ISG Provider Lens™

Cybersecurity – Solutions & Services

Analyse du marché de la cybersécurité, comparaison de l'attractivité des offres des fournisseurs et de leurs forces concurrentielles

BROCHURE | JANVIER 2024 | AUSTRALIE, BRÉSIL, FRANCE, ALLEMAGNE, SUISSE, ROYAUME-UNI, ÉTATS-UNIS, SECTEUR PUBLIC AMÉRICAIN ET MONDE

Table des Matières

Introduction 3

À propos de l'étude

Recherche sur les quadrants 7
Définition 9
Quadrants par régions 18
Calendrier 19

Commentaires des clients Nominations 20

Contacts pour cette étude 21

Participation des conseillers

Participation des conseillers – Description du programme 23
Équipe consultative 23

Entreprises invitées 24

À propos de notre entreprise et de la recherche 29

La cybersécurité à l'ère de l'IA

Le paysage actuel de la cybersécurité évolue rapidement en raison des nouvelles menaces, des avancées technologiques et de l'environnement réglementaire.

L'année 2023 pourrait être qualifiée de tumultueuse du point de vue de la cybersécurité ; l'année a vu une augmentation significative de la sophistication et de la gravité des attaques. Les entreprises ont réagi en augmentant leurs investissements dans la cybersécurité et en donnant la priorité à des initiatives pertinentes pour prévenir les attaques et améliorer leur posture de sécurité. Les enseignements tirés des attaques précédentes en 2022 ont incité les dirigeants et les entreprises de toutes tailles et de tous secteurs à investir dans des mesures de lutte contre les cybermenaces. L'IA apporte à la fois des défis et des opportunités à la cybersécurité, offrant l'automatisation pour l'analyse et la détection tout en posant des risques de biais et d'abus.

Du point de vue des entreprises, même les petites entreprises ont pris conscience de leur vulnérabilité aux cybermenaces, ce qui a alimenté la demande de services de sécurité (gérés) et de cyber résilience qui permettraient une reprise rapide et une restauration des opérations après un incident cybernétique. C'est pourquoi les prestataires de services et les vendeurs proposent des services et des solutions qui aident les entreprises à assurer la reprise et la continuité de leurs activités.

Les fournisseurs 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 émergentes, comprendre l'impact transformateur de technologies telles que l'IA et le ML, et rester à l'écoute de l'évolution des cadres réglementaires sur la protection des données, tels que le NIS-2, dans l'Union européenne.

Introduction

Les cybercriminels ont exploité des vulnérabilités à grande échelle, en utilisant constamment des ransomwares pour perturber les activités des entreprises, en particulier les services de santé, la chaîne d'approvisionnement et le secteur public.

Par conséquent, les entreprises ont commencé à investir dans des solutions telles que la gestion des identités et des accès (IAM), la prévention des pertes de données (DLP), la détection et réponse gérées (MDR), ainsi que la sécurité des clouds et des terminaux. Le marché s'oriente vers des solutions intégrées telles que le Security Service Edge (SSE) et la Détection et Réponse Etendues (XDR), qui s'appuient sur les meilleurs outils et l'expertise humaine, complétés par une intelligence comportementale et contextuelle et par l'automatisation, afin d'offrir une posture de sécurité supérieure.

Cybersecurity Services: 2024

Quadrants	Attributes		Application Security	Cloud and Data Center Security	Network Security	Data Security	Endpoint Security
Strategic Security Services	Security Consulting	Compliance and Risk Advisory Services					
	Security Assessments and Audits	Awareness and Training					
Technical Security Services	Security Solutions Implementation	Architecture and roadmap					
	Expertise and Technical Support	Security Tools and Technologies Maintenance					
Managed Security Services - SOC	Security Monitoring	Advanced Security Analytics					
	Orchestration and Automation	Managed Detection and Response					
Digital Forensics and Incident Response	Response Planning	Investigation					
	Analysis	Incident Mitigation					
Vulnerability Assessment and Penetration Testing	Vulnerability Detection	Analysis					
	Reporting	Escalation					

Cybersecurity Solutions: 2024

Quadrants	On-Premises or SaaS Offering based on Proprietary Software		Application Security	Cloud and Data Center Security	Network Security	Data Security	Endpoint Security
Identity and Access Management	Identity Management	Privileged Access Management					
	Access Management	Zero Trust					
Extended Detection and Response	Unified Endpoint Management	Network Detection and Response					
	Threat Intelligence	Endpoint Detection, Protection and Response					
Security Service Edge (SSE)	Zero Trust Network Access	Cloud Access Security Broker					
	Secure Web Gateways	Firewall as a Service					
Data Leakage/Loss Prevention (DLP) and Data Security	Data Identification and Classification	Data Protection					
	Data Monitoring	Enforce Policies					

Principaux domaines d'intérêt pour Cybersécurité – Solutions et services 2024.

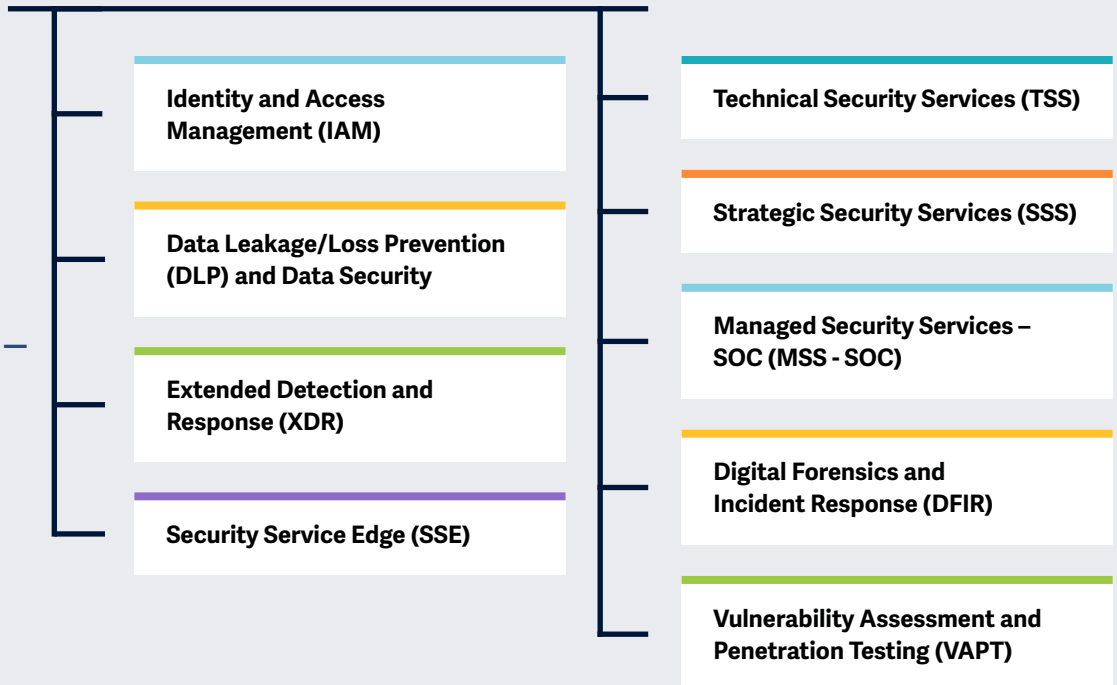


Illustration simplifiée Source: ISG 2024

Le rapport ISG Provider Lens™ Cybersecurity - Solutions et services offre les éléments suivants aux décideurs commerciaux et informatiques :

- Transparence sur les forces et les faiblesses des prestataires concernés
- Un positionnement différencié des fournisseurs par segments sur leurs forces concurrentielles et l'attractivité de leur portefeuille
- L'accent est mis sur différents marchés, notamment les États-Unis, le Royaume-Uni, l'Allemagne, la Suisse, la France, le Brésil, l'Australie et le secteur public américain. Les thèmes SSE et XDR seront analysés pour le marché mondial.
- Pour tenir compte des caractéristiques propres à chaque pays dans cette étude mondiale, l'analyse de XDR s'étend au Brésil, tandis que l'Allemagne analyse exclusivement la DLP. L'introduction du DFIR sera pilotée aux États-Unis et en France, et le nouveau thème de l'évaluation de la vulnérabilité et des tests de pénétration fera ses débuts au 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 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.

Définition

Les 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 appareils des utilisateurs de l'entreprise. Ce quadrant inclut également les offres SaaS basées sur des logiciels propriétaires. **Il exclut les fournisseurs de services purs qui ne proposent pas de produit IAM (sur site et/ou dans le cloud) basé sur un logiciel propriétaire.** En fonction des besoins de l'entreprise, ces offres peuvent être déployées de différentes manières, par exemple sur site, dans des clouds gérés par le client ou dans des modèles "as-a-service", ou encore une combinaison des deux.

Les solutions IAM visent à gérer (collecter, enregistrer et administrer) les identités des utilisateurs et les droits d'accès correspondants, et comprennent un accès spécialisé aux actifs critiques par le biais de la gestion des accès privilégiés (PAM), où l'accès est accordé sur la base 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 sécurisés, à des frameworks et à l'automatisation (par exemple, l'analyse des risques) afin de fournir des fonctionnalités de profilage des utilisateurs et des attaques en temps réel. Les fournisseurs de solutions devraient également proposer des fonctionnalités supplémentaires pour les réseaux sociaux et l'utilisation mobile afin de répondre aux besoins de sécurité spécifiques au-delà de la gestion traditionnelle des droits web et contextuels. Ce quadrant inclut également la gestion de l'identité des machines.

Critères d'éligibilité

1. Proposer des solutions qui peuvent être **déployées sur site, dans le cloud, sous forme d'identité en tant que service** (IDaaS) ou de modèle géré par un tiers
2. Proposer 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 fondé sur les rôles** et le PAM
4. Fournir une **gestion des accès** pour un ou plusieurs besoins 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 anciennes et nouvelles**, notamment SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust et SCIM
6. Proposer une offre comprenant 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) - pour prendre en charge l'accès sécurisé

Définition

Les fournisseurs de solutions DLP évalués pour ce quadrant se caractérisent par leur capacité à offrir des logiciels propriétaires et des services associés, y compris des solutions SaaS. Ce quadrant **exclut 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 de DLP permettent d'identifier et de surveiller les données sensibles, de fournir l'accès qu'aux utilisateurs autorisés et de prévenir les pertes/fuites de données. Les solutions des fournisseurs dans ce domaine comprennent un ensemble de produits offrant une visibilité et un contrôle sur les données sensibles résidant dans les applications dans le cloud, les terminaux, les réseaux et divers appareils.

Ces solutions prennent une importance considérable en raison des défis croissants auxquels sont confrontées les entreprises en matière de contrôle des mouvements et des transferts de données, plus d'un tiers des violations de données ayant une origine interne. Le nombre d'appareils, y compris les appareils mobiles, utilisés pour le stockage des données amplifie ces préoccupations. La connectivité Internet permet à ces appareils d'échanger des données sans passer par une passerelle centrale. Les solutions de sécurité des données protègent les données contre l'accès non autorisé, la divulgation ou le vol en hiérarchisant, classant et surveillant les données (au repos et en transit) tout en permettant aux organisations de rendre compte de la sécurité des données et de l'améliorer.

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 sa capacité à **gérer la** protection des **données sensibles, qu'elles soient structurées ou non**, textuelles ou binaires.
4. Offrir une solution avec une **aide à la gestion de base**, y compris, mais sans s'y limiter, l'**établissement de rapports, le contrôle des politiques**, l'installation et la maintenance et les fonctionnalités de détection des menaces avancées
5. Proposer une solution capable 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 caractérisent par leur capacité à offrir une plateforme qui intègre, met en corrélation, contextualise les données et les alertes provenant de multiples composants de prévention, de détection et de réponse aux menaces. La technologie XDR est une technologie cloud qui comprend des solutions en plusieurs points. Elle utilise des analyses avancées pour corréler des alertes provenant de sources multiples, y compris des signaux individuels faibles, afin de permettre des détections précises. Les solutions XDR consolident et intègrent plusieurs produits, offrant une sécurité complète pour les espaces de travail, les réseaux et les charges de travail. En règle générale, les solutions XDR visent à améliorer considérablement la visibilité et la compréhension du contexte des menaces identifiées dans l'entreprise. Les caractéristiques de ces solutions comprennent la télémétrie et l'analyse des données contextuelles pour la détection et la réponse. Les solutions XDR comprennent plusieurs produits intégrés dans une seule interface pour des capacités sophistiquées de visualisation, de détection et de réponse. Leur grande maturité en matière d'automatisation et d'analyse contextuelle permet d'apporter des réponses sur mesure aux systèmes affectés, en hiérarchisant les alertes en fonction de leur gravité par rapport à des cadres de référence connus. Ce quadrant exclut les **fournisseurs de services purs qui n'offrent pas de solution XDR basée sur un logiciel propriétaire.** Les solutions XDR visent à réduire la prolifération des produits, la fatigue des alertes, les difficultés d'intégration et les dépenses opérationnelles. Elles sont particulièrement adaptées aux équipes chargées des opérations de sécurité qui s'efforcent de gérer des portefeuilles de solutions diversifiés ou de 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 éléments 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 des terminaux, les plateformes de protection des terminaux**, la protection des réseaux (pare-feu, IDPS), la **détection et la réponse des réseaux**, la gestion des identités, la sécurité du courrier électronique, la détection des menaces mobiles, la protection des charges de travail dans le cloud et l'identification de la tromperie.
4. Fournir une solution avec une **couverture et une visibilité complète et totale de tous les terminaux d'**un réseau
5. Offrir une solution capable de **bloquer les** menaces sophistiquées telles que les **menaces persistantes avancées, les ransomwares** et les logiciels malveillants.
6. Fournir une solution à l'aide de **renseignements sur les menaces** et d'**informations en temps réel sur les menaces** émanant des terminaux
7. Proposer une solution comprenant des **fonctions de réponse automatisée**

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, aux SaaS, aux services web et aux applications privées. Les fournisseurs proposent des solutions SSE sous la forme d'un service de sécurité intégré par le biais de points de présence (PoP) positionnés à l'échelle mondiale, avec une prise en charge du stockage local des données, qui combine des solutions individuelles telles que l'accès au 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 pertes et fuites de données (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 fournisseurs mettent en avant leur expertise en matière de respect des lois locales, régionales et nationales, telles que la souveraineté des données, pour les clients internationaux.

Ce quadrant exclut les composants réseau du SASE (Secure Access Service Edge), tels que le SD-WAN, qui sont traités dans l'étude ISG Provider Lens™ Network - Software Defined Solutions and Services 2024.

Les solutions de SSE mettent fortement l'accent sur l'utilisateur, en fournissant la sécurité aux utilisateurs finaux à la périphérie ou aux appareils via le cloud - plutôt que de permettre aux utilisateurs d'accéder aux applications et aux bases de données de l'entreprise - via des réseaux dédiés de manière centralisée. ZTNA crée une connectivité exclusive entre les utilisateurs et les applications, en utilisant une analyse comportementale basée sur le contexte pour gérer l'accès. CASB offre une visibilité, applique les politiques de sécurité et la conformité, et contrôle l'utilisation de l'informatique dématérialisée, 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, avec une automatisation avancée pour évaluer l'UX.

Critères d'éligibilité

1. Fournir le SSE en tant que **solution intégrée** avec l'**accès au 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)**
2. Offrir des solutions **principalement fondées sur des** logiciels **propriétaires**, elles peuvent **s'appuyer partiellement sur des solutions de partenaires** tout en évitant une **dépendance totale à l'égard de** logiciels **tiers**
3. Maintenir des **points de contact dans le monde entier** pour fournir ces solutions
4. **Fournir le 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)** afin de détecter et de prévenir les intentions malveillantes ou suspectes
6. Offrir une **assistance de base à la gestion**, 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 globale de la solution**

Définition

Les fournisseurs de TSS évalués pour ce quadrant assurent l'intégration, la maintenance et le support des produits ou solutions de sécurité IT et OT. Les TSS couvrent tous les produits de sécurité, y compris les antivirus, la sécurité du cloud et des centres de données, l'IAM, la DLP, la sécurité des réseaux, la sécurité des terminaux, la gestion unifiée des menaces (UTM), la sécurité OT, SASE, et d'autres.

Les fournisseurs de services de sécurité proposent des plans d'action et des feuilles de route standardisés qui aident à transformer un environnement de sécurité existant avec les meilleurs outils et technologies, améliorant ainsi la posture de sécurité et réduisant l'impact des menaces. Leurs offres sont conçues pour permettre des transformations complètes des architectures de sécurité existantes dans des domaines tels que les réseaux, le cloud, les postes de travail, l'OT, l'IAM, la confidentialité et la protection des données, la gestion des risques et de la conformité et SASE, entre autres. Les offres comprennent également l'identification de produits ou de solutions, l'évaluation, la conception et le développement, la mise en œuvre, la validation, les tests de pénétration, l'intégration et le déploiement.

Les fournisseurs de TSS 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 la portée de leur offre. Ce quadrant englobe également les services de sécurité gérés classiques 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, mais qui sont capables de mettre en œuvre et d'intégrer des solutions d'autres fournisseurs.

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. Avoir obtenu l'**autorisation des fournisseurs de technologies de sécurité** (matériel et logiciel) de distribuer et de soutenir des solutions de sécurité
3. **Employer des experts certifiés** (les certifications peuvent être parrainées par des vendeurs, des associations, des organisations ou des agences gouvernementales) capables de prendre en charge les technologies de sécurité

Définition

Les fournisseurs de SSS évalués dans le cadre de ce quadrant proposent des services de conseil en matière de sécurité IT et OT. Ces services comprennent des audits de sécurité, des services de conseil en matière de conformité et de risque, des évaluations de sécurité, des conseils en matière de solutions de sécurité , ainsi que de la sensibilisation et de la formation. Ces fournisseurs aident également à évaluer la maturité de la sécurité et la position des risques et à définir des stratégies de cybersécurité pour les entreprises en fonction de leurs besoins spécifiques.

Ces fournisseurs devraient employer des consultants en sécurité ayant une grande expérience de la planification, du développement et de la gestion de programmes de sécurité de bout en bout pour les entreprises. Étant donné que les PME ont de plus en plus besoin de ce type de services et qu'il n'y a pas assez de talents disponibles, les fournisseurs de SSS devraient également rendre ces experts disponibles à la demande par le biais de services vCISO (virtual Chief Information Security 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 critiques pour la reprise. Ils devraient également organiser périodiquement des exercices cyber pour les membres du conseil d'administration, les principaux dirigeants d'entreprise et les employés afin de les aider à acquérir une connaissance cyber et afin d'établir les meilleures pratiques pour mieux répondre aux menaces et aux cyberattaques réelles. Ils devraient également connaître les technologies et les produits de sécurité disponibles sur le marché et donner des conseils sur le choix du meilleur produit et du meilleur fournisseur en fonction des besoins spécifiques de l'entreprise.

Ce quadrant examine les fournisseurs de services qui ne se concentrent pas exclusivement sur des produits ou des solutions propriétaires. Les services analysés ici couvrent toutes les technologies de sécurité, y compris la sécurité OT et SASE.

Critères d'éligibilité

1. Démontrer des aptitudes dans les domaines du SSS tels que l'**évaluation, la sélection des fournisseurs, le conseil en solutions et le conseil en matière de risques**
2. **Offrir au moins l'un des** services de sécurité stratégique **susmentionnés** dans le pays concerné
3. Fournir des **services de conseil en matière de sécurité à l'aide de méthodologies éprouvées**
4. **Pas d'orientation exclusive** sur des **produits** ou des solutions propriétaires

Définition

Les fournisseurs évalués dans le quadrant MSS-SOC offrent des services liés à la surveillance continue des infrastructures IT et OT et à la gestion de l'infrastructure sécurité pour un ou plusieurs clients par un centre d'opérations de sécurité (SOC). **Ce quadrant examine les fournisseurs de services qui ne sont pas exclusivement axés sur des produits propriétaires, mais qui peuvent gérer et exploiter les meilleurs outils de sécurité**. Ces fournisseurs de services peuvent gérer l'ensemble du cycle de vie des incidents de sécurité, de l'identification à la réponse.

Les fournisseurs sont de plus en plus sollicités pour aider les entreprises à renforcer leur position globale en matière de sécurité et à maximiser l'efficacité à long terme de leurs programmes de sécurité grâce à une amélioration continue. Les fournisseurs de MSS-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 technologies et infrastructures les plus récentes. Ils doivent également posséder une expertise en matière de chasse aux menaces et de gestion des incidents afin d'aider les entreprises à détecteret réagir activement à travers l'atténuation et l'endiguement des menaces . Pour répondre aux attentes croissantes des clients en matière de chasse aux menaces proactive, les fournisseurs améliorent leurs environnements SOC avec des renseignements sur les menaces de sécurité et les vulnérabilités, grâce à des investissements importants dans des technologies telles que l'automatisation, le big data, l'analytique, l'IA et le ML. Ces SOC sophistiqués prennent en charge la réponse aux renseignements de sécurité pilotée par des experts, offrant aux clients une approche holistique et unifiée de la sécurité de niveau avancé.

Critères d'éligibilité

1. 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** 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 la prévention et la **détection, les solutions de gestion des informations et des événements de sécurité (SIEM), les** conseillers en sécurité et l'aide à l'audit, à distance ou sur le site d'un client
3. Posséder des **accréditations** de fournisseurs d'outils de sécurité.
4. **Gérer ses propres SOCs**
5. Maintenir le **personnel** avec des certifications telles que Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) et Global Information Assurance Certification (GIAC)
6. Proposer différents modèles de tarification

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 fournisseurs de services qui proposent des techniques et des méthodologies DFIR éprouvées et qui sont capables de travailler avec les meilleurs outils pour répondre aux incidents de cybersécurité. DFIR implique l'identification, l'investigation, le confinement et la remédiation des incidents de cybersécurité. L'escalade de la fréquence et de la gravité des incidents de cybersécurité a favorisé l'adoption des services DFIR. Les fournisseurs de services devraient présenter des capacités approfondies et pratiques en matière de criminalistique numérique, de découverte électronique, de triage fondé sur des critères prédéfinis, d'analyse de la chronologie, d'analyse des logs, d'analyse des logiciels malveillants et d'examen des artefacts. À la suite d'une violation, la DFIR joue un rôle essentiel dans la découverte des pertes de données et des dommages spécifiques.

Les services DFIR aident à mettre en place une réponse efficace à la menace , en utilisant des playbooks de réponse à incident et des analyses pour comprendre le comportement des acteurs de la menace et les causes profondes. Les fournisseurs de services de DFIR doivent posséder une expérience dans l'assistance aux entreprises en cas de litige pour les réclamations d'assurance et les audits réglementaires postérieurs à la violation. Ils savent utiliser des outils internes et tiers tels que la gestion des informations et des événements de sécurité (SIEM), l'orchestration de la sécurité, l'automatisation et la réponse (SOAR), la détection et la réponse sur les dispositifs (EDR) et la détection et la réponse étendues (XDR).

Critères d'éligibilité

1. Disposer d'une **équipe spécialisée dans la réponse aux incidents** (CERT, CSIRT), composée d'experts titulaires de certifications pertinentes telles que GCFA, GCFE et CISSP, qui témoignent de leur expertise et de leur engagement à respecter les normes du secteur
2. Posséder une expérience et une expertise dans la **gestion d'une variété de** solutions SIEM, SOAR, EDR et XDR
3. Les services de la DFIR **ne se contenteront pas d'identifier la violation**, mais établiront également la chronologie, la cause première et l'impact de la violation
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 pertinents et les prestataires de services de sécurité gérés afin de recueillir des informations sur les menaces, de surveiller le "dark web" et de disposer de capacités SOC pour atténuer les menaces persistantes et sophistiquées

Définition

Les prestataires de services de VAPT se caractérisent par le fait qu'ils offrent des compétences techniques raffinées qui nécessitent un degré élevé de mise à jour, non seulement en ce qui concerne les lacunes connues et découvertes au jour le jour, mais aussi en ce qui concerne les approches et mécanismes de plus en plus élaborés permettant de contourner les lignes de défense établies.

L'année 2023 a été marquée par l'accès à des outils d'IA générative, permettant à un nombre illimité de personnes d'identifier et d'exploiter les vulnérabilités des actifs technologiques, en particulier ceux qui sont directement exposés à l'internet. En outre, on a assisté à une prolifération d'incidents impliquant des ransomwares, avec des cas récurrents, soulignant la nécessité d'une protection continue du périmètre, qui ne se limite plus à des évaluations annuelles ou semestrielles ponctuelles.

Compte tenu de la fréquence actuelle des mises à jour des services exposés à l'internet par les entreprises, l'insertion de services de détection continue des vulnérabilités (avant et après l'entrée en production) est devenue fondamentale dans la stratégie de cybersécurité et, avec les autres tendances, constitue le défi et la mission des fournisseurs de ce quadrant.

Le scénario est celui d'une course effrénée contre des menaces orchestrées, de plus en plus sophistiquées sur le plan méthodologique et technique et dotées d'un fort pouvoir de destruction. Les fournisseurs de ce quadrant doivent donc proposer des antidotes appropriés en plus de l'approche traditionnelle, désormais reconnue comme insuffisante pour atténuer les risques et les impacts.

Critères d'éligibilité

1. Disposer d'équipes internes spécialisées capables d'**évaluer rigoureusement les vulnérabilités et d'indiquer des solutions** pour éliminer les failles et/ou réduire progressivement leur gravité, sur la base de preuves concrètes des vecteurs d'attaque
2. Proposer des services comprenant des **approches de type boîte noire, boîte grise et boîte blanche**, capables d'évaluer, par exemple, 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 **DAST, SAST et Pentesting** des objectifs spécifiques à l'aide d'outils manuels et/ou automatisés pour la fourniture de services
4. **Les normes industrielles reconnues** telles que SOC 2, ISO27001, NIST 800-53, PCI-DSS et HIPPA doivent être utilisées et prouvées lorsqu'elles indiquent des failles de sécurité
5. Proposer de **nouveaux tests, un soutien spécialisé et des mécanismes de** suivi des actions correctives, reflétés de manière dynamique dans la mise à jour de la matrice des risques et de la gravité (exposition aux vecteurs restants)

Quadrants par région

Dans le cadre de cette étude des quadrants ISG Provider Lens™, nous présentons les neuf quadrants suivants sur la cybersécurité - Solutions et services 2024 :

Quadrant	ÉTATS-UNIS	ROYAUME-UNI	Allemagne	Suisse	France	Brésil	Australie	Secteur public américain	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 (TSS)	✓	✓	✓	✓	✓	✓	✓	✓	
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	✓	✓	✓	
Managed Security Services – SOC (MSS - SOC)	✓	✓	✓	✓	✓	✓	✓	✓	
Digital Forensics and Incident Response (DFIR)	✓				✓				
Vulnerability Assessment and Penetration Testing (VAPT)						✓			

La phase de recherche se situe entre janvier et février 2024, période au cours de laquelle auront lieu l'enquête, l'évaluation, l'analyse et la validation. Les résultats seront publiés en juillet 2024.

Jalons	Début	Fin
Lancement de l'étude	8 janvier 2024	
Phase d'étude	8 janvier 2024	22 février 2024
Avant-première	mai 2024	
Communiqué de presse et publication	juillet 2024	

Veuillez vous référer au lien pour consulter/télécharger le programme de recherche ISG Provider Lens™ 2024.

Accès au portail en ligne :

Vous pouvez visualiser/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 nous réjouissons de votre participation !

Recherche Production Disclaimer :

ISG recueille des données dans le but d'effectuer des recherches et de créer des profils de prestataires/fournisseurs. Les profils et les données qui les accompagnent sont utilisés par les conseillers d'ISG pour faire des recommandations et informer leurs clients de l'expérience et des qualifications de tout fournisseur applicable à l'externalisation du travail identifié par les clients. Ces données sont collectées dans le cadre du processus FutureSource™ 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 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 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™ – Call for nominations

L'étoile d'excellence est une reconnaissance indépendante de l'excellence de la prestation de services basée sur le concept de la "voix du client". L'étoile de l'excellence est un programme conçu par l'ISG pour recueillir les commentaires des clients sur la réussite des fournisseurs 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 associés aux études IPL. Par conséquent, tous les analystes d'ISG recevront en permanence des informations sur l'expérience des clients de tous les fournisseurs de services concernés. Ces informations viennent s'ajouter aux commentaires de première main des conseillers que l'IPL exploite dans le cadre de son approche de conseil dirigée par les praticiens.

Les fournisseurs 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'ISGanonymise toutes les données relatives aux clients et ne les partage pas avec des tiers.

Notre vision est que l'Étoile de l'excellence soit reconnue comme la principale reconnaissance du secteur pour l'excellence du service à la clientèle et qu'elle serve de référence pour mesurer les sentiments des clients. Pour vous assurer que les clients que vous avez sélectionnés remplissent le questionnaire relatif à votre mission, veuillez utiliser la section de nomination des clients sur le site web de l'Étoile de l'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, veuillez prévoir jusqu'à 24 heures pour une réponse.

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

Contacts pour cette étude

Frank Heuer

Analyste en chef – Allemagne, Suisse

Gowtham Kumar

Analyste en chef – États-Unis

Bhuvaneshwari Mohan

Analyste en chef – Royaume-Uni

Benoit Scheuber

Analyste en chef – France

Maxime Martelli

Analyste en chef – France

Craig Baty

Analyste en chef – Australie

Christian Horst Alves Reis

Analyste en chef – Brésil

Phil Hassey

Analyste en chef – Secteur public américain

Monica K

Analyste de recherche

Contacts pour cette étude

Bhuvaneshwari Mohan

Analyste de recherche

Sandya Kattimani

Analyste de recherche

Bruno Nakazone

Analyste de recherche

Shreemadhu Rai B

Chef de projet

Rajesh Chillappagari

Analyste de données

Laxmi Sahebrao Kadve

Analyste de données

Programme de participation des conseillers ISG

ISG Provider Lens propose des évaluations de marché qui intègrent les points de vue des praticiens, reflètent l'orientation régionale et la recherche indépendante. ISG s'assure de 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 d'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 participent à l'équipe d'examen de la qualité et de la cohérence (QCRT) de chaque étude.

Le QCRT veille à ce que chaque étude reflète l'expérience des conseillers d'ISG sur le terrain, 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 QCRT et contribuent à différents niveaux en fonction de leur disponibilité et de leur expertise.

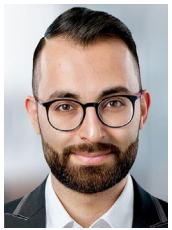
Les conseillers du QCRT :

- Aident à définir et à valider les quadrants et les questionnaires,
- Conseillent sur l'inclusion des fournisseurs 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

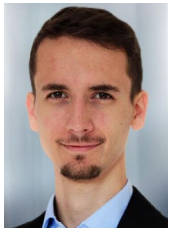
Doug Saylors

Associé, codirigeant ISG Cybersecurity



Reza Memarian

Consultant principal en cybersécurité



Anas Barmo

Consultant principal en cybersécurité

Joyce Harkness

Directrice de la cybersécurité

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 dans l'itération précédente

Solution Providers

Absolute Software*
Acronis*
Akamai*
Alice&Bob.Company*
Aruba*
Atos*
Avatier*
AWS*
BAYOONET*
Brainloop*
Broadcom*
Cato Networks*
Check Point*
Cipher*
Cisco*
CoSoSys*
Cross Identity*
CrowdStrike*
CyberArk*
Cybereason*
Cynet*
Darktrace*
DriveLock*
Elastic Security
EmpowerID*
Ergon*
Ericom Software*
eSentire*
ESET*
E-TRUST*
Fidelis Cybersecurity*
Fischer Identity*
Forcepoint*
ForgeRock*
Fortinet*
Fortra
FusionAuth*
GBS*
GoCache*
Google*
HarfangLab*
Hashicorp*
HCLTech*
Heimdal Security*
Huge Networks*
IBM*
iboss*
Imprivata*
IN Groupe*
Infinite Networks*
itWatch*
Kasada*
Kaspersky*
LastPass*
Logpoint*

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 dans l'itération précédente

Lookout*
ManageEngine*
Mandiant*
Matrix42*
Microland*
Microsoft*
Netskope*
NetWitness*
Nevis*
Nok Nok Labs*
Okta*
Omada*
One Identity (OneLogin)*
Open Systems*
OpenText*
Oracle*
Orange Cyberdefense*
Palo Alto Networks*
Perimeter 81*
Ping Identity*
Proofpoint*
Rapid7*
RSA*
SailPoint*
SAP*
Saviynt*
SecureAuth*
Secureworks*
senhasegura*
SenseOn*
SentinelOne*
SilverSky*
Skyhigh Security*
Solarwinds*
Sophos*
Systancia*
TEHTRIS*
Tenfold
Thales*
Trellix*
Trend Micro*
Unisys*
United Security Providers*
Varonis*
Versa Networks*
VMware*
Wallix*
WatchGuard*
WithSecure*
Zscaler*

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 dans l'itération précédente

Service Providers

Accenture*
ActioNet*
Adarma*
Advens*
Agility*
Airbus CyberSecurity*
All for One Group*
ASG*
AT&T Cybersecurity*
Atos*
Aveniq*
Avertium*
Axians*
Bechtle*
Beta Systems*
BeyondTrust*
Bitdefender*
BlackBerry*
BluePex*
BlueVoyant*
BT*
CANCOM*
Capgemini*
CGI*
Cipher*
Cirion*
Cisco*
Claranet*
Cloudflare*
Comline
Compugraf*
Computacenter*
Conscia*
Controlware*
Critical Start*
CTM*
CyberSecOp*
Cyderes*
Data#3*
Datacom*
Deloitte*
Deutsche Telekom*
DIGITALL*
ECSC*
Edge UOL*
EY*
FastHelp*
Getronics*
glueckkanja-gab*
HackerSec*
Happiest Minds*
HCLTech*
HiSolutions*
IBLISS*
IBM*

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 dans l'itération précédente

iC Consult*
indevis*
InfoGuard*
Infosys*
Integrity360*
Intrinsec*
ISH*
ISPIN*
IT.eam*
Italtel*
ITC Secure*
I-Tracing
Itrust*
Khipu Networks*
KPMG*
Kudelski Security*
Kyndryl*
Leidos*
Logicalis*
LTIMindtree*
Lumen*
Macquarie Telecom Group*
Materna*
Microland*
Mphasis*
NCC Group*
NEC*
Nettitude*
Nextios*
Nomios*
NTT DATA*
NTT Ltd.*
NXO*
Obrela Security*
Open Systems*
Optiv*
Orange Cyberdefense*
Performanta*
Persistent Systems*
Presidio*
Proficio*
PurpleSec*
PwC*
Quorum Cyber*
Rackspace Technology*
Redbelt*
SCC*
Secureworks*
SecurityHQ*
Sekuro*
Service IT*
SFR*
Shearwater Group*
SilverSky*
SLK Software*
Softcat*

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 dans l'itération précédente

SONDA*
Sopra Steria*
Stefanini*
suresecure*
SVA System Vertrieb Alexander
Swisscom*
Syntax*
Talion*
Tata Communications*
TCS*
TDEC*
Tech Mahindra*
Telstra*
Tempest*
terreActive*
Tesserent*
Thales*
TIVIT*
Trustwave*
T-Systems*
UMB*
Unisys*
United Security Providers*
ValueLabs*
Vectra*
Verizon Business*
Wavestone*
Wipro*
Zensar*

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 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 1600 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 www.isg-one.com.

ISG Provider Lens™

JANVIER, 2024

REPORT: CYBERSECURITY – SOLUTIONS & SERVICES