ISG Provider Lens™

# Cybersecurity – Solutions and Services

Análise do mercado de segurança cibernética, comparando atratividade do portfólio de fornecedores e pontos fortes competitivos

**CATÁLOGO | JANEIRO DE 2024 | AUSTRÁLIA, BRASIL, FRANÇA, ALEMANHA, SUÍÇA, REINO UNIDO, EUA, SETOR PÚBLICO DOS EUA E GLOBAL**

Índice

**Segurança cibernética na era da IA**

O cenário atual da segurança cibernética é dinâmico, com mudanças ocorrendo rapidamente devido a ameaças emergentes, avanços tecnológicos e ambientes regulatórios em evolução.

O ano de 2023 pode ser considerado tumultuado em termos de segurança cibernética, com aumento na sofisticação e severidade dos ataques. As empresas responderam aumentando os investimentos em segurança cibernética e priorizando iniciativas relevantes para prevenir ataques e melhorar a postura de segurança. Os aprendizados obtidos com ataques em 2022 levaram executivos e empresas de todos os portes e setores a investir em medidas de combate às ameaças cibernéticas. A IA traz desafios e oportunidades para a segurança cibernética. Oferece automação para análise e detecção, mas apresenta riscos de enviesamento e uso indevido.

Do ponto de vista empresarial, até pequenas empresas perceberam sua vulnerabilidade às ameaças cibernéticas, aumentando a procura por serviços de segurança (gerenciados) e de resiliência cibernética para recuperar e restaurar a operação após incidentes cibernéticos. Assim, os fornecedores de serviços e fabricantes estão oferecendo serviços e soluções que ajudam empresas a garantir a recuperação e a continuidade dos negócios.

Os fornecedores de serviços de segurança ajudam clientes a enfrentar o cenário da segurança cibernética, em que a vigilância é crucial para identificar e mitigar ameaças emergentes, entender o impacto transformador de tecnologias como IA e ML e permanecer atentas à evolução dos regulamentos sobre proteção de dados, como NIS-2, na União Europeia.

Os cibercriminosos exploraram vulnerabilidades em grande escala, utilizando persistentemente ransomware para perturbar as atividades empresariais, especificamente no segmento de saúde, em cadeias de suprimentos e nos serviços do setor público.

Consequentemente, as empresas começaram a investir em soluções, como gestão de identidade e acesso (IAM), prevenção contra perda de dados (DLP), gerenciamento de detecção e resposta (MDR) e segurança em nuvem e endpoint. O mercado está migrando para soluções integradas, como security service edge (SSE) e detecção e resposta estendida (XDR), que aplicam as melhores ferramentas e experiência humana, melhoradas com inteligência comportamental e contextual e automação para oferecer uma postura de segurança superior.

## Cybersecurity Services: 2024

| Quadrants | Attributes | | | | | | |
|---|---|---|---|---|---|---|---|
| Strategic Security Services | Security Consulting | Compliance and Risk Advisory Services | Application Security | Cloud and Data Center Security | Network Security | Data Security | Endpoint Security |
| | 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 | | | | | |

# Key focus areas for Cybersecurity – Solutions and Services 2024.

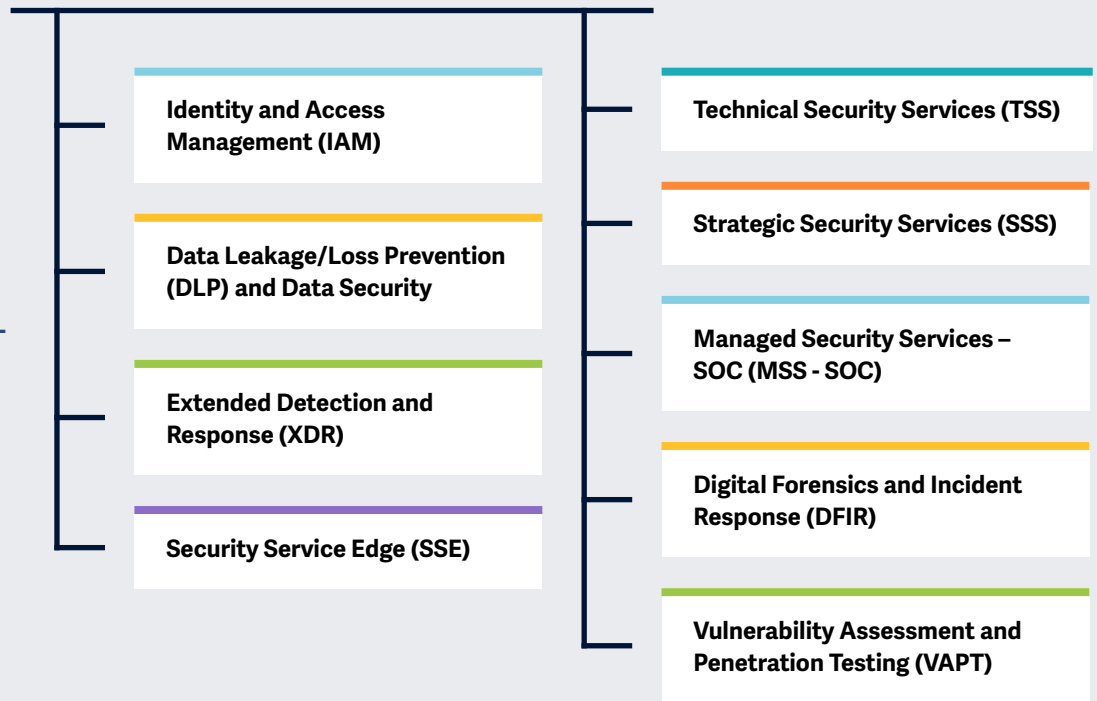



Ilustração simplificada Fonte: ISG 2024

**O relatório ISG Provider Lens™ Cybersecurity – Solutions and Services oferece o seguinte aos tomadores de decisão de negócios e de TI:**

- Transparência sobre os pontos fortes e fracos dos fornecedores relevantes
- Um posicionamento diferenciado de fornecedores por segmentos, sobre seus pontos fortes competitivos e atratividade de portfólio
- O foco em diferentes mercados, incluindo EUA, Reino Unido, Alemanha, Suíça, França, Brasil, Austrália e Setor Público dos EUA. Os tópicos sobre SSE e XDR serão analisados quanto ao mercado global.
- Para considerar as características específicas dos países neste estudo global, a análise de XDR se estende ao Brasil, enquanto, para a Alemanha, analisa-se a DLP. A introdução da DFIR será testada nos EUA e na França. O novo tópico de Avaliação de Vulnerabilidade e Teste de Penetração será lançado no Brasil.

Nosso estudo serve como uma importante base de tomada de decisão para o posicionamento de relacionamentos chave e considerações de estratégia de vendas. Consultores e clientes corporativos do ISG usam informações desses relatórios para avaliar seus relacionamentos com fabricantes atuais e novos relacionamentos em potencial.

**Definição**

Os fornecedores de soluções IAM avaliados neste quadrante são caracterizados por sua capacidade de oferecer softwares exclusivos e serviços associados para gerenciar identidades e dispositivos de usuários corporativos. O quadrante também inclui ofertas de SaaS para softwares exclusivos. **Exclui fornecedores de serviços puros que não oferecem um produto IAM (local ou em nuvem) baseado em softwares exclusivos**. Dependendo dos requisitos organizacionais, as ofertas podem ser implantadas de diversas maneiras: no local, em nuvens gerenciadas pelo cliente ou em modelos como serviço ou uma combinação destes.

As soluções IAM destinam-se a gerenciar (coletar, registar e administrar) identidades de usuários e respectivos direitos de acesso, incluindo acesso especializado a ativos críticos pelo gerenciamento de acesso privilegiado (PAM), em que o acesso é concedido conforme políticas definidas. Para lidar com os requisitos de aplicativos novos e existentes, as soluções IAM incorporam cada vez mais estruturas, automação e mecanismos seguros (por exemplo, análise de risco) para oferecer funcionalidades de criação de perfis de usuários e ataques em tempo real. Espera-se também que os fornecedores ofereçam recursos adicionais para mídias sociais e uso móvel para atender a necessidades de segurança específicas além do gerenciamento tradicional de direitos contextuais e da Web. Este quadrante também inclui gestão de identidades de máquina.

Critérios de Qualificação

1. Oferecer soluções que podem ser **implantadas** como um modelo **local, na nuvem, identidade como serviço** (IDaaS) ou gerenciado por terceiros
2. Oferecer soluções **compatíveis com autenticação**, como uma combinação de logon único (SSO), **autenticação multifatores** (MFA) e modelos baseados em risco e em contexto
3. Oferecer soluções **compatíveis com acesso baseado em funções** e PAM
4. Fornecer **gerenciamento de acesso** para uma ou mais necessidades empresariais, como **nuvem, endpoint, dispositivos móveis, APIs** e **aplicações web**
5. Oferecer soluções **compatíveis com um ou mais padrões IAM novos e legados**, incluindo SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust, SCIM etc.
6. Possuir portfólio com um ou mais dos seguintes – **soluções de diretório, gerenciamento por autoatendimento ou painel** e soluções de gerenciamento de ciclo de vida (migração, sincronização e replicação) – para oferecer suporte ao acesso seguro

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

**Definição**

Os fornecedores de soluções DLP avaliados neste quadrante são caracterizados por sua capacidade de oferecer softwares exclusivos e serviços associados, incluindo soluções SaaS. Este quadrante **exclui fornecedores de serviços puros que não oferecem um produto DLP (local ou em nuvem)** baseado em softwares exclusivos. As soluções DLP podem identificar e monitorar dados confidenciais, fornecer acesso apenas para usuários autorizados e evitar perda/vazamento de dados. As soluções dos fabricantes nesse espaço incluem uma combinação de produtos que proporcionam visibilidade e controle sobre dados confidenciais em aplicativos em nuvem, endpoints, redes e vários dispositivos.

Essas soluções estão ganhando importância considerável devido aos crescentes desafios das empresas no controle de movimentos e transferências de dados, visto que mais de um terço das violações de dados são originadas internamente. O número de dispositivos, incluindo dispositivos móveis, utilizados para armazenar dados amplifica estas preocupações. A conectividade com a Internet permite que os dispositivos troquem dados sem passar por um gateway central. As soluções de segurança protegem os dados contra acesso não autorizado, divulgação ou roubo, priorizando, classificando e monitorando os dados (em repouso e em trânsito), bem como permitem que as organizações relatem e melhorem a segurança dos dados.

Critérios de Qualificação

1. Oferecer soluções DLP baseadas em **softwares exclusivos**, e não em softwares de terceiros
2. Demonstrar capacidade de suporte a DLP **em qualquer arquitetura, como nuvem, rede, armazenamento ou endpoint**
3. Demonstrar capacidade de **lidar com proteção de dados confidenciais** em **dados estruturados ou não**, em texto ou binários
4. Oferecer solução com **suporte básico de gerenciamento**, incluindo, sem limitação, **geração de relatórios, controles de políticas**, instalação e manutenção e funcionalidades avançadas de detecção de ameaças
5. Oferecer solução capaz de **identificar dados confidenciais, aplicar políticas**, monitorar tráfego e melhorar a conformidade dos dados

**Definição**

Os fornecedores de soluções XDR avaliados neste quadrante são caracterizados pela capacidade de oferecer uma plataforma que integra, correlaciona e contextualiza dados e alertas de múltiplos componentes de prevenção, detecção e resposta a ameaças. XDR é uma tecnologia em nuvem com soluções de múltiplos pontos. Com análises avançadas, ela correlaciona alertas de diversas fontes, incluindo sinais individuais fracos, para permitir detecções precisas. As soluções XDR consolidam e integram vários produtos, proporcionando segurança abrangente para espaços de trabalho, redes e cargas de trabalho. Normalmente, as soluções XDR visam a melhorar significativamente a visibilidade e a compreensão do contexto das ameaças identificadas em toda a empresa. As características dessas soluções incluem telemetria e análise contextual de dados para detecção e resposta. As soluções XDR compreendem vários produtos integrados em um único painel para recursos sofisticados de visualização, detecção e resposta. Sua alta maturidade de automação e análise contextual oferecem respostas personalizadas para sistemas afetados, priorizando alertas com base na gravidade em termos de estruturas de referência conhecidas. Este quadrante exclui **fornecedores de serviços puros que não oferecem uma solução XDR baseada em softwares exclusivos**. As soluções XDR destinam-se a reduzir a dispersão de produtos, fadiga de alertas, desafios de integração e despesas operacionais. São particularmente adequadas para equipes de operações de segurança que precisam gerenciar diversos portfólios de soluções ou obter valor de soluções de gerenciamento de informações e eventos de segurança (SIEM) ou de orquestração, automação e resposta de segurança (SOAR).

Critérios de Qualificação

1. Oferecer soluções XDR baseadas em **softwares exclusivos**, e não softwares de terceiros
2. Certificar-se de que uma solução XDR tenha dois componentes principais: **XDR front-end e XDR back-end**
3. Oferecer front-end com **três ou mais soluções ou sensores**, incluindo, entre outros, **detecção e resposta de endpoint, plataformas de proteção de endpoint**, proteção de rede (firewalls, IDPS), **detecção e resposta de rede**, gestão de identidade, segurança de e-mail, detecção de ameaças móveis, proteção de carga de trabalho na nuvem e identificação de fraude
4. Fornecer solução com **cobertura e visibilidade abrangentes e totais de todos os endpoints** em uma rede
5. Oferecer solução capaz de **bloquear** ameaças sofisticadas, como **ameaças persistentes avançadas, ransomware** e malware
6. Fornecer soluções usando **inteligência de ameaças e insights em tempo real sobre ameaças** provenientes de endpoints
7. Oferecer solução com **recursos de resposta automatizada**

**Definição**

Os fornecedores de soluções de SSE avaliados neste quadrante oferecem soluções centradas na nuvem que combinam software ou hardware exclusivo e serviços associados, permitindo acesso seguro aos aplicativos em nuvem, SaaS, serviços da Web e aplicativos privados. Os fabricantes oferecem soluções de SSE como um serviço de segurança integrado por meio de pontos de presença (PoP) posicionados globalmente, com suporte para armazenamento local de dados que combina soluções individuais, como acesso à rede com zero trust (ZTNA), agente de segurança de acesso à nuvem (CASB), gateways seguros da internet (SWG) e firewall como serviço (FWaaS). O SSE também pode incluir outras soluções de segurança, tais como prevenção contra perda/vazamento de dados (DLP), isolamento de navegador e firewall de próxima geração (NGFW) para garantir acesso seguro a aplicativos na nuvem e no local.

Os fabricantes demonstram experiência no cumprimento de leis locais, regionais e nacionais, como soberania de dados, para clientes globais.

**Este quadrante exclui os componentes de** rede de secure access service edge **(SASE), como SD-WAN**, que são abordados no estudo ISG Provider Lens™ Network – Software Defined Solutions and Services 2024.

As soluções de SSE estão voltadas ao foco do usuário, proporcionando segurança aos usuários finais da edge ou dispositivos por meio da nuvem – em vez de permitir que os usuários acessem aplicativos e bancos de dados corporativos de forma centralizada – em redes dedicadas. A ZTNA cria conectividade exclusiva entre usuários e aplicativos, com análise comportamental baseada em contexto para gerenciar o acesso. O CASB oferece visibilidade, impõe políticas de segurança e conformidade e controla o uso da nuvem de TI oculta; já o FWaaS e o SWG evitam ameaças maliciosas e o acesso a sites e aplicativos infectados. Normalmente, uma solução de SSE conta com um console unificado para visibilidade e governança, com automação avançada para avaliar a experiência do usuário.

Critérios de Qualificação

1. Fornecer SSE como uma **solução integrada** com **rede zero trust (ZTNA), agente de segurança de acesso à nuvem (CASB), gateways seguros da internet (SWG) e firewall como serviço (FWaaS)**
2. Oferecer soluções **predominantemente baseadas em softwares exclusivos**, podendo **contar parcialmente com soluções de parceiros,** evitando a **total dependência em softwares de terceiros**
3. Manter **PoPs globais** para oferecer essas soluções
4. **Oferecer SSE para nuvem e ambientes locais** (incluindo ambientes híbridos)
5. Apresentar **avaliações e análises contextuais e comportamentais (análise de comportamento e entidade do usuário/UEBA)** para detectar e prevenir intenções maliciosas ou suspeitas
6. Oferecer **suporte básico de gerenciamento**, incluindo, sem limitação, **geração de relatórios, controles de políticas**, instalação e manutenção e funcionalidades avançadas de detecção de ameaças
7. Garantir a **disponibilidade global da solução**

**Definição**

Os fornecedores de TSS avaliados neste quadrante oferecem integração, manutenção e suporte para produtos ou soluções de segurança de TI e OT. Os TSS abordam produtos de segurança, incluindo antivírus, segurança para nuvem e data center, IAM, DLP, segurança de rede, segurança de endpoint, gerenciamento unificado de ameaças (UTM), segurança OT e SASE etc.

Os fornecedores de TSS oferecem manuais e roteiros padronizados que ajudam a transformar um ambiente de segurança existente com as melhores ferramentas e tecnologias, melhorando a postura de segurança e reduzindo o impacto das ameaças. Os portfólios são criados para permitir transformações completas ou individuais de arquiteturas de segurança em domínios como redes, nuvem, local de trabalho, OT, IAM, privacidade e proteção de dados, gerenciamento de risco e conformidade e SASE, entre outros. As ofertas também incluem identificação, avaliação, design e desenvolvimento de produtos ou soluções, implementação, validação, testes de penetração, integração e implantação.

Os fornecedores de TSS investem no estabelecimento de parcerias com soluções de segurança e fabricantes de tecnologia para obter credenciamentos especializados e expandir o escopo de seu portfólio. Este quadrante também abrange serviços clássicos de segurança gerenciados fornecidos sem um centro de operações de segurança (SOC).

**Este quadrante analisa fornecedores de serviços que não estão exclusivamente focados em seus produtos exclusivos, mas que são capazes de implementar e integrar soluções de outros fabricantes**.

Critérios de Qualificação

1. Demonstrar experiência na criação e **implementação de soluções de segurança cibernética** para empresas no respectivo país
2. Possuir **autorização de fabricantes de tecnologia de segurança** (hardware e software) para distribuir e oferecer suporte a soluções de segurança
3. **Empregar especialistas certificados** (as certificações podem ser credenciais patrocinadas por fabricantes, lideradas por associações e organizações ou por órgãos governamentais) capazes de oferecer suporte a tecnologias de segurança

**Definição**

Os fornecedores de SSS avaliados neste quadrante oferecem consultoria de segurança de TI e OT, com serviços de auditorias de segurança, consultoria de conformidade e risco, avaliações de segurança, consultoria de soluções de segurança e programas de conscientização e treinamento. Também ajudam a avaliar a maturidade da segurança e postura de risco e a definir estratégias de segurança cibernética para empresas, conforme requisitos específicos.

Esses fornecedores devem contratar consultores de segurança com vasta experiência em planejamento, desenvolvimento e gestão de programas de segurança ponta a ponta para empresas. Devido à crescente necessidade desses serviços pelas PMEs e à falta de disponibilidade de talentos, fornecedores de SSS também devem disponibilizar especialistas, mediante solicitação, pelos serviços de vCISO (virtual Chief Information Security Officer). Dado o foco na resiliência cibernética, fornecedores que oferecem SSS devem ser capazes de formular roteiros de continuidade dos negócios e priorizar aplicativos críticos para os negócios para recuperação. Devem também realizar exercícios práticos e simulações cibernéticas para membros do conselho, principais executivos e empregados, para desenvolverem o conhecimento de cibernética e estabelecerem melhores práticas, respondendo melhor a ameaças e ataques cibernéticos reais. Ademais, devem ser adeptos das tecnologias e produtos de segurança no mercado e aconselhar na escolha do melhor produto e fabricante conforme os requisitos específicos da empresa.

**Este quadrante examina fornecedores de serviços que não estão apenas focados em produtos ou soluções exclusivos**. Os serviços aqui analisados abrangem todas as tecnologias de segurança, incluindo segurança OT e SASE.

Critérios de Qualificação

1. Demonstrar habilidades em áreas de SSS, como **avaliações, seleção de fabricantes, consultoria de soluções e consultoria de risco**
2. **Oferecer pelo menos um** dos serviços estratégicos de segurança acima no respectivo país
3. Fornecer **serviços de consultoria de segurança usando frameworks**
4. **Não focar exclusivamente** em **produtos ou soluções exclusivos**

**Definição**

Os fornecedores avaliados no quadrante MSS-SOC oferecem serviços relacionados ao monitoramento contínuo de infraestruturas de segurança de TI e OT e gerenciamento de infraestrutura de TI para um ou vários clientes por um centro de operações de segurança (SOC). **Este quadrante analisa fornecedores de serviços que não estão apenas focados em produtos exclusivos, mas podem gerenciar e operar as melhores ferramentas de segurança**. Esses fornecedores de serviços abordam todo o ciclo de vida do incidente de segurança, desde a identificação até a resposta.

Há uma crescente procura de fornecedores que auxiliem empresas a melhorar a postura geral de segurança e maximizar a eficácia a longo prazo dos programas de segurança pela melhoria contínua. Os fornecedores de MSS-SOC devem combinar serviços de segurança gerenciados tradicionais com inovação para fortalecer os clientes com um mecanismo integrado de defesa cibernética. Devem fornecer gerenciamento de detecção e resposta (MDR) e ter as mais recentes tecnologias e infraestruturas. Também devem ter experiência em busca de ameaças e gestão de incidentes para auxiliar empresas na detecção e resposta proativa por meio da mitigação e contenção de ameaças. Para atender às expectativas dos consumidores quanto à identificação proativa de ameaças, estão aprimorando os ambientes SOC com inteligência sobre ameaças à segurança e vulnerabilidades e investimentos significativos em tecnologias, como automação, big data, análise, IA e ML. Os sofisticados SOCs oferecem suporte a respostas de inteligência de segurança orientadas por especialistas, oferecendo uma abordagem holística e unificada para segurança avançada.

Critérios de Qualificação

1. Os serviços habituais incluem **monitoramento de segurança, análise de comportamento, detecção de acesso não autorizado, consultoria sobre medidas de prevenção, testes de penetração** e todos os demais serviços operacionais para proporcionar proteção contínua e em tempo real sem comprometer o desempenho dos negócios.
2. Fornecer serviços de segurança, como prevenção e **detecção, serviços de gerenciamento de informações e eventos de segurança (SIEM)**, consultores de segurança e suporte a auditorias, seja remotamente ou no local do cliente
3. Possuir **credenciamentos** de fabricantes de ferramentas de segurança
4. **Gerenciar os próprios SOCs**
5. Manter **equipe** com certificações, como Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) e Global Information Assurance Certification (GIAC)
6. Possuir diversos modelos de preços

**Definição**

Os fornecedores avaliados no quadrante DFIR oferecem serviços relacionados a atividades de resposta a ameaças, preservando evidências contra invasores.

**Este quadrante analisa fornecedores de serviços que contam com técnicas e metodologias comprovadas de DFIR e podem trabalhar com as melhores ferramentas para responder a incidentes de segurança cibernética**. A DFIR envolve a identificação, investigação, contenção e remediação de incidentes de segurança cibernética. O escalonamento da frequência e gravidade dos incidentes de segurança cibernética contribuiu para a adoção de serviços de DFIR. Os fornecedores de serviços devem apresentar capacidades aprofundadas e práticas para lidar com análise forense digital, e-discovery, triagem baseada em critérios predefinidos, análise de linhas do tempo, análise de registros, análise de malware e de artefatos. Após uma violação, a DFIR é crucial para a descoberta de perdas de dados e detalhes específicos de danos.

Os serviços de DFIR ajudam a estabelecer uma resposta eficaz a ameaças, utilizando manuais sofisticados de resposta a incidentes e análises forenses para compreender o comportamento dos envolvidos na ameaça e as causas principais. Os fornecedores devem possuir experiência em ajudar empresas com apoio a ações judiciais para indenizações de seguros e auditorias regulatórias pós-violação. São adeptos do uso de ferramentas internas e de terceiros, como gerenciamento de eventos e informações de segurança (SIEM), orquestração, automação e resposta de segurança (SOAR), detecção e resposta de endpoint (EDR) e detecção e resposta estendida (XDR).

Critérios de Qualificação

1. Deve ter uma **equipe dedicada de resposta a incidentes** (CERT ou CSIRT), com especialistas certificados (GCFA, GCFE, CISSP etc.), demonstrando sua experiência e compromisso em manter os padrões do setor
2. Possuir experiência e conhecimento no **manuseio de uma variedade** de soluções SIEM, SOAR, EDR e XDR
3. Os serviços DFIR não só **identificam a violação**, como também criam a linha do tempo, a causa raiz e o impacto da violação
4. **Possuir recursos** de análise de malware, descriptografia de ransomware e recuperação de dados
5. Demonstrar **parceria** com fabricantes de produtos relevantes e prestadores de serviços de segurança gerenciados para reunir inteligência sobre ameaças, monitoramento da dark web e recursos SOC, de forma a mitigar ameaças avançadas persistentes e sofisticadas

**Definição**

Os fornecedores de serviços VAPT caracterizam-se por oferecer competências técnicas refinadas que requerem um elevado grau de atualização, não apenas sobre lacunas conhecidas e descobertas no dia a dia, mas também sobre abordagens e mecanismos cada vez mais elaborados para contornar as linhas de defesa estabelecidas.

O ano de 2023 foi marcado pelo acesso a ferramentas de IA generativa, permitindo que inúmeras pessoas pudessem identificar e explorar vulnerabilidades em ativos tecnológicos, em particular, aqueles diretamente expostos à Internet. Além disso, tem havido uma proliferação de incidentes envolvendo ransomware, com casos recorrentes, destacando a necessidade de proteção perimetral contínua, não mais limitada a avaliações esporádicas anuais ou semestrais.

Considerando a atual frequência de atualizações de serviços expostos à Internet pelas empresas, a inserção de serviços contínuos de detecção de vulnerabilidades (pré e pós-entrada em produção) agora é vital para a estratégia de segurança cibernética e, juntamente com as demais tendências, compõe o desafio e a missão dos fornecedores deste quadrante.

O cenário é o de uma corrida acelerada contra ameaças orquestradas com crescente sofisticação metodológica e técnica e elevado potencial destrutivo. Os fornecedores deste quadrante devem, portanto, oferecer antídotos apropriados, além da abordagem tradicional, que atualmente é insuficiente para mitigar riscos e impactos.

Critérios de Qualificação

1. Possuir equipes internas especializadas que podem **avaliar com rigor as vulnerabilidades e indicar soluções** para remoção de falhas e/ou redução gradativa de sua gravidade, com base em evidências concretas de vetores de ataque
2. Oferecer serviços que incluem **abordagens Back Box, Grey Box e White Box**, capazes de avaliar, por exemplo, aplicações web, dispositivos móveis, redes internas, nuvem, APIs, IoT e outros ativos expostos
3. Utilizar métodos como **DAST, SAST e Teste de Penetração** para objetivos específicos, utilizando ferramentas manuais e/ou automatizadas para prestar serviços
4. Usar e evidenciar **normas e padrões reconhecidos da indústria**, como SOC 2, ISO27001, NIST 800-53, PCI-DSS e HIPPA ao apontar falhas de segurança
5. Oferecer **retestes, suporte especializado e mecanismos** de monitoramento de ações corretivas, refletidos dinamicamente na atualização da matriz de riscos e gravidade (exposição a vetores remanescentes)

## Quadrantes Por Região

Como parte deste estudo de quadrantes do ISG Provider Lens™, estamos apresentando os nove quadrantes a seguir sobre Cybersecurity – Solutions and Services 2024:

| Quadrantes | EUA | Reino Unido | Alemanha | Suíça | França | Brasil | Austrália | Setor Público dos EUA | Global |
|---|---|---|---|---|---|---|---|---|---|
| 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) | | | | | | ✓ | | | |

A fase de pesquisa situa-se no período entre janeiro e fevereiro de 2024, durante o qual ocorrerão o levantamento, avaliação, análise e validação. Os resultados serão apresentados à imprensa em julho de 2024.

| Marcos Históricos | Início | Fim |
|---|---|---|
| Lançamento da Pesquisa | 8 de janeiro de 2024 | |
| Fase da Pesquisa | 8 de janeiro de 2024 | 22 de fevereiro de 2024 |
| Prévia dos Resultados | Maio de 2024 | |
| Comunicado à Imprensa e Publicação | Julho de 2024 | |

Consulte o link para visualizar/baixar o calendário de pesquisa de 2024 do ISG Provider Lens™.

**Acesso ao Portal On-line**

Você pode visualizar e baixar o questionário aqui usando as credenciais que você já criou ou consulte as instruções fornecidas no e-mail de convite para gerar uma nova senha. Aguardamos a sua participação!

**Isenção de Responsabilidade de Produção de Pesquisa:**

O ISG coleta dados para fins de redação de pesquisas e criação de perfis de fornecedores/fabricantes de serviços. Os perfis e dados de suporte são usados pelos consultores do ISG para fazer recomendações e informar os seus clientes sobre a experiência e as qualificações de fornecedores/fabricantes de serviços aplicáveis para a terceirização do trabalho identificado pelos clientes. Esses dados são coletados como parte do processo do ISG FutureSource™ e do processo Qualificação de Fornecedores Candidatos (CPQ). O ISG pode optar por utilizar apenas esses dados coletados referentes a determinados países ou regiões para a educação e propósitos de seus consultores e não produzir relatórios do ISG Provider Lens™. Essas decisões serão tomadas com base no nível e integridade das informações recebidas diretamente dos fornecedores/fabricantes e na disponibilidade de analistas experientes para esses países ou regiões. As informações enviadas também podem ser usadas para projetos de pesquisa individuais ou para apresentação de notas que serão escritas pelos analistas líderes.

**ISG Star of Excellence™ – Chamada para indicações**

O Star of Excellence é um reconhecimento independente da excelente prestação de serviços com base no conceito de "opinião do consumidor". O Star of Excellence é um programa, desenvolvido pelo ISG, para coletar feedback do cliente sobre o sucesso dos fornecedores de serviços em demonstrar os mais altos padrões de excelência no atendimento ao cliente e centrado no consumidor.

A pesquisa global é sobre serviços associados a estudos IPL. Consequentemente, todos os Analistas do ISG receberão continuamente informações sobre a experiência do cliente de todos os fornecedores de serviços relevantes. Essas informações são adicionadas ao feedback do consultor existente em primeira mão, as quais o IPL aproveita no contexto de sua abordagem de consultoria conduzida por profissionais.

Os fornecedores são convidados a indicar seus clientes para participar. Assim que a indicação for enviada, o ISG enviará uma confirmação por correio para ambas as partes. É evidente que o ISG mantém o anonimato de todos os dados dos consumidores e não os compartilha com terceiros.

É nossa visão que o Star of Excellence será reconhecido como o reconhecimento do setor líder pela excelência no atendimento ao cliente, e servirá como referência para medir os sentimentos dos clientes. Para garantir que seus clientes selecionados concluam o feedback para sua participação, use a seção de indicação de clientes no site web.

Criamos um e-mail onde você pode direcionar qualquer dúvida ou fazer comentários. Esse e-mail será verificado diariamente. Aguarde até 24 horas para receber uma resposta.

O endereço de e-mail é:
ISG.star@isg-one.com

## Contatos Para Este Estudo

Frank Heuer

**Analista Líder – Alemanha, Suíça**

Gowtham Kumar

**Analista Líder – EUA**

Bhuvaneshwari Mohan

**Analista Líder – Reino Unido**

Benoit Scheuber

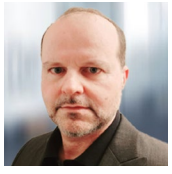
**Analista Líder – França**

Dr. Maxime Martelli

**Analista Líder – França**

Craig Baty

**Analista Líder – Austrália**



Christian Horst Alves Reis

**Analista Líder – Brasil**

Phil Hassey

**Analista Líder – Setor Público dos EUA**

Monica K

**Analista de Pesquisa**

## Contatos Para Este Estudo

Bhuvaneshwari Mohan

**Analista de Pesquisa**

Sandya Kattimani

**Analista de Pesquisa**

Bruno Nakazone

**Analista de Pesquisa**

Rajesh Chillappagari

**Analyste de données**

Laxmi Sahebrao Kadve

**Analyste de données**

Shreemadhu Rai B

**Gerente de Projetos**

**Programa de Envolvimento de Consultores do ISG Provider Lens™**

O ISG Provider Lens™ oferece avaliações de mercado que incorporam insights de profissionais, refletindo o foco regional e pesquisas independentes. O ISG garante o envolvimento do consultor em cada estudo para cobrir os detalhes de mercado relevantes alinhados às respectivas linhas de serviço/tendências de tecnologia, presença do fornecedor de serviços e contexto empresarial.

Em cada região, o ISG tem líderes de pensamento especializados e consultores respeitados que conhecem os portfólios e ofertas dos fornecedores, bem como os requisitos da empresa e as tendências do mercado. Em média, três consultores participam como parte da Equipe de Revisão de Qualidade e Consistência (QCRT) de cada estudo.

O QCRT garante que cada estudo reflita a experiência dos consultores ISG no campo, o que complementa a pesquisa primária e secundária conduzida pelos analistas. Os consultores do ISG participam de cada estudo como parte do grupo QCRT e contribuem em diferentes níveis, dependendo de sua disponibilidade e especialização.

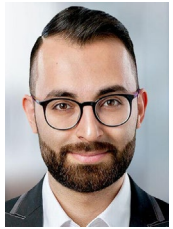
Os consultores de QCRT:

- Ajudam a definir e validar quadrantes e questionários,
- Aconselham sobre a inclusão de fornecedores de serviços, participam de chamadas de apresentação,
- Fornecem as suas perspectivas sobre as classificações dos fornecedores de serviços e revisam os rascunhos dos relatórios.

## Consultores do ISG para este estudo

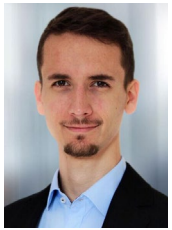
Doug Saylors

**Parceiro, Colíder de Segurança Cibernética ISG**



Reza Memarian

**Consultor Principal de Segurança Cibernética**



Anas Barmo

**Consultor Sênior de Segurança Cibernética**

Joyce Harkness

**Diretora de Segurança Cibernética**

**Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.**

* Avaliado na iteração anterior

## 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*

## Empresas convidadas

**Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.**

* Avaliado na iteração anterior

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*

**Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.**

* Avaliado na iteração anterior

## 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*

## Empresas convidadas

**Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.**

* Avaliado na iteração anterior

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*

## Empresas convidadas

**Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.**

* Avaliado na iteração anterior

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™

O quadrante ISG Provider Lens™ série de pesquisa é o único serviço avaliação do provedor de seu tipo para combinar empírica, baseada em dados pesquisa e análise de mercado com a experiência do mundo real e observações da assessoria global do ISG equipe. As empresas encontrarão uma riqueza de dados detalhados e análise de mercado para ajudar a orientar sua seleção de parceiros de fornecimento apropriados, enquanto Os conselheiros do ISG usam os relatórios para validar seu próprio conhecimento de mercado e fazer recomendações para a empresa ISG clientes. A pesquisa atualmente abrange provedores que oferecem seus serviços em múltiplas geografias globalmente.

Para mais informações sobre Pesquisa ISG Provider Lens™, visite esta página da web.

## ISG Research™

ISG Research™ fornece pesquisa por assinatura, consultoria consultoria e evento executive serviços focados nas tendências do mercado e tecnologias disruptivas impulsionando mudança na computação empresarial. A ISG Research™ oferece orientação que ajuda as empresas a acelerar crescimento e criar mais valor.

O ISG oferece pesquisas especificamente sobre provedores para estado e local governos (incluindo condados, cidades), bem como o ensino superior instituições. Visite: Setor Público.

Para mais informações sobre o ISG Assinaturas™ de pesquisa, por favor e-mail contact@isg-one.com, ligue para +1.203.454.3900 ou visite research.isg-one.com.

## ISG

O ISG (Information Services Group) (NASDAQ: III) é uma empresa líder mundial em pesquisa consultoria tecnológica. Um parceiro comercial confiável para mais de 900 clientes, incluindo 75 das 100 maiores empresas do mundo, o ISG está comprometido em ajudar corporações, organizações do setor público e provedores de serviços e tecnologia a alcançar excelência operacional e crescimento mais rápido. A empresa é especializada em serviços de transformação digital, incluindo automação, analytics de nuvens e dados; consultoria em sourcing; governança gerenciada e serviços de risco; serviços de operadoras de rede; estratégia tecnológica e projeto de operações; gerenciamento de mudanças; inteligência de mercado e pesquisa e análise de tecnologia.

Fundado em 2006, e sediado em Stamford, Connecticut, o ISG emprega mais de 1.600 profissionais operando em mais de 20 países - uma equipe global conhecida por seu pensamento inovador, influência de mercado, profunda experiência na indústria e tecnologia, e capacidade de pesquisa e análise de classe mundial com base nos dados de mercado mais abrangentes da indústria.

Para mais informações visite isg-one.com.

ISG Provider Lens™

**JANEIRO DE 2024**

# CATÁLOGO: CYBERSECURITY – SOLUTIONS AND SERVICES