ISG Provider Lens™

Cybersecurity – Solutions and Services 2023

Eine Analyse des Cybersicherheitsmarktes, die die Attraktivität der Portfolios und die Wettbewerbsstärke der Anbieter vergleicht

BROCHURE | JANUAR 2023 | GLOBAL

Table of Contents

Einleitung 3

About the Study

Quadrants Research 4
Definition 5-15
Quadrants by Regions 16
Zeitplan 17

Kundenfeedback Nominierungen 18

Kontaktpersonen für diese Studie 19

Advisor Involvement

Advisor Involvement - Program Description 20
Advisory Team 20

Eingeladene Unternehmen 21-24

Über ISG 25

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

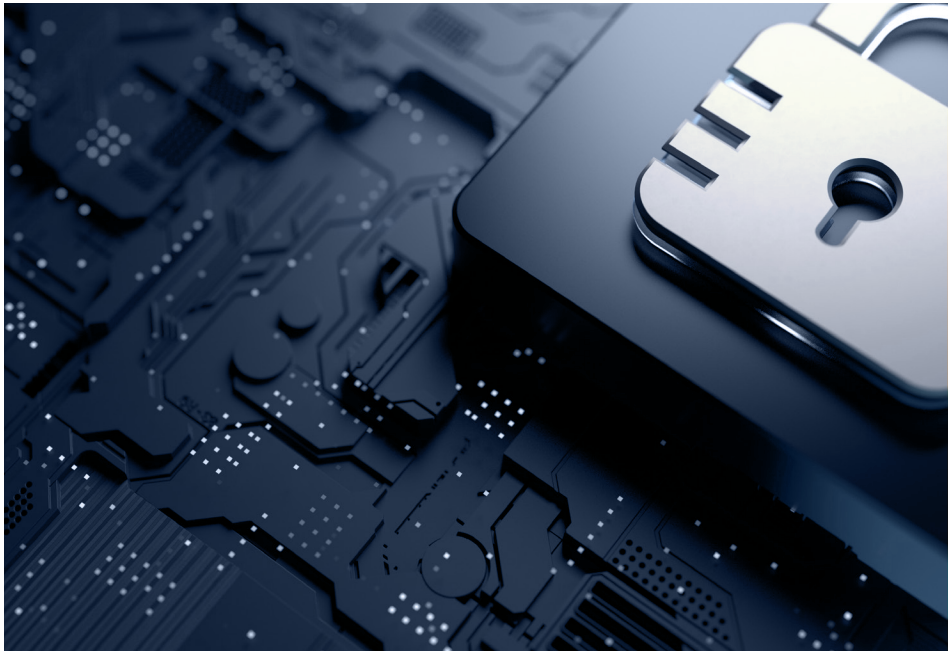
Einleitung

Aus Cybersicherheitssicht könnte man das Jahr 2022 als turbulent bezeichnen; trotz sinkender Datenschutzverletzungen waren die Angriffe in diesem Jahr deutlich raffinierter und schwerer. Im Jahr 2022 haben die Unternehmen ihre Investitionen in die Cybersicherheit erhöht und entsprechenden Initiativen zur Verhinderung von Angriffen und zur Verbesserung ihres Sicherheitsstatus eine hohe Priorität eingeräumt. Sie hatten aus den Angriffen von 2021 ihre Lektion gelernt; Führungskräfte und Unternehmen aller Größen und Branchen investierten entsprechend in Maßnahmen, um auf Bedrohungen der Cybersicherheit und auf Cyberangriffe reagieren und diese überstehen zu können.

Auch kleine Unternehmen wissen inzwischen, welche Gefahren von Cyber-Bedrohungen ausgehen, und haben erkannt, dass sie aktiv ins Visier genommen werden und sehr anfällig für Cyberangriffe sind. Dadurch stieg der Bedarf an (verwalteten) Sicherheitsdiensten und Cyber Resiliency Services, die es Unternehmen ermöglichen, nach einem Cybervorfall schnell den Betrieb wieder aufzunehmen. Dienstleister und Anbieter offerieren daher Services und Lösungen zur Unterstützung der Wiederherstellung und der Geschäftskontinuität.

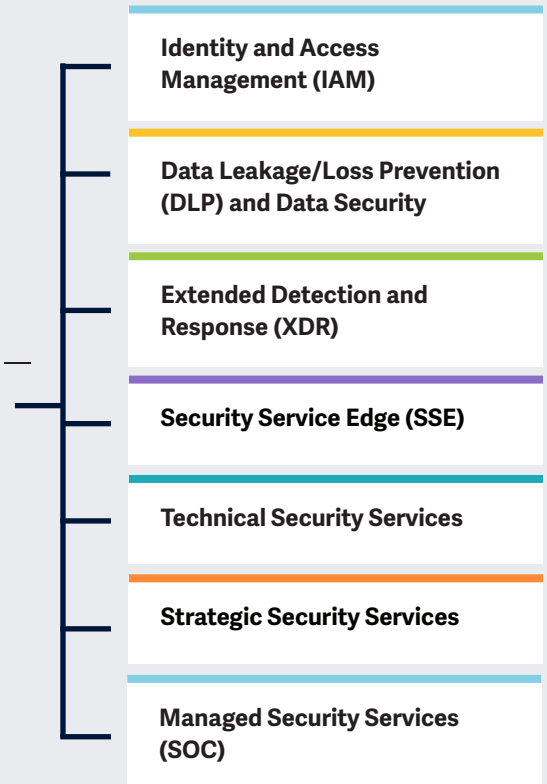
Cyberkriminelle nutzten große Schwachstellen wie Log4shell aus und störten die Geschäftsaktivitäten auch weiterhin mit Ransomware; insbesondere das Gesundheitswesen, die Lieferkette und der öffentliche Sektor gerieten ins Visier.

Unternehmen investierten daraufhin 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, der Expertise der Mitarbeiter und ergänzender verhaltens- und kontextbezogener Intelligenz und Automatisierung soll der Sicherheitsstatus verbessert werden.



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

Schwerpunktbereiche der Studie „Cybersecurity – Solutions und Services 2023"



Simplified Illustration Source: ISG 2023

Die ISG Provider Lens™ Studie „Cybersecurity – Solutions und Services" bietet Geschäfts- und IT-Entscheidern folgende Vorteile:

- Transparente Darstellung der Stärken und Schwächen relevanter Anbieter
- Eine differenzierte Positionierung der Anbieter nach Segmenten, basierend auf Wettbewerbsstärken und Portfolio-Attraktivität
- Fokus auf verschiedene Märkte: weltweit, USA, Großbritannien, nordische Länder, Deutschland, Schweiz, Frankreich, Brasilien, Australien, Singapur & Malaysia sowie den öffentlichen Sektor in den USA; das Thema SSE wird für den globalen Markt analysiert.

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

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

Definition

Die im Rahmen dieses Quadranten bewerteten IAM-Vendoren und -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-Premise oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert.** Entsprechend den individuellen Unternehmensanforderungen können diese Angebote auf verschiedene Arten bereitgestellt werden, z.B. vor Ort oder in der Cloud (vom Kunden verwaltet), 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 im Zusammenhang mit Social Media und mobilen Anwendungen erwartet, um deren spezifische Sicherheitsbedarfe abzudecken, die über web- und kontextbezogenes Berechtigungsmanagement hinausgehen. Auch das 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. **Authentifizierungsunterstützung** anhand einer Kombination von **Single-Sign-On (SSO), Multifaktor-Authentifizierung (MFA)**, risiko- und kontextbasierten Modellen
3. Unterstützung von **rollenbasiertem Zugriff und** Privileged Access Management (PAM)
4. **Zugriffsmanagement** für eine oder mehrere Unternehmensanforderungen wie **Cloud, Endpunkte, mobile Geräte,** dungsprogrammierschnittstellen (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)

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

Definition

Die im Rahmen dieses Quadranten bewerteten DLP-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Dienstleistungen. Dieser Quadrant umfasst auch SaaS-Lösungen auf Basis von proprietärer Software. **Reine Dienstleister, die keine DLP-Produkte (On-Premise oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert.** DLP-Lösungen können sensible Daten identifizieren und überwachen, den Zugriff nur für autorisierte Benutzer ermöglichen und Datenverluste 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 gewährleisten.

Sie gewinnen erheblich an Bedeutung, da es für Unternehmen immer schwieriger wird, Datenbewegungen und -übertragungen zu kontrollieren (über ein Drittel aller Datenverletzungen sind auf eine interne Quelle zurückzuführen). Die Zahl der Geräte, einschließlich der Mobilgeräte, die zur Datenspeicherung genutzt werden, nimmt in Unternehmen zu. Sie sind mit einer Internetverbindung ausgestattet und können Daten senden und empfangen, ohne diese über ein zentrales Internet-Gateway zu leiten. 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-Angebot auf Basis von **proprietärer Software** und nicht auf Basis von Software von Drittanbietern
2. DLP-Unterstützung über eine **beliebige Architektur wie Cloud, Netzwerk, Speicher oder Endpunkt**
3. 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. Diese Lösungen sollten in der Lage sein, **sensible Daten zu erkennen, Richtlinien durchzusetzen,** den Datenverkehr zu überwachen und die Daten-Compliance zu verbessern.

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

Definition

Die in diesem Quadranten bewerteten XDR-Lösungsanbieter zeichnen sich dadurch 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 sind auf umfassende Arbeitsplatz-, Netzwerk- oder Workload-Sicherheit ausgelegt. Sie zielen normalerweise darauf ab, die Transparenz und den kontextuellen Rahmen der identifizierten Bedrohung und deren Kontext unternehmensweit zu verbessern. Daher verfügen diese Lösungen über spezifische Merkmale, u.a. Telemetrie und kontextbezogene Datenanalyse, Erkennung und Reaktion. XDR-Lösungen umfassen mehrere Produkte und Lösungen, die in einer einzigen Konsole integriert sind, so dass man dank ausgefeilter Funktionen Bedrohungen sehen, erkennen und darauf entsprechend darauf reagieren kann. Der hohe Automatisierungsgrad und die kontextbezogene Analyse bieten spezifische Reaktionsmöglichkeiten, die auf das betroffene System zugeschnitten sind und Warnmeldungen nach Schweregrad im Vergleich zu bekannten Referenz-Frameworks priorisieren. **Reine Dienstleister, die keine XDR-Lösungen auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert.** XDR-Lösungen zielen darauf ab, die Produktvielfalt, die Alarmmüdigkeit, die Integrationsprobleme und die Betriebskosten zu reduzieren, und eignen sich besonders für Sicherheitsteams, die Schwierigkeiten damit haben, ein Best-of-Breed-Lösungsportfolio zu verwalten oder einen Mehrwert aus einer Security Information & Event Management (SIEM) oder Security, Orchestration, Automation & Response (SOAR)-Lösung zu generieren.

Auswahlkriterien

1. XDR-Angebot auf Basis von **proprietärer Software** und nicht auf Basis von Software von Drittanbietern
2. XDR-Lösung mit zwei Hauptkomponenten: **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-Einblicke in Bedrohungen**, die von den Endpunkten ausgehen
7. Lösung mit **automatischen Reaktionsfunktionen**

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

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-Diensten, 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 Firewall (NGFW) umfassen, um einen sicheren Zugriff auf Anwendungen in der Cloud und 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 Secure Edge (SASE), wie SD-WAN oder Mikrosegmentierung, werden in diesem Quadranten nicht berücksichtigt, werden aber in der Studie „Network – Software-Defined Solutions & Services“ behandelt.

SSE-Lösungen sind stark nutzerorientiert; sie bieten den Endanwendern Edge- oder Gerätesicherheit über die Cloud, anstatt ihnen den zentralen Zugriff auf Unternehmensanwendungen und Datenbanken über dedizierte Netzwerke zu gewähren. ZTNA (Zero Trust Network Access) stellt eine exklusive Verbindung zwischen einem Benutzer und einer Anwendung her und nutzt kontextbasierte Verhaltensanalysen für die Zugriffskontrolle. CASB (Cloud Access Security Broker) bietet Transparenz, setzt Sicherheitsrichtlinien und Compliance durch und ermöglicht die Kontrolle der 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 bewertet die Benutzererfahrung unter Einsatz fortschrittlicher Automatisierung.

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

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 der oben genannten Komponenten **überwiegend auf Basis proprietärer** Software, **teilweise evtl. auf Basis von 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. V**ollständige und weltweite** Verfügbarkeit

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

Definition

Die in diesem Quadranten bewerteten Anbieter von technischen Sicherheitsdiensten (Technical Security Services, TSS) offerieren Integrations-, Wartungs- und Supportleistungen für IT- und OT-Sicherheitsprodukte oder -lösungen sowie DevSecOps Services. Diese Dienste adressieren alle Sicherheitsprodukte, 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 einer bestehenden Sicherheitsarchitektur mit relevanten Produkten 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. Die Anbieter setzen auch hochentwickelte Lösungen ein, die anhand von umfassenden Schwachstellen-Scans über Anwendungen, Netzwerke, Endgeräte und einzelne Benutzer hinweg Schwachstellen aufdecken und externe und interne Bedrohungen entschärfen.

TSS Provider investieren in den Aufbau von Partnerschaften in den Bereichen Sicherheitstechnologie, Cloud, Daten und Netzwerke; so erhalten sie spezialisierte Akkreditierungen und erweitern ihren Tätigkeitsbereich und ihr Portfolio. Dieser Quadrant umfasst auch klassische Managed Security Services, also Services, die ohne ein Security Operations Center (SOC) erbracht werden.

In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf ihre jeweiligen proprietären Produkte konzentrieren und Produkte oder Lösungen anderer Anbieter implementieren und integrieren können.

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

Auswahlkriterien

1. Nachweisliche Erfahrung mit der **Implementierung von Sicherheitslösungen** für Unternehmen im jeweiligen Land
2. **Autorisierung durch Sicherheitstechnologie-Anbieter** (Hardware und 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

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

Definition

Die in diesem Quadranten bewerteten Provider von Strategic Security Services (SSS) bieten Beratung für IT- und OT-Sicherheit an. Die abgedeckten Services umfassen Sicherheitsaudits, Compliance- und Risikoberatung, Sicherheitsbewertungen, Beratung zur Architektur von Sicherheitslösungen sowie Aufklärung und Schulungen. Diese Services dienen der Bewertung des Sicherheitsreifegrads sowie der Risikolage und der Definition einer auf die individuellen Anforderungen zugeschnittenen Cybersecurity-Strategie für Unternehmen.

SSS Provider sollten Sicherheitsberater beschäftigen, die über umfassende Erfahrung in 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 vCSIO (Virtual Chief Security Information Officer) Services zur Verfügung gestellt werden. Angesichts der zunehmenden Bedeutung der Cyber-Resilienz sollten SSS Provider 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 konzentrieren. Die hier analysierten Dienste decken alle Sicherheitstechnologien ab, insbesondere OT-Sicherheit und SASE.

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

Auswahlkriterien

1. Nachweis von 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. Die **Durchführung von Sicherheitsberatungen unter Verwendung von Frameworks** ist von Vorteil.
4. **Kein ausschließlicher Fokus auf proprietäre Produkte** oder Lösungen

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

Definition

Die im Rahmen der Managed Security Services (SOC) (MSS (SOC)) bewerteten Anbieter offerieren Dienstleistungen im Zusammenhang mit dem Betrieb und der Verwaltung von IT- und OT-Sicherheitsinfrastrukturen für einen oder mehrere Kunden durch ein Security Operations Center (SOC). Dieser Quadrant untersucht Dienstleister, die sich nicht ausschließlich auf proprietäre Produkte konzentrieren, 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.

Es besteht eine steigende Nachfrage nach Anbietern, die Unternehmen dabei unterstützen, ihre IT-Sicherheit insgesamt zu verbessern und die Wirksamkeit ihrer Sicherheitsprogramme durch kontinuierliche Verbesserungen langfristig zu maximieren. Zu diesem Zweck müssen MSS (SOC)-Anbieter 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 Services (MDR) zu erbringen, mit den neuesten Technologien, Infrastrukturen ausgestattet sein und Threat Hunting und Incident Management Experten beschäftigen, so dass Unternehmen aktiv Bedrohungen erkennen und sie in Reaktion darauf abwehren und eindämmen können. Aufgrund der steigenden Kundenerwartungen in Bezug auf die proaktive Bedrohungsjagd sind die Anbieter dabei, ihre SOC-Umgebungen mit Sicherheitsintelligenz auszubauen und erhebliche Investitionen in Technologien wie Automatisierung, Big Data, Analytik, KI und maschinelles Lernen zu tätigen. Diese hochmodernen SOCs sollten eine von Experten gesteuerte Reaktion auf Sicherheitsinformationen unterstützen und gleichzeitig den Kunden einen ganzheitlichen und einheitlichen Ansatz für Sicherheit auf hohem Niveau bieten.

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

Auswahlkriterien

1. Zu den typischen Dienstleistungen gehören **Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmaßnahmen, Penetrationstests, Firewall-Betrieb, Anti-Virus-Betrieb, Identity & Access Management (IAM)-Betriebsservice, Data Leakage/Loss Prevention (DLP)-Betrieb** und alle anderen Betriebsservices, um einen kontinuierlichen Echtzeitschutz zu bieten, ohne die Leistungsfähigkeit des Unternehmens zu beeinträchtigen. Insbesondere ist auch Secure Access Service Edge (SASE) mit berücksichtigt.
2. Angebot von Sicherheitsdiensten wie **Erkennung und Vorbeugung, Security Information & Event Management (SIEM)** sowie Sicherheitsberatung und Audits, entweder remote oder vor Ort beim Kunden
3. **Akkreditierungen** von Anbietern von Security Tools
4. **SOCs idealerweise im Besitz und unter der Leitung des Anbieters** und nicht überwiegend von Partnern
5. **Zertifizierte Mitarbeiter,** z.B. Zertifizierungen wie Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) und Global Information Assurance Certification (GIAC)

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

Quadrants By Region

Im Rahmen dieser ISG Provider Lens™ Quadrantenstudie zum Thema „Cybersecurity – Solutions & Services 2023" werden die folgenden sieben Quadranten vorgestellt:

Quadrants	U.S.	U.K.	Nordische Länder	Deutschland	Schweiz	Frankreich	Brasilien	Australien	Singapur & Malaysia	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	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Strategic Security Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Managed Security Services (SOC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

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

Zeitplan

Die Research-Phase umfasst die Befragung, Evaluierung, Analyse und Validierung und läuft von Januar bis Februar 2023. Die Ergebnisse werden den Medien im Juli 2023 präsentiert.

Meilensteine	Beginn	Ende
Start der Umfrage	12. Januar 2023	
Umfrage-Phase	12. Januar 2023	13. Februar 2023
Sneak Preview	Mai 2023	
Pressemitteilung & Veröffentlichung	Juli 2023	

Mit Klick auf diesen Link können Sie die ISG Provider Lens™ 2023 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.

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

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.

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

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

Kontaktpersonen für diese Studie

Frank Heuer

Lead Analyst - Germany, Switzerland

Benoit Scheuber

Lead Analyst - France

David Pereira

Lead Analyst - Brazil

Deepika B

Research Analyst

Gowtham Kumar

Lead Analyst - U.S.

Dr. Maxime Martelli

Lead Analyst - France

Phil Hassey

Lead Analyst - U.S. Public Sector

Gabriel Sobanski

Research Analyst

Arun Kumar Singh

Lead Analyst - U.K., Nordics

Andrew Milroy

Lead Analyst - Australia

Bhuvaneshwari Mohan

Research Analyst

Ridam Bhattacharjee

Project Manager

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

ISG Provider Lens Advisors Involvement Program

Das ISG Provider LensTM Programm bietet Marktbewertungen von praxiserfahrenen Experten; sie haben einen regionalen Fokus und beruhen auf unabhängiger 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

ISG Advisors für diese Studie

Doug Saylors

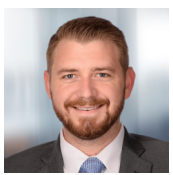
Co-lead, ISG Cybersecurity

Anand Balasubramanium

Senior Consultant

Roger Albrecht

Co-lead, ISG Cybersecurity



Alex Perry

Director

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

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.

* In der vorherigen Ausgabe bewertet

Solution Providers

Absolute Software*
Acronis*
Akamai*
Aruba
Attivo Networks*
Avatier*
Axis Security
Barracuda Networks
BAYOONET*
Beta Systems*
Bitdefender*
Blackberry (Cylance)*
Brainloop*
Broadcom*
Cato Networks
Check Point*
Cisco*
Cloudflare*
CoSoSys*
CrowdStrike*
CyberArk*
Cybereason*
DriveLock*
Elastic
Ergon*
Ericom Software
ESET*
Fidelis Cybersecurity*
FireEye*
Forcepoint*
ForgeRock
Fortinet
GBS
Google
HelpSystems
IBM
iboss
Ilantus Products*
Infinite Networks
itWatch*
Kaspersky*
Lookout*
Matrix42*
Menlo Security
Micro Focus*
Microsoft*
Netskope*
Nevis*
Nexus
NordLayer
OGiTiX*
Okta*
Omada*
One Identity (OneLogin) *
Open Systems*
OpenText*
Oracle*
Palo Alto Networks*
Perimeter 81

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

Eingeladene Unternehmen

If your company is listed on this page or you feel your company should be listed, please contact ISG to ensure we have the correct contact person(s) to actively participate in this research.

* In der vorherigen Ausgabe bewertet

Ping Identity*
Proofpoint*
Rapid7*
RSA*
SailPoint*
SAP*
Saviynt*
Senhasegura*
SentinelOne*
SolarWinds*
Sophos*
Tehtris
Thales*
Trellix*
Trend Micro*
United Security Providers*
Varonis*
Versa Networks
VMware Carbon Black*
WithSecure
Zscaler

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

If your company is listed on this page or you feel your company should be listed, please contact ISG to ensure we have the correct contact person(s) to actively participate in this research.

* In der vorherigen Ausgabe bewertet

Service Providers

Accenture*
Adarma
Alice&Bob.Company*
All for One Group*
AT&T Cybersecurity*
Atea
Atos*
Avanade Inc.
Aveniq*
Axians*
Bechtle*
Booz Allen Hamilton
Bridewell Consulting
BT Security
CANCOM*
Capgemini*
CGI*
Cognizant*
Computacenter*
Controlware*
Datacom*
Deloitte*
Deutsche Telekom*
DIGITALL*
DXC Technology*
Edge UOL*
EY*
Fujitsu*
Getronics*
glueckkanja-gab*
Happiest Minds*
HCLTech*
IBM*
iC Consult*
Indevis*
InfoGuard*
Infosys*
Insight UK
ISH Tecnologia
ISPIN*
KHIPU Networks
KPMG*
Kudelski Security*
Logicalis*
LTIMindtree
Lumen*
Mphasis*
MW Group
NCC Group*
Netic
Nixu*
NTT*
Orange Cyberdefense*
Performanta
Persistent Systems*
Proact IT Group
PwC*
Sapphire
Satisnet

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

Eingeladene Unternehmen

If your company is listed on this page or you feel your company should be listed, please contact ISG to ensure we have the correct contact person(s) to actively participate in this research.

* In der vorherigen Ausgabe bewertet

Secureworks*
SecurityHQ
Siemens
Six Degrees
Softcat
Sopra Steria*
Stefanini
Sunny Valley
suresecure*
Swisscom*
Syntax*
Talion
Talion
Tata Communications*
Tata Consultancy Services (TCS) *
Tech Mahindra*
Telia Cygate
Tempest*
terreActive*
Tesserent*
Thales*
Tietoevry*
Trustwave*
T-Systems*
UMB*
Unisys*
United Security Providers*
UST Global
Venzo Group
Verizon*
Wipro*
Zensar*

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

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 800 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 1.300 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.

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

ISG Provider Lens™

JANUAR, 2023

REPORT: CYBERSECURITY - SOLUTIONS AND SERVICES

© 2023 Information Services Group, Inc.
All Rights Reserved