ISG Provider Lens™

2022

Cybersécurité - Solutions et services 2022

imagine your future®

ISG (Information Services Group) (NASDAQ: III) est une entreprise mondiale majeure de conseil et de recherche en technologie. Elle est un partenaire commercial fiable pour plus de 800 clients, dont 75 figurant parmi les 100 premières entreprises du monde. ISG vise à aider les corporations, les organisations du secteur public et les prestataires de technologie à atteindre l'excellence opérationnelle et une croissance plus rapide. L'entreprise est spécialisée dans les services de transformation numérique, dont l'automatisation, l'analyse du cloud et des données, le conseil sur le sourçage, les services de gouvernance et de risque gérés, les services de support de réseau, la stratégie de technologie et la conception des opérations, la gestion des changements, l'intelligence du marché et la recherche et l'analyse technologiques. Fondée en 2006 et possédant son siège à Stamford dans le Connecticut, ISG emploie plus de 1300 personnes dans plus de 20 pays, une équipe mondiale reconnue pour ses idées novatrices, son influence sur le marché, son expertise approfondie de l'industrie et de la technologie, ses capacités avérées en matière de recherche et d'analytique basées sur les données de marché les plus exhaustives du secteur. Pour plus d'informations, rendez-vous sur le site www.isg-one.com.

Table of Contents

Introduction

Les entreprises adoptent les nouvelles technologies pour amorcer leur transformation numérique afin de rester compétitives et de s'aligner sur les besoins en constante évolution des utilisateurs finaux. Une transformation rendue encore plus nécessaire par la pandémie de COVID-19, qui accélère l'adoption par les entreprises du télétravail, des applications en nuage et d'autres technologies numériques en vue de survivre et de prospérer. L'adoption progressive de ces technologies, ainsi que de nouveaux outils permettant de gagner en efficacité et en rapidité, a entraîné une expansion du champ d'attaque des menaces. Les logiciels rançonneurs, les menaces persistantes avancées et les attaques par hameçonnage sont apparus comme certaines des principales cybermenaces en 2022. La nature et la complexité des cyberattaques ne cessant d'augmenter, la cybersécurité est désormais une priorité non seulement pour les entreprises, mais aussi pour les organismes publics, qui doivent protéger leurs économies, leurs industries ainsi que leurs citoyens.

Face à ces menaces en constante évolution, les entreprises doivent adopter une approche détaillée et globale de la cyber-sécurité pour protéger leurs activités en mettant en œuvre une combinaison de produits et de services de sécurité dans des domaines tels que la gestion des identités et des accès (GIA), la prévention des fuites et des pertes de données (DLP) et les services de sécurité gérés (SSG), afin de mettre en place un cadre solide et sécurisé visant à réduire l'exposition aux risques.

Outre le besoin d'autoprotection, des règlementations comme le règlement général sur la protection des données (RGPD) en Europe, et d'autres instruments de conformité régionaux, ont contraint les entreprises à mettre en œuvre des mesures de protection solides pour contrer les cyberattaques. Une législation similaire a été adoptée dans d'autres pays comme le Brésil et l'Australie pour protéger les utilisateurs contre les cybermenaces.

Bien que la cybersécurité soit devenue un domaine d'activité important pour les RSSI des entreprises, les responsables informatiques ont souvent du mal à justifier les investissements en matière de sécurité, car il n'est pas toujours possible de mesurer et de démontrer le retour sur investissement, ni de quantifier les risques liés aux menaces. La complexité des technologies disponibles, les difficultés en matière d'identification et de correction des vulnérabilités ainsi que le manque de sensibilisation des utilisateurs finaux ne cessent de mettre à mal les entreprises et leurs dirigeants.

Par ailleurs, le déploiement d'outils de sécurité adéquats ne signifie pas qu'une entreprise sera à l'abri des vulnérabilités ; le facteur humain reste le maillon le plus faible du mur de sécurité, qui est continuellement exploité par les pirates par le biais de cybermenaces comme les chevaux de Troie et les attaques d'hameçonnage. Le manque de sensibilisation des utilisateurs finaux peut avoir pour conséquence des attaques ciblées comme les menaces persistantes avancées (MPA) et les logiciels rançonneurs, qui ont un impact sur la réputation des entreprises, entraînent des pertes de données et des pertes financières et précipitent les pannes opérationnelles. C'est pourquoi la formation des utilisateurs, l'évaluation des risques et les services consultatifs continueront à jouer un rôle clé dans la sécurisation des infrastructures des technologies de l'information et des communications (TIC) des entreprises.

L'étude ISG Provider Lens™ Cybersecurity - Solutions and Services 2022 a pour objectif d'aider les décideurs TIC à utiliser au mieux leurs budgets serrés en matière de sécurité en proposant les éléments suivants:

- Transparence sur les forces et les réserves des prestataires concernés.
- Un positionnement différencié des prestataires par segments de marché.
- Une perspective sur les marchés locaux.

Pour les fournisseurs de services informatiques et les vendeurs, cette étude constitue une base de décision importante pour le positionnement, les relations clés et les considérations de mise sur le marché (GTM). Les conseillers d'ISG et les entreprises clientes exploitent également les informations des rapports ISG Provider Lens™ tout en identifiant et en évaluant leurs relations actuelles avec les fournisseurs et les engagements potentiels.

Recherche en quadrant

Dans le cadre de l'étude ISG Provider Lens™ quadrant, ce rapport comprend six quadrants sur la cyber sécurité, comme illustré ci-dessous:

Illustration simplifiée

Cybersécurité Solutions et services 2022		
Solutions pour la sécurité		
Gestion des Identités et des Accès (GIA)	Prévention des Fuites et Pertes de Données (DLP) et Sécurité des Données	Protection, Détection et Réponse Avancées aux Menaces contre les Terminaux (PDR Avancées MT)
Solutions de sécurité		
Services de Sécurité Technique (SST)	Services de Sécurité Stratégiques	Services de Sécurité Gérés

Source: ISG 2022

Solutions pour la sécurité

Le champ d'application des solutions suivantes couvre uniquement les fournisseurs de logiciels et de solutions qui proposent des logiciels de sécurité avec un modèle de licence et comme solution à la demande en tant que service. Les prestataires de services proposant des solutions équivalentes qui apportent une valeur ajoutée dans le cadre d'un projet plus vaste, mais qui ne proposent pas de modèles de licence, ne seront pas pris en compte pour les quadrants de solutions.

Gestion des Identités et des Accès (GIA)

Les vendeurs et fournisseurs qui proposent des solutions GIA se caractérisent par leur capacité à offrir des logiciels propriétaires et des services associés pour gérer en toute sécurité les identités et les dispositifs des utilisateurs de l'entreprise. Ce quadrant comprend également les logiciels sous forme de services basés sur des logiciels propriétaires. **Les simples fournisseurs de services qui ne proposent pas de produit GIA (sur site et/ou dans le nuage) basé sur un logiciel propriétaire ne sont pas inclus ici**. En fonction des besoins de l'organisation, ces solutions peuvent être déployées de plusieurs manières, par exemple sur site ou dans le nuage (géré par le client), selon un modèle « as-a-service » ou une combinaison des deux.

Les solutions GIA visent à collecter, enregistrer et administrer les identités des utilisateurs et les droits d'accès associés, ainsi que les accès spécialisés aux actifs critiques, y compris la gestion des accès privilégiés (GAP). Elles veillent à ce que les droits d'accès soient accordés en fonction des politiques définies. Pour répondre aux exigences des applications existantes et nouvelles, les solutions IAM intègrent de plus en plus de mécanismes, de cadres et de systèmes d'automatisation sécurisés (par exemple, des analyses de risques) dans leurs suites de gestion afin de fournir des fonctionnalités de profilage des utilisateurs et des attaques en temps réel. Les fournisseurs de solutions doivent également proposer des fonctionnalités supplémentaires liées aux médias sociaux et aux utilisateurs mobiles pour répondre à leurs besoins spécifiques en matière de sécurité, qui vont au-delà de la gestion traditionnelle des droits liés au web et au contexte. La gestion des informations sur l'identité des machines est également incluse ici.

Critères d'éligibilité:

- La solution doit pouvoir être déployée en combinaison avec des systèmes sur site, en nuage, en tant que service d'identité (IDaaS) et un modèle de tiers géré.
- La solution doit être capable de prendre en charge l'authentification en combinant l'authentification unique (SSO), l'authentification multifactorielle (AMF) et les modèles basés sur le risque et le contexte.
- La solution doit être en mesure de prendre en charge l'accès basé sur les rôles et la GAP.
- Le fournisseur GIA devrait être en mesure d'assurer la gestion des accès pour un ou plusieurs besoins de l'entreprise, tels que le Cloud, les extrémités, les appareils mobiles, les interfaces de programmation d'applications (API) et les applications Web.
- La solution doit pouvoir prendre en charge une ou plusieurs normes de GIA, anciennes ou plus récentes, notamment SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust et SCIM.
- Afin de prendre en charge l'accès sécurisé, le portefeuille devrait offrir un ou plusieurs des éléments suivants: solutions d'annuaire, tableau de bord ou gestion en libre-service et gestion du cycle de vie (migration, synchronisation et réplication).

Prévention des Fuites et Pertes de Données (DLP) et Sécurité des Données

Les vendeurs et fournisseurs de solutions DLP se distinguent par leur capacité à proposer des logiciels propriétaires et des services associés. Ce quadrant comprend également les logiciels sous forme de services basés sur des logiciels propriétaires. **Les simples fournisseurs de services qui ne proposent pas de produit DLP (sur site ou dans le cloud) basé sur un logiciel développé par eux-mêmes ne figurent pas ici**. Les solutions DLP sont des offres qui permettent d'identifier et de surveiller les données sensibles, de réserver l'accès aux seuls utilisateurs autorisés et de prévenir les fuites de données. Les solutions des fournisseurs sur le marché se caractérisent par un ensemble de produits capables de fournir une visibilité et un contrôle des données sensibles résidant dans les applications en nuage, les extrémités, le réseau et d'autres dispositifs.

Ces solutions prennent une importance considérable car il est devenu plus difficile pour les entreprises de contrôler les mouvements et les transferts de données. Le nombre d'appareils, y compris ceux qui sont mobiles et qui sont utilisés pour stocker des données, est en hausse dans les entreprises. Ils sont généralement équipés d'une connexion Internet et peuvent envoyer et recevoir des données sans passer par une passerelle Internet centrale. Les mesures de sécurité des données protègent les données contre l'accès non autorisé, la divulgation ou le vol.

Critères d'éligibilité:

- L'offre DLP doit être basée sur un logiciel propriétaire et non sur un logiciel tiers.
- La solution doit être en mesure de prendre en charge la DLP sur n'importe quelle architecture, comme le nuage, le réseau, le stockage ou le point d'extrémité.
- La solution doit être en mesure de gérer la protection des données sensibles, qu'il s'agisse de données structurées ou non structurées, de texte ou de données binaires.
- La solution doit être proposée avec un support de gestion de base, comprenant, sans s'y limiter, des rapports, des contrôles de politiques, l'installation et la maintenance, et des fonctionnalités de détection des menaces avancées.
- La solution doit être en mesure d'identifier les données sensibles, d'appliquer des politiques, de surveiller le trafic et d'améliorer la conformité des données.

Protection, détection et réponse avancées aux menaces contre les points finaux (ETPDR avancée)

Les vendeurs et fournisseurs de solutions ETPDR avancées se caractérisent par leur capacité à proposer des logiciels propriétaires et des services associés. Ce quadrant comprend également les logiciels sous forme de services basés sur des logiciels propriétaires. **Les simples fournisseurs de services qui ne proposent pas un produit ETPDR avancé (sur site ou dans le cloud) basé sur un logiciel développé par eux-mêmes ne sont pas inclus ici**. Ce quadrant évalue les fournisseurs proposant des produits capables d'assurer une surveillance continue et une visibilité totale de tous les points finaux, ainsi que d'analyser, de prévenir et de répondre aux menaces avancées. Les solutions de sécurité des points finaux qui intègrent le Secure Access Service Edge (SASE) sont également incluses ici. À notre avis, la sécurité des extrémités comprend aussi la protection correspondante des solutions technologiques opérationnelles (OT).

Ces solutions vont au-delà d'une simple protection basée sur les signatures et englobent la protection contre des risques comme les logiciels rançonneurs, les menaces persistantes avancées (MPA) et les logiciels malveillants, en examinant les incidents sur l'ensemble du parc de terminaux. La solution doit être en mesure d'isoler le terminal infecté et de prendre les mesures correctives ou de remédier à la situation. Ces solutions comprennent une base de données, dans laquelle les informations collectées à partir du réseau et des points d'extrémité sont regroupées, analysées et étudiées, et l'agent qui réside dans le système hôte offre les capacités de surveillance et de rapport des événements.

Critères d'éligibilité:

- La solution offre une couverture et une visibilité complètes et totales de tous les points finaux du réseau.
- La solution démontre son efficacité à bloquer les menaces complexes telles que les menaces persistantes avancées, les rançongiciels et les logiciels malveillants.
- La solution exploite les renseignements sur les menaces, analyse et fournit des informations en temps réel sur les menaces émanant des points finaux.
- La solution doit inclure des fonctions de réponse automatisée qui comprennent, entre autres, la suppression des fichiers malveillants, le sandboxing, l'arrêt des processus suspects, l'isolement du terminal infecté et le blocage des comptes suspects.

Solutions de sécurité

Le champ d'application des services suivants ne concerne que les prestataires qui offrent des services de sécurité avec une équipe d'experts dédiée et certifiée. Les fournisseurs de produits et de solutions ayant des offres équivalentes qui n'apportent de la valeur ajoutée qu'avec leur solution dans le cadre des services

d'assistance, ne seront pas pris en compte pour les quadrants de services.

Services de Sécurité Gérés (SSG)

Le MSS comprend les opérations et la gestion des infrastructures de sécurité IT et OT pour un ou plusieurs clients par un centre d'opérations de sécurité (SOC). **Ce quadrant examine les fournisseurs de services qui ne se concentrent pas exclusivement sur les produits propriétaires mais peuvent gérer et exploiter les meilleurs outils de sécurité**. Ces fournisseurs de services peuvent prendre en compte l'ensemble du cycle de vie des incidents de sécurité, de l'identification à la résolution.

Critères d'éligibilité:

- Les services typiques comprennent 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, les opérations de pare-feu, les opérations antivirus, les services d'exploitation de la gestion des identités et des accès (GIA), les opérations de prévention des fuites/pertes de données (DLP) et tous les autres services d'exploitation afin de fournir une protection continue et en temps réel sans compromettre les performances de l'entreprise. En particulier, le Secure Access Service Edge (SASE) est également inclus.
- Capacité à fournir des services de sécurité tels que la détection et la prévention, la gestion des informations et des événements de sécurité (SIEM), ainsi que le soutien aux conseillers et aux audits de sécurité, à distance ou sur le site du client.
- Posséder des accréditations délivrées par des fournisseurs d'outils de sécurité.
- Les COS sont en principe détenus et gérés par le fournisseur et non par des partenaires de façon prédominante.
- Maintenir un personnel certifié, par exemple en matière de Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) et Global Information Assurance Certification (GIAC).

Services de Sécurité Technique (SST)

Les SST couvrent l'intégration, la maintenance et le support des produits ou solutions de sécurité des technologies informatiques et opérationnelles (OT). Les services DevSecOps sont également inclus ici. Les SST s'intéressent à tous les produits de sécurité, y compris les antivirus, la sécurité du cloud et des centres de données, la GIA, la DLP, la sécurité des réseaux, la sécurité des points finaux, la gestion unifiée des menaces (UTM), la sécurité des technologies de l'information, le SASE et d'autres encore. **Ce quadrant examine les fournisseurs de services qui ne se concentrent pas exclusivement sur leurs produits propriétaires respectifs et qui peuvent mettre en œuvre et intégrer les produits ou solutions d'autres fournisseurs**.

Critères d'éligibilité:

- Démontrer une expérience dans la mise en œuvre de solutions de cybersécurité pour les entreprises dans le pays concerné.
- Autorisé par les fournisseurs de technologies de sécurité (matériel et logiciels) à distribuer et à prendre en charge des solutions de sécurité.
- Les prestataires doivent faire appel à des experts certifiés (par les fournisseurs, par des associations et des organisations, par des organismes gouvernementaux) capables de prendre en charge les technologies de sécurité.

Services de Sécurité Stratégiques (SSS)

Les SSS couvrent principalement les services de conseil en matière de sécurité IT et OT. Les services couverts par ce quadrant comprennent les audits de sécurité, les services de conseil en matière de conformité et de risque, les évaluations de sécurité, le conseil en architecture de solutions de sécurité, ainsi que la sensibilisation et la formation. Ces services sont utilisés pour évaluer la maturité de la sécurité et le profil de risque, et pour définir la stratégie de cybersécurité des entreprises (adaptée aux besoins spécifiques). **Ce quadrant examine les fournisseurs de services qui ne se concentrent pas exclusivement sur les produits ou solutions propriétaires**. Les services analysés ici couvrent toutes les technologies de sécurité, notamment la sécurité OT et les SASE.

Critères d'éligibilité:

- Les fournisseurs de services doivent démontrer leurs capacités dans les domaines SSS tels que l'évaluation, les évaluations, la sélection des fournisseurs, le conseil en architecture et le conseil en matière de risques.
- Les prestataires de services doivent proposer au moins l'un des systèmes de règlement-livraison ci-dessus dans le pays concerné.
- L'exécution de services de conseil en sécurité à l'aide de cadres sera un avantage.
- Pas de concentration exclusive sur des produits ou des solutions propriétaires.

Quadrants par région

Dans le cadre de l'étude ISG Provider Lens™ Quadrant, nous présentons les six quadrants (marché) d'étude suivants sur la cybersécurité - Solutions et services 2022 par région:

Quadrants	États-Unis	Royaume-Uni	Pays Nordiques	Allemagne	Suisse	France	Brésil	Australie	Singapour et Malaisie	Secteur public américain
Identité et accès Gestion (GIA)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Prévention des Fuites et Pertes de Données (DLP) et Sécurité des Données	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Protection, Détection et Réponse Avancées aux Menaces contre les Terminaux (PDR Avancées MT)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Services de Sécurité Gérés (SSG)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Services de Sécurité Technique (SST)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Services de Sécurité Stratégiques (SSS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Calendrier

La phase de recherche se situe entre **février et mars 2022**, période au cours de laquelle auront lieu l'enquête, l'évaluation, l'analyse et la validation. Les résultats seront présentés aux médias en **juillet 2022**.

Étapes	Début	Fin
Lancement	Le 16 février 2022	
Phase d'enquête	Le 16 février 2022	Le 14 mars 2022
Avant-première	Avril 2022	
Communiqué de presse	Juillet 2022	

Prière de cliquer sur le lien pour consulter ou télécharger le programme de recherche de l'ISG Provider Lens™ 2022:

Accès au portail en ligne

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

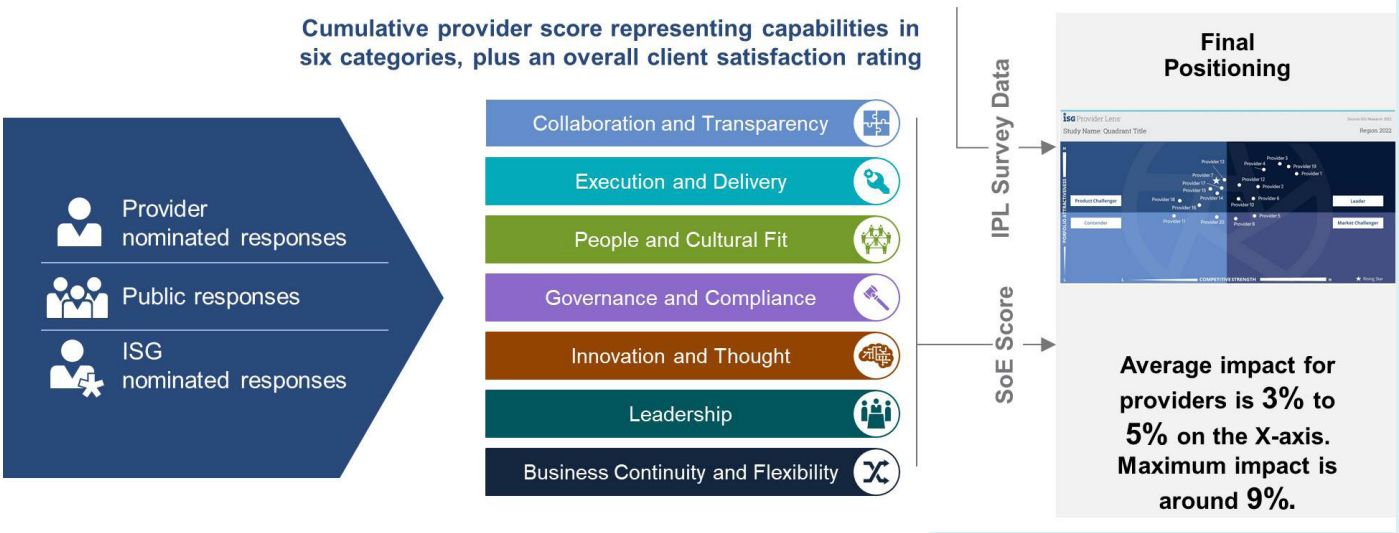
Research Production Disclaimer:

ISG recueille des données aux fins de la rédaction de rapports de recherche et de la création de profils de prestataires/vendeurs. Les profils et les données justificatives sont requises par les conseillers ISG pour émettre des recommandations et informer leurs clients de l'expérience et des qualifications de tout prestataire/vendeur potentiel afin d'externaliser une activité identifiée. Ces données sont collectées dans le cadre du processus ISG FutureSource et le processus de qualification Candidate Provider Qualification. ISG pourra choisir d'utiliser uniquement les données collectées appartenant à certains pays ou certaines régions pour l'éducation et les objectifs de ses conseillers et de ne pas produire de rapports ISG Provider Lens™. Ces décisions seront prises en fonction du niveau et de la complétude des informations reçues directement par les prestataires/vendeurs, et de la présence d'analyses expérimentés disponibles pour ces pays et ces régions. Les informations soumises pourront également être utilisées pour des projets de recherche individuels ou pour des notes d'information qui seront rédigées par les analystes responsables.

ISG Star of Excellence™ - Appel à nominations

Star of Excellence est une reconnaissance indépendante de l'excellence de la prestation de services basée sur le concept de la « Voix du client ». Le programme, conçu par l'ISG, recueille les commentaires des clients sur la capacité d'un prestataire de services à démontrer les normes les plus élevées en matière d'excellence du service à la clientèle et de centrage sur le client.

L'enquête globale porte sur les services qui sont associés aux études IPL. Tous les analystes d'ISG recevront en permanence des informations sur l'expérience client de tous les prestataires de services concernés. Ces informations viennent s'ajouter aux commentaires de première main des conseillers qu'IPL exploite dans le cadre de son approche de conseil dirigée par des praticiens.



Les fournisseurs sont invités à proposer leurs clients pour participer. Une fois que la candidature a été soumise, ISG envoie un courrier de confirmation aux deux parties. Il est évident qu'ISG anonymise toutes les données des clients et ne les partage pas avec des tiers.

Notre vision est que Star of Excellence sera reconnue comme la principale distinction du secteur pour l'excellence du service à la clientèle et servira de référence pour évaluer les sentiments des clients.

Pour vous assurer que les clients que vous avez sélectionnés remplissent le formulaire d'évaluation de votre mission, veuillez utiliser la section « Nomination des clients » du site web de Star of Excellence.

Nous avons mis en place une adresse électronique où vous pouvez adresser vos questions ou vos commentaires. Cette adresse électronique sera vérifiée quotidiennement. Patientez jusqu'à 24 heures pour recevoir une réponse. Voici l'adresse électronique: Star@isg-one.com.

Liste partielle des entreprises invitées à participer à l'enquête

Êtes-vous sur la liste ou voyez-vous votre entreprise comme un fournisseur pertinent qui manque à la liste? Alors n'hésitez pas à nous contacter pour assurer votre participation active à la phase de recherche.

2Secure
Absolute Software
Accenture
Actifio
Acuity Risk Management
ADT Cybersecurity (Datashield)
Advanced
Advenica
Agility Networks Tecnologia
Akamai
Alert Logic
AlgoSec
All for One
Amazon Web Services
Aqua Security Software
Arcserve
Arctic Wolf
Ascentor
AT&T
Atomicorp
Atos
Attivo Networks
Auth0
Avatier
Avectris
Axians
Axis Security
BAE Systems
Barracuda Networks
BDO Norway
Bechtle
BehavioSec
Beijaflore
Beta Systems
BetterCloud
BeyondTrust
BigID
Bitdefender
Bitglass
Bittium
BlueSteel Cybersecurity
BlueVoyant
BluVector
BoldonJames
Booz Allen Hamilton
Brainloop
Bricata
Bridewell Consulting
Broadcom
BT
CANCOM
Capgemini
Carbon Black
Censornet
Centrify
CenturyLink
CGI
Check Point
Chronicle Security
CI Security
Cigniti
Cipher
Cisco
Citrix
Claranet
Clavister
Clearswift
Cloud Range
CloudCodes
Cloudflare
CloudPassage
Cocus
Code42
Cognizant

ColorTokens
Column Information Security
Combitech
Comodo
Compasso UOL
Compugraf
Computacenter
Confluera
Contrast Security
Controlware
Core
Coromatic
CorpFlex
CoSoSys
Crowdstrike
Cryptomathic
CSIS Security Group
CTR Secure Services
Cyber 1
Cyber CX
Cyber Security Services
Cyber Swiss
CyberArk
Cybercom Group
Cybereason
CyberSecOp Consulting
Cygilant
Cylance
CymbiQ
Cynet
Cypher
Darktrace
Datadog
deepwatch
Deloitte
Deutsche Telekom Security
DeviceLock
Digital Guardian
DriveLock
Dubex
Duo Security, Inc (part of Cisco)
DXC
Econet
ECSC
Efecte
Elastic
Embratel
EmpowerID
Enfogroup
Ergon
Ericsson
eSentire Inc.
ESET
E-Trust
Evidian
Exabeam
Expel, Inc.
ExtraHop
EY
fasthelp
Fidelis
FireEye
Fischer Identity
Forcepoint
Forescout Technologies
Forgerock
Fortinet
Framework Security
F-Secure
Fujitsu
GBS
Giesecke + Devrient
Google DLP
GuidePoint Security
HCL

Heimdal Security

Herjavec Group

Hexaware

HID Global

Hitachi

Huawei

HyTrust

IBLISS

IBM

ID North

Idaptive

Imperva

InfoGuard

Infosys

Ingalls Information Security

Innofactor

Insta

Intercede

Intrinsec

Inuit

IronDefense

ISH Tecnologia

ISPIN

It4us

itWatch

Juniper Networks

Kasada

Kaspersky

KPMG

Kudelski

Lacework

Logicalis

LogicMonitor

LogRhythm

Lookout

LTI

Malwarebytes

ManagedMethods

ManageEngine

Masergy

Matrix42

McAfee

Micro Focus

Microland

Microsoft

Mnemonic

MobileIron

MonoSign

Morphisec

Mphasis

Napatech

Nazomi Networks

NCC group

NEC (Arcon)

NetNordic Group

Netsecurity AS

Netskope

Nettitude

NEVIS

Nextios

Nexus

Nixu Corporation

NTT

Okta

Omada

One Identity

OneLogin

Onevinn

Open Systems

Open Text

Optimal IdM

Optiv Security

Oracle

Orange Cyberdefense

Orca Security

Outpost24

Paladion

Palo Alto Networks

Panda Security

Perimeter 81

Persistent

Ping Identity

Pointsharp

PrimeKey

Privitar

Proficio Carlsbad

Proofid

ProofPoint

Protiviti/ICTS

PwC

QinetiQ

Qualys

Radiant Logic

Radware

Rapid7

Raytheon

Red Canary

Redscan

RiskIQ

Rook Security

RSA

SailPoint

Salesforce

Salt Security

SAP

Saviynt

Schneider Electric

SecureAuth

SecureTrust

Secureworks

Securonix

senhasegura

SentinelOne

Sentor

Service IT

Simeio

SIX Group

Software AG

SoftwareONE

SolarWinds

Sonda

SonicWall

Sophos

Sopra Steria

Spirion

SSH Communications Security

Stefanini

StratoKey

Sumo Logic

Swisscom

Synopsys

Synoptek

Sysdig

Tanium

TBG Security

TCS

TDec Network

Tech Mahindra

Telefonica Cibersecurity Tecnologia SA

Telia Cygate

Telos

Tempest Security Intelligence

Tesserent

Thales/Gemalto

Thirdspace

Threat Stack

ThreatConnect

Thycotic

ti8m

TietoEvry

Titus

TIVIT

Trend Micro

TrueSec

Trustwave

Ubisecure

Unisys

United Security Providers

Varonis

Vectra

Verizon

VMware

Watchcom Security Group

Watchguard

Webroot

Wipro

XenonStack

Yubico

Zacco

Zensar

ZeroFOX

Zscaler

Contacts pour cette étude

Frank Heuer
Analyste principal - Allemagne, Suisse

Gowtham Kumar
Analyste principal, États-Unis

Arun Kumar Singh
Analyste principal - Royaume-Uni, Pays nordiques

Benoit Scheuber
Analyste principal, France

Dr. Maxime Martelli
Co-Analyste principal, France

Craig Baty
Analyste principal, Australie

Sergio Rezende
Analyste principal, Brésil

Keao Caindec
Analyste principal, secteur public des États-Unis

Monica K
Analyste de recherche

Ridam Bhattacharjee
Directeur de projet

Description du programme QCRT d'ISG Provider Lens

ISG Provider Lens propose des évaluations du marché qui intègrent les points de vue des praticiens et reflètent une orientation régionale et des recherches indépendantes. ISG veille à l'implication des conseillers dans chaque étude afin de couvrir les détails appropriés du marché en fonction des lignes de services/ tendances technologiques, de la présence des fournisseurs de services et du contexte de l'entreprise. Dans chaque région, ISG dispose de leaders d'opinion experts et de conseillers respectés qui connaissent les portefeuilles et les offres des fournisseurs ainsi que les exigences des entreprises et les tendances du marché. En moyenne, trois conseillers siègent au sein de l'équipe d'examen de la qualité et de la cohérence (QCRT) de chaque étude. La QCRT veille à ce que chaque étude reflète l'expérience des conseillers d'ISG en la matière, ce qui complète les recherches primaires et secondaires menées par les analystes. Les conseillers de l'ISG interviennent dans chaque étude en tant que membres du groupe QCRT et contribuent à différents niveaux en fonction de leur disponibilité et de leur expertise.

Les conseillers du QCRT:

- participent à définir et à valider les quadrants et les questionnaires,
- conseillent 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.

Le programme QCRT d'ISG Provider Lens permet de compléter le processus de recherche, en soutenant des études complètes axées sur la recherche.

Équipe d'examen de la qualité et de la cohérence (QCRT) de cette étude

Doug Saylors
Co-responsable, ISG Cybersécurité

Roger Albrecht
Co-responsable, ISG Cybersécurité

Anand Balasubramanium
Consultant senior

Avez-vous besoin d'autres informations ?

Si vous avez des questions, n'hésitez pas à nous contacter à l'adresse isglens@isg-one.com.