ISG Provider Lens™

Cybersecurity – Solutions and Services

Une analyse du marché de la cybersécurité, consistant à comparer l'attractivité du portefeuille de fournisseurs et les forces concurrentielles.

BROCHURE | JANVIER 2023 | GLOBAL

Table of Contents

Introduction 3 - 4

À propos de l'étude

Recherche en quadrants 5
Définition 7 - 18
Quadrants par région 19
Calendrier 20

Nominations pour le feedback des clients 21

Contacts pour cette étude 22

Implication du conseiller

Participation des conseillers - Description du programme 23
Équipe consultative 23

Entreprises invitées 24 - 26

À propos de notre entreprise et de nos recherches 27

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Introduction

L'année 2022 peut être qualifiée de tumultueuse du point de vue de la cybersécurité ; bien que le nombre de violations de données ait diminué, les attaques ont gagné en sophistication et en gravité. En 2022, les entreprises ont augmenté leurs investissements dans la cybersécurité et ont donné la priorité aux initiatives pertinentes pour prévenir les attaques et améliorer leur posture de sécurité. Les enseignements tirés des attaques de 2021 ont incité les dirigeants et les entreprises de toutes tailles et de tous les secteurs à investir dans des mesures visant à répondre aux menaces et aux cyberattaques en matière de cybersécurité et à y survivre.

Du point de vue des entreprises, même les petites entreprises ont compris l'impact des cybermenaces et se sont rendu compte qu'elles sont activement ciblées et sont très vulnérables aux cyberattaques. Cela a renforcé le besoin de services de sécurité (gérés) et de services de cyber résilience qui permettraient aux entreprises de se rétablir et de reprendre leurs activités rapidement après un cyber incident.

Les fournisseurs de services et les éditeurs de logiciels proposent donc des services et des solutions qui facilitent la reprise et la continuité des activités.

Du point de vue des cybercriminels, ils ont commencé à exploiter des vulnérabilités à grande échelle, telles que Log4shell, et ont continué à utiliser des ransomwares pour perturber les activités commerciales, en ciblant spécifiquement les services de santé, la chaîne d'approvisionnement et le secteur public.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

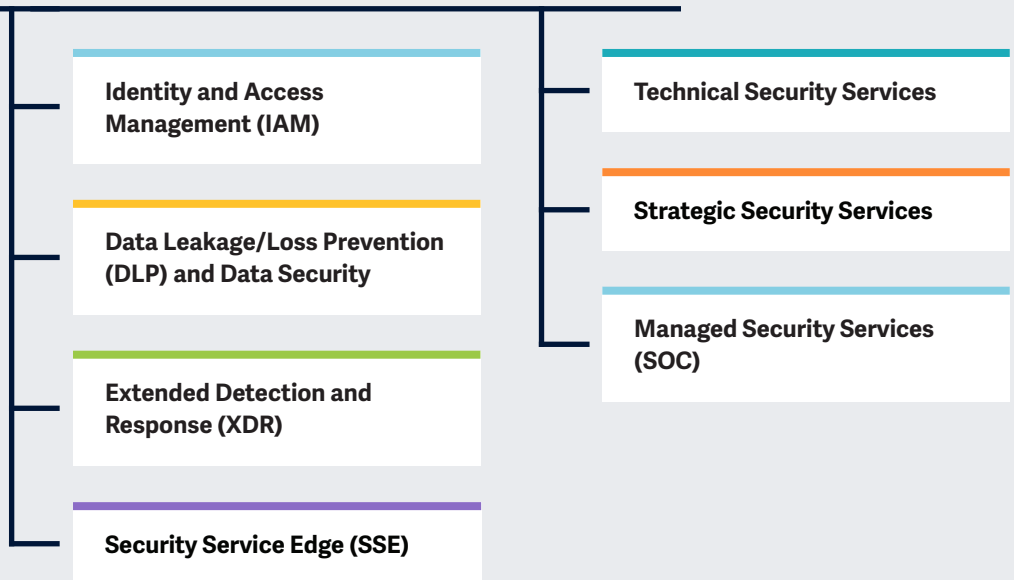
Introduction

Cela a incité les entreprises à investir dans des capacités telles que la gestion des identités et des accès (IAM), la prévention des pertes de données (DLP), la détection et la réponse gérées (MDR) et la sécurisation du cloud et des terminaux. Le marché s'oriente vers des solutions intégrées, telles que les services de sécurité en périphérie (SSE) et la détection et la réponse étendues (XDR), qui tirent parti des meilleurs outils et de l'expertise humaine et sont complétés par une intelligence comportementale et contextuelle ainsi que par l'automatisation afin d'obtenir une posture de sécurité supérieure.

ISG reports constant demand for infrastructure services as enterprises are becoming more vigilant toward spending on large and complex cloud implementations. The demand for managed services, especially application development and maintenance services, also is growing. According to the ISG 3Q 2022 ISG Index™ figures, the global market has grown 11.5 percent in combined-market ACV to reach its current value of $71.8 billion for the first nine months. Managed services ACV increased by 6 percent year-over-year and reached $27.7 billion, while the XaaS ACV increased by 15 percent to reach $44.1 billion. Also, IaaS spending witnessed flat growth to reach $10.5 billion, while the SaaS market declined by 12 percent to reach $3.6 billion during the same period.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Principaux domaines d'intérêt pour la cybersécurité - Solutions et services 2023



Simplified Illustration Source: ISG 2023

Definition

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

- La transparence sur les forces et les faiblesses des prestataires concernés
- Un positionnement différencié des prestataires par segments sur leurs atouts concurrentiels et l'attrait de leur portfolio.
- Focus sur différents marchés, notamment les États-Unis, le Royaume-Uni, les pays nordiques, l'Allemagne, la Suisse, la France, le Brésil, l'Australie, Singapour et la Malaisie, ainsi que le secteur public américain. La thématique SSE sera analysée pour le marché mondial.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Recherche par Quadrants

Notre étude sert de base de décision importante pour le positionnement, les relations clés et les considérations de mise sur le marché (go-to-market). Les conseillers d'ISG et les entreprises clientes utilisent également les informations de ces rapports pour évaluer leurs relations actuelles avec les fournisseurs et leurs engagements potentiels.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Definition

Les éditeurs et fournisseurs de solutions IAM évalués dans ce quadrant se caractérisent par leur capacité à proposer des logiciels propriétaires et des services associés pour gérer les identités et les dispositifs des utilisateurs de l'entreprise. Ce quadrant comprend également les offres SaaS basées sur des logiciels propriétaires. **Cela n'inclut pas** les fournisseurs de services **purs qui ne proposent pas de produit IAM (sur site et/ou dans le nuage) basé sur un logiciel propriétaire**. En fonction des besoins de l'organisation, ces offres peuvent être déployées de plusieurs manières, par exemple sur site ou dans le nuage (géré par un client), ou comme un modèle de service ou une combinaison de ceux-ci.

Les solutions IAM visent à gérer (collecter, enregistrer et administrer) les identités des utilisateurs et les droits d'accès associés. Elles comprennent également l'accès spécialisé aux actifs critiques par le biais de la gestion des accès privilégiés (PAM), où l'accès est accordé en fonction de politiques définies. Pour répondre aux exigences des applications existantes et nouvelles, les suites de solutions IAM sont de plus en plus intégrées à des mécanismes de sécurité, des cadres et des automatismes (par exemple, l'analyse des risques) afin de fournir des fonctionnalités de profilage des utilisateurs et des attaques en temps réel. On attend également des fournisseurs de solutions qu'ils proposent des fonctionnalités supplémentaires liées à l'utilisation des médias sociaux et de la téléphonie mobile afin de répondre à des besoins spécifiques en matière de sécurité, au-delà de la gestion traditionnelle du web et des droits contextuels. Ceci comprend également la gestion des informations sur l'identité des appareils.

Critères d'éligibilité

1. La solution doit pouvoir être déployée sur site, dans le cloud, en tant qu'identité en tant que service (IDaaS) et en tant que modèle géré par un tiers.
2. La solution doit être capable de prendre en charge l'authentification en combinant l'authentification unique (SSO), l'authentification multifactorielle (MFA) et les modèles basés sur le risque et le contexte.
3. La solution doit être en mesure de prendre en charge l'accès basé sur les rôles et la GAP.
4. L'éditeur de solutions IAM doit être en mesure de fournir une gestion des accès pour un ou plusieurs besoins de l'entreprise, tels que le cloud, les terminaux, les appareils mobiles, les interfaces de programmation d'applications (API) et les applications web.
5. La solution doit être capable de prendre en charge une ou plusieurs normes IAM anciennes et nouvelles, notamment SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust et SCIM.
6. Pour prendre en charge l'accès sécurisé, le portefeuille devrait inclure un ou plusieurs des éléments suivants: solutions d'annuaire, tableau de bord ou gestion en libre-service et solutions de gestion du cycle de vie (migration, synchronisation et réplication).

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Definition

Les éditeurs et fournisseurs de solutions DLP évalués dans ce quadrant se caractérisent par leur capacité à proposer des logiciels propriétaires et des services associés. Ce quadrant comprend également les solutions SaaS basées sur des logiciels propriétaires. Cela n'inclut pas les fournisseurs de services purs qui ne proposent pas de produit DLP (sur site ou dans le cloud) basé sur un logiciel propriétaire. Les solutions DLP permettent d'identifier et de surveiller les données sensibles, de réserver l'accès aux seuls utilisateurs autorisés et de prévenir les pertes/fuites de données. Les solutions des fournisseurs dans ce domaine comprennent un ensemble de produits capables de fournir une visibilité et un contrôle des données sensibles résidant dans les applications en cloud, les endpoints, les réseaux et divers dispositifs.

Ces solutions prennent une importance considérable car il est devenu de plus en plus difficile pour les entreprises de contrôler les mouvements et les transferts de données (plus d'un tiers des violations de données proviennent d'une source interne). Le nombre de dispositifs, y compris les appareils mobiles, utilisés pour stocker des données est en augmentation dans les entreprises. Équipés d'une connexion Internet, ces appareils peuvent envoyer et recevoir des données sans passer par un gateway Internet central. Les solutions de sécurité des données protègent les données contre les accès non autorisés, la divulgation ou le vol en hiérarchisant, classant et surveillant les données (au repos et en transit), tout en permettant aux organisations d'établir des rapports et d'améliorer la sécurité de leurs données à risque.

Critères d'éligibilité

1. L'offre DLP doit être basée sur un **logiciel propriétaire** et non sur un logiciel tiers.
2. La solution doit pouvoir prendre en charge la DLP **sur n'importe quelle architecture, comme le cloud, le réseau, le stockage ou l'endpoint**.
3. La solution doit pouvoir **gérer la protection des données sensibles, structurées ou non**, de texte ou de données binaires.
4. La solution devrait 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.
5. La solution doit pouvoir **identifier les données sensibles, appliquer des politiques**, surveiller le trafic et améliorer la conformité des données.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Definition

Les fournisseurs de solutions XDR évalués pour ce quadrant se caractérisent par leur capacité à offrir une plateforme qui intègre, met en corrélation et contextualise les données et les alertes provenant de multiples composants de prévention, de détection et de réponse aux menaces. XDR est une technologie fournie par le cloud, comprenant des solutions à points multiples. Elle fait appel à des analyses avancées pour corréler les alertes provenant de sources multiples, y compris de signaux individuels faibles, afin de permettre des détections précises. Les solutions XDR consolident et intègrent plusieurs produits et sont conçues pour assurer une sécurité complète de l'espace de travail, du réseau ou de la charge de travail. En général, les solutions XDR visent à améliorer considérablement la visibilité et le contexte de la menace identifiée dans toute l'entreprise.

Ces solutions présentent donc des caractéristiques spécifiques, notamment la télémétrie et l'analyse des données contextuelles, la détection et la réaction. Les solutions XDR comprennent de multiples produits et solutions intégrés dans un seul et même panneau de verre pour visualiser, détecter et répondre avec des capacités sophistiquées. Une maturité d'automatisation élevée et une analyse contextuelle offrent des capacités de réponse uniques adaptées au système affecté, et hiérarchisent les alertes en fonction de leur gravité par rapport à des référentiels connus. Les fournisseurs de services purs qui n'offrent pas de solution XDR basée sur un logiciel propriétaire ne sont pas pris en compte ici. Les solutions XDR visent à réduire la prolifération des produits, la lassitude à l'égard des alertes, les problèmes d'intégration et les dépenses opérationnelles. Elles conviennent particulièrement aux équipes chargées des opérations de sécurité qui ont des difficultés à gérer un portefeuille de solutions de pointe ou à tirer profit d'une solution de gestion des informations et des événements de sécurité (SIEM) ou d'une solution de sécurité, d'orchestration, d'automatisation et de réponse (SOAR).

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Critères d'éligibilité

1. L'offre XDR doit être basée sur un logiciel propriétaire et non sur un logiciel tiers.
2. Une solution XDR doit comporter deux composants principaux: le front-end XDR et le back-end XDR.
3. Le front-end devrait comporter au moins trois solutions ou capteurs, y compris, mais sans s'y limiter, la détection et la réponse aux endpoints, les plateformes de protection des endpoints, la protection des réseaux (pare-feu, IDPS), la détection et la réponse aux réseaux, la gestion des identités, la sécurité du courrier électronique, la détection des menaces mobiles, la protection des charges de travail en cloud et l'identification des supercheries.
4. La solution offre une couverture et une visibilité complètes et totales de tous les endpoints du réseau.
5. La solution démontre son efficacité à bloquer les menaces complexes telles que les menaces persistantes avancées, les ransomware et les logiciels malveillants.
6. La solution s'appuie sur les renseignements sur les menaces, et analyse et offre des informations en temps réel sur les menaces émanant des endpoints.
7. La solution doit comporter des fonctionnalités de réponse automatisée.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Definition

Les fournisseurs de solutions SSE évalués pour ce quadrant offrent des solutions centrées sur le cloud qui combinent des logiciels propriétaires, et/ou du matériel et des services associés, permettant un accès sécurisé aux services cloud, aux applications SaaS, aux services web et aux applications privées. Les éditeurs proposent des solutions SSE sous la forme d'un service de sécurité intégré via des points de présence (PoP) positionnés à l'échelle mondiale, avec prise en charge du stockage local des données, qui combine des solutions individuelles telles que l'accès réseau sans confiance (ZTNA), le courtier de sécurité d'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 prévention des fuites/pertes de données (DLP), l'isolation du navigateur et le pare-feu de nouvelle génération (NGFW) pour offrir un accès sécurisé aux applications sur le cloud et sur site.

Les fournisseurs mettent en avant leur expérience en matière de respect des lois locales, régionales et nationales (comme la souveraineté des données) pour les clients internationaux.

Les composants réseau de l'accès sécurisé en périphérie (SASE), tels que le SD-WAN ou la micro-segmentation, ne sont pas inclus dans ce quadrant mais sont couverts par l'étude Network - Software Defined Solutions and Services.

Les solutions SSE sont fortement centrées sur l'utilisateur, en fournissant la sécurité aux utilisateurs finaux à la périphérie ou aux appareils par le biais du cloud - plutôt que de permettre aux utilisateurs d'accéder de manière centralisée aux applications et aux bases de données de l'entreprise - par des réseaux dédiés. ZTNA crée une connectivité exclusive entre un utilisateur et une application, en utilisant une analyse comportementale basée sur le contexte pour contrôler l'accès. CASB offre de la visibilité, applique des politiques de sécurité et de conformité, et permet de contrôler l'utilisation du cloud computing shadow IT, tandis que FWaaS et SWG empêchent les menaces malveillantes et l'accès aux sites web et applications infectés. En général, une solution SSE dispose d'une console unifiée pour la visibilité et la gouvernance, et évalue l'expérience utilisateur grâce à une automatisation avancée.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Critères d'éligibilité

1. Le SSE doit être proposé comme une **solution intégrée** et doit comporter ces composants essentiels: **accès réseau sans confiance (ZTNA), courtier de sécurité d'accès au cloud (CASB), passerelles web sécurisées (SWG) et pare-feu en tant que service (FWaaS)**.
2. Les composants ci-dessus doivent être **principalement basés sur des** logiciels propriétaires, ils peuvent **s'appuyer partiellement sur des solutions partenaires mais ne peuvent pas s'appuyer complètement sur des** logiciels tiers.
3. Les éditeurs de solutions doivent disposer de **PoPs situés dans le monde entier** pour fournir ces solutions.
4. La solution doit être capable de **fournir le SSE à la fois dans les environnements en cloud et sur site** (y compris les environnements hybrides).
5. La solution doit présenter **des évaluations et des analyses contextuelles et comportementales (user entity and bevavior analytics/UEBA**) pour détecter et prévenir les intentions malveillantes ou suspectes.
6. La solution devrait 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.
7. La solution doit être **entièrement accessible au niveau mondial**.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Definition

Les fournisseurs de services de sécurité technique (TSS) évalués pour ce quadrant couvrent l'intégration, la maintenance et le support pour les produits ou solutions de sécurité informatique et de technologie opérationnelle (OT). Ils proposent également des services DevSecOps. Les services TSS couvrent tous les produits de sécurité, notamment les antivirus, la sécurité des centres de données et du cloud computing, l'IAM, la DLP, la sécurité des réseaux, la sécurité des points de terminaison, la gestion unifiée des menaces (UTM), la sécurité OT et les SASE, entre autres.

Les fournisseurs de TSS proposent des guides et des feuilles de route standardisés qui aident à transformer un environnement de sécurité existant avec les meilleurs outils et technologies, à améliorer la posture de sécurité et à réduire l'impact des menaces. Leurs portfolios sont conçus pour permettre la transformation complète ou individuelle d'une architecture de sécurité existante avec des produits pertinents dans des domaines tels que les réseaux, le cloud, le lieu de travail, l'OT, l'IAM, la confidentialité et la protection des données, la gestion des risques et de la conformité et le SASE, entre autres. Les offres comprennent également l'identification, l'évaluation, la conception et le développement de produits ou de solutions, la mise en œuvre, la validation, les tests de pénétration, l'intégration et le déploiement. Les fournisseurs s'appuient également sur des solutions sophistiquées qui permettent une analyse complète de la vulnérabilité des applications, des réseaux, des endpoints et des utilisateurs individuels afin de découvrir les faiblesses et d'atténuer les menaces externes et internes.

Les fournisseurs de TSS investissent dans l'établissement de partenariats dans les domaines des technologies de sécurité, du cloud, des données et des réseaux afin d'obtenir des accréditations spécialisées et d'étendre la portée de leur travail et de leurs portfolios. Ce quadrant englobe également les services de sécurité gérés classiques, c'est-à-dire ceux fournis sans centre d'opérations de sécurité (SOC).

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 éditeurs.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Critères d'éligibilité

1. Démontrent une expérience dans **la mise en œuvre de solutions de cybersécurité** pour les entreprises dans le pays respectif.
2. **Autorisé par les éditeurs de technologie de sécurité** (matériel et logiciels) à distribuer et à prendre en charge des solutions de sécurité.
3. Les fournisseurs doivent **employer des experts certifiés** (les certifications peuvent être parrainées par les fournisseurs, par des associations et des organisations ou par des agences gouvernementales) capables de prendre en charge les technologies de sécurité.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Definition

Les fournisseurs de services de sécurité stratégique (SSS) évalués dans ce quadrant offrent des services de conseil en matière de sécurité des technologies de l'information et des technologies de l'information. Les services couverts dans 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 servent à évaluer la maturité de la sécurité et la position du risque et à définir des stratégies de cybersécurité pour les entreprises (adaptées aux besoins spécifiques).

Les fournisseurs de SSS devraient employer des consultants en sécurité qui ont une grande expérience dans la planification, le développement et la gestion de programmes de sécurité de bout en bout pour les entreprises. Compte tenu du besoin croissant des PME pour de tels services et du manque de talents disponibles, les fournisseurs de SSS devraient également rendre ces experts disponibles à la demande par le biais de services vCSIO (virtual chief security information officer). Compte tenu de l'importance accrue accordée à la cyber résilience, les fournisseurs de SSS devraient être en mesure de formuler des feuilles de route pour la continuité des activités et de donner la priorité aux applications essentielles à la reprise. Ils doivent également organiser périodiquement des exercices sur table et des cyber exercices pour les membres du conseil d'administration, les principaux dirigeants d'entreprise et les employés, afin de les aider à acquérir une cyberculture et à établir les meilleures pratiques pour mieux répondre aux menaces et aux cyberattaques réelles. Ils doivent également connaître les technologies et les produits de sécurité disponibles sur le marché et offrir des conseils pour choisir le meilleur produit et le meilleur fournisseur en fonction des besoins spécifiques de l'entreprise.

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.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Critères d'éligibilité

1. 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**.
2. Les prestataires de services doivent **offrir au moins un des services de sécurité stratégiques ci-dessus** dans le pays concerné.
3. La capacité d'exécuter des **services de conseil en sécurité en utilisant des cadres** sera un avantage.
4. **Pas de priorité exclusive** aux **produits ou** solutions **propriétaires**.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Definition

Les fournisseurs évalués dans le quadrant des services de sécurité gérés (SOC) (MSS (SOC)) offrent des services liés aux opérations et à la gestion des infrastructures de sécurité informatique 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 charge l'ensemble du cycle de vie des incidents de sécurité, de l'identification à la résolution.

Les fournisseurs sont de plus en plus sollicités pour aider les entreprises à renforcer leur position globale en matière de sécurité informatique et à maximiser l'efficacité de leurs programmes de sécurité à long terme grâce à une amélioration continue. Pour y parvenir, les fournisseurs de services de sécurité gérés (SOC) doivent combiner les services de sécurité gérés traditionnels avec l'innovation afin de doter leurs clients d'un mécanisme de cyberdéfense intégré. Ils doivent être capables de fournir des services de détection et de réponse gérés (MDR) et être équipés des dernières technologies, d'une infrastructure et d'experts qualifiés dans la chasse aux menaces et la gestion des incidents, ce qui permet aux entreprises de détecter et de répondre activement en atténuant et en contenant les menaces. En raison des attentes croissantes des clients en matière de chasse proactive aux menaces, les fournisseurs améliorent leurs environnements SOC grâce à l'intelligence de sécurité, avec des investissements importants dans des technologies telles que l'automatisation, le big data, l'analytique, l'IA et le machine learning. Ces SOC sophistiqués devraient permettre de répondre aux demandes de renseignements sur la sécurité par des experts, tout en offrant aux clients une approche holistique et unifiée de la sécurité de haut niveau.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Critères d'éligibilité

1. Les services classiques comprennent **la surveillance de la sécurité, l'analyse du comportement, la détection des accès non autorisés, la fourniture de 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 (IAM), 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 bord de service d'accès sécurisé (SASE) est inclus.
2. Capacité à fournir des services de sécurité, tels que **la détection et la prévention, la gestion des informations et des événements de sécurité (SIEM)** et le soutien aux conseillers et aux audits de sécurité, à distance ou sur le site d'un client.
3. Détient des **accréditations** d'éditeurs d'outils de sécurité.
4. **Les SOC sont idéalement détenus et gérés par le fournisseur** et non par des partenaires en majeure partie.
5. Maintient un **personnel certifié**, par exemple avec des certifications telles que Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) et Global Information Assurance Certification (GIAC).

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Quadrants par région

Dans le cadre de cette étude ISG Provider Lens™ quadrant, nous présentons les sept quadrants suivants sur la cybersécurité - solutions et services 2023:

Quadrants	États-Unis	Royaume-Uni	Pays Nordiques	Allemagne	Suisse	France	Brésil	Australie	Singapour et Malaisie	Secteur public États-Unis	Mondial
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	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Strategic Security Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Managed Security Services (SOC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

La phase de recherche se situe entre janvier et février 2023, période au cours de laquelle auront lieu les enquêtes, l'évaluation, l'analyse et la validation. Les résultats seront présentés aux médias en juillet 2023.

Étapes	Début	Fin
Lancement de l'enquête	12 janvier 2023	
Phase de l'enquête	12 janvier 2023	13 fevrier 2023
Présentation préliminaire	Mai 2023	
Communiqué de presse & publication	Juillet 2023	

Veuillez cliquer sur le lien pour afficher/télécharger le programme de recherche ISG Provider Lens™ 2023

Accès au portail en ligne:

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

Avis de non-responsabilité concernant la production de recherche:

ISG collecte des données dans le but de rédiger des travaux de recherche et de créer des profils de fournisseurs et d'éditeurs de logiciels. Les profils et les données justificatives sont utilisés par les conseillers d'ISG pour faire des recommandations et informer leurs clients de l'expérience et des qualifications de tout fournisseur/éditeur de logiciel applicable pour les travaux d'outsourcing identifiés par les clients. Ces données sont collectées dans le cadre du processus ISG Future Source TM et du processus Candidate Provider Qualification (CPQ). ISG peut choisir de n'utiliser ces données collectées relatives à certains pays ou régions que pour la formation et les besoins de ses conseillers 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 fournisseurs/éditeurs de logiciels 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.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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 ». Star of Excellence est un programme conçu par ISG pour recueillir les commentaires des clients sur le succès des fournisseurs de services à démontrer les plus hauts standards d'excellence du service client et de centricité du client.

L'enquête globale porte sur les services qui sont associés aux études IPL. Par conséquent, tous les analystes d'ISG recevront constamment des informations sur l'expérience des clients de tous les fournisseurs de services pertinents. Ces informations viennent s'ajouter aux commentaires directs des conseillers, exploités par IPL dans le cadre de son approche de conseil dirigée par des professionnels.

Les fournisseurs sont invités à nominer 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 soit reconnue comme la principale distinction du secteur pour l'excellence du service à la clientèle et servira de référence pour évaluer les impressions 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 de clients du site web Star of Excellence.

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

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Contacts pour cette étude

Frank Heuer

analyste principal - Allemagne, Suisse

Benoit Scheuber

analyste principal - France

David Pereira

analyste principal - Brésil

Deepika B

analyste de la recherche

Gowtham Kumar

analyste principal - États-Unis

Dr Maxime Martelli

analyste principal - France

Phil Hassey

analyste principal - secteur public américain

Gabriel Sobanski

analyste de recherche

Arun Kumar Singh

analyste principal - Royaume-Uni, pays nordiques

Andrew Milroy

analyste principal - Australie

Bhuvaneshwari Mohan

Bhuvaneshwari Mohan

Ridam Bhattacharjee

chef de projet

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Programme d'implication des conseillers en études ISG Provider Lens

ISG Provider Lens propose des évaluations de marché intégrant les points de vue des praticiens,

reflétant une orientation régionale et une recherche indépendante. ISG veille

à l'implication des conseillers dans chaque étude afin de couvrir les détails appropriés du marché en fonction des lignes de services et des 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 d'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.

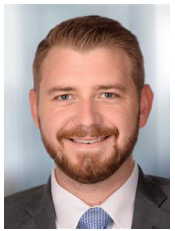
Les conseillers en QCRT:

- Contribuent à définir et à valider les quadrants et les questionnaires,
- Conseillent sur l'inclusion des fournisseurs de services et participent aux réunions de briefing,
- Donnent leur point de vue sur les évaluations des fournisseurs de services et examinent les projets de rapports.

ISG Advisors to this study

Doug Saylors

co-responsable, ISG Cybersécurité



Alex Perry

Directeur

Roger Albrecht

co-responsable, ISG Cybersécurité

Anand Balasubramanium

consultant sénior

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Si votre entreprise figure sur cette page ou si vous pensez que votre entreprise devrait y figurer, veuillez contacter ISG pour vous assurer que nous disposons de la ou des personnes de contact correctes pour participer activement à cette recherche.

* Notée lors de la mouture précédente

Fournisseurs de solutions

Absolute Software*
Acronis*
Akamai*
Aruba
Attivo Networks*
Avatier*
Axis Security
Barracuda Networks
BAYOONET*
Beta Systems*
Bitdefender*
Blackberry (Cylance)*
Brainloop*
Broadcom*
Cato Networks
Check Point*
Cisco*
Cloudflare*
CoSoSys*
CrowdStrike*
CyberArk*
Cybereason*
DriveLock*
Elastic
Ergon*
Ericom Software
ESET*
Fidelis Cybersecurity*

Prestataires de services

Accenture*
Alice&Bob.Company*
All for One Group*
AT&T Cybersecurity*
Atos*
Aveniq*
Axians*
Bechtle*
Booz Allen Hamilton
BT Security
CANCOM*
Capgemini*
CGI*
Cognizant*
Computacenter*
Controlware*
Datacom*
Deloitte*
Deutsche Telekom*
DIGITALL*
DXC Technology*
Edge UOL*
EY*
Fujitsu*
Getronics*
glueckkanja-gab*
Happiest Minds*
HCLTech*

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Entreprises Invitées

FireEye*
Forcepoint*
ForgeRock
Fortinet
WithSecure
GBS
Google
HelpSystems
IBM
iboss
Ilantus Products*
Infinite Networks
itWatch*
Kaspersky*
Lookout*
Matrix42*
Menlo Security
Micro Focus*
Microsoft*
Netskope*
Nevis*
Nexus
NordLayer
OGiTiX*
Okta*
Omada*
One Identity (OneLogin) *
Open Systems*
OpenText*
Oracle*
IBM*
iC Consult*
Indevis*
InfoGuard*
Infosys*
ISH Tecnologia
ISPIN*
KPMG*
Kudelski Security*
Logicalis*
LTIMindtree
Lumen*
Mphasis*
NTT*
Orange Cyberdefense*
Persistent Systems*
PwC*
Secureworks*
Siemens
Sopra Steria*
Stefanini
Sunny Valley
suresecure*
Swisscom*
Syntax*
Tata Communications*
Tata Consultancy Services (TCS) *
Tech Mahindra*
Tempest*
terreActive*

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Entreprises Invitées

Palo Alto Networks*
Perimeter 81
Ping Identity*
Proofpoint*
Rapid7*
RSA*
SailPoint*
SAP*
Saviynt*
Senhasegura*
SentinelOne*
SolarWinds*
Sophos*
Tehtris
Thales*
Trellix*
Trend Micro*
United Security Providers*
Varonis*
Versa Networks
VMWare Carbon Black*
Zscaler
Tesserent*
Thales*
Tietoevry*
Trustwave*
T-Systems*
UMB*
Unisys*
United Security Providers*
UST Global
Verizon*
Wipro*
Zensar*
Telia Cygate
Atea
Netic
Sapphire
Insight UK
Softcat
SecurityHQ
Performanta
Avanade Inc.
Talion
MW Group
Proact IT Group
Venzo Group
Adarma
KHIPU Networks
Nixu*
NCC Group*
Satisnet
Bridewell Consulting
Six Degrees

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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. 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 700 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 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 1 300 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'informations, visitez www.isg-one.com.

COPYRIGHTS. © 2023 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

ISG Provider Lens™

JANVIER, 2023

BROCHURE: CYBERSECURITY – SOLUTIONS AND SERVICES

© 2023 Information Services Group, Inc.
All Rights Reserved