.

ISG

ISG (Nasdaq : III) est une entreprise mondiale de conseil et de recherche technologique centrée sur l'IA. Partenaire de confiance de plus de 900 clients, dont 75 des 100 plus grandes entreprises mondiales, ISG est un leader de longue date dans le sourcing de services technologiques et commerciaux. Aujourd'hui, l'entreprise est à la pointe de l'IA et permet aux organisations d'atteindre l'excellence opérationnelle tout en accélérant leur croissance.

Fondée en 2006, ISG est reconnue pour ses données exclusives sur le marché, sa connaissance approfondie des écosystèmes de fournisseurs et l'expertise de ses 1 600 professionnels à travers le monde, qui contribuent à maximiser la valeur des investissements technologiques de ses clients.

Pour plus d'inform isg-one.com.

ISG Provider Lens®

JANVIER, 2026

BROCHURE: CYBERSÉCURITÉ — SERVICES ET SOLUTION