ISG Provider Lens™

# Cybersecurity – Services and Solutions

Analyser le marché de la cybersécurité et comparer l'attractivité du portefeuille des prestataires et leurs forces concurrentielles

**BROCHURE | JANVIER 2025 | AUSTRALIE, BRÉSIL, FRANCE, ALLEMAGNE, SUISSE, ROYAUME-UNI, ÉTATS-UNIS, SECTEUR PUBLIC AMÉRICAIN ET MONDE**

Table des Matières

**La cybersécurité à l'ère de l'IA et des technologies émergentes**

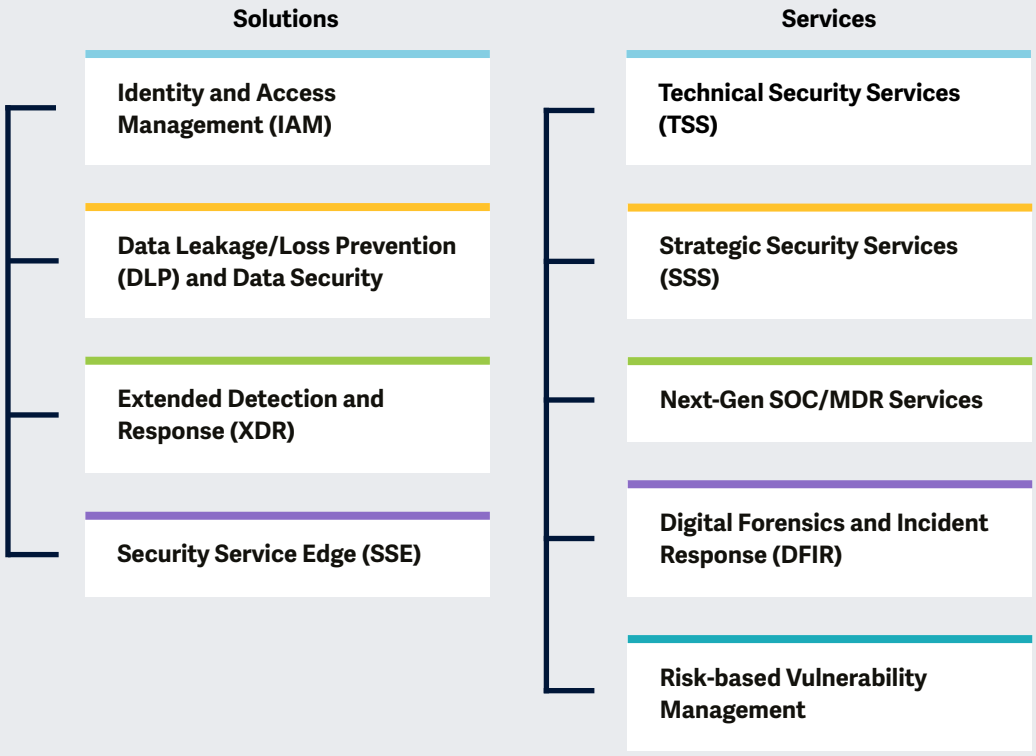
À l'ère des avancées technologiques rapides et de l'intégration de l'IA dans les opérations quotidiennes, le paysage de la cybersécurité est devenu de plus en plus complexe. Les exigences réglementaires telles que la directive Network and Information Security (NIS) 2 dans l'Union européenne augmentent la demande de mesures de cybersécurité robustes, obligeant les organisations à réévaluer leurs cadres de sécurité au milieu des menaces émergentes. Parallèlement, la banalisation des outils de piratage a considérablement réduit les barrières à l'entrée pour les acteurs malveillants, ce qui a entraîné une recrudescence des activités cybercriminelles et une escalade correspondante des risques.

La prolifération des technologies a élargi la surface d'attaque, posant des défis critiques aux organisations qui naviguent entre les technologies opérationnelles et les technologies de l'information. La pénurie de personnel qualifié dans le domaine de la cybersécurité a amplifié cette complexité, suscitant une demande accélérée de services de sécurité gérés, les entreprises recherchant une expertise externe pour renforcer leurs défenses.

Le développement continu de l'IA présente des risques et des opportunités dans le domaine de la cybersécurité. Les prestataires de services de sécurité aident leurs clients à naviguer dans le paysage de la cybersécurité, où la vigilance est cruciale pour identifier et atténuer les menaces et comprendre l'impact transformateur des nouvelles technologies telles que l'informatique quantique. En réponse à ces défis, les entreprises investissent de plus en plus dans des solutions telles que la gestion des identités et des accès (IAM), la prévention des fuites et pertes de données (DLP), la détection et réponse étendues (XDR) et les services de sécurité des terminaux (SSE), combinant des outils avancés et une expertise humaine avec une intelligence comportementale et contextuelle afin d'améliorer leur posture de sécurité.

# Principaux domaines d'intérêt pour la **cybersécurité – Services et solutions** 2025.

Illustration simplifiée Source: ISG 2025




**L'étude ISG Provider Lens™ Cybersecurity - Services et solutions 2025 offre les éléments suivants aux décideurs commerciaux et informatiques :**

- Transparence sur les forces et les faiblesses des prestataires concernés.
- Un positionnement différencié des prestataires par segments sur leurs forces concurrentielles et l'attractivité de leur portefeuille.
- 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.
- Les thèmes IAM, SSE et XDR seront analysés pour le marché mondial.
- Afin de prendre en compte les caractéristiques propres à chaque pays dans cette étude mondiale, l'analyse XDR sera étendue au Brésil, l'analyse DLP portera exclusivement sur l'Allemagne, l'accent sera mis sur le DFIR pour la France et la gestion des vulnérabilités basée sur le risque sera évaluée pour la France et le Brésil.

## Recherche sur les quadrants

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

**Définition**

Les fournisseurs de solutions IAM évalués dans ce quadrant se distinguent par leurs logiciels propriétaires, y compris SaaS, et leurs services de gestion des identités des utilisateurs de l'entreprise. Ce quadrant exclut les prestataires de services qui n'offrent pas de produit IAM, sur site ou dans le cloud, développé avec un logiciel propriétaire. En fonction des besoins de l'entreprise, ces solutions peuvent être déployées sur site, dans des clouds gérés par le client, en tant que modèles de service ou une combinaison de ces options.

Les solutions IAM se concentrent sur la gestion des identités des utilisateurs et des droits d'accès, y compris l'accès spécialisé par le biais de la gestion des accès privilégiés (PAM) régie par des politiques définies. Les suites IAM intègrent des mécanismes sécurisés, des cadres et une automatisation pour le profilage en temps réel des utilisateurs et des attaques afin de répondre aux besoins évolutifs des applications. On s'attend également à ce que les prestataires intègrent des fonctionnalités d'accès aux médias sociaux et aux téléphones portables, afin de répondre aux besoins de sécurité au-delà de la gestion traditionnelle des droits sur le web. Ce quadrant englobe également la gestion de l'identité des machines.

Critères d'éligibilité

1. Proposer des solutions qui peuvent être **déployées sur site,** dans le **cloud, comme identité en tant que service** (IDaaS) ou par le biais d'un modèle géré par un tiers.
2. Fournir des solutions capables de **prendre en charge l'authentification** en combinant **l'authentification unique (SSO), l'authentification multifactorielle (MFA)** et les modèles fondés sur le risque et le contexte.
3. Proposer des solutions capables de **prendre en charge l'accès basé sur les rôles** et le PAM
4. Fournir une **gestion des accès** pour répondre aux besoins multiples de l'entreprise, tels que les **clouds, les terminaux, les appareils mobiles, les API et les applications Web**.
5. Proposer des solutions capables de **prendre en charge une ou plusieurs normes IAM existantes et nouvelles**, notamment SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust et SCIMOffrir, un portefeuille comprenant une ou plusieurs des solutions suivantes - **annuaire, tableau de bord ou gestion en libre-service** et gestion du cycle de vie (migration, synchronisation et réplication) - afin de prendre en charge l'accès sécurisé.

## Data Leakage/Loss Prevention (DLP) and Data Security

**Définition**

Les fournisseurs de solutions DLP évalués dans ce quadrant se distinguent par leur logiciel propriétaire, y compris SaaS, et les services associés. Ce quadrant exclut les prestataires de services qui n'offrent pas de produit DLP, sur site ou dans le cloud, développé à l'aide d'un logiciel propriétaire. Les solutions DLP permettent d'identifier et de surveiller les données sensibles et d'en autoriser l'accès aux utilisateurs autorisés. Elles comprennent un ensemble de produits offrant une visibilité et un contrôle sur les données sensibles résidant dans les applications cloud, les terminaux, les réseaux et divers appareils.

Les solutions DLP aident les entreprises à relever les défis liés au contrôle des transferts de données, plus d'un tiers des violations de données ayant une origine interne. La prolifération des appareils mobiles et autres pour le stockage des données accentue ces préoccupations, car ils peuvent échanger des données sans passerelles centrales.

Les solutions de sécurité des données protègent contre les accès non autorisés et le vol en hiérarchisant, classant et surveillant les données au repos et en transit, ce qui permet aux entreprises de renforcer la sécurité des données.

Critères d'éligibilité

1. Proposer des solutions DLP basées sur des **logiciels propriétaires** et non sur des logiciels tiers.
2. Démontrer la capacité à prendre en charge la DLP **dans n'importe quelle architecture, telle que le cloud, le réseau, le stockage ou les terminaux**.
3. Démontrer la capacité à **protéger les données sensibles**, qu'elles soient **structurées ou non structurées**, sous forme de texte ou binaires.
4. Fournir des solutions avec un **support de base**, y compris, mais sans s'y limiter, des **rapports, des contrôles**, l'installation et la maintenance, et des fonctionnalités avancées de détection des menaces.
5. Proposer des solutions capables **d'identifier les données sensibles, d'appliquer des politiques**, de surveiller le trafic et d'améliorer la conformité des données.

**Définition**

Les fournisseurs de solutions XDR évalués dans ce quadrant se distinguent par leurs plateformes qui intègrent, mettent en corrélation et contextualisent les données et les alertes provenant de multiples composants de prévention, de détection et de réponse aux menaces. XDR est une technologie basée sur le cloud qui intègre plusieurs solutions de sécurité et utilise l'analyse pour améliorer la précision de la détection. Elle consolide les produits de sécurité pour améliorer la visibilité et le contexte des menaces dans les espaces de travail, les réseaux et les workloads de l'entreprise.

Les solutions XDR utilisent la télémétrie et les données contextuelles pour la détection et la réponse, en intégrant plusieurs produits dans une interface unifiée. Elles se caractérisent par un haut degré d'automatisation et classent les alertes par ordre de priorité en fonction de leur gravité afin de déterminer les réponses personnalisées nécessaires. Ce quadrant exclut les prestataires de services qui n'offrent pas de solution XDR **basée sur un logiciel propriétaire**. Les solutions XDR visent à réduire la prolifération des produits, la fatigue due aux alertes et à résoudre les problèmes d'intégration. Elles aident les équipes chargées des opérations de sécurité à gérer ou à tirer parti des solutions de gestion des informations et des événements de sécurité (SIEM) ou d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR).

Critères d'éligibilité

1. Offrir des solutions XDR basées sur des **logiciels propriétaires** et non sur des logiciels tiers.
2. Veiller à ce qu'une solution XDR comporte deux composants principaux : **XDR front end et XDR back end**.
3. Offrir un front-end avec **trois solutions ou capteurs ou plus**, y compris, mais sans s'y limiter, la **détection et la réponse sur les terminaux, les plateformes de protection des terminaux**, la protection des réseaux (pare-feu et IDPS), la **détection et la réponse sur les réseaux**, la gestion des identités, la sécurité du courrier électronique, la détection des menaces mobiles, la protection des workloads cloud et les leurres numériques.
4. Fournir des solutions offrant une **couverture et une visibilité complètes et totales de tous les terminaux** d'un réseau.
5. Proposer des solutions capables de **bloquer les menaces sophistiquées** telles que les **menaces persistantes avancées, les ransomwares** et les logiciels malveillants.
6. Fournir des solutions à l'aide de **renseignements sur les menaces** et d'**informations en temps réel sur les menaces** émanant des terminaux.
7. Fournir des solutions avec des **fonctions de réponse automatisée**.

## Security Service Edge (SSE)

**Définition**

Les fournisseurs de solutions SSE évalués dans ce quadrant proposent des solutions centrées sur le cloud, combinant des logiciels ou du matériel propriétaires et des services associés, permettant un accès sécurisé au cloud, au SaaS, aux services web et aux applications privées. Les prestataires proposent des solutions de SSE sous la forme d'un service de sécurité intégré par le biais de points de présence positionnés à l'échelle mondiale, avec prise en charge du stockage local des données, qui combine des solutions individuelles telles que l'accès au réseau sans confiance (ZTNA), l'agent de sécurité des accès au cloud (CASB), les passerelles web sécurisées (SWG) et le pare-feu en tant que service (FWaaS). Le SSE peut également inclure d'autres solutions de sécurité telles que la DLP, l'isolation du navigateur et le pare-feu de nouvelle génération (NGFW) pour sécuriser l'accès aux applications dans le cloud et sur site.

Les prestataires mettent en avant leur expertise en matière de respect des lois locales, régionales et nationales, telles que la souveraineté des données, pour les clients mondiaux. Ce quadrant exclut les composants réseau du secure access service edge (SASE), tels que le SD-WAN, qui seront traités dans l'étude ISG Provider Lens™ Network - Software Defined Services and Solutions 2025.

Critères d'éligibilité

1. Fournir le SSE en tant que **solution intégrée** avec les composants **ZTNA, CASB, SWG et FWaaS**
2. Proposer des solutions **principalement basées sur** des logiciels **propriétaires** ; ces solutions peuvent **s'appuyer partiellement sur des solutions de partenaires** tout en évitant une **dépendance totale à l'égard de** logiciels de **tiers**.
3. Maintenir des **points de présence dans le monde entier** pour fournir des solutions
4. Fournir des **fonctionnalités SSE aux** environnements cloud **et sur site** (y compris les environnements hybrides).
5. Effectuer des **évaluations et des analyses contextuelles et comportementales (analyse de l'entité et du comportement de l'utilisateur [UEBA])** pour détecter et prévenir les intentions malveillantes ou suspectes.
6. Offrir un **support de base**, y compris, mais sans s'y limiter, **l'établissement de rapports, le contrôle des politiques**, l'installation et la maintenance, ainsi que les fonctionnalités de détection des menaces avancées.
7. Assurer la **disponibilité des solutions au niveau mondial**

**Définition**

Les fournisseurs de TSS évalués dans ce quadrant couvrent l'intégration, la maintenance et le support des produits ou solutions de sécurité IT et OT. Les TSS englobent une large gamme de produits de sécurité, y compris la sécurité du cloud et des centres de données, l'IAM, la DLP, la sécurité du réseau, la sécurité des terminaux, la sécurité OT, SASE et d'autres.

Ces prestataires proposent des guides et des feuilles de route pour renforcer la sécurité à l'aide des meilleurs outils, en améliorant la posture et en réduisant les menaces. Leurs portefeuilles prennent en charge les transformations complètes ou individuelles de l'architecture de sécurité, ainsi que l'identification, l'évaluation, la conception et la mise en œuvre de produits ou de solutions. Ils investissent dans l'établissement de partenariats avec des fournisseurs de solutions et de technologies de sécurité afin d'obtenir des accréditations spécialisées et d'élargir leur portefeuille.

Ce quadrant comprend également les services de sécurité gérés classiques fournis sans centre d'opérations de sécurité. Il examine les prestataires de services qui ne se concentrent pas exclusivement sur leurs produits propriétaires mais qui sont capables de mettre en œuvre et d'intégrer des solutions d'autres fournisseurs de solutions et de prestataires de services.

Critères d'éligibilité

1. Démontrer une expérience dans la conception et la **mise en œuvre de solutions de cybersécurité** pour les entreprises dans le pays concerné.
2. Obtenir **l'autorisation des fournisseurs de technologies de sécurité** (matériel et logiciels) pour distribuer et soutenir les solutions de sécurité.
3. **Employer des experts certifiés** (les certifications peuvent être parrainées par des vendeurs, des associations et des organisations ou des agences gouvernementales) capables de prendre en charge les technologies de sécurité.
4. **Ne pas se concentrer exclusivement** sur des **produits** ou des solutions **propriétaires.**
5. Présenter des **études de cas** qui démontrent la réussite de la conception, du déploiement et de la gestion de solutions de cybersécurité pour les entreprises du pays cible.

**Définition**

Les fournisseurs de SSS évalués dans ce quadrant offrent des services de conseil en sécurité IT et OT. Les services comprennent les audits de sécurité, les évaluations, la sensibilisation et la formation. Ces prestataires aident également à évaluer la maturité de la sécurité et à définir des stratégies de cybersécurité pour répondre aux exigences spécifiques de l'entreprise.

Les prestataires emploient des consultants en sécurité expérimentés pour planifier et gérer des programmes de sécurité de bout en bout pour les entreprises. Compte tenu de la demande croissante des PME et de la pénurie de talents, les fournisseurs de SSS proposent des experts à la demande par le biais de services CISO virtuels. Ces experts établissent des feuilles de route pour la continuité des activités, classent par ordre de priorité les applications critiques à restaurer et organisent des exercices sur table afin d'améliorer la cyberconnaissance et la réaction des membres du conseil d'administration et des employés de l'entreprise. Ils fournissent également des conseils sur la sélection des technologies et des fournisseurs de sécurité, l'examen des structures organisationnelles pour la cybersécurité, l'évaluation des processus et des pratiques de sécurité, et l'amélioration de ces derniers en fonction des risques encourus. Ce quadrant examine les prestataires de services qui ne se concentrent pas exclusivement sur des produits ou des solutions propriétaires.

Critères d'éligibilité

1. Démontrer des capacités dans les domaines de la SSS tels que **l'évaluation, la sélection des prestataires, le conseil en solutions et le conseil en matière de risques.**
2. Faire preuve de compétence dans l'application des bonnes pratiques et des cadres de sécurité du marché tels que ISO 27000, NIST et CIS.
3. **Offrir au moins un des** services de sécurité stratégique susmentionnés dans les pays respectifs évalués dans le cadre de cette étude.
4. Fournir des **services de conseil en sécurité en utilisant les modèles tels que NIST et ISO.**
5. **Ne pas se concentrer exclusivement** sur des **produits** ou des solutions **propriétaires.**

**Définition**

Les prestataires évalués dans ce quadrant offrent des services liés à la surveillance continue des infrastructures IT et OT par un centre d'opérations de sécurité (SOC). Ce quadrant examine les prestataires de services qui ne se concentrent pas exclusivement sur des produits propriétaires, mais qui peuvent gérer et exploiter les meilleurs outils de sécurité. Ces prestataires de services peuvent gérer l'ensemble du cycle de vie des incidents de sécurité, de l'identification à la réponse et la remédiation.

Les fournisseurs de SOC de nouvelle génération sont très demandés pour renforcer la posture de sécurité des entreprises et améliorer l'efficacité des programmes de sécurité. Ils associent les services de sécurité gérés traditionnels à l'innovation pour fournir des services intégrés de cyberdéfense et de détection et réponse gérées (MDR). Ces prestataires investissent également dans la détection et la chasse aux menaces, le renseignement sur les menaces, la modélisation et la criminalistique, la gestion des incidents et les technologies avancées, telles que l'automatisation, le big data, l'IA et ML, afin d'offrir une approche holistique de l'atténuation proactive des menaces et de la sécurité avancée.

Critères d'éligibilité

1. Offrir des services standard, y compris la **surveillance de la sécurité, l'analyse du comportement, la détection des accès non autorisés, les conseils sur les mesures de prévention, les tests de pénétration** et tous les autres services opérationnels, afin de fournir une protection continue et en temps réel sans compromettre les performances de l'entreprise.
2. Fournir des services de sécurité, tels que des **services de prévention et de détection, de gestion des informations et des événements de sécurité (SIEM),** des conseillers en sécurité et des services d'audit, soit à distance, soit sur site, directement chez le client.
3. Capacités spécifiques au MDR, y compris le **renseignement avancé sur les menaces** et la **chasse aux menaces basée sur le comportement et dirigée par l'homme,** offrant des capacités de sécurité **offensives et défensives** avec une **vue unifiée** pour les rapports et les mesures.
4. Posséder **des accréditations de fournisseurs d'outils de sécurité**.
5. **Gérer ses propres SOC.**
6. Former le **personnel** avec des certifications telles que Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) et Global Information Assurance Certification (GIAC).
7. Proposer une variété de modèles de tarification échelonnée.

**Définition**

Les prestataires évalués dans le quadrant DFIR offrent des services liés aux activités de réponse aux menaces tout en préservant les preuves contre les attaquants. Ce quadrant examine les prestataires de services qui proposent des techniques et des méthodologies DFIR éprouvées et qui peuvent travailler avec les meilleurs outils pour répondre aux incidents de cybersécurité.

La DFIR implique l'identification, l'investigation, l'endiguement et la remédiation des incidents de cybersécurité. L'augmentation de la fréquence et de la gravité des incidents de cybersécurité a conduit à l'adoption de services de DFIR. La DFIR est essentielle pour identifier les pertes de données à la suite d'une atteinte à la sécurité et pour mettre en place des réponses efficaces aux menaces par le biais de plans d'action. Les prestataires de services font preuve d'expertise en matière d'investigation numérique, notamment en ce qui concerne le triage, l'analyse de la chronologie et des journaux, l'examen des logiciels malveillants et l'analyse des artefacts. Ils ont également de l'expérience dans le soutien aux litiges pour les réclamations et les audits et maîtrisent des outils tels que SIEM, SOAR, la détection et la réponse sur les terminaux (EDR) et XDR.

Critères d'éligibilité

1. Employer une **équipe de réponse aux incidents** (CERT ou CSIRT) composée d'experts possédant des certifications pertinentes telles que GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE) et CISSP, démontrant ainsi leur expertise et leur engagement à maintenir les normes du secteur.
2. Posséder une expérience et une expertise dans la **gestion de diverses** solutions SIEM, SOAR, EDR et XDR.
3. Proposer des services de DFIR permettant d'**identifier les causes profondes** d'une **violation** et d'évaluer son impact à court et à long terme.
4. Posséder **des capacités** d'analyse des logiciels malveillants, de décryptage des ransomwares et de récupération des données.
5. Démontrer un **partenariat** avec les fournisseurs de produits et les prestataires de services de sécurité gérés afin d'améliorer la veille sur les menaces, la surveillance du « dark web » et les capacités SOC et d'atténuer les menaces avancées, persistantes et sophistiquées.

**Définition**

Les prestataires de services de gestion des vulnérabilités basée sur le risque évalués dans ce quadrant se distinguent par leurs compétences techniques avancées et leur capacité à entreprendre des mises à jour continues sur les vulnérabilités connues et les méthodes sophistiquées contournant les défenses établies par le biais de pratiques telles que les tests de pénétration. Les outils d'IA générative (GenAI) ont permis aux cybercriminels d'identifier et d'exploiter les vulnérabilités des actifs technologiques, en particulier ceux qui sont exposés à internet. Cette tendance, associée à une augmentation des incidents liés aux ransomwares, souligne la nécessité d'une gestion continue des vulnérabilités plutôt que d'une approche d'évaluations sporadiques.

Compte tenu de la fréquence rapide des mises à jour des services en ligne, la mise en œuvre d'une détection continue des vulnérabilités est devenue essentielle à une stratégie de cybersécurité efficace basée sur les risques. Les prestataires doivent désormais proposer des solutions ciblées qui transcendent les pratiques traditionnelles, en reconnaissant qu'un cadre basé sur les risques est vital pour gérer efficacement les vulnérabilités et minimiser l'impact dans le paysage des menaces qui évoluent rapidement aujourd'hui.

Critères d'éligibilité

1. Posséder des équipes internes spécialisées capables d'**évaluer rigoureusement les vulnérabilités et d'indiquer des solutions** pour éliminer les failles et réduire progressivement leur gravité sur la base de preuves concrètes des vecteurs d'attaque.
2. Offrir des services comprenant des **approches de type boîte noire, boîte grise et boîte blanche**, capables d'évaluer les applications web, les appareils mobiles, les réseaux internes, le cloud, les API, l'IoT et d'autres actifs exposés.
3. Utiliser des méthodes telles que les **tests dynamiques de sécurité des applications (DAST), les tests statiques de sécurité des applications (SAST) et les tests de pénétration** avec objectifs spécifiques à l'aide d'outils manuels et/ou automatisés pour la fourniture de services.
4. Utiliser les **normes industrielles reconnues** telles que SOC 2, ISO27001, NIST 800-53, PCI-DSS et HIPPA pour indiquer les failles de sécurité.
5. Proposer de **nouveaux tests, un soutien spécialisé et des mécanismes de suivi** des actions correctives, en mettant à jour la matrice des risques et de la gravité (exposition aux vecteurs restants) si nécessaire.
6. Employer une **équipe d'experts techniques** (Ethical Hackings) avec des certifications telles que Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP), CompTIA PenTest+ (CompTIA PenTest) et GIAC Penetration Tester (GPEN).

## Quadrants par région

Dans le cadre de cette étude des quadrants ISG Provider Lens™, nous présentons les neuf quadrants suivants sur la cybersécurité – Services et solutions 2025:

| Quadrant | États-Unis | Royaume-Uni | Allemagne | Suisse | France | Brésil | Australie | Secteur public américain | Monde |
|---|---|---|---|---|---|---|---|---|---|
| Identity and Access Management (IAM) | | | | | | | | | ✓ |
| Data Leakage/Loss Prevention (DLP) and Data Security | | | ✓ | | | | | | |
| Extended Detection and Response (XDR) | | | | | | ✓ | | | ✓ |
| Security Service Edge (SSE) | | | | | | | | | ✓ |
| Technical Security Services (TSS) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Strategic Security Services (SSS) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Next-Gen SOC/MDR Services | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Digital Forensics and Incident Response (DFIR) | | | | | ✓ | | | | |
| Risk-based Vulnerability Management | | | | | ✓ | ✓ | | | |

**Principales caractéristiques du modèle:**

- Résume ce que font les entreprises sur le marché de la cybersécurité.
- Représente l'ensemble de la chaîne de valeur de l'offre et de la demande au sein du marché.
- Les tuiles intérieures représentent les thèmes des objectifs de l'entreprise.
- Les carreaux extérieurs représentent des initiatives.
- Derrière chaque tuile extérieure se cache un ensemble spécifique de capacités, avec des prestataires et des solutions uniques, leaders sur le marché.

La phase de recherche se situe entre janvier et février 2025, période au cours de laquelle l'enquête, l'évaluation, l'analyse et la validation auront lieu. Les résultats seront publiés en juillet 2025.

| Jalons | Début | Fin |
|---|---|---|
| Lancement de l'enquête | 7 janvier | |
| Phase d'enquête | 7 janvier 2025 | 7 février 2025 |
| Avant-première | Mai 2025 | Juin 2025 |
| Communiqué de presse et publication | Juillet 2025 | |

La collecte de témoignages de clients par le biais du programme Star of Excellence nécessite des références de clients précoces (aucune référence officielle n'est nécessaire), car les scores CX ont une influence directe sur la position du prestataire dans le quadrant IPL et sur les récompenses.

Veuillez vous référer au lien pour consulter/télécharger le programme de recherche ISG Provider Lens™ 2025.

**Accès au portail en ligne**

Vous pouvez consulter/télécharger le questionnaire à partir de ici en utilisant les informations d'identification que vous avez déjà créées ou en vous référant aux instructions continues dans l'e-mail d'invitation pour générer un nouveau mot de passe. Nous nous réjouissons de votre participation !

**Guide de l'acheteur:**

ISG Software Research, anciennement « Ventana Research », offre des informations sur le marché en évaluant les fournisseurs de technologie et les produits par le biais de ses guides d'achat. Les résultats sont tirés de l'analyse basée sur la recherche des catégories de produits et d'expériences des clients, classant et évaluant les fournisseurs de logiciels et les produits afin de faciliter la prise de décision éclairée et les processus de sélection de la technologie.

A l'occasion du lancement de l'IPL Cybersecurity – Services and Solutions, nous souhaitons profiter de l'occasion pour attirer votre attention sur les recherches et les analyses connexes que ISG Research publiera en 2025. Pour plus d'informations, consultez le calendrier de recherche du Buyer Guide.

**Avertissement:**

ISG recueille des données dans le but de mener des recherches et de créer des profils de prestataires/fournisseurs. Les profils et les données qui les accompagnent sont utilisés par les consultants d'ISG pour faire des recommandations et informer leurs clients de l'expérience et des qualifications de tout prestataire applicable à l'externalisation du travail identifié par les clients. Ces données sont collectées dans le cadre du processus FutureSource(TM) d'ISG et du processus de qualification des candidats-fournisseurs (CPQ). ISG peut choisir de n'utiliser ces données collectées relatives à certains pays ou régions que pour l'éducation et les besoins de ses consultants et de ne pas 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 commentaires des clients sur la réussite des prestataires de services à démontrer les plus hauts standards d'excellence de service à la clientèle et de centrage sur le client.

L'enquête globale porte sur les services associés aux études IPL. Par conséquent, tous les analystes d'ISG 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 consultants 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, ISG envoie un courrier de confirmation aux deux parties. Il va de soi qu'ISG rend anonymes toutes les données relatives aux clients et qu'elle ne les divulgue pas.

Notre vision de Star of Excellence est d'être reconnue comme la principale reconnaissance du secteur pour l'excellence du service à la clientèle et de servir de référence pour mesurer les sentiments des clients. Pour vous assurer que les clients que vous avez sélectionnés complètent les commentaires relatifs à votre mission, veuillez utiliser la section « Nominate (for Providers) » sur le site web de Star of Excellence.

Nous avons mis en place une adresse électronique où vous pouvez poser vos questions ou faire part de vos commentaires. Ce courriel sera vérifié quotidiennement. Vous recevrez une réponse sous 24 heures.

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

**ISG Star of Excellence**

L'étude ISG Provider Lens 2025 – 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

**Analyste en chef :**
Frank Heuer, Gowtham Kumar, Bhuvaneshwari Mohan, Benoit Scheuber, Dr. Maxime Martelli, Andrew Milroy et João Mauro

**Analystes de recherche:**
Monica K, Sandya Kattimani et 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

### Commanditaire de l'étude

Heiko Henkes

**Directeur et analyste principal**

Frank Heuer

**Analyste en chef - Allemagne, Suisse**

Gowtham Kumar

**Analyste principal - États-Unis, secteur public américain, monde**

Bhuvaneshwari Mohan

**Analyste en chef - Royaume-Uni, secteur public américain, monde**

Benoit Scheuber

**Analyste en chef - France**

Dr. Maxime Martelli

**Analyste en chef - Global**

Andrew Milroy

**Analyste en chef - Australie**

João Mauro

**Analyste principal - Brésil**

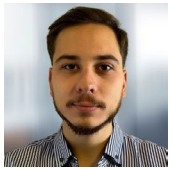
Monica K

**Analyste de recherche**

## Contacts pour cette étude

Sandya Kattimani

**Analyste de recherche**



Rafael Rigotti

**Analyste de recherche**

Rajesh Chillappagari

**Analyste de Données**

Laxmi Sahebrao

**Analyste de Données**

Shreemadhu Rai B

**Chef de projet**

**ISG Provider Lens Programme de participation des consultants**

ISG Provider Lens propose des évaluations de marché qui intègrent les points de vue des acteurs de terrain, reflétant l'orientation régionale et la recherche indépendante. ISG garantit l'implication des consultants dans chaque étude afin de couvrir les détails appropriés du marché en fonction des lignes 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 participent au processus d'examen de la qualité et de la cohérence de chaque étude.

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

Les consultants :

- Aident à définir et à valider les quadrants et les questionnaires,
- Conseillent sur l'inclusion des prestataires de services, participent aux réunions d'information,
- Donnent leur point de vue sur les évaluations des prestataires de services et examinent les projets de rapport.

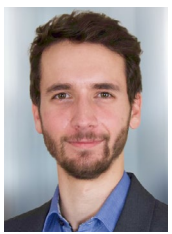
## Conseillers d'ISG pour cette étude

Doug Saylors

**associé, codirigeant ISG Cybersecurity**

David Gordon

**consultant principal en cybersécurité**



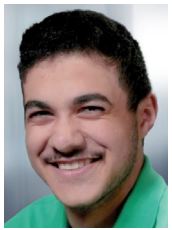
Anas Barmo

**consultant en cybersécurité**

Brendan Prater

**gestionnaire conseil en cybersécurité**

# Conseillers d'ISG pour cette étude



Marco Ezzy

**consultant en cybersécurité**

Tim Merscheid

**gestionnaire conseil en cybersécurité**

Christophe de Boisset

**responsable conseil en cybersécurité**

# Entreprises invitées

**Si votre entreprise figure sur cette page ou si vous pensez qu'elle devrait y figurer, veuillez contacter ISG pour vous assurer que nous disposons de la (des) personne(s) de contact adéquate(s) pour participer activement à cette recherche.**

* Noté lors de l'itération précédente

Absolute Software*
AC3*
Accenture*
ACESI Group
Acronis*
Actar (Peers Group)
ActioNet*
Adarma*
ADIT Group
Advens*
Agility Networks*
Airbus Protect*
AISI
Akamai*
Algosecure
Alice&Bob.Company*
All for One Group*
AlmavivA*
Almond*
Alten*
Amazon Web Services
AntemetA
Apixit
Appdome
Apura Cyber Intelligence S/A
Arcon
Asper*
AT&T Cybersecurity*
Atos*
Avatier*
Aveniq*
Avertium*
Axians*
Axur
Azion
BAYOOSOFT*
BDO
Bechtle*
Berghem*
Beta Systems*
BeyondTrust*
BIP
Bitdefender*
BlackBerry*
Blaze Information Security*
BluePex*
BlueVoyant*
Brainloop*
Bravo GRC
Bridewell
Broadcom
BT*
CANCOM*
Capgemini*
Cato Networks*
CDW*
Century Data
CGI*
ChapsVision CyberGov
Check Point Software*

# Entreprises invitées

**Si votre entreprise figure sur cette page ou si vous pensez qu'elle devrait y figurer, veuillez contacter ISG pour vous assurer que nous disposons de la (des) personne(s) de contact adéquate(s) pour participer activement à cette recherche.**

* Noté lors de l'itération précédente

Cipher*
Cirion*
Cisco*
Citrix
Claranet*
Clavis*
ClearSale
Cloud Target
Cloudflare*
Cognizant*
Combate a Fraude (Caf)
Compugraf
Computacenter*
Consort Group*
Consulteer InCyber
Controlware*
CoSoSys (Netwrix)*
Critical Start*
Cross Identity*
CrowdStrike*
CTM*
CyberArk*
CyberCX*
Cybereason*
CyberProof*
Cyberprotect
CyberSecOp*
Cybersolutions
Cyderes*
Darktrace
Data#3*
Datacom*
DATAGROUP*
dataRain
Delfia
Delinea
Deloitte*
Deutsche Telekom
Devensys
Devoteam*
DIGITALL*
DriveLock*
DXC Technology*
EcoTrust
Edge UOL*
Embratel
EmpowerID*
Ensono
Entrust*
Ergon Informatik*
Ericom Software*
e-Safer
ESET*
E-TRUST*
Eviden*
EY*
FastHelp*
Fidelis Cybersecurity*
FireEye
Fischer Identity*

## Entreprises invitées

**Si votre entreprise figure sur cette page ou si vous pensez qu'elle devrait y figurer, veuillez contacter ISG pour vous assurer que nous disposons de la (des) personne(s) de contact adéquate(s) pour participer activement à cette recherche.**

* Noté lors de l'itération précédente

Forcepoint*
ForgeRock (Ping Identity)
Formind*
Fortinet*
Fortra*
Framatome Cybersecurity
Fujitsu*
FusionAuth*
Future Segurança da Informação
GBS*
GC Security*
Genetec
Getronics*
Gigamon
Globant*
glueckkanja*
GoCache*
Google*
GTT*
HackerOne
HackerSec*
Hakai Offensive Security*
Happiest Minds*
HCLTech*
Headmind Partners*
HiSolutions*
HPE Aruba Networking
HSC Brasil
HubOne (SysDream)*
Huge Networks*
IBLISS Digital Security*
IBM*
iboss*
iC Consult*
Ilex IAM Platform*
Imperva
Imprivata*
IMS Networks
IN Groupe*
indevis*
InfoGuard*
Infosys*
Integrity360*
Interop
Intrinsec*
ISH Tecnologia*
ISPIN*
IT.eam*
It4us
Italtel*
ITC Secure*
I-Tracing
Itrust (Free Pro)*
ITS Group*
itWatch*
Kaspersky*
KnowBe4
KPMG*
Kroll*
Kryptus*

## Entreprises invitées

**Si votre entreprise figure sur cette page ou si vous pensez qu'elle devrait y figurer, veuillez contacter ISG pour vous assurer que nous disposons de la (des) personne(s) de contact adéquate(s) pour participer activement à cette recherche.**

* Noté lors de l'itération précédente

Kudelski Security*
Kyndryl*
Lastpass*
Leidos*
Lexfo*
Logical IT
Logicalis*
Lookout*
LRQA Nettitude*
LTIMindtree*
Lumen Technologies*
Macquarie Telecom Group*
ManageEngine*
Mandiant
Materna Radar*
Matrix42*
McAfee
Metsys*
Micro Focus
Microland*
Microsoft*
Modulo Security Solutions
Mphasis*
MTF*
NAVA*
NBS System
NCC Group*
NEC*
Neosoft
NetSecurity
Netskope*
Network Secure
Neverhack*
Nevis*
Nextios
Nok Nok Labs*
Nomios*
Novared
Noventiq
Npo Sistemas
NRI ANZ*
NTSEC
NTT DATA*
NTT Ltd.
NXO*
NYBBLE
OEDIV
Okta*
Omada*
One Identity (OneLogin)*
Open Systems*
OpenText*
Optiv*
Oracle*
Orange Cyberdefense*
OST Tecnologia
P1 SECURITY
Palo Alto Networks*
pco*
Peers

## Entreprises invitées

**Si votre entreprise figure sur cette page ou si vous pensez qu'elle devrait y figurer, veuillez contacter ISG pour vous assurer que nous disposons de la (des) personne(s) de contact adéquate(s) pour participer activement à cette recherche.**

* Noté lors de l'itération précédente

Performanta*
Perimeter 81*
Persistent Systems*
Ping Identity*
Presidio*
Pride Security*
Proficio*
Proofpoint*
Protega Managed Cybersecurity
Protiviti/ICTS
PurpleSec*
PwC*
Quorum Cyber*
Rackspace Technology*
Radware
Rapid7*
RCZ
Red river
Redbelt
Redscan*
Reply
RSA Security*
Safeway
Safeweb
SailPoint*
SAP*
Saviynt*
SCC*
Scunna*
SCUTUM
SEC4U
SecureAuth*
Secureway
Secureworks*
Securiti
SecurityHQ*
SecurityScorecard
SEK (Security Ecossystem Knowledge)*
Sekuro*
senhasegura*
SenseOn*
SentinelOne*
Seqrite
Sequretek
Service IT*
Servix
Seti
SFR*
Shearwater Group*
Sigma
Sigma Telecom
Skyhigh Security*
SLK Software*
SNS Security
Softcat*
SolarWinds*
Solor
SONDA*
Sophos*
Sopra Steria*

## Entreprises invitées

**Si votre entreprise figure sur cette page ou si vous pensez qu'elle devrait y figurer, veuillez contacter ISG pour vous assurer que nous disposons de la (des) personne(s) de contact adéquate(s) pour participer activement à cette recherche.**

* Noté lors de l'itération précédente

Spie ICS*
Splunk
Squad*
Stefanini*
suresecure*
Swisscom*
Symantec
Synetis*
Syntax*
Sysinterga
Systancia*
Talion*
Tanium
Tata Communications*
TCS*
TDec Network Group*
Tech Mahindra*
TEHTRIS*
Telefonica Tech*
Telstra*
Teltec Solutions*
Tempest Security Intelligence
Tenable
Tenchi Security
terreActive*
Thales*
Think IT*
TIVIT*
Trellix*
Trend Micro*
Trustwave*
T-Systems*
UMB*
Under Protection
Unisys*
United Security Providers*
ValueLabs*
Varonis*
Vectra*
Venturus
Verizon Business*
Versa Networks*
Vigilant
VMware Carbon Black
Vortex Security*
Vortex TI
WALLIX*
WatchGuard
Wavestone*
Wipro*
Xmco
YSSY*
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 (Information Services Group) (NASDAQ: III) est une société de recherche et de conseil technologique de premier plan au niveau mondial. Partenaire commercial de confiance de plus de 900 clients, dont 75 des 100 premières entreprises mondiales, ISG s'engage à aider les entreprises, les organisations du secteur public et privé, et les fournisseurs de services et de technologies à atteindre l'excellence opérationnelle et une croissance plus rapide. La société est spécialisée dans les services de transformation numérique, notamment IA et les l'automatisation, le cloud et l'analyse des données, le conseil en matière d'approvisionnement, les services de gestion de la gouvernance et des risques, les services d'opérateur réseau, la conception de stratégies et d'opérations, la gestion du changement, la veille commerciale et la recherche et l'analyse technologiques. Fondée en 2006 et basée à Stamford, dans le Connecticut, ISG emploie plus de 1 600 professionnels du numérique opérant dans plus de 20 pays – une équipe mondiale connue pour sa pensée novatrice, son influence sur le marché, sa profonde expertise industrielle et technologique, et ses capacités de recherche et d'analyse de classe mondiale basées sur les les données les plus complètes sur les marchés.

Pour plus d'inform isg-one.com.

ISG Provider Lens™

**JANVIER, 2025**

# BROCHURE: CYBERSECURITY – SERVICES AND SOLUTIONS