ISG Provider Lens™

Cybersecurity – Solutions & Services

Eine vergleichende Analyse des Cybersicherheitsmarktes hinsichtlich der Portfolioattraktivität und der Wettbewerbsstärke der Anbieter

BROSCHÜRE | JANUAR 2024 | AUSTRALIEN, BRASILIEN, FRANKREICH, DEUTSCHLAND, SCHWEIZ, GROSSBRITANNIEN, USA, ÖFFENTLICHER SEKTOR DER USA UND GLOBAL

Inhaltsverzeichnis

Cybersicherheit im Zeitalter der künstlichen Intelligenz

Die aktuelle Cybersicherheitslandschaft erlebt im Zuge neuer Bedrohungen, technologischer Fortschritte und gesetzlicher Vorschriften 2024 eine rasche Weiterentwicklung.

Aus Cybersicherheitssicht kann man das Jahr 2023 angesichts deutlich raffinierterer und schwererer Angriffe als herausfordernd bezeichnen. Zahlreiche Unternehmen haben daraufhin ihre Investitionen in die Cybersicherheit erhöht und entsprechenden Initiativen zur Verhinderung von Angriffen und zur Verbesserung ihres Sicherheitsstatus eine hohe Priorität eingeräumt. Führungskräfte und Unternehmen aller Größen und Branchen haben aus den jüngsten Angriffen ihre Lektion gelernt und in entsprechende Maßnahmen zur Abwehr von Cyberbedrohungen investiert. Die Herausforderungen und Chancen, die mit künstlicher Intelligenz (KI) einhergehen, sind in diesem Zusammenhang besonders erwähnenswert.

Auf Unternehmensseite haben selbst kleinere Betriebe erkannt, dass sie anfällig für Cyberbedrohungen sind. Auch das erhöht die Nachfrage nach (gemanagten) Sicherheits- und Cyber-Resiliency-Lösungen. Dienstleister und Hersteller offerieren daher vermehrt Services und Lösungen zur Unterstützung der Wiederherstellung und der Aufrechterhaltung des Geschäftsbetriebes.

Security Service Provider helfen ihren Kunden, sich in der Cybersecurity-Landschaft zurechtzufinden. Es gilt vor allem, wachsam zu sein, um neue Bedrohungen zu erkennen und abzuschwächen, die transformativen Auswirkungen von Technologien wie KI zu verstehen und sich auf die neu entstehenden rechtlichen Rahmenbedingungen für den Datenschutz, wie NIS-2 in der Europäischen Union, einzustellen.

Cyberkriminelle nutzten großflächige Schwachstellen aus; mit beständigen Ransomware-Angriffen wurde versucht, Geschäftsaktivitäten zu stören, insbesondere im Gesundheitswesen, in der industriellen Lieferkette und im öffentlichen Dienst.

Unternehmen investierten infolge dessen in Funktionen wie Identitäts- und Zugriffsmanagement (IAM), Data Loss Prevention (DLP), Managed Detection & Response (MDR) und die Absicherung der Cloud und der Endpunkte. Der Markt verlagert sich hin zu integrierten Lösungen wie Security Service Edge (SSE) und Extended Detection & Response (XDR). Anhand der besten Tools, mit Experten und ergänzender verhaltens- und kontextbezogener Intelligenz und Automatisierung soll der Sicherheitsstand verbessert werden.

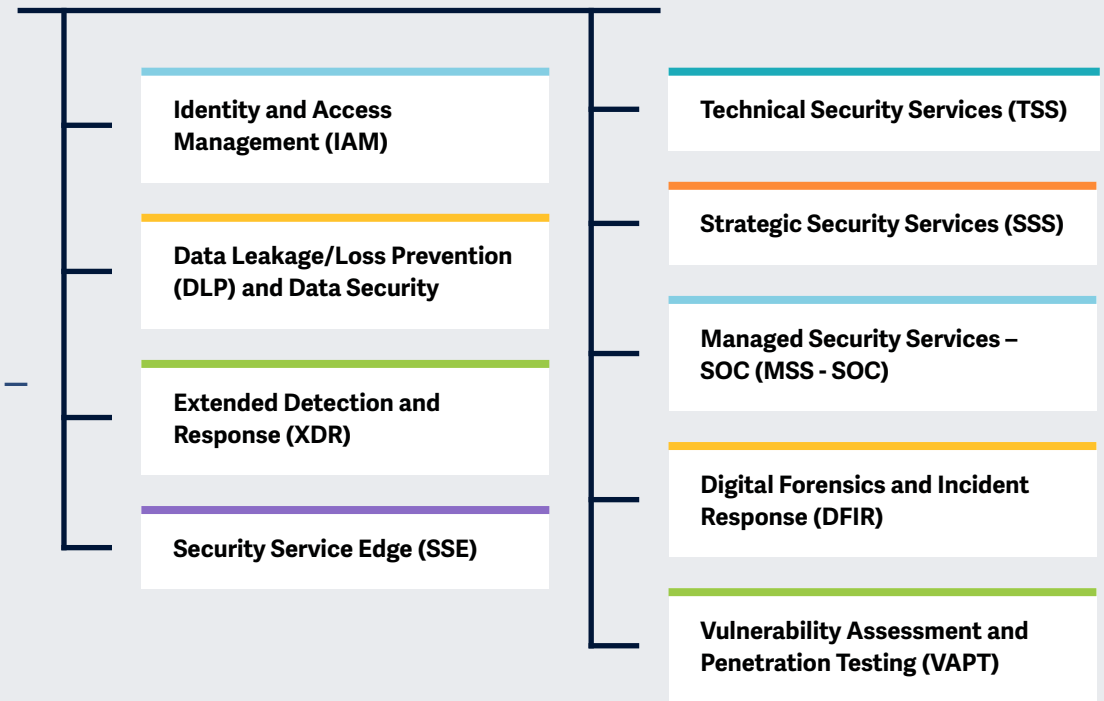
Cybersecurity Services: 2024

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					

Untersuchte Schwerpunkt-themen der Studie „Cybersecurity – Solutions and Services 2024“.



Vereinfachte Illustration Quelle: ISG 2024

Die ISG Provider Lens™ Studie „Cybersecurity – Solutions & Services“ bietet Business- und IT-Entscheidern folgende Vorteile:

- Transparente Darstellung der Stärken und Schwächen relevanter Anbieter
- Eine differenzierte Positionierung der Anbieter, basierend auf Wettbewerbsstärke und Portfolio-Attraktivität
- Fokus auf verschiedene Ländermärkte: USA, Großbritannien, Deutschland, Schweiz, Frankreich, Brasilien, Australien sowie den öffentlichen Sektor in den USA; die Themen SSE und XDR werden für den globalen Markt analysiert.
- Zur Berücksichtigung länderspezifischer Besonderheiten erstreckt sich die Analyse von XDR auch auf Brasilien, während DLP ausschließlich für Deutschland analysiert wird. Die Neuaufnahme von DFIR wird in den USA und Frankreich getestet, VAPT in Brasilien.

Die Studie bietet somit eine wesentliche Entscheidungsgrundlage für Positionierungs-, Partnering- und Go-to-Market-Überlegungen. ISG-Berater und -Anwenderkunden nutzen Informationen aus diesen Reports auch zur Evaluierung ihrer derzeitigen sowie potenzieller neuer Anbieterbeziehungen.

Definition

Die im Rahmen dieses Quadranten bewerteten IAM-Lösungsanbieter offerieren proprietäre Software und zugehörige Services für die Verwaltung von Benutzeridentitäten und -geräten in Unternehmen Dieser Quadrant umfasst auch SaaS-Angebote auf Basis von proprietärer Software. **Reine Dienstleister, die keine IAM-Produkte (On-Premises oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht berücksichtigt**. Entsprechend den individuellen Unternehmensanforderungen können diese Angebote auf verschiedene Arten bereitgestellt werden, z.B. vor Ort oder in vom Kunden verwalteten Clouds, auf Basis eines as-a-Service-Modells oder in Form einer kombinierten Lösung.

IAM-Lösungen dienen dem Management (Erfassung, Aufzeichnung und Verwaltung) von Benutzeridentitäten und zugehörigen Zugriffsrechten sowie dem spezialisierten Zugriff auf kritische Assets auf Basis von Privileged Access Management (PAM), d.h. des Zugriffs anhand von definierten Policies.

Um mit bestehenden und neuen Anforderungen aus der Anwendungswelt umgehen zu können, werden IAM-Lösungs-Suites im Rahmen von Management Suites zunehmend in sichere Mechanismen, Frameworks und Automatisierung (z.B. der Risikobewertung) eingebunden, um Nutzer- und Attacken-Profiling in Echtzeit durchführen zu können. Von den Lösungsanbietern werden zudem weitere Funktionalitäten für Social Media und mobile Anwendungen erwartet, um deren spezifische Sicherheitsbedarfe abzudecken, die über web- und kontextbezogenes Berechtigungsmanagement hinausgehen. Dieser Quadrant umfasst auch Machine Identity Management.

Auswahlkriterien

1. Einsatz der Lösung **vor Ort, in der Cloud, als Identity as a Service** (IDaaS) und auf Basis eines verwalteten Modells eines Drittanbieters
2. Die angebotenen Lösungen sollten die **Authentifizierung** anhand einer Kombination von **Single-Sign-On (SSO), Multifaktor-Authentifizierung (MFA)**, risiko- und kontextbasierten Modellen unterstützen
3. Unterstützung von **rollenbasiertem Zugriff** und PAM
4. **Zugriffsmanagement** für eine oder mehrere Unternehmensanforderungen wie **Cloud, Endpunkte, mobile Geräte, APIs und Webanwendungen**
5. **Unterstützung von einem oder mehreren älteren und neuen IAM-Standards,** einschließlich, aber nicht nur, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust und SCIM
6. Sicherer Zugriff durch eine oder mehrere der folgenden Möglichkeiten: **Directory-Lösungen, Dashboard- oder Self-Service-Management** und Lifecycle Management (Migration, Synchronisierung und Replizierung)

Definition

Die im Rahmen dieses Quadranten bewerteten DLP-Lösungsanbieter offerieren proprietäre Software und zugehörige Dienstleistungen, u.a. auch SaaS-Lösungen. **Reine Dienstanbieter, die kein DLP-Produkt (On-Premises oder in der Cloud) anbieten, das auf eigenentwickelter Software basiert**, werden in diesem Quadranten nicht berücksichtigt. DLP-Lösungen können sensible Daten identifizieren und überwachen, den Zugriff nur für autorisierte Benutzer ermöglichen und Datenverluste/ -lecks verhindern. Die Lösungen der Anbieter in diesem Markt bestehen aus einer Kombination von Produkten, die Transparenz und Kontrolle über sensible Daten in Cloud-Anwendungen, Endpunkten, im Netzwerk und auf diversen Geräten ermöglichen.

Diese Lösungen gewinnen zunehmend an Bedeutung, denn es wird für Unternehmen immer schwieriger, Datenbewegungen und -übertragungen zu kontrollieren; über ein Drittel der Datenverletzungen haben ihren Ursprung innerhalb des Unternehmens. Die Anzahl der Geräte, u.a. mobiler Geräte, die zur Datenspeicherung verwendet werden, verstärkt dieses Problem zusätzlich. Dank Internetkonnektivität können diese Geräte Daten austauschen, ohne ein zentrales Gateway zu passieren. Datensicherheitslösungen schützen Daten vor unbefugtem Zugriff, Offenlegung oder Diebstahl durch die Priorisierung, Klassifizierung und Überwachung von Daten (im Ruhezustand und bei der Übertragung); sie ermöglichen ein Security Reporting und helfen, die Sicherheit der gefährdeten Daten zu verbessern.

Auswahlkriterien

1. DLP-Lösungen auf Basis von **eigenentwickelter Software** und nicht auf Basis von Software von Drittanbietern
2. DLP-Unterstützung über eine **beliebige Architektur wie Cloud, Netzwerk, Speicher oder Endpunkt**
3. Nachweislicher Schutz von **sensiblen Daten**, egal ob es sich dabei um **strukturierte oder unstrukturierte Daten**, Text- oder Binärdaten handelt
4. **Grundlegender Management-Support**, einschließlich, aber nicht nur **Reporting, Richtlinienkontrolle**, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen
5. Fähigkeit der Lösung, **sensible Daten zu erkennen, Richtlinien durchzusetzen**, den Datenverkehr zu überwachen und die Daten-Compliance zu verbessern

Definition

Die in diesem Quadranten bewerteten XDR-Lösungsanbieter zeichnen sich durch eine Plattform aus, die Daten und Warnungen aus verschiedenen Komponenten zur Bedrohungsabwehr, -erkennung und -reaktion integriert, korreliert und kontextualisiert. XDR ist eine aus der Cloud bereitgestellte Technologie, die Multipoint-Lösungen umfasst und anhand von fortschrittlichen Analysen Warnmeldungen aus mehreren Quellen, unter anderem auch von schwachen Einzelsignalen, mit Vorfällen korreliert, um so die Erkennung zu präzisieren. XDR-Lösungen konsolidieren und integrieren mehrere Produkte und bieten umfassende Sicherheit für Arbeitsbereiche, Netzwerke und Workloads; sie sollen für eine erheblich höhere Transparenz und ein besseres kontextbasiertes Verständnis der im Unternehmen aufgedeckten Bedrohungen sorgen. Sie umfassen u.a. Telemetrie und kontextbezogene Datenanalysen zur Erkennung von und Reaktion auf solche Risiken. XDR-Lösungen umfassen mehrere Produkte; sie sind in einer einzigen Konsole mit ausgefeilten Funktionen für das Sichten, Erkennen und Reagieren auf Bedrohungen zusammengeführt. Ihr hoher Automatisierungsgrad und die kontextbezogene Analyse bieten maßgeschneiderte Reaktionsmöglichkeiten für betroffene Systeme; Warnmeldungen werden nach Schweregrad im Vergleich zu bekannten Referenz-Frameworks priorisiert. **Reine Dienstleister , die keine auf eigenentwickelter Software basierende XDR-Lösung anbieten, werden in diesem Quadranten nicht berücksichtigt**. XDR-Lösungen zielen darauf ab, die Produktvielfalt, Alarmmüdigkeit, Integrationsprobleme und Betriebskosten zu verringern. Sie eignen sich besonders für Sicherheitsteams, die mit der Verwaltung verschiedenster Lösungsportfolios zu kämpfen haben oder den Wert von SIEM- (Security Information and Event Management) oder SOAR-Lösungen (Security Orchestration, Automation & Response) steigern wollen.

Auswahlkriterien

1. XDR-Lösungen auf Basis von **eigenentwickelter Software** und nicht auf Basis von Software von Drittanbietern
2. Die XDR-Lösung muss zwei Hauptkomponenten umfassen: **XDR-Frontend und XDR-Backend**
3. Frontend mit **drei oder mehr Lösungen bzw. Sensoren**, einschließlich, aber nicht beschränkt auf, **Endpunkt-Erkennung und -Reaktion, Endpunkt-Schutzplattformen**, Netzwerkschutz (Firewalls, IDPS), **Netzwerk-Erkennung und -Reaktion**, Identitätsmanagement, E-Mail-Sicherheit, Erkennung mobiler Bedrohungen, Schutz von Cloud-Workloads und Betrugsidentifizierung
4. **Umfassende und vollständige Abdeckung und Visibilität aller Endpunkte** im Netzwerk
5. Nachweisliche **effektive Abwehr** von komplexen Bedrohungen wie **Advanced Persistent Threats, Ransomware** und Malware
6. Nutzung und Analyse von **Bedrohungsdaten** sowie **Echtzeit-Insights in Bedrohungen**, die von den Endpunkten ausgehen
7. **Automatische Reaktionsfunktionen**

Definition

Die für diesen Quadranten bewerteten SSE-Lösungsanbieter offerieren cloud-zentrierte Lösungen, die proprietäre Software und/oder Hardware und zugehörige Dienste zusammenführen und einen sicheren Zugang zu Cloud Services, SaaS-Anwendungen, Webdiensten und privaten Anwendungen ermöglichen. Die entsprechenden Provider bieten SSE-Lösungen als integrierten Sicherheitsdienst über global positionierte Points of Presence (PoP) mit Unterstützung für lokale Datenspeicherung an, der Einzellösungen wie Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Secure Web Gateways (SWG) und Firewall as a Service (FWaaS) kombiniert. SSE kann auch andere Sicherheitslösungen wie Data Loss/Leakage Prevention (DLP), Browser-Isolierung und Next-Generation Firewalls (NGFW) umfassen, um einen sicheren Zugriff auf Anwendungen in der Cloud wie auch vor Ort zu ermöglichen.

Die Anbieter demonstrieren ihre Erfahrung bei der Einhaltung lokaler, regionaler und nationaler Gesetze (z.B. hinsichtlich Datensouveränität) für globale Kunden.

Die **Netzwerkkomponenten von Secure Access Service Edge (SASE), wie SD-WAN**, die in der ISG Provider Lens™ Studie „Network – Software-Defined Solutions & Services 2024" abgedeckt werden, sind hier nicht berücksichtigt.

SSE-Lösungen sind stark nutzerorientiert; sie bieten den Endanwendern Edge- oder Gerätesicherheit über die Cloud, anstatt ihnen zentralen Zugriff auf Unternehmensanwendungen und Datenbanken über dedizierte Netzwerke zu gewähren. ZTNA stellt eine exklusive Verbindung zwischen Benutzern und Anwendungen her und nutzt kontextbasierte Verhaltensanalysen für die Zugriffskontrolle. CASB (Cloud Access Security Broker) bietet Transparenz, setzt Sicherheitsrichtlinien und Compliance durch und kontrolliert die Cloud-Nutzung durch die Schatten-IT; FWaaS (Firewall as a Service) und SWG (Secure Web Gateway) wehren bösartige Bedrohungen und den Zugriff auf infizierte Websites und Anwendungen ab. Typischerweise verfügt eine SSE-Lösung über eine einheitliche Konsole für die Gewährleistung der Transparenz und Governance und fortschrittliche Automatisierungsfunktionen zur Auswertung der Benutzererfahrung.

Auswahlkriterien

1. SSE als **integrierte Lösung** und mit folgenden entscheidenden Komponenten: **Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Secure Web Gateways (SWG) und Firewall as a Service (FWaaS)**
2. Bereitstellung von Lösungen **überwiegend auf Basis von proprietärer** Software, **evtl. in Teilen auch basierend auf Partnerlösungen, aber nicht vollständig** auf Basis von Software **von Drittanbietern**
3. **Weltweite Points of Presence** für die Bereitstellung dieser Lösungen
4. Erbringung von **SSE sowohl für Cloud- als auch für On-Premises-Umgebungen** (einschließlich hybrider Umgebungen)
5. **Kontextbezogene und verhaltensbezogene Auswertungen und Analysen** (Nutzeridentitäts- und Verhaltensanalysen bzw. User Entity and Behavior Analytics/UEBA) zur Aufdeckung und Verhinderung bösartiger bzw. verdächtiger Absichten
6. **Grundlegender Management-Support**, einschließlich, aber nicht nur **Reporting, Richtlinienkontrolle**, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen
7. Sicherstellung der **globalen Verfügbarkeit der Lösung**

Definition

Die in diesem Quadranten bewerteten Anbieter von TSS offerieren Integrations-, Wartungs- und Supportleistungen für IT- und OT-Sicherheitsprodukte oder -lösungen. Diese Dienste decken alle Sicherheitsprodukte ab, u.a. Antivirus, Cloud- und Rechenzentrumssicherheit, IAM, DLP, Netzwerksicherheit, Endpunktsicherheit, Unified Threat Management (UTM), OT Security, SASE und weitere Angebote.

TSS Provider bieten standardisierte Playbooks und Roadmaps an, die dabei helfen, eine bestehende Sicherheitsumgebung mit den besten Tools und Technologien umzugestalten, den Sicherheitsstatus zu verbessern und die Auswirkungen von Bedrohungen zu reduzieren. Ihre Portfolios sollen u.a. die vollständige oder individuelle Transformation bestehender Sicherheitsarchitekturen in Bereichen wie Netzwerken, Cloud, Arbeitsplatz, OT, IAM, Datenschutz und -sicherheit, Risiko- und Compliance-Management und SASE ermöglichen. Die Angebote beinhalten zudem die Identifizierung von Produkten oder Lösungen, Bewertung, Design und Entwicklung, Implementierung, Validierung, Penetrationstests, Integration und Bereitstellung.

TSS Provider investieren in den Aufbau von Partnerschaften mit Anbietern von Sicherheitslösungen und -technologien, um spezialisierte Akkreditierungen zu erlangen und ihr Portfolio zu erweitern. Dieser Quadrant umfasst auch klassische Managed Security Services, die ohne ein Security Operations Center (SOC) erbracht werden.

In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf ihre eigenen Produkte fokussieren, sondern auch in der Lage sind, Lösungen anderer Anbieter zu implementieren und zu integrieren.

Auswahlkriterien

1. Nachweisliche Erfahrung mit der **Entwicklung und Implementierung von Sicherheitslösungen** für Unternehmen im jeweiligen Land
2. **Autorisierung durch Sicherheitstechnologie-Anbieter** (Hardware und/oder Software) für den Vertrieb und die Unterstützung von Sicherheitslösungen
3. **Experten mit Zertifizierungen** (von Herstellern, Verbänden und Organisationen, staatlichen Stellen), die in der Lage sind, Sicherheitstechnologien zu unterstützen

Definition

Die in diesem Quadranten bewerteten Provider von Strategic Security Services (SSS) bieten Beratung für IT- und OT-Sicherheit an. Die abgedeckten Leistungen umfassen Sicherheitsaudits, Compliance- und Risikoberatung, Sicherheitsbewertungen, Beratung zu Sicherheitslösungen sowie Sensibilisierungstrainings und Schulungen. Die Anbieter helfen auch bei der Bewertung des Sicherheitsreifegrads sowie der Risikolage und der Definition einer auf den individuellen Anforderungen basierenden Cybersecurity-Strategie für Unternehmen.

Diese Provider sollten Sicherheitsberater beschäftigen, die über umfassende Erfahrung mit der Planung, Entwicklung und Verwaltung von umfassenden Sicherheitsprogrammen für Unternehmen verfügen. Angesichts des wachsenden Bedarfs an solchen Diensten bei KMUs und des Fachkräftemangels sollten diese Experten auch auf Abruf durch vCISO (Virtual Chief Information Security Officer) Services zur Verfügung gestellt werden. Angesichts der zunehmenden Bedeutung der Cyber-Resilienz sollten SSS-Anbieter in der Lage sein, Business Continuity Roadmaps zu formulieren und geschäftskritische Anwendungen für die Wiederherstellung zu priorisieren. Außerdem sollten sie regelmäßig so genannte Tabletop Exercises und Cyber-Drills für Vorstandsmitglieder, wichtige Führungskräfte und Mitarbeiter durchführen, um sie besser mit Cybersecurity-Themen vertraut zu machen und Best Practices einzuführen, damit sie besser auf tatsächliche Bedrohungen und Cyber-Angriffe reagieren können. Sie sollten zudem mit den auf dem Markt erhältlichen Sicherheitstechnologien und -produkten vertraut sein und Unternehmen bei der Auswahl des besten Produkts und Anbieters für die spezifischen Anforderungen entsprechend beraten.

In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf eigene Produkte oder Lösungen fokussieren. Die hier analysierten Dienste decken alle Sicherheitstechnologien ab, u.a. auch OT-Sicherheit und SASE.

Auswahlkriterien

1. Nachweisliche Leistungen in SSS-Bereichen wie **Evaluierung, Assessments, Anbieterauswahl, Architekturberatung und Risikoberatung**
2. **Angebot von mindestens einem der oben genannten** Strategic Security Services im jeweiligen Land
3. Erbringung von **Sicherheitsberatungsdiensten unter Verwendung von Frameworks** ist von Vorteil
4. **Kein ausschließlicher Fokus auf proprietäre Produkte** bzw. Lösungen

Definition

Die im MSS-SOC-Quadranten bewerteten Anbieter offerieren Leistungen für die kontinuierliche Überwachung von IT- und OT-Sicherheitsinfrastrukturen sowie das Management der IT- und OT-Infrastruktur für einen oder mehrere Kunden durch ein Security Operations Center (SOC). **Dieser Quadrant untersucht Dienstleister, die sich nicht ausschließlich auf proprietäre Produkte fokussieren, sondern Best-of-Breed-Sicherheitstools verwalten und betreiben können**. Sie kümmern sich um den gesamten Security Incident Lifecycle, von der Identifizierung bis zur Lösung von Problemen.

Die Nachfrage nach Anbietern, die Unternehmen dabei unterstützen, ihre IT-Sicherheit insgesamt zu verbessern und die Wirksamkeit ihrer Sicherheitsprogramme durch kontinuierliche Verbesserungen langfristig zu maximieren, steigt. MSS-SOC Provider müssen traditionelle Managed Security Services mit Innovationen zusammenführen, um die Sicherheit ihrer Kunden mit einem integrierten Cyber-Abwehrmechanismus stärken zu können. Sie sollten in der Lage sein, Managed-Detection-&-Response-Dienste (MDR) zu erbringen, und über die neuesten Technologien und Infrastrukturen verfügen. Auch Fachwissen in den Bereichen Threat Hunting und Incident Management muss vorhanden sein, um Unternehmen bei der aktiven Erkennung von und Reaktion auf Bedrohungen durch Abwehr und Eindämmung zu unterstützen. Um die steigenden Kundenerwartungen in Bezug auf proaktives Threat Hunting erfüllen zu können, bauen die Anbieter ihre SOC-Umgebungen mit Sicherheitsintelligenz aus und tätigen erhebliche Investitionen in Technologien wie Automatisierung, Big Data, Analytik, KI und Machine Learning. Diese hochmodernen SOCs unterstützen von Experten gesteuerte Reaktionen auf Sicherheitsinformationen und bieten den Kunden gleichzeitig einen ganzheitlichen und einheitlichen Ansatz für Sicherheit auf hohem Niveau.

Auswahlkriterien

1. Typische Leistungen wie **Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmaßnahmen, Penetrationstests** und alle anderen Betriebsservices, um einen kontinuierlichen Echtzeitschutz zu bieten, ohne die Leistungsfähigkeit des Unternehmens zu beeinträchtigen
2. Angebot von Sicherheitsdiensten wie **Vorbeugung und Erkennung, Security Information & Event Management (SIEM)** sowie Sicherheitsberatung und Audits, entweder remote oder vor Ort beim Kunden
3. **Akkreditierungen** von Anbietern von Security Tools
4. **Management eigener SOCs**
5. **Zertifizierte Mitarbeiter**, z.B. mit Zertifizierungen wie Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) und Global Information Assurance Certification (GIAC)
6. Verfügbarkeit verschiedener Preismodelle

Definition

Die im DFIR-Quadranten bewerteten Anbieter offerieren Leistungen im Zusammenhang mit der Reaktion auf Bedrohungen bei gleichzeitiger Sicherung von Beweisen gegen Angreifer.

In diesem Quadranten werden Dienstleister untersucht, die bewährte DFIR-Techniken und -Methoden anbieten und mit Best-of-Breed Tools arbeiten, um auf Cybersicherheitsvorfälle reagieren zu können. DFIR befasst sich mit der Ermittlung, Untersuchung, Eindämmung und Behebung von Cybersicherheitsvorfällen. Die zunehmende Häufigkeit und Schwere solcher Vorfälle hat den Einsatzgrad von DFIR Services weiter erhöht. Die Dienstleister sollten fundierte und praktische Fähigkeiten in den Bereichen digitale Forensik, elektronische Erkennung, vordefinierte kriterienbasierte Triage, Timeline-Analyse, Protokollanalyse, Malware-Analyse und Artefaktuntersuchung vorweisen können. Nach einer Sicherheitsverletzung spielt DFIR eine entscheidende Rolle bei der Aufdeckung von Datenverlusten und Schäden.

DFIR Services helfen bei der Errichtung einer effektiven Bedrohungsabwehr, und zwar mit ausgefeilten Playbooks für die Reaktion auf Vorfälle und Forensik, um das Verhalten der Bedrohungsakteure und die Ursachen zu verstehen. DFIR-Anbieter sollten über Erfahrung mit der Unterstützung von Unternehmen bei Rechtsstreitigkeiten im Zusammenhang mit Versicherungsansprüchen und bei Prüfungen nach Verstößen gegen Rechtsvorschriften verfügen. Sie sind versiert im Umgang mit internen und externen Tools wie Security Information & Event Management (SIEM), Security Orchestration, Automation & Response (SOAR), Endpoint Detection & Response (EDR) und Extended Detection & Response (XDR).

Auswahlkriterien

1. **Spezielles Incident Response Team** (CERT oder CSIRT) mit Experten mit einschlägigen Zertifizierungen wie GCFA, GCFE und CISSP, die nachweislich über Fachwissen hinsichtlich der Einhaltung von Branchenstandards verfügen
2. Erfahrung und Fachwissen im **Umgang mit einer Vielzahl** von SIEM-, SOAR-, EDR- und XDR-Lösungen
3. Die DFIR-Dienste **ermitteln nicht nur den Verstoß**, sondern dokumentieren auch den Zeitrahmen, die Ursache und die Auswirkungen des Verstoßes
4. **Fähigkeiten** in den Bereichen Malware-Analyse, Entschlüsselung von Ransomware und Datenwiederherstellung
5. Nachweisliche **Partnerschaften** mit relevanten Produktanbietern und Managed Security Service Providern, um Bedrohungsdaten zu sammeln, das Dark Web zu überwachen und SOC-Fähigkeiten zur Eindämmung fortschrittlicher und hochentwickelter Bedrohungen nutzen zu können

Definition

Anbieter von VAPT Services offerieren insbesondere hochentwickelte technische Fähigkeiten, die oft aktualisiert werden müssen, nicht nur hinsichtlich bekannter und täglich neu entdeckter Lücken, sondern auch in Bezug auf immer ausgefeiltere Ansätze und Mechanismen zur Umgehung etablierter Verteidigungslinien.

Das Jahr 2023 stand im Zeichen des Zugangs zu generativen KI-Tools, die es einer unbegrenzten Anzahl von Personen ermöglichen, Schwachstellen in technologischen Anlagen zu erkennen und auszunutzen, insbesondere wenn diese direkt mit dem Internet verbunden sind. Zudem gab es vermehrt Ransomware-Vorfälle, die deutlich machten, wie wichtig ein kontinuierlicher Perimeterschutz ist, der sich nicht mehr auf einmalige jährliche oder halbjährliche Auswertung beschränkt.

Angesichts der Häufigkeit, mit der Services aktualisiert werden müssen, die von den Unternehmen ins Internet gestellt werden, ist die Einführung von Diensten zur kontinuierlichen Erkennung von Schwachstellen (vor und nach der Produktivstellung) zu einem elementaren Bestandteil der Cybersicherheitsstrategie geworden und ist neben anderen Trends die Herausforderung und Aufgabe, vor die sich die in diesem Quadranten bewerteten Anbieter gestellt sehen.

Es handelt sich um einen rasanten Wettlauf gegen orchestrierte Bedrohungen mit zunehmender methodischer und technischer Raffinesse und hoher Zerstörungskraft. Anbieter in diesem Quadranten müssen daher zusätzlich zum traditionellen Ansatz, der inzwischen als unzureichend für die Minderung von Risiken und Auswirkungen gilt, geeignete Gegenmaßnahmen anbieten.

Auswahlkriterien

1. Verfügbarkeit spezialisierter interner Teams, die in der Lage sind, **Schwachstellen einer strengen Auswertung zu unterziehen und Lösungen** zur Beseitigung von Schwachstellen bzw. zur schrittweisen Verringerung ihres Schweregrads auf Basis konkreter Hinweise auf Angriffsvektoren **aufzuzeigen**
2. Angebot von Diensten, die **Black-Box-, Grey-Box- und White-Box-Ansätze** umfassen und z.B. Webanwendungen, mobile Geräte, interne Netzwerke, Cloud, APIs, IoT und andere exponierte Vermögenswerte bzw. Risikoelemente auswerten können
3. Einsatz von Methoden wie **DAST, SAST und Pentesting** spezifischer Ziele unter Verwendung manueller bzw. automatisierter Tools für die Leistungserbringung
4. Angabe von Sicherheitsmängeln **nachweislich auf Basis anerkannter Industriestandards** wie SOC 2, ISO27001, NIST 800-53, PCI-DSS und HIPPA
5. Angebot von **Retesting, spezialisierter Unterstützung und Mechanismen** zur Überwachung von Korrekturmaßnahmen, die sich dynamisch in der Aktualisierung der Risiko- und Schweregradmatrix niederschlagen (Exposition gegenüber verbleibenden Vektoren)

Quadranten nach Regionen

Im Rahmen dieser ISG Provider Lens™ Quadrantenstudie zum Thema „Cybersecurity – Solutions & Services 2024“ werden die folgenden neun Themen analysiert:

Quadrant	USA	UK	Deutschland	Schweiz	Frankreich	Brasilien	Australien	USA Öffentlicher Sektor	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)						✓			

Die Research-Phase umfasst die Befragung, Evaluierung, Analyse und Validierung und läuft von Januar bis Februar 2024. Die Ergebnisse werden den Medien im Juli 2024 präsentiert.

Meilensteine	Beginn	Ende
Start der Umfrage	8. Januar 2024	
Umfrage-Phase	8. Januar 2024	22. Februar 2024
Sneak Preview	Mai 2024	
Pressemitteilung & Veröffentlichung	Juli 2024	

Mit Klick auf diesen link können Sie die ISG Provider Lens™ 2024 Research-Agenda einsehen bzw. herunterladen.

Zugang zum Online-Portal

Hier können Sie über Ihre bereits erstellten Zugangsdaten den Fragebogen einsehen bzw. herunterladen. Um ein neues Passwort zu erstellen, befolgen Sie bitte die Anweisungen in der Einladungs-E-Mail. Wir freuen uns auf Ihre Teilnahme!

Haftungsausschluss für die Produktion von Research-Unterlagen

ISG erhebt Daten zum Zwecke der Recherche und Erstellung von Anbieterprofilen. Die Profile und die unterstützenden Daten werden von den ISG-Advisorn verwendet, um Empfehlungen auszusprechen und ihre Kunden über die Erfahrungen und Qualifikationen von geeigneten Anbietern für die von den Kunden identifizierten Outsourcing-Leistungen zu informieren. Diese Daten werden im Rahmen des ISG FutureSource™ Prozesses und des Candidate Provider Qualification (CPQ) Prozesses erhoben. ISG behält sich vor, die erhobenen Daten in Bezug auf bestimmte Länder oder Regionen nur für die Weiterbildung der Advisors und deren Arbeit und nicht zur Erstellung von ISG Provider Lens™ Berichte zu verwenden. Diese Entscheidungen werden auf der Grundlage der Qualität und der Vollständigkeit der direkt von den Anbietern erhaltenen Daten und der Verfügbarkeit von erfahrenen Analysten für die jeweiligen Länder oder Regionen getroffen. Die eingereichten Informationen können auch für einzelne Research-Projekte oder für Briefing Notes verwendet werden, die von den leitenden Analysten verfasst werden.

ISG Star of Excellence™ – Aufruf zur Nominierung

Der „Star of Excellence" ist eine unabhängige Auszeichnung für herausragende Serviceleistungen, die auf dem Konzept der „Stimme des Kunden" basieren. Das Star of Excellence Programm wurde von ISG entwickelt, um Kundenfeedback über den Erfolg von Dienstleistern zu sammeln, die die höchsten Standards für exzellenten Kundenservice und Kundenorientierung demonstrieren.

In der globalen Umfrage geht es um Dienstleistungen, die mit IPL-Studien zu tun haben. Infolgedessen werden alle ISG-Analysten kontinuierlich mit Informationen über die Kundenerfahrungen aller relevanten Dienstleister versorgt. Diese Informationen ergänzen das bereits vorhandene Feedback von Beratern aus erster Hand, welches für die IPL-Studien im Rahmen des praxisorientierten Beratungsansatzes genutzt wird.

Anbieter sind eingeladen, ihre Kunden unter Nominate zur Teilnahme aufzurufen. Nach Abgabe der Nominierung versendet ISG eine E-Mail-Bestätigung an beide Seiten. Selbstverständlich werden alle Kundendaten anonymisiert und nicht an Dritte weitergegeben.

Unsere Vision ist es, den Star of Excellence als die führende Auszeichnung für herausragenden Kundenservice und als Maßstab für die Messung der Kundenzufriedenheit zu etablieren. Bitte nutzen Sie den Abschnitt „Client Nomination" auf der Star of Excellence Website, um sicherzustellen, dass Ihre ausgewählten Kunden das Feedback für Ihr nominiertes Engagement abgeben Website.

Wir haben eine E-Mail eingerichtet, an die Sie Fragen oder Kommentare richten können. Diese E-Mail wird täglich überprüft. Bitte berücksichtigen Sie, dass eine Antwort bis zu 24 Stunden dauern kann.

Hier ist die E-Mail-Adresse:
ISG.star@isg-one.com

Kontaktpersonen für diese Studie

Frank Heuer

Lead Analyst – Deutschland, Schweiz

Gowtham Kumar

Lead Analyst – USA

Bhuvaneshwari Mohan

Lead Analyst – UK

Benoit Scheuber

Lead Analyst – Frankreich

Dr. Maxime Martelli

Lead Analyst – Frankreich

Craig Baty

Lead Analyst – Australien

Christian Horst Alves Reis

Lead Analyst – Brasilien

Phil Hassey

Lead Analyst – U.S.A. Öffentlicher Sektor

Monica K

Research Analyst

Kontaktpersonen für diese Studie

Bhuvaneshwari Mohan

Research Analyst

Sandya Kattimani

Research Analyst

Bruno Nakazone

Research Analyst

Rajesh Chillappagari

Data Analyst

Laxmai Sahebrao Kadve

Data Analyst

Shreemadhu Rai B

Project Manager

ISG Provider Lens™ Advisors Involvement Program

Das ISG Provider Lens™ Programm bietet Marktbewertungen von praxiserfahrenen Experten; sie haben einen regionalen Fokus und beruhen auf unabhängigem Research. ISG stellt sicher, dass in jede Studie Advisors einbezogen werden, um die entsprechenden Marktgegebenheiten in Bezug auf die jeweiligen Servicebereiche/Technologietrends, die Präsenz der Serviceanbieter und den Unternehmenskontext abzudecken.

ISG verfügt in jeder Region über fachkundige Vordenker und angesehene Advisors, die sich sowohl mit den Portfolios und Angeboten der Provider als auch den Anforderungen der Unternehmen und den Markttrends auskennen. Im Durchschnitt nehmen drei Berater als Mitglieder des Quality & Consistency Review Teams (QCRT) für jede Studie teil.

Das QCRT stellt sicher, dass in jede Studie ergänzend zur Primär- und Sekundärrecherche der Analysten auch die Erfahrungen der ISG Advisors im jeweiligen Bereich einfließen. Die ISG Advisors nehmen an jeder Studie als QCRT-Mitglieder teil und leisten entsprechend ihrer Verfügbarkeit und ihres Fachwissen auf verschiedenen Ebenen Beiträge.

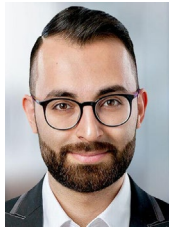
Die QCRT Advisors

- helfen, Quadranten und Fragebögen zu definieren und zu validieren
- beraten bei der Einbeziehung von Dienstleistern, nehmen an Briefing-Gesprächen teil
- stellen ihre Sicht der Bewertungen von Dienstleistern dar und überprüfen Berichtsentwürfe

Kontaktpersonen für diese Studie

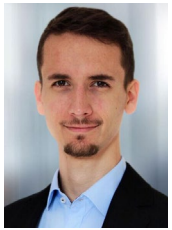
Doug Saylors

Partner, Co-Lead ISG Cybersecurity



Reza Memarian

Principal Consultant Cybersecurity



Anas Barmo

Senior Consultant Cybersecurity

Joyce Harkness

Director Cybersecurity

Eingeladene Unternehmen

Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.

* Bewertet in der vorherigen Ausgabe

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*

Eingeladene Unternehmen

Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.

* Bewertet in der vorherigen Ausgabe

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*

Eingeladene Unternehmen

Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.

* Bewertet in der vorherigen Ausgabe

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*

Eingeladene Unternehmen

Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.

* Bewertet in der vorherigen Ausgabe

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*

Eingeladene Unternehmen

Falls Ihr Unternehmen auf dieser Seite aufgeführt ist oder Sie der Meinung sind, dass Ihr Unternehmen aufgeführt werden sollte, setzen Sie sich bitte mit ISG in Verbindung, um sicherzustellen, dass wir die richtige(n) Kontaktperson(en) für die aktive Teilnahme an dieser Studie haben.

* Bewertet in der vorherigen Ausgabe

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™

Die ISG Provider Lens™ Quadranten-Reports bieten Bewertungen von Dienstleistern und kombinieren als einzige Studien dieser Art datengestützte Forschung und Marktanalysen mit praktischen Erfahrungen und Beobachtungen, gestützt auf das globale ISG-Beraterteam. Unternehmen erhalten eine Fülle detaillierter Daten und Marktanalysen, die ihnen bei der Auswahl geeigneter Sourcing-Partner helfen; die ISG-Berater wiederum nutzen die Berichte, um ihre Marktkenntnisse zu validieren und Empfehlungen für die Unternehmenskunden von ISG abzugeben. Die Studien decken derzeit Provider mit Angeboten in mehreren Regionen weltweit ab. Weitere Informationen über die ISG Provider Lens™ Studien finden Sie auf dieser Webseite.

ISG Research™

Das ISG Research™ Angebot umfasst Research- Subskriptionsservices, Beratungs - Services und Executive Event Services mit Fokus auf Markttrends und disruptive Technologien im Unternehmensumfeld. ISG Research™ zeigt Unternehmen auf, wie sie ein schnelleres Wachstum und einen höheren Mehrwert erzielen können.

ISG bietet Research speziell über Anbieter für staatliche und kommunale Behörden (einschließlich Landkreise und Städte) sowie für Hochschuleinrichtungen an. Besuchen Sie auch: Öffentlicher Sektor.

Weitere Informationen zu den ISG Research™ Subskriptions-Services sind unter contact@isg-one.com, Tel.+49 (0) 561-50697524 oder auf unserer Website unter research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) ist ein führendes, globales Marktforschungs- und Beratungsunternehmen im Informationstechnologie-Segment. Als zuverlässiger Geschäftspartner für über 900 Kunden, darunter über 75 der 100 weltweit größten Unternehmen, unterstützt ISG Unternehmen, öffentliche Organisationen sowie Service- und Technologie-Anbieter dabei, Operational Excellence und schnelleres Wachstum zu erzielen. Der Fokus des Unternehmens liegt auf Services im Kontext der digitalen Transformation, inklusive Automatisierung, Cloud und Daten- Analytik, des Weiteren auf Sourcing-Beratung, Managed Governance und Risk Services, Services für den Netzwerkbetrieb, Strategie- und -Betriebs-Design, Change Management sowie Marktforschung und Analysen in den Bereichen neuer Technologien. 2006 gegründet, beschäftigt ISG mit Sitz in Stamford, Connecticut, über 1.600 mit der Digitalisierung vertraute Experten und ist in mehr als 20 Ländern tätig. Das globale Team von ISG ist bekannt für sein innovatives Denken, seine geschätzte Stimme im Markt, tiefgehende Branchen-und Technologie-Expertise sowie weltweit führende Marktforschungs- und Analyse-Ressourcen, die auf den umfangreichsten Marktdaten der Branche basieren.

Weitere Informationen unter www.isg-one.com.

ISG Provider Lens™

JANUAR, 2024

BROSCHÜRE: CYBERSECURITY – SOLUTIONS & SERVICES