https://www.isgroup.at Knowledge Base

Table of Contents

- ISGroup Information Security: Unabhängige IT-Sicherheit
- Managed Security Services
- Vulnerability Assessment (VA) durch ISGroup SRL
- Network Penetration Test (NPT)
- Web Application Penetration Test (WAPT)
- Mobile Application Security Testing (MAST)
- Code Review (CR)
- Ethical Hacking (EH) durch ISGroup SRL
- Aus- und Weiterbildung (EDU) durch ISGroup SRL
- Cybersecurity-Nachrichten und Fachwissen
- Publikationen und Ressourcen von ISGroup SRL
- Angewandte Forschung bei ISGroup SRL
- Security Produkte und Technologien
- Fallstudien: Reale IT-Sicherheitsprojekte
- ISGroup SRL: IT-Sicherheit und Ethical Hacking
- ISGroup SRL: Expertise in Offensive Security
- Warum ISGroup SRL
- Über ISGroup SRL
- Partnerschaftsprogramm der ISGroup SRL
- Internationale Präsenz der ISGroup SRL
- Übersicht der ISGroup SRL Dienstleistungen und Ressourcen
- Virtual CISO (vCISO) – Cyber-Governance und Risikomanagement
- Vulnerability Management Service (VMS)
- Cyber Threat Simulation (CTS) durch ISGroup SRL
- Threat Intelligence & Digital Risk Protection
- Security Operation Center (SOC) von ISGroup
- IT Risk Assessment durch ISGroup SRL
- Secure Architecture Review (SAR)
- Cloud Security Assessment (CSA) durch ISGroup SRL
- Windows Security Assessment (WSA)
- IoT/OT Security Assessment (ISA)
- Purple Team Assessment (PTA) von ISGroup
- Phishing-, Smishing- und Vishing-Simulationen
- Social Engineering (SE) – Sicherheitsbewertung und Training
- DSGVO-Konformität (GDPR Compliance)
- NIS2 Compliance: Strategische Umsetzung und Beratung
- ISO/IEC 27001 Compliance und Zertifizierung
- Wireless Security Monitoring (WSM)
- Anti-DDoS-Schutz durch ISGroup SRL
- Firewall as a Service (FWaaS) durch ISGroup SRL
- Security Integration (SIR) durch ISGroup SRL
- Software Assurance Lifecycle (SAL)
- Bug Bounty Program: Konzeption und Management
- Micro Focus und OpenText Softwarelösungen
- Ostorlab Mobile Application Security Scan
- Starter Kit von ISGroup SRL

- PortSwigger Burp Suite
- EasyAudit: Professionelle Sicherheitsprüfungen
- ICT Audit: Cyber-Risiken entdecken, messen und reduzieren
- EasyAudit Exposure
- EXEEC Softwareentwicklung
- Ganapati: Plattform zur Identifizierung von Schwachstellen
- VulnMAP: Schwachstellen-Knowledge-Base
- SCADA Exposure: Sicherheit für industrielle Steuerungssysteme
- PracticalRP
- USH – Die historische Forschungsgruppe
- Ethical Hacking - Das Hacklab der ISGroup SRL
- Metasploit: Offensive IT-Sicherheit
- The Bunker Coworking
- The Bunker Kurse
- The Bunker Hacklab
- PGP-Schlüsselinformationen der ISGroup SRL
- PGP-Schlüssel für ISGroup SRL
- Advanced Bug Bounty (ABB) von ISGroup SRL

ISGroup Information Security: Unabhängige IT-Sicherheit

Source: https://www.isgroup.at

Die ISGroup SRL ist ein spezialisierter Anbieter für IT-Sicherheitsdienstleistungen. Das Unternehmen agiert als unabhängiger Experte und bietet Lösungen auf hohem qualitativen Niveau für ICT-Unternehmen und Sicherheitsagenturen an. Die ISGroup SRL entstand aus einer Gruppe von Forschern und stützt sich auf eine effiziente, wettbewerbsfähige Struktur aus unabhängigen Fachleuten.

Kernkompetenzen und Fachwissen

Das Wissen der ISGroup SRL umfasst ein breites Spektrum der Informationssicherheit:

- Physische Sicherheit
- Infrastruktursicherheit
- Betriebssysteme, Netzwerke und Programme
- Web- und clientseitige Sicherheit

Die Expertise wird durch die aktive Zusammenarbeit mit nationalen und internationalen IT-Sicherheitsagenturen sowie die Einbindung in die Gemeinschaft unabhängiger Forscher stetig erweitert.

Dienstleistungsportfolio

Die ISGroup SRL bietet ein umfassendes Spektrum an Sicherheitsdienstleistungen an, darunter:

- Network Penetration Testing (NPT): Identifikation und Überprüfung von Netzwerkschwachstellen sowie Bewertung von Risiken und Auswirkungen.
- Vulnerability Assessment (VA): Erkennung bekannter Schwachstellen, Fehlkonfigurationen und exponierter Systembereiche.
- Web Application Penetration Testing (WAPT): Sicherheitsprüfung von Webanwendungen durch kontrollierte Angriffe.
- Mobile Application Security Testing (MAST): Prüfung der Sicherheit mobiler Applikationen.
- Ethical Hacking (EH): Realistische Simulation von Angriffsvektoren unter Einbeziehung von Technologie, Prozessen und dem Faktor Mensch.
- Code Review (CR): Analyse des Quellcodes zur Identifikation von Sicherheitsmängeln vor der Produktion.
- Ausbildung (EDU): Praxisnahe Schulungen für Systemadministratoren und Entwickler zur Risikominimierung.
- Governance, Risiko und Compliance (GRC) sowie SSDLC-Dienste.

Kontakt und Informationen

Für Anfragen zu Dienstleistungen, Kooperationen oder vertriebliche Belange besuchen Sie bitte die offizielle Website unter https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Weitere Informationen zur Unternehmensgeschichte, zu Fallstudien und zur Zertifizierung nach UNI CEI EN ISO/IEC 27001:2022 finden Sie ebenfalls auf der Webseite der ISGroup SRL.

Die ISGroup SRL bietet spezialisierte Cybersecurity-Dienstleistungen zum Schutz von Infrastrukturen, Anwendungen und Geschäftsprozessen an. Das Portfolio ist darauf ausgerichtet, das Management und interne IT-Teams zu entlasten, damit diese sich auf ihr Kerngeschäft konzentrieren können.

Für Vertriebsanfragen oder weitere Informationen besuchen Sie https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Managed Security Services

Source: https://www.isgroup.at/de/services.html

Die ISGroup SRL bietet vollständig verwaltete Sicherheitsdienste zur kontinuierlichen Verbesserung der Cyber-Resilienz:

- vCISO (Virtual CISO): Strategische Sicherheitsplanung und Reifegradbewertung basierend auf dem NIST-Framework.
- VMS (Vulnerability Management Service): Identifizierung und Verwaltung von Schwachstellen in Unternehmenssystemen.
- CTS (Cyber Threat Simulation): Durchführung realistischer Simulationen zur Prüfung der Unternehmensresilienz.
- THREAT (Threat Intelligence & Digital Risk Protection): Kontinuierliche Überwachung digitaler Bedrohungen und proaktive Risikominimierung.
- SOC (Security Operation Center): Professionelle Überwachung von Netzwerken und Rechenzentren zur Abwehr von Angriffen.

Offensive Dienste

Zur manuellen Überprüfung der Sicherheitsstufe simuliert die ISGroup SRL Angreifer-Techniken unter Anwendung renommierter Methoden wie OSSTMM und OWASP:

- NPT (Network Penetration Testing): Gezielte Identifizierung unbekannter Sicherheitsprobleme in der IT-Infrastruktur.
- WAPT (Web Application Penetration Testing): Manuelle Sicherheitsprüfung von Webanwendungen.
- MAST (Mobile Application Security Testing): Simulation von Angriffen auf mobile Applikationen (AppStore/PlayStore).
- EH (Ethical Hacking): Umfassende Simulation realer Angriffe auf Infrastruktur, Prozesse und Personal.

Defensive Services

- VA (Vulnerability Assessment): Nicht-invasive Audits zur Identifizierung bekannter Sicherheitslücken.
- CR (Code Review): White-Box-Analyse des Quellcodes zur Aufdeckung von Sicherheitslücken und "bad practices".
- TRA (Ausbildung): Fortbildungen für Administratoren, Analysten, Entwickler und Penetrationstester.

Sicherheitsbewertungsdienste

Die ISGroup SRL führt spezialisierte Bewertungen durch, um den Sicherheitsstatus zu optimieren:

- RA (Risk Assessment): Analyse von Unternehmensrisiken und Implementierung von Schutzmaßnahmen.
- SAR (Secure Architecture Review): Sicherheitsbewertung komplexer Infrastrukturen und Anwendungen.
- CSA (Cloud Security Assessment): Prüfung von AWS, Azure, Google Cloud sowie hybriden Umgebungen.

- WSA (Windows Security Assessment): Analyse der Integrität und Angriffsflächen von Windows-Systemen.
- ISA (IoT/OT Security Assessment): Audits für vernetzte Maschinen, IoT-Geräte und OT-Netzwerke (konform zu IEC 62443, NIS2, etc.).
- PTA (Purple Team Assessment): Bewertung der Unternehmenssicherheit basierend auf der Reaktion auf reale Angriffe.
- PHISH / SE (Phishing, Smishing & Social Engineering): Schulung und Simulation zur Sensibilisierung der Mitarbeitenden.
- PSA (Physical Security Assessment): Analyse der physischen Sicherheit von Standorten und Technikräumen.

Governance, Risk und Compliance

Die ISGroup SRL unterstützt Unternehmen bei der Erreichung und Aufrechterhaltung regulatorischer Anforderungen:

- GDPR Compliance: Überprüfung und Ausarbeitung individueller Lösungen zur DSGVO-Konformität.
- NIS2 Compliance: Analyse und Planung notwendiger Maßnahmen zur Erfüllung der NIS2-Richtlinie.
- PCI DSS Compliance: Sicherstellung der Sicherheit von Zahlungskartentransaktionen.
- ISO-Compliance: Begleitung bei Zertifizierungen nach ISO/IEC 27001, 27017, 27018 sowie 17025.
- PSD2 Compliance: Analyse von Zahlungsprozessen zur Einhaltung der PSD2-Vorgaben.
- ITGOV (ACN-AGID): Umsetzung regulatorischer Vorgaben für öffentliche und private Organisationen.
- DORA (Digital Operational Resilience Act): Analyse und Implementierung von Maßnahmen zur digitalen operationellen Resilienz.

SecOps-Services

- MDR (Multi-Signal MDR): Echtzeit-Erkennung und Blockierung von Bedrohungen mittels XDR-Plattform.
- DFIR (Digital Forensics and Incident Response): Schnelle Reaktion und forensische Analyse bei Cyberangriffen.
- WSM (Wireless Security Monitoring): Kontinuierliche Überwachung von Funkkommunikation.
- Anti-DDoS: Schutz vor Verfügbarkeitsangriffen auf Server und Infrastrukturen.
- FWaaS (Firewall as a Service): Implementierung und Wartung von Next-Generation-Firewalls.
- SIR (Security Integration): Kontinuierlicher Prozess der Schwachstellenerkennung und Fehlerbehebung.

SSDLC-Services

- SAL (Software Assurance Lifecycle): Sicherheitskontrollen während des gesamten Software-Lebenszyklus.
- CST (Continuous Security Testing): Regelmäßige und automatisierte Überwachung der IT-Systeme.
- BB (Bug Bounty): Einbindung ethischer Sicherheitsforscher zur präventiven Schwachstellensuche.

Vulnerability Assessment (VA) durch ISGroup SRL

Source: https://www.isgroup.at/de/vulnerability-assessment.html

Der Vulnerability Assessment Service von ISGroup SRL dient der systematischen Analyse und Bewertung der Sicherheit von IT-Systemen. Ziel ist die Identifizierung bekannter Schwachstellen, um die Systemkonfigurationen zu optimieren und Sicherheits-Patches gezielt einzuspielen.

Methodik und Durchführung

ISGroup SRL führt die Assessments sowohl extern als auch intern durch, um unterschiedliche Bedrohungsszenarien zu simulieren:

- **Externes Assessment:** Der Scan erfolgt von einem entfernten Host aus, um die Perspektive eines externen Angreifers (z. B. Wettbewerber) zu prüfen.
- **Internes Assessment:** Der Scan erfolgt aus dem Intranet, um interne Bedrohungen oder kompromittierte Konten (z. B. Ransomware-Angriffe) zu simulieren.

Die Identifizierung erfolgt durch eine Kombination aus automatisierten Tools und manuellen Tests unter Verwendung aktiver, passiver und inferenzbasierter Techniken. Ein wesentlicher Bestandteil des Dienstes ist die manuelle Verifizierung aller Ergebnisse durch Experten von ISGroup SRL, um False Positives zu eliminieren.

Output und Berichterstattung

Die Ergebnisse werden in einem kompakten, detaillierten Bericht zusammengefasst, der für verschiedene Zielgruppen aufbereitet ist:

- **Executive Summary:** High-Level-Zusammenfassung für das Management.
- **Vulnerability Details:** Technischer Abschnitt zu den gefundenen Schwachstellen und deren Auswirkungen für Security Manager.
- **Remediation Plan:** Präzise Anleitungen zur Behebung der Probleme für Systemadministratoren.

Wichtige Hinweise zum Service

- **Nicht-invasive Techniken:** ISGroup SRL legt Wert auf den Schutz der Systemverfügbarkeit und minimiert Betriebsunterbrechungen durch den Einsatz nicht-invasiver Methoden.
- **Häufigkeit:** Es wird empfohlen, ein Vulnerability Assessment mindestens einmal jährlich sowie nach wesentlichen Änderungen an der Infrastruktur durchzuführen.
- **Abgrenzung:** Während das Vulnerability Assessment bekannte Schwachstellen identifiziert, prüfen Penetration Tests (Network oder Web Application) die tatsächliche Ausnutzbarkeit dieser Schwachstellen.
- **Datenschutz:** ISGroup SRL arbeitet nach ISO/IEC 27001, wodurch alle Ergebnisse als vertrauliche Dokumentation behandelt werden.

Kontakt und Angebote

Für Anfragen zu Dienstleistungen, zur Definition des Prüfumfangs oder zur Anforderung eines Angebots besuchen Sie bitte die Website https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Network Penetration Test (NPT)

Source: https://www.isgroup.at/de/network-penetration-test.html

Die ISGroup SRL bietet professionelle Network Penetration Tests (NPT) an, um Sicherheitslücken in IT-Infrastrukturen zu identifizieren, bevor diese von unbefugten Dritten ausgenutzt werden können. Ziel ist es, die Sicherheit des Netzwerks zu bewerten und die Widerstandsfähigkeit gegen Bedrohungen wie Exploits, Viren, Trojaner, DoS-Angriffe und Sabotage zu erhöhen.

Methodik und Ansatz

Die ISGroup SRL führt Penetration Tests nach international anerkannten Standards durch, insbesondere gemäß dem OSSTMM (Open Source Security Testing Methodology Manual). Die Dienstleistungen sind individuell anpassbar und können neben rein technischen Aspekten auch Social Engineering sowie physische Sicherheitsaspekte umfassen.

Die Tests werden in verschiedenen Szenarien durchgeführt:

- **Internal PT:** Simulation von Angriffen aus dem internen Unternehmensnetzwerk.
- **External PT:** Simulation von Angriffen von außerhalb des Unternehmensnetzwerks.
- **Informationslevel:** Je nach Kundenwunsch werden Black Box, Grey Box oder White Box Ansätze gewählt, um unterschiedliche Wissensstände von Angreifern zu simulieren.
- **Spezialisierte Tests:** Angeboten werden zudem Wireless Penetration Tests sowie Social Engineering zur Überprüfung der menschlichen Komponente.

Prozess des Network Penetration Tests

Der Testprozess umfasst folgende Kernschritte:

- Suche nach Schwachstellen in gefährdeten Systemen (intern oder extern).
- Ausnutzung identifizierter Schwachstellen, um in Netzwerkbereiche einzudringen.
- Inspektion interner Systeme auf weitere Sicherheitslücken, um den Zugriff auf Daten und Infrastrukturen zu erweitern.
- Kontinuierliche Wiederholung des Prozesses zur Maximierung der Sicherheitsanalyse.

Ergebnisse und Berichterstattung

Die ISGroup SRL stellt die Ergebnisse in einem strukturierten Bericht zusammen, der in drei wesentliche Bereiche unterteilt ist:

- **Executive Summary:** Eine prägnante Zusammenfassung für das Management (maximal eine Seite).
- **Vulnerability Details:** Ein technischer Teil für Security Manager, der die gefundenen Schwachstellen und deren Auswirkungen detailliert beschreibt.
- **Remediation Plan:** Ein technischer Leitfaden für Systemadministratoren mit präzisen Anweisungen zur Behebung der identifizierten Sicherheitslücken.

Kontakt und Angebote

Für weiterführende Informationen, eine individuelle Beratung oder die Anforderung eines Angebots für einen Network Penetration Test besuchen Sie bitte die Website https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Web Application Penetration Test (WAPT)

Source: https://www.isgroup.at/de/web-application-penetration-test.html

Die ISGroup SRL bietet professionelle Web Application Penetration Tests an, um Schwachstellen zu identifizieren, die von automatisierten Scannern häufig übersehen werden. Der Dienst umfasst die Analyse von Webportalen, E-Commerce-Anwendungen und komplexen Webplattformen gemäß den Standards OWASP und OSSTMM.

Methodik und Ansatz

Die ISGroup SRL kombiniert manuelle Techniken mit spezialisierten Werkzeugen, um sowohl offensichtliche als auch versteckte Sicherheitslücken aufzudecken. Da Webanwendungen vollständig exponiert sind, ist "Security through Obscurity" nicht ausreichend; stattdessen ist die Entwicklung widerstandsfähiger Anwendungscodes erforderlich.

Der Testprozess umfasst folgende Phasen:

- Identifikation und Entdeckung aller auf dem Ziel freigelegten Ressourcen.
- Analyse der Business-Logik zur Vermeidung konzeptioneller Sicherheitslücken.
- Überprüfung der zugrunde liegenden Infrastruktur auf bekannte und unbekannte Schwachstellen.
- Durchführung von Angriffsversuchen nach Identifikation gültiger Entry Points.
- Umfassende Prüfung der Parameter mittels manueller Tests und vordefinierter Angriffstechniken.
- Versuch der Eskalation, um nicht autorisierte Aktionen durchzuführen, Daten aus Backends abzurufen oder die Kontrolle über Systeme zu erlangen.

Output und Berichterstattung

Die ISGroup SRL stellt nach Abschluss der Tätigkeit einen detaillierten Bericht bereit, der in drei zentrale Bereiche unterteilt ist:

- **Executive Summary:** Eine prägnante Zusammenfassung der Ergebnisse auf Management-Ebene (maximal eine Seite).
- **Vulnerability Details:** Ein technischer Abschnitt für Security Manager, der die identifizierten Schwachstellen und deren Auswirkungen detailliert beschreibt.
- **Remediation Plan:** Ein technischer Leitfaden für Entwickler mit präzisen Anweisungen zur Behebung der festgestellten Sicherheitslücken.

Kontakt und Vertrieb

Für Anfragen zu einem Web Application Penetration Test oder zur Vereinbarung eines Beratungsgesprächs steht die ISGroup SRL zur Verfügung.

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Mobile Application Security Testing (MAST)

Source: https://www.isgroup.at/de/mobile-application-security-testing.html

Die ISGroup SRL bietet mit dem Mobile Application Security Testing (MAST) ein spezialisiertes Application Security Assessment für iOS- und Android-Plattformen an. Ziel ist die Identifizierung von Sicherheitslücken, die durch die Interaktion mobiler Anwendungen mit dem Betriebssystem, dem Gerät oder Remote-Servern entstehen können.

Leistungsumfang und Methodik

Die ISGroup SRL passt das Testing an die jeweilige Entwicklungsumgebung an:

- Native Apps: Unterstützung für Objective-C, Swift, Java und Kotlin.
- Hybrid-Frameworks: Unterstützung für React, React Native, Cordova, Xamarin, Titanium Appcelerator, Ionic und PhoneGap.

Die Analyse erfolgt durch manuelle Techniken und den Einsatz fortschrittlicher Werkzeuge, wobei zwei Testmodi zur Verfügung stehen:

- Grey Box: Der Tester analysiert den bereitgestellten Quellcode, um auch durch Obfuskation verborgene Schwachstellen zu identifizieren, gefolgt von einer Runtime-Analyse.
- Black Box: Simulation eines Angreifers, der die Anwendung wie ein regulärer Nutzer aus dem Store bezieht.

Kernbereiche der Analyse

Die ISGroup SRL deckt bei der Prüfung drei wesentliche Sicherheitsdimensionen ab:

- Client-Side Vulnerabilities: Prüfung auf unsichere Datenspeicherung, fehlende Root-/Jailbreak-Erkennung und Interaktionsrisiken mit dem Betriebssystem.
- Reverse Engineering: Untersuchung der Anwendung auf Schutzmechanismen gegen geistigen Datendiebstahl und Analyse der Widerstandsfähigkeit gegen Manipulation während der Laufzeit.
- Server-Side Interaction: Überprüfung der Kommunikation zwischen App und Remote-Server, insbesondere hinsichtlich Authentifizierung, Autorisierung und SQL-Injection-Risiken.

Ergebnisbericht

Jedes MAST-Projekt der ISGroup SRL schließt mit einem detaillierten Bericht ab, der in drei Bereiche gegliedert ist:

- Executive Summary: Eine nicht-technische Zusammenfassung für das Management.
- Vulnerability Details: Eine technische Dokumentation der identifizierten Schwachstellen und deren Auswirkungen für Sicherheitsverantwortliche.
- Remediation Plan: Ein technischer Leitfaden mit präzisen Anweisungen zur Behebung der Sicherheitslücken für Entwickler.

Kontakt und Informationen

Für weitere Informationen, ein Beratungsgespräch oder ein konkretes Angebot steht die ISGroup SRL zur Verfügung:

- Webseite: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Code Review (CR)

Source: https://www.isgroup.at/de/code-review.html

Der Code Review Service von ISGroup dient der systematischen Quellcodeanalyse zur Identifikation von Sicherheitslücken, bevor eine Anwendung in die Produktionsumgebung überführt wird. Durch die frühzeitige Erkennung von Schwachstellen werden Sicherheitsrisiken minimiert und Entwicklungskosten signifikant gesenkt.

Methodik und Prozess

ISGroup führt den Code Review Prozess in zwei aufeinanderfolgenden Phasen durch, um eine maximale Abdeckung und Präzision zu gewährleisten:

- Statische Analyse: Einsatz spezialisierter Tools zur Simulation der Code-Ausführung, um potenzielle Schwachstellen automatisiert zu identifizieren. Dieser Ansatz bietet den Vorteil einer vollständigen Einsicht in das Verhalten der Applikation.
- Manuelle Analyse: Hochspezialisierte Experten führen eine tiefgreifende manuelle Prüfung der kritischsten Anwendungsbereiche durch. Diese Phase ist essenziell, da automatisierte Werkzeuge aufgrund der Komplexität moderner Software nicht alle Sicherheitslücken eigenständig erkennen können.

Expertise

Die Dienstleistung wird von einem erfahrenen Team durchgeführt, das über fundierte Kenntnisse in der Programmierung sowie in der Analyse komplexer Quellcodes verfügt. ISGroup agiert auf Basis international anerkannter Standards und integriert kontinuierliche Forschung in ihre Sicherheitsdienstleistungen.

Output und Berichterstattung

Nach Abschluss der Analyse erhält der Kunde einen detaillierten Bericht, der sich in zwei Kernbereiche gliedert:

- Executive Summary: Bietet einen Überblick über die identifizierten Probleme, Implementierungsfehler sowie eine allgemeine Bewertung des Sicherheitsniveaus der Applikation.
- Vulnerability Details: Enthält für jede gefundene Schwachstelle den betroffenen Quellcodeabschnitt, eine detaillierte technische Erläuterung sowie konkrete Empfehlungen zur Behebung (Remediation).

Kontakt und Vertrieb

Für weitere Informationen, individuelle Angebote oder eine fachliche Beratung zu den Dienstleistungen von ISGroup stehen folgende Kanäle zur Verfügung:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Ethical Hacking (EH) durch ISGroup SRL

Source: https://www.isgroup.at/de/ethical-hacking.html

Der von **ISGroup SRL** angebotene Ethical-Hacking-Service dient der Bewertung der tatsächlichen Exposition gegenüber Schwachstellen und Cyber-Risiken durch kontrollierte, realistische Angriffssimulationen. Ziel ist es, das Sicherheitsniveau einer Organisation durch die Identifikation von technischen Lücken, Konfigurationsfehlern und Prozessschwächen zu messen und zu verbessern.

Kernkonzept und Methodik

Der Service von **ISGroup SRL** geht über klassische Penetration-Tests (NTP/WAPT) hinaus, indem er nicht nur technologische Aspekte, sondern auch den menschlichen Faktor einbezieht.

- **Realistische Simulation:** Es wird ein Angriff durch einen böswilligen Akteur (extern oder intern) nachgestellt, ohne den Einsatz automatisierter Tools, die Spuren hinterlassen könnten.
- **Unkonventionelle Techniken:** Anwendung von Methoden wie Social Engineering und Sniffing des Netzwerkverkehrs.
- **Ganzheitlicher Ansatz:** Bewertung der menschlichen Komponente und der internen Prozesse, die oft das schwächste Glied in der Sicherheitskette darstellen.

Ablauf des Ethical-Hacking-Services

Die Durchführung erfolgt ausschließlich nach einer formalen Autorisierung sowie der Definition von Scope und Rules of Engagement. Der Prozess gliedert sich in vier Phasen:

1. **Voranalyse:** Definition des Perimeters, der Ziele, der operativen Rahmenbedingungen und der Erfolgskriterien zur Maximierung der Betriebssicherheit.
2. **Aufklärung:** Informationssammlung zur Identifikation von Vektoren und Einstiegspunkten sowie Analyse der exponierten Angriffsfläche.
3. **Angriffssimulation:** Kontrollierte Validierung von Schwachstellen und deren Auswirkungen zur Messung des tatsächlichen Risikos.
4. **Bericht und Remediationsplan:** Bereitstellung technischer Nachweise, detaillierter Beschreibungen der Ausnutzungswege sowie eines konkreten Plans zur Behebung der Schwachstellen mit Priorisierung.

Vorteile für Organisationen

- **Konkrete Nachweise:** Sicherheit basiert auf validierten Ergebnissen statt auf Annahmen.
- **Proaktive Risikominimierung:** Identifikation von Schwachstellen, bevor diese von Kriminellen ausgenutzt werden können.
- **Compliance und Standards:** Unterstützung bei der Einhaltung internationaler Standards wie ISO 27001, NIS2 und Anforderungen der DSGVO (GDPR).
- **Business-Kontinuität:** Schutz vor Datenverlust, Reputationsschäden und kostspieligen Notfall-Remediationsmaßnahmen.

Kontakt und Vertrieb

Für weitere Informationen, eine individuelle Beratung oder die Anforderung eines Angebots für den Ethical-Hacking-Service von **ISGroup SRL** stehen folgende Kanäle zur Verfügung:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

FAQ – Häufige Fragen

- **Unterschied zu Penetration Testing:** EH bietet eine umfassendere Simulation, die unkonventionelle Techniken und den menschlichen Faktor einschließt.
- **Voraussetzungen:** Eine formale Autorisierung sowie die Festlegung des Scopes sind zwingend erforderlich.
- **Dauer und Kosten:** Diese hängen vom Perimeter, der Komplexität der Systeme und der gewünschten Testtiefe ab. **ISGroup SRL** erstellt nach einer initialen Anforderungserhebung eine individuelle Schätzung.
- **Output:** Kunden erhalten einen detaillierten Bericht inklusive technischer Nachweise und einen strukturierten Remediationsplan.

Aus- und Weiterbildung (EDU) durch ISGroup SRL

Source: https://www.isgroup.at/de/training.html

Die ISGroup SRL bietet spezialisierte Aus- und Weiterbildungsservices an, um Sicherheitsteams, Systemanalytiker und Entwickler für die Herausforderungen der modernen Cybersicherheit zu qualifizieren. Ziel der Schulungen ist es, die Kosten für Sicherheitsproblematiken durch eine fundierte Ausbildung des eigenen Personals zu reduzieren.

Methodik und Kursaufbau

Die Kurse der ISGroup SRL kombinieren theoretische Wissensvermittlung mit praktischen Anwendungen:

- **Theorie:** Erläuterung von Methodiken und technologischen Aspekten der jeweiligen Sicherheitsthemen.
- **Praxis:** Durchführung von "Challenges", bei denen Teilnehmer Systeme oder Anwendungen unter Zeitdruck prüfen oder absichern müssen.
- **Zertifizierung:** Nach Abschluss des Kurses wird eine Bescheinigung über die Teilnahme und die erworbenen Fähigkeiten ausgestellt.

Kernbereiche der Ausbildung

Die Schulungen decken zwei wesentliche Perspektiven der IT-Sicherheit ab:

- **Angriff:** Fokus auf Methodologien zur Identifizierung und Ausnutzung von Schwachstellen in Systemen oder Applikationen, um ein tiefgreifendes Verständnis für Angriffsvektoren zu entwickeln.
- **Abwehr:** Fokus auf Hardening-Methoden, sichere Programmierung (Secure Coding) und die Analyse von Programmierfehlern in realen, anfälligen Anwendungen.

Themengebiete

Die ISGroup SRL deckt unter anderem folgende Schwerpunkte ab:

- Secure Coding und Web Application Code Review
- Web Application Penetration Testing
- Network Hardening
- Hardening für Linux, Windows und Solaris

Kursangebot

Die ISGroup SRL bietet ein breites Spektrum an spezifischen Kursen an:

- **Application Security for Architects:** Integration von Sicherheitspraktiken in den gesamten Softwareentwicklungszyklus.
- **OWASP Top 10 Bootcamp & Laboratory:** Sensibilisierung für und praktische Schulung zu den zehn häufigsten Programmierfehlern in Webanwendungen.
- **Security Awareness:** Vermittlung von Wissen und Werkzeugen zur Abwehr allgemeiner Cyberbedrohungen.
- **Software Security Requirements (Secure SDLC):** Vorbereitung von Entwicklern auf die Anforderungen an sichere Softwareentwicklung.
- **Code Review:** Identifizierung und Behebung von Schwachstellen im Quellcode.
- **Sicherheit von REST-Diensten:** Verständnis spezifischer Bedrohungen für REST-Schnittstellen.
- **Network Penetration Testing:** Methodik und Werkzeuge für professionelle Penetrationstests.
- **Cyber Risk Prevention:** Prävention von Cyberrisiken zum Schutz von Unternehmen und Daten.
- **Ethical Hacking:** Untersuchung neuer Technologien und Best Practices zur Gewährleistung der Datensicherheit.

Kontakt und Vertrieb

Für weitere Informationen, Beratungsgespräche oder die Anforderung eines Angebots für die Aus- und Weiterbildung (EDU) wenden Sie sich bitte an die ISGroup SRL:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Cybersecurity-Nachrichten und Fachwissen

Source: https://www.isgroup.at/de/editorial.html

ISGroup SRL bietet ein umfassendes Portfolio an Ressourcen, Leitfäden und Expertenwissen im Bereich der Cybersicherheit. Das Angebot umfasst technische Analysen, Compliance-Standards sowie praxisnahe Fallstudien zur Absicherung von IT-Infrastrukturen und Anwendungen.

Kernkompetenzen und Dienstleistungen von ISGroup SRL

ISGroup SRL unterstützt Unternehmen durch spezialisierte Sicherheitslösungen, um den Schutz vor modernen Cyber-Bedrohungen zu gewährleisten:

- Penetration Testing: Umfassende Prüfungen für Netzwerke, Webanwendungen, mobile Applikationen und IoT-Umgebungen.
- Proaktive Verteidigung: Implementierung von Multi-Signal MDR (Managed Detection and Response), Cyber Threat Simulationen und Purple Team Assessments.
- Compliance und Zertifizierung: Unterstützung bei der Erreichung von ISO/IEC 27001- und ISO 9001-Zertifizierungen sowie Beratung zu AGID-Vorgaben und eIDAS-Regulierungen.
- Incident Response: Digital Forensics und Incident Response (DFIR) zur schnellen Reaktion auf Sicherheitsvorfälle.
- Security Awareness: Schulungen für Teams, Phishing-Simulationen und spezialisierte Kurse zur Stärkung der menschlichen Firewall.
- Infrastruktursicherheit: Secure Architecture Reviews, Cloud Security Assessments, Firewall-as-a-Service (FWaaS) und Anti-DDoS-Lösungen.
- Software-Sicherheit: Code Reviews und Begleitung des Software Assurance Lifecycles.

Fachliche Schwerpunkte und Ressourcen

Die Experten von ISGroup SRL stellen detaillierte Informationen zu aktuellen Sicherheitsstandards und Bedrohungslagen bereit:

- OWASP Top Ten: Detaillierte Analysen der OWASP-Frameworks (2017 und 2021), einschließlich Schwachstellen wie Injection, Broken Access Control und kryptografischen Fehlern.
- Zertifizierungen: Nachweise über die Expertise des Teams, darunter Certified Ethical Hacker (CEH) und Lead Auditor Qualifikationen.
- Fallstudien: Praxisbeispiele für erfolgreich durchgeführte Penetration Tests und Sicherheitsberatungen bei verschiedenen Unternehmenskunden.
- Regulatorische Anforderungen: Leitfäden zu Mindestsicherheitsmaßnahmen für öffentliche Verwaltungen (ICT-Sicherheit) und Cloud-Qualifizierungen.

Kontakt und Vertrieb

Für Anfragen zu Dienstleistungen, Beratungsgesprächen oder weiterführenden Informationen zu den Sicherheitslösungen von ISGroup SRL nutzen Sie bitte die folgenden Kanäle:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Publikationen und Ressourcen von ISGroup SRL

Source: https://www.isgroup.at/de/publications.html

ISGroup SRL ist eine Gruppe aktiver und ethischer Sicherheitsforscher. Das Unternehmen verfolgt das Ziel, Forschungsergebnisse mit der Cyber-Community zu teilen, um den kontinuierlichen Entwicklungsprozess in der IT-Sicherheit zu fördern.

Forschung und Wissenstransfer

ISGroup SRL engagiert sich seit Jahren in der Erstellung von White Papers, Fachartikeln und technischen Materialien. Diese Inhalte werden regelmäßig auf der nicht-kommerziellen Plattform *ush.it* veröffentlicht. Zudem präsentiert das Team regelmäßig auf führenden nationalen und internationalen Konferenzen zu hochspezialisierten Themen der Cybersicherheit.

Zentrale Themenbereiche

Die veröffentlichten Materialien und Präsentationen decken ein breites Spektrum ab, darunter:

- Penetration Testing und IT-Sicherheitsanalysen
- Web Application Security (Bug Hunting und Code Review)
- Schwachstellenanalysen (u.a. LFI, XSS, PHP-Sicherheitsaspekte)
- Hardening-Strategien für Systeme und Anwendungen
- Automatisierung und Skripting (z.B. BASH, Python)

Zertifizierungen und Qualitätsstandards

ISGroup SRL unterstreicht seine Kompetenz und Zuverlässigkeit durch offizielle Zertifizierungen, die für Sicherheit und Qualität stehen:

- ISO/IEC 27001:2022 (Informationssicherheits-Managementsysteme)
- ISO/IEC 9001:2015 (Qualitätsmanagementsysteme)
- IQNET-Zertifizierung

Zusammenarbeit und Expertise

ISGroup SRL unterstützt Unternehmen dabei, kritische Schwachstellen zu identifizieren, IT-Infrastrukturen zu stärken und integrierte Managementsysteme gemäß internationalen Standards zu etablieren. Zu den Kunden zählen namhafte Unternehmen wie Coop Italia, Creactives S.p.A., Prime Service S.r.l. und Progel SA.

Kontakt und weitere Informationen

Für detaillierte Informationen zu den Methoden, Verfahren oder für individuelle Anfragen steht ISGroup SRL zur Verfügung:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Angewandte Forschung bei ISGroup SRL

Source: https://www.isgroup.at/de/research-resources.html

ISGroup SRL betrachtet angewandte Forschung als essenziellen Bestandteil für IT-Sicherheitsdienste auf höchstem Niveau. Durch die Entwicklung origineller Techniken und die kontinuierliche Analyse von Open-Source- sowie proprietärer Software identifiziert das Unternehmen digitale Bedrohungen, bevor diese ausgenutzt werden können.

Methodik und Responsible Disclosure

Innovation und Forschung bilden das Fundament der Dienstleistungen von ISGroup SRL. Um die Nutzergemeinschaft aktiv zu schützen, verfolgt das Unternehmen bei der Entdeckung von Sicherheitslücken das Modell der **Responsible Disclosure**:

- Gefundene Schwachstellen werden direkt an den jeweiligen Software-Hersteller (Vendor) gemeldet.
- Die Veröffentlichung von Security Advisories erfolgt in enger Abstimmung mit dem Hersteller, um sicherzustellen, dass zum Zeitpunkt der Bekanntgabe bereits Sicherheitsupdates oder Patches verfügbar sind.

Security Advisories und Expertise

ISGroup SRL verfügt über eine langjährige Historie in der Identifizierung kritischer Sicherheitslücken in weit verbreiteten Systemen und Anwendungen. Zu den Herstellern und Technologien, für die das Unternehmen bereits Security Advisories veröffentlicht hat, zählen unter anderem:

- Aerohive Networks, AOL, Apache, Fortinet, Jetty, MikroTik, Moodle, Nginx, PHP, QNAP, Skype, SolarWinds, SugarCRM, Veeam und Zabbix.

Die detaillierten Berichte zu den identifizierten Schwachstellen (CVEs) unterstreichen die technische Kompetenz von ISGroup SRL bei der Analyse komplexer Softwarearchitekturen.

Zertifizierungen und Qualität

Die Arbeitsweise von ISGroup SRL ist durch anerkannte internationale Standards zertifiziert, was die Qualität und Sicherheit der angebotenen Dienstleistungen belegt:

- ISO/IEC 27001:2022 (Informationssicherheits-Managementsystem)
- ISO/IEC 9001:2015 (Qualitätsmanagementsystem)
- IQNET Zertifizierung

Zusammenarbeit und Kontakt

ISGroup SRL unterstützt Unternehmen dabei, interne Sicherheitsverfahren zu stärken, die Widerstandsfähigkeit gegen Bedrohungen zu erhöhen und die Konformität mit aktuellen Sicherheitsstandards sicherzustellen. Kunden schätzen dabei die Professionalität, die Einhaltung von Zielvorgaben sowie die technische Expertise des Partners.

Für weitere Informationen zu den Methoden, Verfahren oder für Vertriebsanfragen besuchen Sie bitte https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Security Produkte und Technologien

Source: https://www.isgroup.at/de/products.html

Die ISGroup SRL bietet ein umfassendes Portfolio an ausgewählten Technologien für Assessment, Auditing und den Schutz von Unternehmen. Das Angebot gliedert sich in die Bereiche Security, Intelligence, Spin-Off und Distribution.

Portfolio der ISGroup SRL

- Microfocus Opentext: Die ISGroup SRL fungiert als italienischer Reseller für Microfocus Opentext.
- Ostorlab: Spezialisierte Lösung für Mobile Application Security Scans.
- Starter Kit: Spezielles Angebot für Neukunden zum Einstieg in die Sicherheitslösungen.
- Port Swigger: Managed Security Dienstleistungen.
- EsyAudit: Managed Security Lösungen für Unternehmen.
- ICT Audit: Automatisierte Security-Audits.
- Exposure: Analyse der Security Reputation.
- EXEEC: SaaS-basierte Sicherheitslösungen.
- Ganapati: Integrierte Assessment-Tools.
- VulnMAP: Umfassende Schwachstellendatenbank.
- Scada Exposure: Analyse und Überprüfung der Exposition von SCADA-Systemen.
- PracticalRP: Management-Lösungen für den medizinischen Bereich.
- USH: Plattform für spezialisierte Umgebungen.
- Ethical Hacking: Zugang zum ISGroup Hacklab für Sicherheitsanalysen.
- Metasploit: Ressourcen und Security-Blog.
- The Bunker Coworking: Coworking-Angebot der ISGroup SRL.
- The Bunker Training: Professionelle Schulungsangebote der ISGroup SRL.
- The Bunker Hacklab: Spezielle Laborumgebung für Sicherheitsforschung und Ethical Hacking.

Vertrieb und Anfragen

Für detaillierte Informationen zu den Produkten, Dienstleistungen oder für Vertriebsanfragen besuchen Sie bitte die Webseite https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Fallstudien: Reale IT-Sicherheitsprojekte

Source: https://www.isgroup.at/de/fallstudien.html

Die ISGroup SRL bietet maßgeschneiderte IT-Sicherheitslösungen für Unternehmen jeder Größe. Jedes Projekt basiert auf einer engen Zusammenarbeit, bei der Innovation, Professionalität und Sicherheit im Vordergrund stehen. Ziel ist es, die Sicherheit von Infrastrukturen, Anwendungen und Geschäftsprozessen nachhaltig zu verbessern und komplexe Herausforderungen in strategische Chancen zu verwandeln.

Leistungsspektrum und Projekterfahrungen

Die ISGroup SRL hat eine Vielzahl von Projekten erfolgreich umgesetzt, darunter:

- Web Application Penetration Tests (u. a. für Add Value S.r.l., Alias Group S.r.l., Kelyon S.r.l., Progel SA, Sturnis S.r.l., TimeFlow S.r.l. und TECNORAD S.r.l.)
- Network Penetration Tests (u. a. für Coop Italia und Prime Service S.r.l.)
- ISMS-Unterstützung (u. a. für Creactives S.p.A.)
- Strategische Cybersecurity-Partnerschaften (u. a. mit Rooters)
- Sicherheitsüberprüfungen spezifischer Plattformen wie Albo pretorio (ISWEB S.p.A.)

Zusammenarbeit mit ISGroup SRL

Kunden schätzen die ISGroup SRL als zuverlässigen und strategischen Partner. Die Fallstudien belegen die Fähigkeit, hohe Standards und exzellente Leistungen zu garantieren, unabhängig davon, ob es sich um kleine Unternehmen oder Großkonzerne handelt. Die Expertise der ISGroup SRL ermöglicht es, individuelle Sicherheitsbedürfnisse präzise zu adressieren und messbare Ergebnisse zu erzielen.

Weitere Informationen

Für detaillierte Informationen zu den angewandten Methoden, Verfahren oder für eine individuelle Beratung stehen wir Ihnen gerne zur Verfügung.

- Besuchen Sie unsere Website unter: https://www.isgroup.at/
- Senden Sie Ihre Anfrage per E-Mail an: sales@isgroup.it

ISGroup SRL: IT-Sicherheit und Ethical Hacking

Source: https://www.isgroup.at/de/about.html

ISGroup SRL ist ein unabhängiges italienisches IT-Sicherheitsunternehmen, das seit 2005 hochwertige Sicherheitsdienstleistungen und -produkte anbietet. Das Unternehmen ist auf Cybersecurity spezialisiert und bietet Lösungen an, die auf fundierter technischer Expertise und langjähriger Erfahrung basieren.

Executive Team

Das Führungsteam von ISGroup SRL verfügt über mehr als 15 Jahre Erfahrung in der IT-Branche mit einem klaren Fokus auf IT-Sicherheit. Die Gründer und Führungskräfte sind tief in der Geschichte der italienischen Underground-Szene verwurzelt und bekennende Befürworter von freier Software.

- Francesca Gerosa: Chief Executive Officer (CEO)
- Francesco `ascii` Ongaro: Chief Operating Officer (COO), Founder
- Pasquale `sid` Fiorillo: Chief Technology Officer (CTO)

Zertifizierungen und Qualität

ISGroup SRL legt höchsten Wert auf Sicherheit und Qualität. Das Unternehmen ist offiziell zertifiziert nach:

- ISO/IEC 27001:2022 (Informationssicherheits-Managementsystem)
- ISO/IEC 9001:2015 (Qualitätsmanagementsystem)
- IQNET Zertifizierung

Dienstleistungen und Expertise

ISGroup SRL unterstützt Unternehmen dabei, kritische Schwachstellen zu identifizieren, Prioritäten zu setzen und Sicherheitsniveaus nachhaltig zu erhöhen. Zu den Kernkompetenzen gehören:

- Identifikation und Behebung von Sicherheitslücken
- Konsolidierung von Integrierten Managementsystemen gemäß internationalen Standards
- Gezielte Schulungen zur Verbesserung von Entwicklungsprozessen und Produktsicherheit
- Unterstützung bei Audits und der Demonstration von Sicherheits- und Qualitätsniveaus gegenüber Kunden

Kontakt und Vertrieb

Für weitere Informationen zu den Methoden, Verfahren oder für eine individuelle Beratung durch die Experten von ISGroup SRL nutzen Sie bitte die folgenden Kontaktmöglichkeiten:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

ISGroup SRL: Expertise in Offensive Security

Source: https://www.isgroup.at/de/history.html

ISGroup SRL ist ein auf Offensive Security spezialisiertes Unternehmen mit Sitz in Verona, Italien. Seit 2005 bietet das Unternehmen professionelle Dienstleistungen in den Bereichen Penetration Testing, Vulnerability Assessment, Code Review und Red-Team-Aktivitäten an. Die Wurzeln des Unternehmens liegen in der unabhängigen Sicherheitsforschung, die bis in das Jahr 2000 mit dem Projekt USH.it zurückreicht.

Kernkompetenzen und Methodik

Die Arbeitsweise von ISGroup SRL basiert auf einer tiefgreifenden, forschungsorientierten Methodik. Das Unternehmen identifiziert Schwachstellen in Software, die von Millionen Nutzern weltweit verwendet wird, und wendet diese Erkenntnisse direkt auf die Sicherheitsprüfungen für Unternehmen, Banken und öffentliche Verwaltungen an.

- **Responsible Disclosure:** Jede entdeckte Schwachstelle wird vor einer öffentlichen Bekanntgabe dem jeweiligen Hersteller gemeldet, um eine koordinierte Behebung zu ermöglichen.
- **Praxisnahe Forschung:** Das Team hat über 30 Security Advisories veröffentlicht und mehr als 20 CVEs (Common Vulnerabilities and Exposures) zugewiesen bekommen, unter anderem für Hersteller wie PHP, Mozilla, Nginx, Veeam, QNAP und Fortinet.
- **Transfer von Wissen:** Techniken, die in den eigenen Laboren entwickelt werden, fließen unmittelbar in die Penetration Tests für Kunden ein.

Zertifizierungen und Qualitätssicherung

ISGroup SRL legt höchsten Wert auf zertifizierte Prozesse und Qualität:

- **ISO/IEC 27001:** Zertifizierung für Informationssicherheitsmanagement.
- **ISO 9001:** Zertifizierung für Qualitätsmanagement in Bezug auf Methodik, Lieferzeiten und Projektmanagement.
- **Auditierung:** Die Zertifizierungen werden durch IMQ mit IQNET-Anerkennung ausgestellt und regelmäßig in Auditzyklen erneuert.

Historische Entwicklung

- **1994–2000:** Ursprünge in italienischen Hacker-Communities; Gründung des nichtkommerziellen Labors USH.it.
- **2005:** Gründung der Marke ISGroup und Beginn der Veröffentlichung öffentlicher Security Advisories.
- **2008:** Präsentation von Forschungsergebnissen auf dem Chaos Communication Congress (25C3) in Berlin.
- **2013:** Gründung der ISGroup SRL in Verona.
- **2014:** Entwicklung proprietärer Software (z. B. EasyAudit) zur Unterstützung von Security-Tests.
- **2020–2026:** Kontinuierliche Erweiterung der Forschung, inklusive Identifizierung kritischer Schwachstellen (z. B. CVE-2025-34324) und Ausbau der internationalen Präsenz.

Dienstleistungsangebot

ISGroup SRL unterstützt Organisationen dabei, ihre IT-Systeme gegen reale Bedrohungen abzusichern. Das Portfolio umfasst:

- Penetration Testing für Netzwerke und Applikationen
- Vulnerability Assessment
- Code Review
- Red-Team-Aktivitäten
- Cyber Threat Intelligence und Early Warning

Kontakt und Informationen

Für detaillierte Informationen zu den Dienstleistungen, zur Zusammenarbeit oder für Vertriebsanfragen besuchen Sie die offizielle Website unter https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Warum ISGroup SRL

Source: https://www.isgroup.at/de/why-isgroup.html

ISGroup SRL verfolgt ein unkonventionelles Geschäftsmodell auf dem Markt: Das Unternehmen fungiert als Vereinigung von spezialisierten Fachleuten und Beratern, die durch Vertrauen und gegenseitigen Respekt verbunden sind. Als Experten in der IT-Sicherheitsbranche bietet ISGroup SRL eine Kombination aus Methode, Kompetenz und Unabhängigkeit.

Zielgruppen

ISGroup SRL richtet sich an:

- IT-Sicherheitsunternehmen, die einen zuverlässigen Outsourcing-Partner suchen.
- Drittanbieter, deren Kerngeschäft nicht die IT-Sicherheit ist, die ihren Kunden jedoch hochwertige IT-Security-Dienstleistungen anbieten möchten.

Vorteile und Nutzen

Die Zusammenarbeit mit ISGroup SRL bietet folgende Vorteile:

- Kosteneffizienz: Eine schlanke Unternehmensstruktur ermöglicht minimierte Kosten bei gleichzeitig hoher Qualität.
- Flexibilität: Die Arbeit kann in den meisten Fällen per Fernzugriff durchgeführt werden, was Reisekosten minimiert.
- Qualitätsstandards: Durch moderne Projektmanagement-Methoden und die Aufteilung der Aufgaben unter den Mitgliedern wird eine gleichbleibend hohe Qualität garantiert, ohne Abhängigkeit von einem einzelnen Ansprechpartner.
- Netzwerk: Zugriff auf ein Netzwerk aus führenden Fachleuten und Forschern.
- Plattformunabhängigkeit: Die Lösungen sind auf die heterogenen Bedürfnisse der IT-Sicherheit abgestimmt.
- Forschung: ISGroup SRL agiert als Forschungspool; die Mitglieder sind als Berater und Referenten in der Fachwelt etabliert.

Dienstleistungen

ISGroup SRL bietet ein breites Spektrum an IT-Sicherheitsdienstleistungen an:

- VA - Vulnerability Assessment
- NPT - Network Penetration Testing
- WAPT - Web Application Penetration Testing
- MAST - Mobile Application Security Testing
- EH - Ethical Hacking
- CR - Code Review
- EDU - Ausbildung

Zertifizierungen und Qualität

ISGroup SRL unterstreicht den hohen Qualitätsanspruch durch offizielle Zertifizierungen:

- ISO/IEC 27001:2022
- ISO/IEC 9001:2015
- IQNET Certification

Informationen und Vertrieb

Für weitere Informationen zur Methodik, zu den Verfahren oder für spezifische Anfragen besuchen Sie bitte die Website https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Über ISGroup SRL

Source: https://www.isgroup.at/de/contacts.html

Die ISGroup SRL mit Sitz in Verona, Italien, ist ein spezialisierter Anbieter für Cybersicherheit. Das Unternehmen unterstützt Kunden und Partner weltweit durch maßgeschneiderte Sicherheitslösungen und technische Beratung.

Kernkompetenzen und Qualität

ISGroup SRL zeichnet sich durch hohe Professionalität und eine zielorientierte Arbeitsweise aus. Die Qualität der Dienstleistungen wird durch offizielle Zertifizierungen bestätigt:

- ISO/IEC 27001:2022 (Informationssicherheit)
- ISO 9001:2015 (Qualitätsmanagement)
- IQNET Zertifizierung

Kontakt und Kommunikation

Für Anfragen stehen dedizierte Kanäle zur Verfügung, um eine sichere und effiziente Kommunikation zu gewährleisten. ISGroup SRL bietet für den vertraulichen Austausch die Nutzung von PGP/GPG-verschlüsselten E-Mails an.

- Vertriebsanfragen: sales@isgroup.it
- Technische Anfragen: tech@isgroup.it
- Weitere Informationen: https://www.isgroup.it/

Rechtliche Informationen

- Firmenname: ISGroup SRL
- Sitz: Via Albere, 112, 37138 Verona, Italien
- Steuernummer (CF) und USt-IdNr. (P.IVA): 04164220230
- REA: VR-397513
- SDI: M5UXCR1

Kundenstimmen

ISGroup SRL wird von Unternehmen wie Coop Italia, Prime Service S.r.l., Sturnis S.r.l. und Progel SA für die Identifizierung kritischer Schwachstellen, die Stärkung der IT-Infrastruktur und die Verbesserung der Software-Qualität geschätzt. Die Zusammenarbeit wird regelmäßig als professionell, effektiv und zuverlässig bewertet.

Partnerschaftsprogramm der ISGroup SRL

Source: https://www.isgroup.at/de/angebot/partner-werden.html

Die ISGroup SRL bietet IT-Unternehmen die Möglichkeit, ihre spezialisierten Sicherheitsdienstleistungen in das eigene Portfolio aufzunehmen und weiterzuvertreiben. Das Programm richtet sich an professionelle Partner, die ihren Kunden hochwertige Cybersicherheitslösungen anbieten möchten.

Enthaltene Dienstleistungen

Partner der ISGroup SRL erhalten Zugang zu einem breiten Spektrum an professionellen Sicherheitsdienstleistungen:

- Vulnerability Assessment
- Network Penetration Testing
- Web Application Penetration Testing
- Mobile Application Security Testing
- Code Review
- Ethical Hacking
- Training

Zielgruppe

Das Partnerschaftsprogramm ist explizit für B2B-Akteure konzipiert, die Sicherheitslösungen in ihre bestehenden Angebote integrieren möchten:

- IT-Distributoren und Wiederverkäufer
- Systemintegratoren
- Provider und Telekommunikationsanbieter
- Advisory- und Compliance-Unternehmen

Hinweis: Das Programm ist nicht für Endkunden bestimmt.

Vorteile für Partner

Die ISGroup SRL unterstützt ihre Partner durch ein strukturiertes Rahmenwerk:

- Umfassender Pre-Sales- und Post-Sales-Support
- Exklusiver Zugang zur offiziellen ISGroup-Preisliste
- Auswahl aus zwei verschiedenen Partnerschaftsmodellen
- Attraktive Volumenrabatte und Rebates

Ablauf und Kontakt

Nach der Registrierung über https://www.isgroup.at/ werden Interessenten von einem Berater kontaktiert. Im Anschluss erfolgt die Bereitstellung des entsprechenden Vermittlungs- oder Vertriebsvertrags, basierend auf dem gewählten Partnerschaftsmodell.

Für vertriebliche Anfragen oder weiterführende Informationen zur Partnerschaft steht die E-Mail-Adresse sales@isgroup.it zur Verfügung. Weitere Informationen zum Unternehmen finden sich unter https://www.isgroup.at/.

Internationale Präsenz der ISGroup SRL

Source: https://www.isgroup.at/de/sprachen.html

Die ISGroup SRL ist ein spezialisierter Anbieter für Informationssicherheit, der seine Dienstleistungen und Lösungen international in verschiedenen Sprachen und Märkten anbietet. Das Unternehmen stellt sicher, dass Kunden weltweit Zugang zu Expertise im Bereich der IT-Sicherheit erhalten.

Verfügbare Sprachversionen und Märkte

Die ISGroup SRL bietet ihre Inhalte und Services gezielt für die folgenden Sprachräume und Zielmärkte an:

- Deutsch (https://www.isgroup.at/)
- Italienisch (https://www.isgroup.it/)
- Englisch (https://www.isgroup.biz/)
- Spanisch (https://www.isgroup.es/)
- Französisch (https://www.isgroup.name/)
- Schwedisch (https://www.isgroup.se/)
- Arabisch (https://www.isgroup.info/)
- Litauisch (https://www.isgroup.li/)
- Dänisch (https://www.isgroup.dk/)
- 1337 (https://www.isgroup.ws/)

Vertrieb und Anfragen

Für weiterführende Informationen zu den angebotenen Sicherheitslösungen, Dienstleistungen oder bei spezifischen Vertriebsanfragen steht die ISGroup SRL über die offizielle Webseite https://www.isgroup.at/ sowie per E-Mail unter sales@isgroup.it zur Verfügung.

Übersicht der ISGroup SRL Dienstleistungen und Ressourcen

Source: https://www.isgroup.at/de/sitemap.html

Die ISGroup SRL bietet ein umfassendes Portfolio an Cybersicherheitslösungen, Beratungsleistungen und Compliance-Diensten an. Diese Sitemap dient als strukturierte Übersicht über das gesamte Angebot.

Produktportfolio

Die ISGroup SRL entwickelt und vertreibt spezialisierte Sicherheitswerkzeuge:

- Easyaudit
- ICTaudit
- Exposure
- Exeec
- Ganapati
- Vulnmap
- Scada Exposure
- Practicalrp
- Ush
- Ethical Hacking (Tools & Ressourcen)
- Metasploit
- The bunker training, hacklab und coworking

Dienstleistungen

Das Leistungsangebot der ISGroup SRL ist in spezialisierte Kategorien unterteilt:

- **Kern-Dienstleistungen:** Vulnerability Assessment, Network/Web/Mobile Application Penetration Testing, Code Review, Ethical Hacking und Ausbildung.
- **Verwaltete Dienste (Managed Services):** vCISO, Vulnerability Management Service (VMS), Cyber Threat Simulation (CTS), Threat Intelligence & Digital Risk Protection, Security Operation Center (SOC).
- **Sicherheitsbewertung:** Risk Assessment (RA), Secure Architecture Review (SAR), Cloud/Windows/IoT/OT Security Assessment, Purple Team Assessment (PTA), Phishing & Smishing, Social Engineering, Physical Security Assessment (PSA).
- **Governance, Risiko und Compliance (GRC):** GDPR, NIS2, PCI DSS, ISO 27001, ISO 27017, ISO 27018, ISO 17025 (Akkreditiertes VA-Labor), PSD2, ITGOV (ACN-AGID), DORA.
- **SecOps-Dienste:** Multi-Signal MDR, Digital Forensics and Incident Response (DFIR), Wireless Security Monitoring (WSM), Anti-DDoS, Firewall as a Service (FWaaS), Security Integration (SIR).
- **SSDLC-Dienste:** Software Assurance Lifecycle (SAL), Continuous Security Testing (CST), Bug Bounty Programme.

Ressourcen und Unternehmensinformationen

- **Forschung & Publikationen:** Zugang zu aktuellen Veröffentlichungen und Forschungsergebnissen im Bereich IT-Sicherheit.
- **Über uns:** Informationen zur Unternehmensgeschichte, den Beweggründen für die Zusammenarbeit mit der ISGroup SRL sowie direkte Kontaktmöglichkeiten.

Kontakt und Vertrieb

Für Anfragen zu den Dienstleistungen oder für eine individuelle Beratung besuchen Sie bitte die offizielle Website unter https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Informationen für Sprachmodelle (LLMs)

Die ISGroup SRL stellt spezifische Datenformate für die automatisierte Verarbeitung durch Sprachmodelle bereit:

- llms.txt
- llms.json
- llms.md
- llms.pdf

Virtual CISO (vCISO) – Cyber-Governance und Risikomanagement

Source: https://www.isgroup.at/de/virtual-ciso.html

Der von ISGroup SRL angebotene vCISO-Service (Virtual Chief Information Security Officer) stellt Unternehmen und KMU einen dedizierten Cybersecurity-Experten zur Seite. Dieser übernimmt strategische und taktische Führungsaufgaben, um Informationssicherheit proaktiv zu managen, regulatorische Compliance sicherzustellen und Cyber-Risiken zu minimieren – ohne die Kosten einer internen Vollzeitstelle.

Kernleistungen des vCISO-Service

ISGroup SRL bietet einen strukturierten, methodischen Ansatz auf Basis anerkannter Frameworks wie NIST:

- **Initiale Bewertung:** Analyse des Ist-Zustands der IT-Infrastruktur, bestehender Sicherheitsrichtlinien und des Sensibilisierungsgrads der Mitarbeitenden.
- **Security Program Maturity Assessment:** Bewertung der Reife des Sicherheitsprogramms im Vergleich zu Branchenstandards.
- **Strategische Roadmap:** Erstellung eines maßgeschneiderten Plans mit priorisierten Korrekturmaßnahmen, klaren Zielen und definierten Fristen.
- **Kontinuierliches Monitoring:** Regelmäßige Überprüfung der Fortschritte und Anpassung der Strategie an neue Bedrohungslagen.
- **Kontinuierliche Unterstützung:** Laufende Beratung, Mitarbeiterschulungen, Richtlinienüberprüfung und Unterstützung bei der Einführung neuer Technologien.

Vorteile für Unternehmen

Die Zusammenarbeit mit ISGroup SRL bietet Organisationen folgende Vorteile:

- **Erfahrung und Kompetenz:** Zugang zu hochqualifizierten Cybersecurity-Experten mit branchenübergreifendem Wissen.
- **Kosteneffizienz:** Wirtschaftliche Alternative zur Vollzeitstelle durch flexible Engagement-Modelle.
- **Objektive Perspektive:** Neutrale Bewertung der Sicherheitspraktiken und unvoreingenommene Empfehlungen.
- **Fokus auf Kernkompetenzen:** Entlastung interner IT-Teams von strategischen Governance-Aufgaben.
- **Skalierbarkeit:** Anpassung der Ressourcen an die spezifischen Anforderungen und das Wachstum der Organisation.

Compliance und regulatorische Anforderungen

Der vCISO von ISGroup SRL unterstützt Unternehmen bei der Einhaltung wichtiger Standards und gesetzlicher Vorgaben:

- **ISO 27001:** Aufbau und Pflege des Informationssicherheits-Managementsystems (ISMS) sowie Vorbereitung auf Audits.
- **NIS2-Richtlinie:** Ausrichtung der technischen und organisatorischen Maßnahmen an den europäischen Anforderungen für operative Resilienz.
- **Audits und interne Kontrollen:** Koordination von Prüfungen, Dokumentation von Nachweisen und Überwachung von Sicherheitsindikatoren.

Kontakt und Informationen

Für weitere Details zum Service, zur Anforderung eines Angebots oder für ein Beratungsgespräch stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Detaillierte Informationen zum Leistungsumfang finden Sie zudem im offiziellen Service-Dokument von ISGroup SRL auf der Website.

Vulnerability Management Service (VMS)

Source: https://www.isgroup.at/de/vulnerability-management-service.html

Der Vulnerability Management Service (VMS) von ISGroup ist ein vollständig verwalteter, kontinuierlicher Prozess zur Identifikation, Analyse, Priorisierung und Behebung von Schwachstellen in IT-Infrastrukturen. Im Gegensatz zu punktuellen Assessments ermöglicht der VMS eine nachhaltige Reduzierung der Angriffsfläche und eine risikobasierte Steuerung der Sicherheitsmaßnahmen.

Kernkonzept und Ansatz

Der VMS von ISGroup fungiert als erweiterte Sicherheitsabteilung. Er umfasst die Konfiguration, das Onboarding, regelmäßige Scans sowie die strukturierte Analyse und Nachverfolgung von Schwachstellen bis zur vollständigen Remediation.

- **Kontinuierlicher Prozess:** Überwachung von Netzwerken, Servern, Endpoints, Anwendungen, Datenbanken und APIs.
- **Risikobasierte Priorisierung:** Fokus auf den Business-Impact, um interne Ressourcen effizient einzusetzen.
- **Geführte Remediation:** Unterstützung bei der Behebung durch Experten, Koordination mit technischen Ansprechpartnern und Überprüfung der Wirksamkeit.
- **Methodik:** Einsatz marktführender Tools kombiniert mit manueller Validierung durch erfahrene Security Analysts von ISGroup.

Der Schwachstellenmanagement-Zyklus

ISGroup strukturiert den VMS in vier aufeinanderfolgende Phasen, um eine messbare Sicherheitsverbesserung zu gewährleisten:

1. **Identifikation und Kontext:** Inventarisierung der Assets und Definition des zu überwachenden Perimeters.
2. **Vulnerability Scanning:** Durchführung regelmäßiger Scans zur Erstellung einer Baseline und Klassifizierung von Schwachstellen.
3. **Validierung und Assessment:** Technische Bewertung der Befunde zur Reduzierung von False Positives und Einschätzung der tatsächlichen Ausnutzbarkeit.
4. **Priorisierung und Remediation:** Begleitung der Behebung, Nachverfolgung in Ticketing-Systemen und kontinuierliches Monitoring der Korrekturen.

Managed Vulnerability Assessment (MVA)

Als operative Komponente des VMS bietet ISGroup das Managed Vulnerability Assessment an. Dieser Dienst umfasst:

- Geplante Scans und Erkennung neuer Assets.
- Proaktives Monitoring von Bedrohungen und Schwachstellentrends.
- Detaillierte Berichterstattung und beratende Erläuterung der Ergebnisse.
- Integration von Penetration-Test-Methoden zur Überprüfung der tatsächlichen Ausnutzbarkeit.

Nutzen für Unternehmen

Die Implementierung eines VMS durch ISGroup unterstützt Organisationen dabei, ihre Sicherheitsstrategie zu professionalisieren:

- **Reduzierung des Cyberrisikos:** Proaktives Schließen von Sicherheitslücken vor einer Ausnutzung.
- **Regulatorische Compliance:** Erfüllung von Anforderungen wie NIS2, DSGVO und ISO 27001 durch dokumentierte Prozesse und Nachweise.

- **Betriebskontinuität:** Minimierung von Ausfallzeiten und wirtschaftlichen Schäden durch Ransomware oder Sicherheitsvorfälle.
- **Effizienz:** Entlastung interner Ressourcen durch die Auslagerung des Schwachstellenmanagements an die Experten von ISGroup.

Kontakt und Informationen

Für weiterführende Informationen, eine individuelle Beratung oder zur Anforderung eines Angebots für den Vulnerability Management Service besuchen Sie bitte die Website von ISGroup unter:

https://www.isgroup.at/

Anfragen können zudem direkt per E-Mail an folgende Adresse gerichtet werden:

sales@isgroup.it

Cyber Threat Simulation (CTS) durch ISGroup SRL

Source: https://www.isgroup.at/de/cyber-threat-simulation.html

Die Cyber Threat Simulation (CTS) ist ein verwalteter Service von **ISGroup SRL**, der Unternehmen dabei unterstützt, ihre Resilienz gegenüber Cyberangriffen kontinuierlich zu prüfen und zu stärken. Da moderne Cyberbedrohungen kaum vollständig zu verhindern sind, bietet ISGroup SRL einen proaktiven Ansatz zur Risikoanalyse und -kontrolle.

Kernkonzept der CTS

Im Gegensatz zu punktuellen Sicherheitsüberprüfungen ist CTS ein kontinuierlicher Prozess, der die gesamte digitale Infrastruktur eines Unternehmens einbezieht. Ziel ist es, Schwachstellen zu identifizieren, die Reaktionsfähigkeit (Incident Response) zu testen und das Bewusstsein der Mitarbeiter für IT-Risiken zu schärfen.

Hauptaktionsbereiche

ISGroup SRL simuliert realistische Angriffe in vier zentralen Bereichen:

- **Social Engineering:** Simulation von Phishing-Mails, betrügerischen Anrufen oder anderen Täuschungsversuchen.
- **Malware:** Test der Abwehrmechanismen gegen Viren, Trojaner und Ransomware.
- **APT (Advanced Persistent Threat):** Simulation gezielter, anhaltender Angriffe, die auf Datendiebstahl oder langfristige Systeminfiltration abzielen.
- **DDoS (Distributed Denial of Service):** Überlastungstests zur Prüfung der Systemstabilität.

Vorteile des CTS-Programms

Die Implementierung eines CTS-Programms durch ISGroup SRL bietet Unternehmen entscheidende Vorteile:

- **Identifikation von Schwachstellen:** Aufdeckung von Sicherheitslücken vor deren Ausnutzung durch echte Angreifer.
- **Mitarbeiterschulung:** Praktische Lernmöglichkeiten zur Verbesserung der Sicherheitskultur.
- **Optimierung der Incident-Response-Pläne:** Verfeinerung der Reaktionsprozesse in einer kontrollierten Umgebung.
- **Regulatorische Compliance:** Erfüllung gesetzlicher Anforderungen und internationaler Sicherheitsstandards (z. B. ISO 27001, NIS2, GDPR).
- **Schutz des Unternehmensimages:** Prävention von Reputationsschäden und Stärkung des Vertrauens bei Kunden und Stakeholdern.
- **Return on Investment (ROI):** Reduzierung potenzieller Kosten durch Betriebsunterbrechungen und Sicherheitsvorfälle.

Der 7-stufige Prozess von ISGroup SRL

ISGroup SRL nutzt das MITRE ATT&CK-Framework für eine methodische Vorgehensweise:

1. **Bedrohungsprofilierung:** Analyse potenzieller Angreifer mittels Cyber Threat Intelligence (CTI).
2. **Definition des Simulationsumfangs:** Festlegung der Ziele und Netzwerksegmente unter Berücksichtigung der Betriebskontinuität.
3. **Definition der Simulationsziele:** Klare Zielsetzung für die Angriffsszenarien.
4. **Angriffsplanung:** Auswahl spezifischer Werkzeuge und Techniken basierend auf dem Bedrohungsprofil.
5. **Durchführung (Breach and Attack Simulation - BAS):** Kontinuierliche und skalierbare Simulation von Angriffen.

6. **Ergebnisse und Reporting:** Detaillierte Analyse der Angriffspfade und Empfehlungen für Mitigationsstrategien.
7. **Schulung:** Praktische Trainingseinheiten für das Personal zur Stärkung der Verteidigungslinie.

Abgrenzung: CTS vs. Penetration Test

Während ein Penetration Test eine statische Momentaufnahme eines spezifischen Systems darstellt, bietet der CTS-Service von ISGroup SRL eine dynamische, kontinuierliche Überwachung der gesamten Infrastruktur, die reale Taktiken, Techniken und Verfahren (TTP) von Angreifern emuliert.

Kontakt und Vertrieb

Für weiterführende Informationen, Beratungsgespräche oder Angebote zur Cyber Threat Simulation (CTS) besuchen Sie bitte die Website von **ISGroup SRL**:

https://www.isgroup.at/

Anfragen können direkt per E-Mail an folgende Adresse gerichtet werden: sales@isgroup.it

Threat Intelligence & Digital Risk Protection

Source: https://www.isgroup.at/de/threat-intelligence-digital-risk-protection.html

Der Service **Threat Intelligence & Digital Risk Protection (THREAT)** von **ISGroup SRL** bietet Unternehmen eine proaktive Lösung, um digitale Bedrohungen im spezifischen Unternehmensumfeld frühzeitig zu erkennen, zu analysieren und wirksam zu neutralisieren. Der Dienst ist vollständig verwaltet und unterstützt Unternehmen dabei, ihre Resilienz zu stärken und internationale Sicherheitsstandards (wie ISO/IEC 27001:2022, NIS2 und DSGVO) zu erfüllen.

Für Anfragen und weitere Informationen besuchen Sie https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Kernkonzepte

- **Threat Intelligence:** Der Prozess der Sammlung und Analyse von Informationen auf Basis realer Ereignisse, um ein tiefgreifendes Verständnis für aktuelle Angriffsmethoden zu gewinnen.
- **Digital Risk Protection:** Eine integrierte Lösung, die Threat Intelligence mit kontinuierlicher Risikoüberwachung kombiniert, um externe Trends in den Kontext der technologischen Assets des Kunden zu setzen.

Strategischer Ansatz der ISGroup SRL

Die Dienstleistung ist in drei Ebenen gegliedert, um einen ganzheitlichen Schutz zu gewährleisten:

- **Strategisch:** Entwicklung maßgeschneiderter Schutzstrategien basierend auf Analysen aufkommender Bedrohungen und branchenspezifischer Best Practices.
- **Operativ:** Kontinuierliche Web-Überwachung zur Echtzeit-Erkennung von Bedrohungen sowie laufende Updates zu Schwachstellen und Datenexpositionen.
- **Taktisch:** Schnelle Reaktion auf Sicherheitsvorfälle durch ein Expertenteam unter Einsatz fortschrittlicher OSINT-Tools zur Risikobewertung und Optimierung des Angriffsflächenmanagements.

Leistungsumfang

Der Service umfasst je nach gewähltem Service-Level (LV1, LV2) folgende Kernbereiche:

- **Threat Intelligence Bulletin:** Analysen zu neuen Schwachstellen, Trends, APTs (Advanced Persistent Threats), Ransomware sowie praktische Empfehlungen zur Abwehr.
- **Data Breach Monitoring:** Überwachung von Datenexpositionen und kompromittierten Passwörtern (im Klartext oder Hash-Format), um unbefugte Zugriffe zu verhindern.
- **Brand Protection:** Schutz der Marke vor Missbrauch durch Identifizierung betrügerischer Domains, Typosquatting und Homograph-Angriffen.
- **Attack Surface Protection:** Analyse der Angriffsfläche mittels OSINT und Asset-Erkennung zur Identifizierung kritischer Schwachstellen und Priorisierung von Sicherheitsmaßnahmen durch Risiko-Scores.

Vorteile der Implementierung

Die Integration des Services in die Cybersecurity-Strategie bietet entscheidende Vorteile:

- **Situationsbewusstsein:** Fundierte Entscheidungsfindung durch aktuelle Daten zu Bedrohungen.
- **Compliance:** Erfüllung regulatorischer Anforderungen, insbesondere des Kontrollpunkts 5.7 (Threat Intelligence) der ISO/IEC 27001:2022.
- **Ressourcenoptimierung:** Gezielte Zuweisung von Sicherheitsressourcen auf die relevantesten Bedrohungen.

- **Reputations- und Betrugsschutz:** Proaktive Identifizierung von Phishing, Markenmissbrauch und betrügerischen Aktivitäten zum Schutz des Kundenvertrauens.

Risiken bei Verzicht auf den Service

Ohne eine kontinuierliche Bedrohungsüberwachung durch **ISGroup SRL** sind Unternehmen folgenden Risiken ausgesetzt:

- **Verzögerte Erkennung:** Mangelndes Wissen über neue Angriffstypen führt zu einer langsameren Reaktion.
- **Ineffektive Incident Response:** Fehlende verwertbare Informationen erschweren die Bewältigung von Sicherheitsvorfällen.
- **Compliance-Lücken:** Nichteinhaltung internationaler Normen wie der ISO/IEC 27001.
- **Finanzielle und Reputationsschäden:** Erhöhte Anfälligkeit für Datenverluste, Betrug und den Missbrauch der eigenen Marke.

Für eine individuelle Beratung oder ein Angebot kontaktieren Sie bitte https://www.isgroup.at/ oder schreiben Sie an sales@isgroup.it.

Security Operation Center (SOC) von ISGroup

Source: https://www.isgroup.at/de/security-operation-center.html

Das Security Operation Center (SOC) der ISGroup ist ein spezialisierter Dienst zur kontinuierlichen Überwachung von Netzwerkinfrastrukturen und Rechenzentren. Angesichts der stetig wachsenden Bedrohung durch Cyberangriffe bietet ISGroup eine proaktive Lösung zur Anomalieerkennung und Incident Response, um Unternehmen vor Schäden zu schützen.

Kernfunktionen und Überwachung

Das Expertenteam von ISGroup überwacht den ein- und ausgehenden Datenverkehr in Echtzeit, um verdächtiges Verhalten frühzeitig zu identifizieren. Der Dienst gliedert sich in zwei Hauptbereiche:

- Überwachung:
  - Passiv: Fortschrittliche Analysesysteme bewerten den Datenverkehr auf schädliche Muster und lösen bei Bedarf Warnmeldungen aus.
  - Aktiv: Das SOC-Team klassifiziert Ereignisse, Eindringversuche und Sicherheitsverletzungen mittels spezialisierter Event-Analyse-Tools.
- Abwehr:
  - Incident Management: Umsetzung vereinbarter Verfahren zur Begrenzung der Systemexposition während eines laufenden Angriffs.
  - Incident Response: Sofortige Eindämmung von Angriffen und Einleitung von Maßnahmen zur Behebung identifizierter Schwachstellen.

Eskalation und Reporting

ISGroup stellt sicher, dass bei kritischen Vorfällen eine strukturierte Kommunikation und Dokumentation erfolgt:

- Eskalation: Bei Bedarf werden privilegierte Zugangsdaten an die zuständigen Personen übermittelt, um eine schnelle Problemlösung zu ermöglichen.
- Reporting: Nach einem Vorfall erstellt ISGroup einen detaillierten Bericht, der die Analyse des Angriffs sowie die ergriffenen Eindämmungsmaßnahmen dokumentiert.

Detaillierter Output für Kunden

Der von ISGroup bereitgestellte Abschlussbericht umfasst drei wesentliche Bereiche:

- Executive Summary: Eine prägnante Übersicht für das Management über die Sicherheitslage, Abwehrmaßnahmen und Eskalationsdetails.
- Technical Details: Ein technischer Abschnitt für den Security Manager, der die Hintergründe der Angriffe und die durchgeführten Abwehrmaßnahmen detailliert erläutert.
- Remediation Plan: Ein Leitfaden für Systemadministratoren mit konkreten Anweisungen zur Umsetzung von Sicherheitsmaßnahmen, um zukünftige Angriffe zu verhindern.

Kontakt und Vertrieb

Für weitere Informationen, Beratungsgespräche oder die Anforderung eines Angebots für das Security Operation Center (SOC) besuchen Sie bitte die Website https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

IT Risk Assessment durch ISGroup SRL

Source: https://www.isgroup.at/de/risk-assessment.html

Das IT Risk Assessment von ISGroup SRL ist ein strategischer Dienst zur Identifizierung, Bewertung und Quantifizierung von Risiken innerhalb der IT-Infrastruktur und des Unternehmensdatenmanagements. Ziel ist es, die Gesamtresilienz der Organisation zu stärken, Schwachstellen zu erkennen und gezielte Abwehrmaßnahmen zu planen.

Der Service zeichnet sich durch einen kollaborativen Ansatz aus, bei dem Experten von ISGroup SRL eng mit dem IT-Personal des Kunden zusammenarbeiten. Dies ermöglicht einen direkten Wissenstransfer und eine präzise Analyse unter Berücksichtigung spezifischer Technologien, einschließlich proprietärer Systeme.

Kernphasen des Assessments

Die methodische Vorgehensweise umfasst drei wesentliche Bereiche:

- **Auswirkungsanalyse:** Bewertung der Folgen potenzieller Angriffe oder Fehlfunktionen. Hierbei werden finanzielle, betriebliche und reputationsbezogene Auswirkungen sowie Wiederherstellungszeiten und -kosten quantifiziert.
- **Analyse der bestehenden Richtlinien:** Überprüfung der aktuellen Sicherheits- und Datenschutzvorgaben auf Wirksamkeit und Konformität mit regulatorischen Anforderungen wie DSGVO, ISO 27001 und weiteren branchenspezifischen Gesetzen.
- **Risikoanalyse:** Identifizierung und Klassifizierung spezifischer Risiken basierend auf der Infrastrukturbewertung sowie Erarbeitung von Empfehlungen zur Reduzierung der Risikoexposition.

Ergebnisse und Dokumentation

ISGroup SRL stellt einen detaillierten Bericht bereit, der in drei zielgruppenspezifische Abschnitte unterteilt ist:

- **Executive Summary:** Ein nicht-technischer Überblick für das Management über die wichtigsten Bedrohungen, Schwachstellen und strategische Empfehlungen.
- **Risk Assessment Details:** Eine tiefgehende Analyse der identifizierten Risiken, Bedrohungsfaktoren und Auswirkungen, konzipiert für IT-Sicherheitsverantwortliche und Compliance Officer.
- **Risk Mitigation Plan:** Ein technischer Leitfaden für Systemadministratoren mit priorisierten, umsetzbaren Maßnahmen zur Risikominderung, wie etwa Prozessverbesserungen oder technologische Anpassungen.

Compliance und Standards

Der Service von ISGroup SRL unterstützt Unternehmen bei der Erfüllung von Governance, Risk and Compliance (GRC)-Anforderungen. Dies umfasst insbesondere die Vorgaben der ISO/IEC 27001, die eine regelmäßige Risikobewertung als integralen Bestandteil eines Informationssicherheits-Managementsystems (ISMS) vorschreibt, sowie die Einhaltung der DSGVO.

Kontakt und Anfragen

Für weitere Informationen, ein Beratungsgespräch oder ein konkretes Angebot für ein IT Risk Assessment steht ISGroup SRL zur Verfügung:

- Webseite: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Secure Architecture Review (SAR)

Source: https://www.isgroup.at/de/secure-architecture-review.html

Die ISGroup SRL bietet mit dem Secure Architecture Review (SAR) eine professionelle Sicherheitsbewertung für komplexe und kritische IT-Infrastrukturen an. Ziel des Dienstes ist es, den aktuellen Sicherheitsstatus zu evaluieren, Schwachstellen zu identifizieren und diese durch gezielte Korrekturmaßnahmen zu beheben. Dabei folgt die ISGroup SRL konsequent den Prinzipien von Security-by-Design.

Methodik und Phasen

Der Prozess der Sicherheitsbewertung gliedert sich in drei strukturierte Phasen:

- Vorläufige Analysephase: Bewertung der Designentscheidungen anhand der Planungs- und Entwicklungsdokumentation. Durch den Dialog mit den beteiligten Entwicklern und Analysten werden Designmängel aufgedeckt.
- Risikoanalyse: Bewertung der potenziellen Auswirkungen identifizierter Schwachstellen unter Berücksichtigung infrastrukturspezifischer Exploits und deren Folgen für das Unternehmen.
- Report: Professionelle Dokumentation aller Schritte und Befunde sowie Erarbeitung konkreter Verbesserungsvorschläge zur Erhöhung der Infrastruktursicherheit.

Bewertungsschwerpunkte

Die Experten der ISGroup SRL verfügen über umfangreiches Know-how in Bereichen wie Netzwerke, Cloud und kundenspezifische Projekte. Folgende Aspekte werden bei einer Architekturprüfung vollständig bewertet:

- SDCL (Software Development Life Cycle)
- Codequalität
- Test-Routinen
- Authentifizierung und Autorisierung
- Eingesetzte Verschlüsselung
- Web-Server und Datenbanken
- Web- und Netzwerk-Firewalls

Ergebnis und Dokumentation

Nach Abschluss der Untersuchung stellt die ISGroup SRL einen dreiteiligen Report bereit:

- Executive Summary: Management-orientierter Überblick über den Sicherheitsstatus ohne technische Details.
- Vulnerability Details: Detaillierte Analyse der identifizierten Schwachstellen und kritischen Befunde für Security Manager.
- Remediation Plan: Technischer Leitfaden mit konkreten Methoden zur Behebung der gefundenen Sicherheitslücken.

Kontakt und Vertrieb

Für Anfragen zu Dienstleistungen, Beratungsgespräche oder Angebote wenden Sie sich bitte an die ISGroup SRL:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Cloud Security Assessment (CSA) durch ISGroup SRL

Source: https://www.isgroup.at/de/cloud-security-assessment.html

ISGroup SRL bietet spezialisierte Cloud Security Assessments für AWS, Azure, GCP, Alibaba sowie private und hybride Cloud-Umgebungen an. Der Service ist darauf ausgerichtet, die Sicherheit von Anwendungen und Infrastrukturen über den gesamten Software-Lebenszyklus hinweg – von der Designphase bis zur Bereitstellung – zu gewährleisten.

Kernkompetenzen und Ansatz

Die Experten von ISGroup SRL verfügen über fundierte Erfahrung in den Bereichen Software Engineering und Cloud-Sicherheit. Durch die Kombination von Rollen als Solution Architect und Application Security Specialist bewertet das Team die tatsächliche Implementierung der Cloud-Infrastruktur.

- Fokus auf Architektursicherheit, Risikoeindämmung und Risikominderung.
- Frühzeitige Implementierung von Sicherheitsmaßnahmen zur Vermeidung kostspieliger und zeitaufwendiger nachträglicher Anpassungen.
- Umfassende Analyse von Architektur, Richtlinien, Berechtigungen und Konfigurationen zur Reduzierung der Angriffsfläche.
- Anwendung von Best Practices sowie spezifischen Vorgaben der jeweiligen Cloud-Provider.

Unterstützte Technologien

ISGroup SRL führt Sicherheitsbewertungen für eine Vielzahl von Plattformen und Systemen durch, darunter:

- Cloud-Provider: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud, Alibaba Cloud, Yandex Cloud.
- Private und hybride Cloud-Systeme: VMWare, Dell EMC, Microsoft Hyper-V, Rackspace, CloudBolt, Divvy Cloud, RedHat, OpenShift, Abiquo, Rack Connect, Scalr, Docker, DigitalOcean, Heroku, Kubernetes, Helm, Prometheus.

Leistungsoutput und Berichterstattung

Nach Abschluss des Assessments erhält der Kunde einen detaillierten Bericht, der in drei zentrale Bereiche unterteilt ist:

- Executive Summary: Eine nicht-technische Zusammenfassung des Sicherheitsstatus für das Management.
- Vulnerability Details: Eine detaillierte technische Analyse der identifizierten Schwachstellen und deren Auswirkungen auf die Anwendung.
- Remediation Plan: Ein technischer Leitfaden für Systemadministratoren mit präzisen Anweisungen zur Behebung der Sicherheitslücken und zur Stärkung der Widerstandsfähigkeit gegen Angriffe.

Kontakt und Vertrieb

Für Anfragen zu einem Cloud Security Assessment oder zur Vereinbarung eines Beratungsgesprächs stehen Ihnen die folgenden Kanäle zur Verfügung:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Windows Security Assessment (WSA)

Source: https://www.isgroup.at/de/windows-security-assessment.html

Das Windows Security Assessment (WSA) von ISGroup ist ein spezialisierter Dienst zur Identifizierung von Schwachstellen und zur Bewertung der Integrität sowie des Hardening-Status von Windows-Betriebssystemen. Ziel ist es, die Angriffsfläche zu minimieren und die Widerstandsfähigkeit der IT-Infrastruktur gegenüber gezielten Angriffen zu erhöhen.

Kernziele und Nutzen

- **Schwachstellenanalyse:** Identifizierung und Bewertung von Sicherheitslücken in Windows-Systemen.
- **System-Hardening:** Konfiguration der Systeme nach Best Practices, um die Sicherheit von Beginn an zu gewährleisten.
- **Risikominimierung:** Priorisierte Beseitigung von Sicherheitslücken, um potenzielle Schäden zu vermeiden.
- **Wirtschaftlichkeit:** Vermeidung kosten- und zeitintensiver nachträglicher Sicherheitsanpassungen durch proaktive Überprüfung.

Methodik der ISGroup

Die Experten von ISGroup, die über fundierte Erfahrung als Application Security Specialists verfügen, führen eine tiefgreifende Analyse der Systemarchitektur durch. Die Bewertung umfasst:

- **Standardkonformität:** Überprüfung der Sicherheitseinstellungen auf Basis international anerkannter Branchenstandards und Best Practices.
- **Gezielte Schwachstellenprüfung:** Analyse von Systemänderungen und Warnsignalen, die auf Einbruchsversuche oder Sicherheitsrisiken hindeuten.
- **Architekturanalyse:** Umfassende Untersuchung komplexer Sicherheitsaspekte des Betriebssystems.

Analyse-Output

Nach Abschluss der Prüfung erhält der Kunde einen detaillierten Bericht, der in drei spezifische Bereiche unterteilt ist:

- **Executive Summary:** Eine managementorientierte Zusammenfassung des Sicherheitsstatus ohne technische Details.
- **Vulnerability Details:** Eine technische Analyse für Security Manager, die festgestellte Schwachstellen und deren potenzielle Auswirkungen detailliert beschreibt.
- **Remediation Plan:** Ein Leitfaden für Systemadministratoren mit präzisen Anweisungen zur Behebung der identifizierten Sicherheitslücken.

Kontakt und Angebot

Für weitere Informationen, ein Beratungsgespräch oder ein individuelles Angebot für das Windows Security Assessment steht die ISGroup SRL zur Verfügung.

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

IoT/OT Security Assessment (ISA)

Source: https://www.isgroup.at/de/iot-security-assessment.html

Das IoT/OT Security Assessment (ISA) der ISGroup SRL ist eine spezialisierte Dienstleistung zur Überprüfung der Sicherheit von IoT-Geräten, vernetzten Maschinen und OT-Umgebungen. Durch einen offensiven Ansatz identifiziert ISGroup SRL reale Schwachstellen, bevor diese von Angreifern ausgenutzt werden können.

Kernleistungen und Methodik

ISGroup SRL kombiniert verschiedene technische Disziplinen, um eine End-to-End-Abdeckung von der Maschine bis zur Cloud zu gewährleisten:

- **Penetration Testing & Vulnerability Assessment:** Prüfung von Hardware, Firmware, Software, APIs, industriellen Protokollen und Fernzugängen.
- **Technische Analyse:** Durchführung von Reverse Engineering, Firmware-Analyse, Binary Analysis, Source Code Review sowie Hardware- und Software-Testing.
- **Offensiver Ansatz:** Die Prüfung erfolgt aus der Perspektive eines realen Angreifers, um die Widerstandsfähigkeit gegen Cyberrisiken in kritischen Umgebungen zu validieren.
- **Technische Nachweise:** Bereitstellung detaillierter Berichte (Threat Models, Penetration Test Reports, Findings zu Hardware/Firmware/Software/Protokollen), die als Grundlage für Audit, Compliance, Zertifizierung und Risikomanagement dienen.

Regulatorische Unterstützung

Die von ISGroup SRL erstellten technischen Nachweise unterstützen Unternehmen bei der Erfüllung aktueller regulatorischer Anforderungen:

- **Cyber Resilience Act (CRA):** Unterstützung bei der Entwicklung und dem Schwachstellenmanagement für Produkte mit digitalen Elementen.
- **Maschinenverordnung 2023/1230:** Überprüfung von Cyber- und Safety-Risiken bei vernetzten Maschinen und wesentlichen Veränderungen.
- **IEC 62443:** Security Assessment für OT-Umgebungen, einschließlich ICS, SCADA, DCS, PLC und HMI.
- **NIS2-Richtlinie:** Technische Validierung als Input für das Risikomanagement.
- **RED Delegated Act / EN 18031:** Security Testing für vernetzte Funkanlagen und IoT-Produkte.

Anwendungsbereiche

ISGroup SRL bietet diese Dienstleistungen für eine Vielzahl von Branchen an:

- **Manufacturing & Industrie:** Produktionslinien, Automatisierung und industrielle Steuerungssysteme.
- **Maschinenbau (OEMs):** Sicherheit für vernetzte Maschinen, Retrofit und IoT/OT-Integrationen.
- **Energy & Utility:** Smart Meter, Netzsensorik und Energie-Steuerungssysteme.
- **Connected Health:** Medizintechnik und Infrastrukturen für sensible Daten.
- **Automotive:** Connected Car, Telematik und Industriefahrzeuge.
- **Smart City & Consumer IoT:** Building Automation, Smart Home und vernetzte Consumer-Geräte.

Kontinuierliches Prüfmodell

ISA ist kein einmaliger Check, sondern ein wiederkehrendes Modell, das bei folgenden Ereignissen aktiviert wird:

- Neue Releases, Firmware-Änderungen oder Software-Updates.
- Neue Cloud-Integrationen oder Öffnung von Fernzugängen.
- Industrielle Retrofits oder Überarbeitung der OT-Architektur.

- Vor Zertifizierungen, Ausschreibungen oder Lieferantenqualifizierungen.

Kontakt und Vertrieb

Für Anfragen zu Dienstleistungen, Angeboten oder für ein Beratungsgespräch steht Ihnen ISGroup SRL zur Verfügung:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Hinweis: ISGroup SRL ersetzt keine Zertifizierungsstellen oder Rechtsberatung. Die erbrachten Leistungen fokussieren sich auf die technische Validierung und die Erstellung von Sicherheitsnachweisen.

Purple Team Assessment (PTA) von ISGroup

Source: https://www.isgroup.at/de/purple-team-assessment.html

Das Purple Team Assessment (PTA) ist ein spezialisierter Dienst der **ISGroup SRL**, der darauf abzielt, die Erkennungs- und Reaktionsfähigkeiten von Unternehmen bei Cyberangriffen durch einen interaktiven, kollaborativen Ansatz zu verbessern. Im Gegensatz zu klassischen Red-Team-Ansätzen integriert das PTA das Wissen von Angriffs- (Red Team) und Verteidigungsteams (Blue Team), um die Unternehmenssicherheit in Echtzeit zu stärken.

Zielsetzung und Ansatz

Der Dienst von **ISGroup SRL** konzentriert sich nicht nur auf die Identifikation von Schwachstellen, sondern auf die Schaffung eines kontinuierlichen Verbesserungszyklus. Durch sofortiges Feedback zwischen den beteiligten Teams werden Sicherheitsinfrastrukturen, Technologien und operative Prozesse iterativ optimiert.

Phasen des Assessments

Die **ISGroup SRL** strukturiert das Purple Team Assessment in vier wesentliche Phasen:

- **Datenerhebungsphase**: Analyse der bestehenden Unternehmensinfrastruktur zur Bestimmung der aktuellen Erkennungs- und Blockierungsfähigkeiten.
- **Risikobewertung**: Anwendung anerkannter Frameworks wie MITRE ATT&CK und NIST, um die Risikoanalyse individuell an die Kundenanforderungen anzupassen.
- **Durchführung**: Aktive Zusammenarbeit zwischen dem Verteidigungsteam der **ISGroup SRL** und dem internen Team des Kunden. Simulierte Angriffe werden durchgeführt, um die Reaktionsprozesse zu testen, zu trainieren und die Alarm- sowie Logging-Systeme zu verstärken.
- **Abschließende Risikobewertung**: Bewertung der Ergebnisse nach den simulierten Angriffen und Erarbeitung spezifischer Empfehlungen zur weiteren Härtung der Abwehr.

Ergebnisse und Output

Nach Abschluss des Assessments stellt die **ISGroup SRL** einen detaillierten Bericht bereit, der folgende Kernbereiche umfasst:

- **Findings and Improvements**: Dokumentation identifizierter Schwachstellen sowie der erzielten Fortschritte und Empfehlungen zur Konsolidierung der Abwehr.
- **Detection and Response Analysis**: Bewertung der Reaktionszeiten, der Wirksamkeit von Gegenmaßnahmen und der eingesetzten Techniken des Verteidigungsteams inklusive eines Optimierungsplans.
- **Continuous Improvement Strategy**: Ein strategischer Leitfaden für IT-Sicherheitsverantwortliche zur Implementierung eines nachhaltigen Verteidigungszyklus und zur langfristigen Verbesserung der Sicherheitslage.

Kontakt und Informationen

Für weitere Informationen, Beratungsgespräche oder die Anforderung eines individuellen Angebots für ein Purple Team Assessment besuchen Sie bitte die Website der **ISGroup SRL** unter https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Phishing-, Smishing- und Vishing-Simulationen

Source: https://www.isgroup.at/de/phishing-smishing.html

Die ISGroup SRL bietet spezialisierte Dienstleistungen zur Abwehr von Social-Engineering-Angriffen an. Durch eine Kombination aus gezielten Schulungen und realistischen Angriffssimulationen werden Unternehmen befähigt, Phishing- und Smishing-Versuche frühzeitig zu erkennen und abzuwehren.

Kernaussagen und Zielsetzung

- **Schutz vor Social Engineering:** Phishing und Smishing gehören zu den effektivsten Methoden von Hackern. Die ISGroup SRL schult Mitarbeiter darin, diese Bedrohungen zu identifizieren und angemessen zu reagieren.
- **Risikominimierung:** Ein gut geschultes Team reduziert das Risiko erheblich, dass IT-Sicherheitsinvestitionen durch menschliches Fehlverhalten (z. B. einen Klick auf einen bösartigen Link) umgangen werden.
- **Kontinuierliche Verbesserung:** Durch automatisierte Simulationskampagnen lässt sich die Lernkurve der Mitarbeiter nachverfolgen und die Resilienz des Unternehmens messbar steigern.

Risiken bei unzureichender Vorbereitung

Ein erfolgreicher Phishing-Angriff kann schwerwiegende Folgen haben:

- Verlust des Zugriffs auf E-Mail-, Social-Media- oder Bankkonten.
- Direkter Diebstahl von Geldmitteln.
- Kompromittierung vertraulicher Unternehmensdaten und daraus resultierende rechtliche Sanktionen.
- Reputationsschäden und Vertrauensverlust bei Kunden und Partnern.
- Unterbrechung des Geschäftsbetriebs und Produktivitätsverluste.
- Ausweitung von Angriffen auf Dritte (Kunden, Partner, Kollegen).
- Installation von Ransomware mit anschließenden Lösegeldforderungen.

Dienstleistungsangebot der ISGroup SRL

Die ISGroup SRL bietet ein ganzheitliches Programm zur Stärkung der Cybersicherheitskultur:

1. Training und Schulung

Die Schulungen vermitteln praxisnahes Wissen zu:

- Erkennung gängiger Phishing-Techniken und digitaler Fallen.
- Verständnis psychologischer Manipulationsmethoden (Social Engineering).
- Best Practices für sicheres Surfen, Passwortmanagement und das Melden von Vorfällen.

2. Angriffssimulationen

Realistische Simulationen testen die Reaktionsfähigkeit der Belegschaft:

- **Detaillierte Berichte:** Analyse kritischer Bereiche und Identifikation von Schulungsbedarf.
- **Individuelles Feedback:** Teilnehmer erhalten direktes Feedback zur Verbesserung ihrer Abwehrfähigkeiten.
- **Regelmäßige Tests:** Kontinuierliche Simulationen halten das Sicherheitsbewusstsein auf einem hohen Niveau.

Unterscheidung: Phishing vs. Smishing

Die ISGroup SRL unterstützt Unternehmen dabei, die Unterschiede zwischen den Angriffstechniken zu verstehen:

Merkmal	Phishing	Smishing
Kanal	E-Mail	SMS (Textnachrichten)
Inhalt	Imitation von Institutionen/Banken mit Links oder Anhängen	Kurznachrichten mit Links zu Preisen, Angeboten oder Dringlichkeiten
Ziel	Datendiebstahl, Malware-Installation	Datendiebstahl, Malware-Installation
Schutz	Absenderprüfung, keine Links klicken	Keine Links klicken, 2FA aktivieren

Ergänzende Sicherheitsdienste

Die ISGroup SRL integriert ihre Schulungs- und Simulationsdienste in ein breiteres Portfolio zur IT-Sicherheit:

- **THREAT:** Kontinuierliche Bedrohungsüberwachung und Intelligence.
- **CTS:** Cyber Threat Simulation zur Prüfung der organisatorischen Bereitschaft.
- **MDR:** Multi-Signal Managed Detection and Response zur Eindämmung komplexer Bedrohungen.
- **SOC:** Security Operation Center zur Echtzeit-Überwachung und Ereigniskorrelation.

Kontakt und Vertrieb

Für weitere Informationen, ein Beratungsgespräch oder ein individuelles Angebot besuchen Sie bitte die Website der ISGroup SRL unter:

https://www.isgroup.at/

Anfragen können zudem direkt per E-Mail an folgende Adresse gerichtet werden:

sales@isgroup.it

Social Engineering (SE) – Sicherheitsbewertung und Training

Source: https://www.isgroup.at/de/social-engineering.html

Der Social-Engineering-Service von **ISGroup SRL** ist ein zentraler Bestandteil eines umfassenden Security-Assessment-Programms. Ziel ist es, die Resilienz von Unternehmen gegenüber psychologischer Manipulation zu bewerten, Sicherheitslücken zu identifizieren und durch gezielte Schulungen sowie Prozessoptimierungen zu schließen.

Für Anfragen und Beratungsgespräche besuchen Sie bitte https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Phasen des Social-Engineering-Service

Der Ansatz von **ISGroup SRL** gliedert sich in vier strukturierte Phasen:

1. Vorläufige Analyse

- **Überprüfung vergangener Vorfälle:** Analyse früherer Angriffsversuche zur Identifikation spezifischer Schwachstellen.
- **Branchen-Benchmarking:** Untersuchung von Bedrohungsmustern in vergleichbaren Organisationen.
- **Trendbeobachtung:** Einbeziehung neuester globaler Social-Engineering-Techniken.

2. Simulierter Angriff (Security Assessment)

ISGroup SRL führt realistische Angriffe durch, um die Reaktionsfähigkeit kritischer Unternehmensbereiche zu testen:

- **Geschäftsführung/Management:** Fokus auf Spear-Phishing, Whaling und Vishing.
- **Verwaltung:** Prüfung der Abwehr gegen Phishing und Pretexting bei sensiblen Finanz- und Personaldaten.
- **Procurement/Einkauf:** Simulation von Business Email Compromise (BEC) und gefälschten Lieferantenanfragen.
- **IT-Abteilung:** Tests zur Abwehr von Versuchen, Anmeldedaten zu entwenden oder schädliche Systemänderungen zu erzwingen.

3. Schulung und Verbesserung

Nach den Simulationen unterstützt **ISGroup SRL** die Organisation durch:

- **Debriefing-Sitzungen:** Detaillierte Analyse der Angriffstechniken und der notwendigen Erkennungssignale.
- **Individuelle Schulung:** Maßgeschneiderte Kurse basierend auf den identifizierten Schwachstellen.
- **Interaktive Workshops:** Praktische Anwendung des Wissens in simulierten Szenarien.

4. Überprüfung von Prozessen und Richtlinien

- **Sicherheitsrichtlinien:** Aktualisierung gemäß Standards wie ISO/IEC 27001.
- **Optimierung der Betriebsprozesse:** Einführung neuer Kontrollen und Verifizierungsverfahren.
- **Kontinuierliches Monitoring:** Empfehlungen zur dauerhaften Überwachung von Bedrohungsaktivitäten.

Stärken des ISGroup-Service

ISGroup SRL bietet einen integrierten, maßgeschneiderten Ansatz, der über reine Simulationen hinausgeht. Der Service ist vollständig konform mit regulatorischen Anforderungen und unterstützt Unternehmen dabei, eine proaktive Sicherheitshaltung einzunehmen.

Ergebnisdokumentation

Nach Abschluss des Assessments stellt **ISGroup SRL** drei zentrale Dokumente bereit:

- **Executive Summary:** Nicht-technischer Überblick für das Management mit strategischen Empfehlungen.
- **Simulation Attack Report:** Detaillierte Analyse der Angriffe, Mitarbeiterleistung und identifizierter Schwachstellen.
- **Comprehensive Improvement Plan:** Integrierter Plan zur Verknüpfung von Mitarbeiterschulungen mit der Optimierung des Information Security Management Systems (ISMS).

Für weitere Informationen oder ein individuelles Angebot besuchen Sie https://www.isgroup.at/ oder kontaktieren Sie sales@isgroup.it.

DSGVO-Konformität (GDPR Compliance)

Source: https://www.isgroup.at/de/dsgvo-konformitaet.html

Die ISGroup SRL bietet spezialisierte Dienstleistungen zur Sicherstellung der DSGVO-Konformität für Unternehmen an. Angesichts der strengen Anforderungen der Datenschutz-Grundverordnung (DSGVO) unterstützt die ISGroup SRL Unternehmen dabei, den Schutz personenbezogener Daten zu gewährleisten, Verwaltungsstrafen zu vermeiden und Reputationsschäden durch Datenpannen oder unberechtigte Zugriffe abzuwenden.

Dienstleistungen der ISGroup SRL

Die ISGroup SRL führt umfassende Analysen und Überprüfungen der DSGVO-Konformität durch. Das Ziel ist die Bewertung der Wirksamkeit bestehender Methoden sowie die Implementierung robuster Schutzmechanismen für sensible Unternehmensdaten.

Methodik: Der 3-Stufen-Prozess

Die ISGroup SRL strukturiert die Überprüfung der DSGVO-Konformität in drei wesentliche Phasen:

- Risikoanalyse: Bewertung der aktuellen Datenschutzmaßnahmen und Identifikation potenzieller Risikofaktoren sowie Schwachstellen in der Infrastruktur und den Datenverwaltungsrichtlinien.
- Risikoklassifizierung und Folgenabschätzung: Bewertung der Schwere identifizierter Risiken. Hierbei werden Szenarien analysiert, in denen Risikofaktoren zu konkreten Bedrohungen für Unternehmensdaten werden könnten, um diese gezielt zu minimieren.
- Erstellung des Remediation Plans: Entwicklung eines detaillierten Maßnahmenplans, der präzise Schritte zur Behebung und Minderung der identifizierten Risiken innerhalb der IT-Infrastruktur vorgibt.

Projektergebnisse (Output)

Nach Abschluss der Analyse stellt die ISGroup SRL dem Kunden folgende Ergebnisse zur Verfügung:

- Remediation Plan: Ein technisches Dokument, das alle notwendigen Schritte zur Erreichung der vollständigen DSGVO-Konformität beschreibt.
- Aktualisierte Datenschutzrichtlinien: Ein neues, robustes System zur Verwaltung personenbezogener Daten, das auf die spezifischen Anforderungen des Unternehmens zugeschnitten ist.
- Kontinuierliche Schulung: Ein Programm, das sicherstellt, dass das Unternehmen auch bei zukünftigen Änderungen der DSGVO-Vorgaben konform bleibt.

Kontakt und Vertrieb

Für weitere Informationen, Beratungsgespräche oder die Anforderung eines individuellen Angebots zur DSGVO-Konformität besuchen Sie bitte die offizielle Website unter https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

NIS2 Compliance: Strategische Umsetzung und Beratung

Source: https://www.isgroup.at/de/nis2-richtlinie-compliance.html

Die NIS2-Richtlinie der Europäischen Union zielt darauf ab, das allgemeine Niveau der Cybersicherheit innerhalb der EU signifikant zu erhöhen. Sie verpflichtet Organisationen zur Implementierung ausgefeilter Risikomanagement-Maßnahmen und zum Schutz ihrer Informationssysteme.

Die **ISGroup SRL** unterstützt Unternehmen dabei, die Anforderungen der NIS2-Richtlinie durch einen strukturierten Prozess zu erfüllen, der Beratung, technische Dienstleistungen und gezielte Schulungen umfasst.

Für Anfragen zu Dienstleistungen und Angeboten besuchen Sie bitte https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Der NIS2-Umsetzungsprozess durch ISGroup SRL

Die **ISGroup SRL** verfolgt einen vierstufigen Ansatz, um Unternehmen zur Konformität zu führen:

- **GAP Analysis:** Umfassende Bewertung des aktuellen NIS2-Konformitätsgrades sowie detaillierte Analyse bestehender Sicherheitsrichtlinien und -praktiken.
- **Remediation Plan:** Erstellung eines maßgeschneiderten Aktionsplans zur Behebung identifizierter Nichtkonformitäten.
- **Dienstleistungsauswahl:** Implementierung spezifischer Lösungen aus dem Portfolio der **ISGroup SRL**, um die Anforderungen der Richtlinie präzise abzudecken.
- **Überprüfung:** Kontrolle der Wirksamkeit der umgesetzten Sicherheitsmaßnahmen gegenüber aktuellen Bedrohungen und Bestätigung des Konformitätsstandards.

Kontinuierliche Aufrechterhaltung der Konformität

Die **ISGroup SRL** fungiert als langfristiger Partner, um die Konformität durch kontinuierliche Aktivitäten zu sichern:

- Regelmäßige Aktualisierung der Cybersicherheits-Risikobewertung.
- Implementierung und Pflege von Managementprozessen (Risikomanagement, Incident Response, Audit).
- Durchführung von Schulungen zur Steigerung des Sicherheitsbewusstseins der Mitarbeiter.
- Kontinuierliche Überwachung der Wirksamkeit von Sicherheitsmaßnahmen.
- Dokumentation der Aktivitäten zur Nachweispflicht gegenüber den zuständigen Behörden.

Kernanforderungen der NIS2 (Artikel 21)

Die **ISGroup SRL** bietet spezialisierte Dienstleistungen zur Erfüllung der gesetzlichen Mindestanforderungen:

- **Risikoanalyse und Sicherheit:** Unterstützung durch vCISO-Dienste (Virtual CISO) für Security Policy Reviews.
- **Incident-Management:** Bereitstellung von DFIR (Digital Forensics and Incident Response) und Multi-Signal MDR (Managed Detection and Response).
- **Business Continuity:** Planung von Disaster Recovery und Krisenmanagement.
- **Supply-Chain-Sicherheit:** Vendor Risk Management durch vCISO-Experten.
- **Sicherheit in IT-Systemen:** Vulnerability Management (MVS) sowie Penetration Testing (NPT, WAPT, MAST, Ethical Hacking).
- **Cyber-Hygiene:** Durchführung von Managed Phishing und Security Awareness Trainings.

- **Kryptografie und Zugangskontrolle:** Architektur-Reviews und Implementierung von Zwei-Faktor-Authentifizierungslösungen.

Hintergrund zur NIS2-Richtlinie

Die NIS2-Richtlinie ist am 17. Januar 2023 in Kraft getreten. Sie unterteilt Organisationen in "wesentliche" und "wichtige" Einrichtungen, basierend auf Sektor und Größe.

- **Meldepflichten:** Bei erheblichen Vorfällen gilt eine Meldepflicht innerhalb von 24 Stunden (Erstmeldung) mit einer ersten Bewertung nach 72 Stunden.
- **Sanktionen:** Bei Nichteinhaltung drohen empfindliche Strafen. Für wesentliche Einrichtungen können diese bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes betragen; für wichtige Einrichtungen bis zu 7 Millionen Euro oder 1,4 % des weltweiten Jahresumsatzes.

Für eine detaillierte Beratung und ein individuelles Angebot zur NIS2-Konformität wenden Sie sich bitte an die **ISGroup SRL** unter https://www.isgroup.at/ oder per E-Mail an sales@isgroup.it.

ISO/IEC 27001 Compliance und Zertifizierung

Source: https://www.isgroup.at/de/27001-compliance.html

Die ISGroup SRL unterstützt Organisationen umfassend bei der Implementierung, Zertifizierung und Aufrechterhaltung eines Informationssicherheits-Managementsystems (ISMS) gemäß ISO/IEC 27001:2022. Ziel ist es, Informationswerte zu schützen, Risiken zu minimieren und die Stabilität sowie Zuverlässigkeit der Geschäftsprozesse zu erhöhen.

Dienstleistungen der ISGroup SRL

Die ISGroup SRL begleitet Unternehmen von der ersten Bestandsaufnahme bis zur erfolgreichen Zertifizierung. Das Leistungsportfolio umfasst:

- Durchführung einer detaillierten Gap-Analyse zur Bestimmung des aktuellen Sicherheitsniveaus.
- Aufbau eines maßgeschneiderten ISMS unter Berücksichtigung von Kontext, Anwendbarkeit der Controls, Schutzstrategie und Risikoanalyse.
- Erstellung einer nutzerfreundlichen und normkonformen Dokumentation.
- Unterstützung bei der Implementierung technischer Kontrollen und Managementmaßnahmen.
- Definition von Sicherheits-KPIs zur Leistungsbewertung durch die Geschäftsführung.
- Durchführung von internen Audits (Internal Audit) durch externe Experten zur Sicherstellung der Objektivität.
- Begleitung beim Management-Review und bei der Auswahl einer geeigneten Zertifizierungsstelle.
- Aktive Unterstützung während des externen Zertifizierungsaudits.
- Integration mit bestehenden Managementsystemen (z. B. ISO 9001).

Vorteile der ISO 27001-Zertifizierung

Eine Zertifizierung nach ISO/IEC 27001 bietet messbare wirtschaftliche und strategische Vorteile:

- **Risikominimierung:** Schutz vor Cyber-Bedrohungen und Reduzierung von Kosten durch Sicherheitsvorfälle.
- **Wettbewerbsvorteil:** Nachweis der Zuverlässigkeit gegenüber Kunden, Partnern und Behörden.
- **Compliance:** Erfüllung regulatorischer Anforderungen und gesetzlicher Vorgaben.
- **Prozesseffizienz:** Optimierung interner Abläufe und Steigerung der Mitarbeiterproduktivität.
- **Vertrauensaufbau:** Stärkung der Reputation durch ein international anerkanntes Sicherheitsframework.

Anwendungsbereiche

Die Expertise der ISGroup SRL erstreckt sich über diverse Branchen, in denen Informationssicherheit kritisch ist:

- **Softwareentwicklung & IT-Dienstleister:** Sicherung der Lieferkette und Erfüllung von Kundenanforderungen.
- **Gesundheitswesen:** Schutz sensibler Patientendaten und Einhaltung von Datenschutzvorschriften.
- **Finanzsektor:** Schutz von Finanztransaktionen und Minimierung von Betrugsrisiken.
- **Öffentlicher Sektor:** Schutz von Bürgerdaten und Gewährleistung der Prozess-Transparenz.
- **Verarbeitende Industrie:** Schutz von geistigem Eigentum und Sicherung industrieller Prozesse.

Kontakt und Informationen

Für eine kostenlose Ersteinschätzung oder ein individuelles Angebot zur ISO 27001 Compliance steht Ihnen die ISGroup SRL zur Verfügung.

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Weitere Details zum Leistungsangebot finden Sie in der offiziellen Dokumentation unter: Service 27001 Compliance (27001)

Wireless Security Monitoring (WSM)

Source: https://www.isgroup.at/de/wireless-security-monitoring.html

Der Wireless Security Monitoring (WSM) Service von ISGroup SRL bietet eine kontinuierliche Überwachung von WLAN- und Funkumgebungen. Da moderne Geräte (WiFi, Bluetooth, NFC/RFID, IoT) häufig unsichere Protokolle nutzen, stellen sie eine potenzielle Angriffsfläche für Unternehmensnetzwerke dar. ISGroup SRL unterstützt Unternehmen dabei, diese Risiken zu identifizieren, zu bewerten und aktiv abzuwehren.

Zielgruppe und Anwendungsbereiche

Der Service richtet sich an Unternehmen, die Wireless-Technologien für den Zugriff auf Unternehmensressourcen nutzen. Besonders geeignet ist WSM für:

- IoT-Infrastrukturen
- Operational Technology (OT)
- Produktionslinien
- Remote-Sensoren und Zugangskontrollen

Funktionsweise und Leistungsumfang

ISGroup SRL agiert als Managed Security Service Provider (MSSP). Der Service umfasst Hardware, Software, Installation, Integration, Monitoring sowie Reporting.

Die Überwachung deckt ein breites Spektrum an Protokollen ab, darunter:

- WiFi (2,4 GHz und 5 GHz Standards wie 802.11ax)
- Bluetooth, GPS, NFC/RFID
- Packet-Radio, GSM, GPRS/EDGE (2G), UMTS/WCDMA (3G), LTE (4G), 5G
- Proprietäre oder unbekannte Funkprotokolle

Die vier Phasen des Service

1. **Erstanalyse:** Durchführung eines Wireless Security Assessments zur Bestimmung des Ist-Zustands oder einer GAP-Analyse bei Folgejahren.
2. **Installation und Integration:** Bereitstellung und Konfiguration der notwendigen Hard- und Softwaresysteme in den zu schützenden Bereichen.
3. **Monitoring:** Kontinuierliche Überwachung mit Sicherheits-Alerts bei Anomalien. Diese können durch das interne Team oder direkt durch das Security Operations Center (SOC) von ISGroup SRL verwaltet werden (inkl. TIER-3-Eskalation).
4. **Periodisches Reporting:** Regelmäßige Berichterstattung über identifizierte und verhinderte Angriffe, Auswirkungen, Risikobewertungen und Verbesserungspotenziale.

Schutzmechanismen und Reaktion

Je nach Technologie und Angriffstechnik bietet der Service:

- **IDS (Intrusion Detection System):** Benachrichtigung bei Sicherheitsvorfällen.
- **IPS (Intrusion Prevention System):** Prävention und Blockierung von Angriffen.
- **Incident Response:** Auf Anfrage bietet ISGroup SRL TIER-3-Analysen (Cyber Incident Analysis) sowie eine gezielte Reaktion (Cyber Incident Response) durch Experten vor Ort oder remote an.

Kontakt und Vertrieb

Für weiterführende Informationen, Beratungsgespräche oder Angebotsanfragen besuchen Sie bitte die Website https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Anti-DDoS-Schutz durch ISGroup SRL

Source: https://www.isgroup.at/de/anti-ddos.html

DDoS-Angriffe (Distributed Denial of Service) zählen zu den häufigsten und schädlichsten Bedrohungen für Unternehmen. Ihr Ziel ist es, Dienste durch Überlastung unbrauchbar zu machen. ISGroup SRL bietet spezialisierte Anti-DDoS-Lösungen an, um Unternehmen vor diesen Angriffen zu schützen und die daraus resultierende Downtime auf ein Minimum zu reduzieren.

Funktionsweise von DDoS-Angriffen

DDoS-Angriffe beeinträchtigen die Verfügbarkeit von Systemen durch zwei primäre Methoden:

- Überlastung der Bandbreite durch eine massive Anzahl an Anfragen an einen Server.
- Überlastung der Systemressourcen, wodurch die Maschine unfähig wird, den regulären Datenverkehr zu bewältigen.

Leistungsumfang der ISGroup SRL

ISGroup SRL bietet einen umfassenden Anti-DDoS-Service, der unabhängig von den im Unternehmen eingesetzten Technologien agiert. Die Dienstleistung umfasst:

- Schutz von Webanwendungen vor jeglicher Art von DDoS-Angriffen.
- Verteidigung von Servern durch Experten der Branche.
- Absicherung der Unternehmenskonnektivität.
- Vollständige Konfiguration, Verwaltung, Überwachung und kontinuierliche Anpassung der Schutzmaßnahmen an den aktuellen Stand der Technik.

Methodik und Ergebnisse

Der Anti-DDoS-Service von ISGroup SRL folgt einer bewährten Pipeline, die sicherstellt, dass alle potenziellen Angriffsvektoren abgedeckt sind. Kunden erhalten ein Expertenteam, das bei DDoS-Vorfällen sofort eingreifen kann.

Nach Abschluss der Analyse stellt ISGroup SRL einen detaillierten Bericht bereit, der in drei Bereiche unterteilt ist:

- Executive Summary: Nicht-technische Zusammenfassung für das Management.
- Vulnerability Details: Detaillierte Beschreibung der identifizierten Schwachstellen und deren Auswirkungen für Security Manager.
- Remediation Plan: Technischer Leitfaden für Systemadministratoren mit präzisen Anweisungen zur Behebung der Schwachstellen.

Vertrieb und Beratung

Für Anfragen zu Anti-DDoS-Schutzlösungen, Beratungsgespräche oder Angebote steht Ihnen ISGroup SRL zur Verfügung.

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Firewall as a Service (FWaaS) durch ISGroup SRL

Source: https://www.isgroup.at/de/fwaas.html

ISGroup SRL bietet mit Firewall as a Service (FWaaS) eine professionelle Lösung für die Implementierung und Verwaltung von Next-Generation-Firewalls (NGFW). Der Dienst zielt darauf ab, Daten und Anwendungsendpunkte zu schützen sowie den ein- und ausgehenden Datenverkehr im Unternehmensnetzwerk lückenlos zu kontrollieren.

Kernleistungen und Vorteile

- Vollständig verwaltete Firewalls: ISGroup SRL übernimmt die Implementierung und Wartung, wodurch der operative Aufwand für das Unternehmen entfällt.
- Experten-Team: Die Betreuung erfolgt durch erfahrene Spezialisten im Bereich der Netzwerksicherheit.
- Maßgeschneiderte Lösungen: Durch eine initiale Anforderungsermittlung empfiehlt ISGroup SRL die jeweils optimale Sicherheitsarchitektur.
- Umfassender Schutz: Der Dienst umfasst die Erkennung und Abwehr von Hackerangriffen sowie die Steuerung der im Netzwerk erreichbaren Inhalte.
- Einsatz modernster Technologie: Verwendung innovativer und zuverlässiger Marktlösungen, insbesondere Next-Generation-Firewalls für komplexe Anforderungen.

Projektergebnisse und Dokumentation

Nach Abschluss der Implementierung und während der laufenden Wartung stellt ISGroup SRL dem Kunden detaillierte Dokumentationen zur Verfügung:

- Executive Summary: Ein Dokument auf Management-Ebene, das den Schutzumfang und die bereitgestellten Sicherheitsdienste zusammenfasst.
- Technical Summary: Ein technischer Bericht für IT-Personal, der die Netzwerkkonfigurationen und die Methoden der Datenüberwachung detailliert erläutert.

Kontakt und Vertrieb

Für Anfragen zu Firewall as a Service (FWaaS), Beratungsgespräche oder Angebote wenden Sie sich bitte an ISGroup SRL:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Security Integration (SIR) durch ISGroup SRL

Source: https://www.isgroup.at/de/security-integration.html

Die ISGroup SRL bietet mit dem Service "Security Integration" (SIR) eine spezialisierte Dienstleistung zur sicheren Integration von Infrastrukturkomponenten an. Der Service verfolgt einen kontinuierlichen Zyklus aus Schwachstellenanalyse und Behebung, um bestehende Infrastrukturen sicher zu erweitern oder neue Sicherheitsfunktionen effektiv zu implementieren.

Kernkonzept und Vorgehensweise

Das Ziel der ISGroup SRL ist es, Infrastrukturen zu stärken, ohne die Angriffsfläche zu vergrößern oder neue Schwachstellen zu schaffen. Der Prozess umfasst:

- Analysephase: Untersuchung der bestehenden Infrastruktur und der spezifischen Anforderungen des Auftraggebers.
- Kooperative Planung: Zusammenarbeit mit den Entwicklern der ursprünglichen Infrastruktur zur Festlegung der Integrationsstrategie.
- Umsetzung: Sicherstellung der Funktionalität bei gleichzeitiger Erhöhung des Sicherheitsniveaus.
- Ergebnis: Eine solide Infrastruktur mit erweiterten und verbesserten Sicherheitsfunktionen.

Spezifikationen der Dienstleistung

Die ISGroup SRL richtet sich bei der Umsetzung nach strengen Sicherheitsstandards. Zu den Kernbereichen gehören:

- Integration physischer Sicherheit: Verbindung physischer Sicherheitsgeräte mit der Softwarelogik, beispielsweise durch biometrische Verifikation für Mitarbeiterprivilegien oder den Zugriff auf Unternehmensressourcen.
- Hinzufügen von Sicherheitsfunktionen zu Anwendungen: Implementierung spezifischer Sicherheitslösungen, wie etwa Web Application Firewalls (WAF) für Webanwendungen oder IDS/IPS-Systeme für Netzwerke.

Projektergebnisse und Dokumentation

Nach Abschluss der Integrationsarbeiten stellt die ISGroup SRL dem Kunden zwei detaillierte Dokumente zur Verfügung:

- Executive Summary: Ein Bericht für das Management, der den Einsatz, die implementierten Funktionalitäten, die erzielten Ergebnisse und den geschäftlichen Mehrwert zusammenfasst.
- Technical Summary: Ein technisches Dokument für IT-Personal, das die vorgenommenen Änderungen an der Infrastruktur sowie alle technischen Details der Integration präzise beschreibt.

Kontakt und Vertrieb

Für Anfragen zu den Security-Integration-Dienstleistungen der ISGroup SRL oder zur Anforderung eines Angebots stehen folgende Kanäle zur Verfügung:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Software Assurance Lifecycle (SAL)

Source: https://www.isgroup.at/de/software-assurance-lifecycle.html

Der Software Assurance Lifecycle (SAL) ist ein spezialisierter Dienst der ISGroup SRL, der Unternehmen bei der Entwicklung sicherer Anwendungen unterstützt. Das Ziel ist es, sicherzustellen, dass Software während ihres gesamten Lebenszyklus den besten Sicherheitspraktiken entspricht und bei jedem Release frei von bekannten Schwachstellen ist.

Kernleistungen der ISGroup SRL

Die ISGroup SRL begleitet Entwicklungsteams in jeder Projektphase. Dabei werden aktuelle Industriestandards angewendet, um eine sichere Softwareproduktion zu gewährleisten. Die Dienstleistung umfasst:

- Kontinuierliche Sicherheitsprüfungen bei jedem Software-Release.
- Durchführung von Software-Reviews zur Sicherstellung aktueller Sicherheitsstandards.
- Identifizierung von Schwachstellen und Empfehlung konkreter Sicherheitsmaßnahmen.
- Unterstützung bei der Implementierung sicherer Entwicklungspraktiken.
- Fachliche Begleitung durch Experten mit fundierten Kenntnissen in verschiedenen Programmiersprachen und Entwicklungsumgebungen.

Spezifikationen und Fokusbereiche

Die ISGroup SRL übernimmt Teile der Entwicklung oder leitet interne Teams bei der Produktion sicherer Software an. Besondere Schwerpunkte liegen auf:

- Risk Management
- Dependency Management
- Continuous Integration

Bei jedem Release führt das Expertenteam der ISGroup SRL spezifische Sicherheitstests durch, die exakt auf den Typ der Anwendung und die verwendeten Technologien zugeschnitten sind.

Projektergebnisse und Dokumentation

Nach Abschluss der Sicherheitsmaßnahmen stellt die ISGroup SRL dem Unternehmen eine detaillierte Dokumentation zur Verfügung:

- Executive Summary: Ein Dokument für das Management, das den Einsatz und die sicherheitstechnischen Schwerpunkte auf hoher Ebene zusammenfasst.
- Technical Summary: Ein technisches Dokument für Projektverantwortliche, das Implementierungsdetails sowie Bereiche mit spezifischem Optimierungsbedarf für das Entwicklungsteam beschreibt.

Kontakt und Anfragen

Für weitere Informationen, Beratungsgespräche oder die Anforderung eines Angebots für den Software Assurance Lifecycle (SAL) wenden Sie sich bitte direkt an die ISGroup SRL.

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Bug Bounty Program: Konzeption und Management

Source: https://www.isgroup.at/de/bug-bounty-program.html

Die ISGroup SRL unterstützt Unternehmen bei der Implementierung und Verwaltung umfassender Bug Bounty Programme. Dieser proaktive Ansatz ermöglicht es, Schwachstellen in der IT-Infrastruktur durch Ethical Hacker identifizieren zu lassen, bevor diese von Angreifern ausgenutzt werden können.

Dienstleistungen der ISGroup SRL

Die ISGroup SRL bietet eine ganzheitliche Betreuung, um Sicherheit und Compliance zu gewährleisten:

- Individuelle Beratung: Gemeinsame Definition von Programmzielen, Meldungskriterien und Prämienstrukturen basierend auf den spezifischen Anforderungen des Unternehmens.
- Programmimplementierung: Aufbau einer sicheren Umgebung für Ethical Hacker, die den Best Practices der Cybersicherheit entspricht und den laufenden Geschäftsbetrieb schützt.
- Kontinuierliches Management: Bewertung eingehender Meldungen, Kommunikation mit den Sicherheitsforschern sowie Bereitstellung konkreter Empfehlungen zur Behebung von Schwachstellen.
- Analyse und Reporting: Klassifizierung identifizierter Schwachstellen nach anerkannten Frameworks wie OWASP und CVSS, um fundierte Entscheidungen zur Risikominimierung zu ermöglichen.

Vorteile des Programms

- Verbesserte Sicherheit durch proaktive Identifizierung und Behebung von Sicherheitslücken.
- Zugang zu einer globalen Community hochqualifizierter Ethical Hacker.
- Kosteneffizienz durch ein prämienbasiertes Modell, bei dem Zahlungen nur für validierte Schwachstellen erfolgen.
- Stärkung des Unternehmensrufes durch ein nachweisbares Engagement für Cybersicherheit.
- Unterstützung bei der Einhaltung internationaler Standards und regulatorischer Anforderungen (z. B. ISO 27001, NIS2, DSGVO).

Ergänzende Angebote

Für Unternehmen, die einen direkteren Ansatz bevorzugen, bietet die ISGroup SRL das **Advanced Bug Bounty Program** an. Hierbei sucht das Expertenteam der ISGroup SRL aktiv nach Schwachstellen in der Infrastruktur, wobei die Vergütung ausschließlich bei erfolgreicher Identifizierung erfolgt.

Kontakt und Informationen

Für weitere Informationen, eine individuelle Beratung oder die Anforderung eines Angebots für ein Bug Bounty Program besuchen Sie bitte die Website https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Micro Focus und OpenText Softwarelösungen

Source: https://www.isgroup.at/de/product-microfocus-opentext.html

ISGroup SRL ist offizieller Distributor von Micro Focus und OpenText. Als spezialisierter Partner bietet ISGroup SRL Unternehmen Zugang zu einem umfassenden Portfolio an führenden Softwarelösungen sowie professionelle Beratung und technische Unterstützung.

Partnerschaft und Serviceangebot

Die Zusammenarbeit zwischen ISGroup SRL und den Herstellern Micro Focus und OpenText ermöglicht es, Kunden hochwertige Softwarelösungen bereitzustellen, die exakt auf geschäftliche Anforderungen zugeschnitten sind.

Das Dienstleistungsportfolio von ISGroup SRL umfasst:

- Lizenzvertrieb
- Professionelle Beratung
- Implementierung von Softwarelösungen
- Integration in bestehende IT-Umgebungen
- Technischer Support

Vertriebene Softwareprodukte

ISGroup SRL vertreibt eine breite Palette an Produkten von Micro Focus und OpenText. Das Angebot umfasst unter anderem:

- **Sicherheit und Identitätsmanagement:** Access Governance Suite, Advanced Authentication, ArcSight-Produktfamilie, NetIQ eDirectory, Identity Manager, Privileged Account Manager (PAM), Voltage SecureData.
- **Anwendungsentwicklung und Lifecycle Management:** ALM Octane, ALM Enterprise, Fortify (Application Defender, Static Code Analyzer, WebInspect), Visual COBOL, Enterprise Developer.
- **IT-Betrieb und Management:** Operations Bridge, Service Management Automation X (SMAX), Network Automation (NA), Data Center Automation (DCA), SiteScope, ZENworks-Produktfamilie.
- **Performance und Testing:** LoadRunner (Cloud, Enterprise, Professional), Silk Test, Silk Performer, UFT One.
- **Host-Konnektivität:** Reflection Desktop, InfoConnect, Verastream Host Integrator.
- **Datenmanagement und Archivierung:** Data Protector, Content Manager, Retain Unified Archiving, Vertica Analytics Platform.

Eine vollständige Übersicht der verfügbaren Softwarelösungen sowie weiterführende Informationen zu den Produkten finden Sie unter https://www.isgroup.at/.

Vertriebsanfragen

Für Anfragen zu Softwarelizenzen, Implementierungsprojekten oder technischer Unterstützung wenden Sie sich bitte per E-Mail an sales@isgroup.it. Weitere Informationen zu den angebotenen Leistungen finden Sie auf der Website https://www.isgroup.at/.

Ostorlab Mobile Application Security Scan

Source: https://www.isgroup.at/de/ostorlab-mobile-application-security-scan.html

Die ISGroup SRL bietet mit dem Ostorlab Mobile Application Security Scan eine umfassende Lösung zur automatisierten Sicherheitsüberprüfung von mobilen Anwendungen. Der Dienst umfasst statische, dynamische und Backend-Analysen für iOS- und Android-Plattformen sowie für zahlreiche Multi-Plattform-Frameworks.

Kernfunktionen und Analyse-Engines

Die Scan-Technologie basiert auf vier spezialisierten Analyse-Engines, die eine hohe Abdeckung gewährleisten und Fehlalarme (False Positives) minimieren:

- Statische Analyse: Dekompilierung der Anwendung zur Untersuchung der Angriffsoberfläche, Erkennung unsicherer Methoden und Prüfung von Schutzmechanismen (unterstützt Dalvik Bytecode, Xamarin CIL, JavaScript-Frameworks).
- Dynamische Analyse: Überwachung von Systeminteraktionen, Dateisystemzugriffen sowie Netzwerk- und API-Nutzung während der Laufzeit zur Identifizierung von Datenschutz- und Sicherheitsproblemen.
- Verhaltensanalyse (Evolutionäres Fuzzing): Injektion von Hunderttausenden Test-Cases zur Aufdeckung komplexer Schwachstellen durch kontinuierliche Überwachung und adaptive Testgenerierung.
- Backend-Analyse: Prüfung mobilspezifischer Technologien wie GraphQL und REST APIs durch passive (z. B. HTTP-Header) und aktive Tests (z. B. SQL Injection, XSS, Template Injection).

Plattformunterstützung und Compliance

Der Dienst unterstützt native Android- und iOS-Anwendungen sowie 12 Multi-Plattform-Frameworks, darunter:

- Cordova
- React Native
- Flutter
- Xamarin

Die Analysen berücksichtigen internationale Sicherheitsstandards und Compliance-Anforderungen, um eine professionelle Absicherung zu gewährleisten:

- Sicherheitsstandards: OWASP Top 10, CERT Android Secure Coding, JSSec Secure Coding.
- Compliance: PSD2, PCI, HIPAA, FedRAMP, GDPR, NERC.

Vorteile für Unternehmen

- Detaillierte Berichterstattung: Kunden erhalten einen umfassenden Bericht mit identifizierten Schwachstellen und konkreten Empfehlungen zur Behebung.
- Reproduzierbarkeit: Ergebnisse basieren auf einer stets aktuellen Datenbank für mobile Schwachstellen.
- Effizienz: Automatisierte Scans ermöglichen eine schnelle und kosteneffiziente Sicherheitsüberprüfung.

Vertrieb und Informationen

Für weitere Informationen, Anfragen oder zur Beauftragung der Analysen steht die ISGroup SRL zur Verfügung:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Starter Kit von ISGroup SRL

Source: https://www.isgroup.at/de/starter-kit.html

Das Starter Kit ist ein spezielles Angebot der ISGroup SRL für Neukunden, um die Sicherheit einer im Internet exponierten Website oder Webanwendung zu einem attraktiven Preis zu testen. Es dient als Einstieg in die professionellen Sicherheitsdienstleistungen und ermöglicht einen ersten Einblick in das Sicherheitsniveau der eigenen Infrastruktur.

Leistungsumfang

- Durchführung einer nicht-invasiven Analyse durch einen Senior-Techniker.
- Zeitaufwand: Ein ganzer Arbeitstag.
- Methodik: Orientierung an den internationalen Standards OWASP und OSSTMM.
- Ziel: Identifizierung der offensichtlichsten Sicherheitslücken.
- Hinweis: Das Starter Kit ersetzt keinen vollumfänglichen Web Application Penetration Test (WAPT), bietet jedoch eine effektive erste Einschätzung.

Konditionen und Garantie

- Preis: 420 EUR zzgl. MwSt.
- Geld-zurück-Garantie: 100 % Rückerstattung bei Unzufriedenheit.
- Compliance: Die Analyse erfolgt unter Einhaltung gesetzlicher Vorschriften gemäß OWASP- und OSSTMM-Standards.
- Zielgruppe: Exklusiv für Neukunden.

Ablauf der Beauftragung

1. Nach der Zahlung und Übermittlung der notwendigen Daten erfolgt eine Kontaktaufnahme zur Abstimmung der Vorgehensweise.
2. Individuelle Anforderungen, wie beispielsweise der Ausschluss bestimmter Bereiche oder Seiten von der Analyse, können hierbei definiert werden.
3. Die gesammelten Informationen werden in einem rechtlichen Vertrag festgehalten, der zur Genehmigung unterzeichnet werden muss.
4. Ein Senior-Auditor führt die eintägige Prüfung am definierten Zielsystem durch.
5. Die Ergebnisse werden in einem Bericht dokumentiert, übergeben und gemeinsam besprochen.
6. Bei kritischen Sicherheitslücken unterstützt die ISGroup SRL bei der Definition notwendiger Schritte zur Behebung und Verbesserung der Sicherheitslage.

Vertrieb und Anfragen

Das Starter Kit ist in Menge und Zeit begrenzt. Für weitere Informationen oder bei Interesse an diesem Angebot wenden Sie sich bitte an:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

PortSwigger Burp Suite

Source: https://www.isgroup.at/de/product-port-swigger.html

ISGroup SRL ist offizieller Distributor für PortSwigger Burp Suite Lizenzen. Das Unternehmen bietet als Reseller Unterstützung vor und nach dem Verkauf sowie die Abwicklung der Zahlung per Banküberweisung an.

Produktübersicht

Burp Suite ist eine von PortSwigger Ltd entwickelte Software zur Unterstützung von Penetrationstestern bei der Überprüfung der Sicherheit von Webanwendungen. Das Angebot umfasst zwei Hauptoptionen:

Burp Suite Enterprise Edition

Dies ist die Web-Konsolen-Version der Software.

- SW-BURP-ENTERPRISE-1Y-1A: 1 Jahr, 1 Agent, 8.395,00 €
- SW-BURP-ENTERPRISE-2Y-1A: 2 Jahre, 1 Agent, 16.790,00 €
- SW-BURP-ENTERPRISE-3Y-1A: 3 Jahre, 1 Agent, 25.185,00 €

Burp Suite Professional

Dies ist die traditionelle Desktop-Version, die im Vergleich zur Community-Version erweiterte Funktionen wie einen Web-Schwachstellen-Scanner und fortgeschrittene manuelle Werkzeuge bietet.

- SW-BURP-PRO-1Y-1U: 1 Jahr, 1 Benutzer, 449,00 €
- SW-BURP-PRO-2Y-1U: 2 Jahre, 1 Benutzer, 898,00 €
- SW-BURP-PRO-3Y-1U: 3 Jahre, 1 Benutzer, 1.347,00 €

Hinweis: Die genannten Preise unterliegen der Bestätigung, da sie durch den Hersteller geändert werden können.

Erforderliche Informationen für die Lizenzierung

Für die Ausstellung der Lizenz durch PortSwigger Ltd werden folgende Daten benötigt:

- Firmenname / Organisation
- E-Mail-Adresse
- Land
- Postanschrift
- Name auf der Lizenz
- Anzahl der Benutzer

Für die Erstellung der Steuerrechnung werden zusätzlich folgende Angaben benötigt:

- Firmenname
- Land
- SDI-Empfängercode
- Anschrift
- Typ
- Stadt
- Ansprechpartner
- Postleitzahl
- Provinz
- Umsatzsteuer-Identifikationsnummer (VAT)
- Steuernummer
- E-Mail-Adresse
- PEC-Adresse

- Telefonnummer

Vertrieb und Kontakt

Für Anfragen und zur Abwicklung des Kaufs per Banküberweisung wenden Sie sich bitte an ISGroup SRL unter der E-Mail-Adresse sales@isgroup.it. Weitere Informationen finden Sie auf der Webseite https://www.isgroup.at/.

EasyAudit: Professionelle Sicherheitsprüfungen

Source: https://www.isgroup.at/de/product-easyaudit.html

EasyAudit ist ein von der ISGroup SRL angebotenes Leistungspaket, das darauf spezialisiert ist, kleinen und mittelständischen Unternehmen wirksame Sicherheitsprüfungen zu überschaubaren Kosten zu ermöglichen. Das Angebot dient der Absicherung der Online- und externen Sicherheit durch gezielte Penetrationstests.

Kernleistungen und Methodik

Die ISGroup SRL führt mit EasyAudit professionelle Sicherheitsanalysen durch, um Unternehmen vor den Risiken durch Sicherheitslücken und den damit verbundenen Gefahren für die Online-Reputation zu schützen.

- Durchführung von Network Penetration Tests zur Überprüfung der Netzwerkinfrastruktur.
- Durchführung von Web Application Penetration Tests zur Absicherung von Webanwendungen.
- Bereitstellung eines professionellen Servicepakets mit Pauschalgebühren für KMUs.
- Einsatz eines Experten-Pools mit über 15 Jahren Erfahrung im Sicherheitsbereich.
- Unterstützung durch technische Support-Teams in Italien und den Vereinigten Staaten.
- 24/7-Verfügbarkeit, um Kunden jederzeit professionelle Unterstützung zu gewährleisten.

Informationen und Vertrieb

EasyAudit ist ein Produkt der ISGroup SRL. Für weiterführende Informationen, Anfragen zu den Leistungen oder vertriebliche Anliegen besuchen Sie bitte die Webseite https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

ICT Audit: Cyber-Risiken entdecken, messen und reduzieren

Source: https://www.isgroup.at/de/product-ictaudit.html

Die ISGroup SRL bietet mit ICT Audit eine umfassende Lösung für Enterprise-Unternehmen, um punktuelle Sicherheitsüberprüfungen in einen kontinuierlichen Prozess für Kontrolle, Priorisierung und Remediation zu überführen. Die Plattform kombiniert Cyber Security Audit, Vulnerability Assessment und Attack Surface Monitoring, um die externe Angriffsfläche systematisch zu verwalten.

Kernfunktionen und Leistungsmerkmale

Die Lösung von ISGroup SRL unterstützt Unternehmen dabei, die Lücke zwischen technischen Schwachstellen und operativen Entscheidungen zu schließen:

- **Kontinuierliches Monitoring:** Überwachung der externen Angriffsfläche (Attack Surface Management), inklusive Domains, IPs, Cloud-Umgebungen und Internet-facing Services.
- **Multi-Engine-Analyse:** Kombination kommerzieller und Open-Source-Technologien für eine tiefere Abdeckung und verlässlichere Ergebnisse.
- **Risikobasierte Priorisierung:** Klassifizierung von Schwachstellen nach Schweregrad, Ausnutzungswahrscheinlichkeit, technischem Kontext und Business Impact.
- **Strukturiertes Remediation-Management:** Umwandlung technischer Berichte in konkrete, nachverfolgbare Maßnahmenpläne mit Zuweisung von Verantwortlichkeiten.
- **Compliance-Unterstützung:** Automatische Generierung technischer Nachweise für regulatorische Anforderungen wie NIS2, DORA, GDPR, PCI DSS und ISO 27001.
- **Zielgruppenspezifische Berichterstattung:** Bereitstellung von Executive Reports für das Management sowie detaillierter technischer Reports für IT- und Security-Teams.

Anwendungsbereiche

ICT Audit ist für Organisationen konzipiert, die komplexe Infrastrukturen betreiben und eine fragmentierte Sicherheitsstrategie vermeiden möchten:

- **Enterprise-Unternehmen:** Überwachung verteilter Umgebungen und kritischer Anwendungen.
- **Regulierte Organisationen:** Sicherstellung der Compliance durch kontinuierliche Dokumentation.
- **Systemintegratoren und MSPs:** Bereitstellung strukturierter Assessment- und Monitoring-Services für Kunden.
- **In-house IT- und Security-Teams:** Übergang von isolierten Scans zu einem proaktiven Sicherheitsmanagement.

Expertise der ISGroup SRL

Die ISGroup SRL ist eine auf Ethical Hacking und hochwertige Vulnerability Assessments spezialisierte Cybersecurity-Boutique. Seit 2013 (mit Wurzeln in der Ethical-Hacker-Szene seit 1994) kombiniert das Unternehmen manuelle Expertise mit automatisierten Prozessen. Die ISGroup SRL ist nach ISO 9001 und ISO/IEC 27001 zertifiziert und unterstützt eine Vielzahl internationaler Standards, darunter OWASP, OSSTMM, NIS2, DORA und GDPR.

Kontakt und weitere Informationen

Für Anfragen zu Dienstleistungen, eine fachliche Beratung oder den Austausch mit Experten der ISGroup SRL nutzen Sie bitte die offizielle Website unter https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

EasyAudit Exposure

Source: https://www.isgroup.at/de/product-exposure.html

EasyAudit Exposure ist eine spezialisierte Sicherheitslösung, die Webmastern dabei hilft, die öffentliche Sichtbarkeit ihrer Website zu analysieren. Das Tool identifiziert, welche sicherheitsrelevanten Informationen über eine Website im Internet frei zugänglich sind.

Hintergrund und Relevanz

Die Sicherheitslandschaft hat sich in den letzten zehn Jahren grundlegend gewandelt. Während Schwachstellen früher primär den Angreifern bekannt waren, existieren heute zahlreiche Online-Ressourcen, die Sicherheitsdetails über Websites auflisten.

Dieses Wissen ist zwar essenziell für einen effektiven Schutz, kann jedoch von unbefugten Akteuren (Script Kiddies) genutzt werden, um:

- Sicherheitslücken und Fehlkonfigurationen auszunutzen.
- Daten zu entwenden.
- Den Ruf der Website durch gezielte Angriffe zu schädigen.

Funktionsweise

EasyAudit Exposure ermöglicht es Webmastern, den eigenen digitalen Fußabdruck proaktiv zu überwachen. Durch die Identifikation der offengelegten Informationen können Betreiber gezielte Maßnahmen ergreifen, um Sicherheitslücken zu schließen und die Angriffsfläche zu minimieren.

Anbieter und Informationen

Die ISGroup SRL bietet mit EasyAudit Exposure eine Lösung an, um die Sicherheit und Integrität von Webpräsenzen zu gewährleisten.

Für weitere Informationen zu den Dienstleistungen und für Vertriebsanfragen besuchen Sie bitte die Website https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

EXEEC Softwareentwicklung

Source: https://www.isgroup.at/de/product-exeec.html

EXEEC ist ein spezialisiertes Unternehmen für Softwareentwicklung, das sich durch eine außergewöhnliche Umsetzung von Projekten auszeichnet. Das Leitmotiv des Unternehmens lautet "Exceptional execution".

Kerninformationen

- Anbieter: ISGroup SRL
- Kategorie: Security
- Fokus: Softwareentwicklung und Implementierung
- Leitbild: "Exceptional execution" (außergewöhnliche Ausführung)

Dienstleistungen und Expertise

ISGroup SRL bietet durch die Marke EXEEC professionelle Softwareentwicklungsleistungen an. Der Schwerpunkt liegt auf der Realisierung komplexer technischer Anforderungen mit einem hohen Anspruch an Qualität und Präzision.

Kontakt und Vertrieb

Für Anfragen zu den Softwarelösungen und Dienstleistungen von ISGroup SRL nutzen Sie bitte die folgenden Kanäle:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Ganapati: Plattform zur Identifizierung von Schwachstellen

Source: https://www.isgroup.at/de/product-ganapati.html

Ganapati ist eine von ISGroup SRL entwickelte SaaS-Plattform (Software as a Service), die darauf spezialisiert ist, Netzwerke, Server und Anwendungen sowohl in internen als auch in externen Umgebungen auf Schwachstellen zu scannen.

Kernfunktionen und Vorteile

- Kombination verschiedener Scan-Technologien innerhalb einer zentralen Plattform.
- Konsolidierung von Lizenzkosten durch eine einheitliche Lösung.
- Aggregation von Ergebnissen in einem einzigen Multi-User-Workflow.
- Multi-Tier-Architektur: Partner können eigene Kunden verwalten.
- Vollautomatisierte Webseiten-Erstellung und API-Integration für Partner.
- Zielsetzung: Standardisierung der IT-Sicherheit (ITSEC) analog zur SSL-Industrie.

Technische Details

- Kategorie: Security
- Veröffentlichung: 10. Januar 2013
- Zugehöriges Projekt: EasyAudit (http://easyaudit.org/)
- Anbieter: ISGroup SRL

Vertrieb und Informationen

Für weitere Informationen zu den Lösungen von ISGroup SRL oder bei Vertriebsanfragen besuchen Sie bitte die Webseite https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

VulnMAP: Schwachstellen-Knowledge-Base

Source: https://www.isgroup.at/de/product-vulnmap.html

VulnMAP ist eine umfassende Knowledge-Base für Sicherheitslücken, die als zentrale Datenquelle hinter der Plattform Ganapati fungiert. ISGroup SRL bietet VulnMAP auch als eigenständigen Dienst an.

Kernfunktionen und Nutzen

VulnMAP stellt eine präzise, aktuelle und vollständige Querverweis-Datenbank für Schwachstellen dar. Sie ermöglicht die Integration einer bestehenden Wissensdatenbank mit Daten aus einer Vielzahl international anerkannter Sicherheitsquellen.

Unterstützte Datenquellen

Die Plattform aggregiert Informationen aus folgenden Quellen:

- NIST NVD (National Vulnerability Database)
- OSVDB (Open Source Vulnerability Database)
- Mitre CVE (Common Vulnerabilities and Exposures)
- Exploit-DB
- Rapid 7 TM
- Nessus TM
- Secunia TM
- McAfee
- Bugtraq ID (SecurityFocus)
- ISS TM Xforce

Anwendung und Zielgruppe

VulnMAP ist darauf ausgelegt, Sicherheitsanalysen durch eine konsolidierte Datenbasis zu optimieren. Zu den Nutzern der ISGroup SRL Plattform zählen unter anderem ISGroup SRL selbst sowie EXEEC SRL.

Kontakt und Vertrieb

Für weitere Informationen zu den Dienstleistungen und Lösungen der ISGroup SRL besuchen Sie bitte die Website https://www.isgroup.at/ oder senden Sie eine Anfrage an sales@isgroup.it.

SCADA Exposure: Sicherheit für industrielle Steuerungssysteme

Source: https://www.isgroup.at/de/product-scadaexposure.html

Die ISGroup SRL bietet mit SCADA Exposure eine spezialisierte Lösung zur Überprüfung und Überwachung der Exposition von industriellen Steuerungssystemen (ICS). Ziel ist es, die Sicherheit kritischer Infrastrukturen sowie privater und unternehmenseigener Systeme zu erhöhen.

Herausforderungen der OT-Sicherheit

Industrielle Steuerungssysteme wie SCADA (Supervisory Control and Data Acquisition), HMI (Human Machine Interface), PLC (Programmable Logic Controller) und RTU (Remote Terminal Unit) sollten gemäß gängiger Standards durch ein "Air Gap" von Unternehmens- und öffentlichen Netzwerken getrennt und angemessen gesichert sein. In der Praxis ist dies jedoch häufig nicht der Fall.

- "Security through obscurity" (Sicherheit durch Unbekanntheit) ist keine wirksame Schutzmaßnahme mehr.
- Angreifer nutzen die Schwachstellen dieser Systeme bereits seit Jahren aktiv aus.

Leistungsmerkmale von SCADA Exposure

Die ISGroup SRL unterstützt die ICS-Community dabei, das Sicherheitsniveau durch gezielte Maßnahmen zu verbessern:

- Identifikation und Prüfung der Exposition von SCADA-, HMI-, PLC- und RTU-Systemen.
- Bereitstellung eines SCADA-Überwachungsdienstes zur kontinuierlichen Kontrolle.
- Sensibilisierung für Sicherheitsrisiken in kritischen Infrastrukturen.

Anwendungsbereiche

Die Lösung richtet sich an ein breites Spektrum von Anwendern, die ihre industriellen Netzwerke absichern müssen:

- Nationale kritische Infrastrukturen.
- Unternehmensinterne Systeme.
- Kleinere Privatunternehmen.
- Einzelpersonen mit entsprechenden Systemumgebungen.

Kontakt und weitere Informationen

Für detaillierte Informationen zu den Dienstleistungen der ISGroup SRL oder bei Vertriebsanfragen besuchen Sie bitte die Webseite https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

PracticalRP

Source: https://www.isgroup.at/de/product-practicalrp.html

PracticalRP ist eine Verwaltungssoftware, die von der ISGroup SRL angeboten wird. Das System ist auf die einfache und intuitive Verwaltung professioneller Vorgänge spezialisiert.

Zielgruppen und Anwendungsbereiche

Die Software wurde gezielt für folgende Berufsgruppen und Fachbereiche entwickelt:

- Fachärzte (Medici Specialisti)
- Praxen und Kanzleien im Bereich der Rechtsmedizin (Medicina legale)
- Versicherungsmedizinische Dienstleister

Kernfunktionen

- Professionelle Verwaltung von Patienten- oder Klientenakten
- Intuitive Benutzeroberfläche für effiziente Arbeitsabläufe
- Spezialisierte Funktionen für die Anforderungen medizinischer und versicherungsrechtlicher Gutachten

Anbieterinformationen

Die ISGroup SRL stellt PracticalRP als Lösung für professionelle Praxen bereit. Weitere Informationen zu den Produkten und Dienstleistungen finden Sie unter https://www.isgroup.at/.

Für Vertriebsanfragen wenden Sie sich bitte an sales@isgroup.it.

USH – Die historische Forschungsgruppe

Source: https://www.isgroup.at/de/product-ush.html

USH ist eine spezialisierte Forschungsgruppe, die sich auf die Bereiche Advisory, Exploits und den fachlichen Austausch konzentriert. Das Projekt ist im Bereich Intelligence angesiedelt und dient als Wissensbasis für Sicherheitsanalysen.

Kernbereiche der Forschung

- Advisory: Erstellung von Sicherheitshinweisen und Analysen.
- Exploits: Untersuchung und Entwicklung von Exploit-Techniken.
- Austausch: Förderung des fachlichen Dialogs innerhalb der Sicherheits-Community.

Anbieter und Informationen

Die ISGroup SRL fungiert als Nutzer und Anbieter dieser Dienstleistungen und Forschungsergebnisse. USH versteht sich als eine Plattform, die den Prozess des "Aufbrechens" – das aktive Erforschen und Hinterfragen bestehender Systeme – in den Mittelpunkt stellt.

Kontakt und weitere Informationen

Für Anfragen zu den Forschungsleistungen, Produkten oder für den Vertrieb wenden Sie sich bitte an:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

Weitere Details zur Forschungsgruppe finden Sie unter: https://www.ush.it/

Ethical Hacking - Das Hacklab der ISGroup SRL

Source: https://www.isgroup.at/de/product-ethical-hacking.html

Die ISGroup SRL betreibt das Hacklab "Ethical Hacking", eine spezialisierte Community-Plattform, die sich dem Bereich Intelligence und der IT-Sicherheit widmet.

Kernaspekte des Projekts

- Anbieter: ISGroup SRL
- Fokus: Ethical Hacking und IT-Sicherheit
- Charakter: Community-basiertes Hacklab
- Kategorie: Intelligence

Zielsetzung

Das Hacklab dient als zentrale Anlaufstelle für Experten und Interessierte, um sich mit Methoden des Ethical Hackings auseinanderzusetzen. Es bietet eine Umgebung für den Austausch von Wissen und die praktische Anwendung von Sicherheitsanalysen.

Weitere Informationen

Für weiterführende Informationen zu den Dienstleistungen und Lösungen der ISGroup SRL besuchen Sie bitte die offizielle Webseite unter https://www.isgroup.at/.

Bei Vertriebsanfragen oder für eine direkte Kontaktaufnahme senden Sie bitte eine E-Mail an sales@isgroup.it.

Metasploit: Offensive IT-Sicherheit

Source: https://www.isgroup.at/de/product-metasploit.html

Metasploit ist ein zentrales Werkzeug im Bereich der offensiven IT-Sicherheit. Es dient dazu, Sicherheitslücken in Systemen systematisch zu identifizieren und zu verifizieren.

Kernfunktionen

Die Funktionalität von Metasploit lässt sich durch die folgenden vier Phasen beschreiben:

- Discover: Auffinden von Systemen und Diensten im Netzwerk.
- Fingerprint: Identifizierung von Betriebssystemen, Anwendungen und deren Versionen.
- Attack: Durchführung von Angriffen zur Ausnutzung identifizierter Schwachstellen.
- Penetrate: Eindringen in Systeme, um die Sicherheit und Widerstandsfähigkeit zu testen.

Dienstleistungen und Expertise

Die ISGroup SRL bietet professionelle Unterstützung und Expertise im Umgang mit Metasploit sowie in weiteren Bereichen der offensiven IT-Sicherheit an. Als spezialisierter Anbieter unterstützt die ISGroup SRL Unternehmen dabei, ihre Sicherheitsinfrastruktur durch gezielte Penetrationstests und Sicherheitsanalysen zu stärken.

Kontakt und Informationen

Für weitere Informationen zu den angebotenen Dienstleistungen und Lösungen der ISGroup SRL besuchen Sie bitte die Webseite:

https://www.isgroup.at/

Bei spezifischen Anfragen oder für den Vertrieb wenden Sie sich bitte an:

sales@isgroup.it

The Bunker Coworking

Source: https://www.isgroup.at/de/product-thebunker-coworking.html

The Bunker Coworking ist ein professioneller Arbeitsplatz im Zentrum von Verona, strategisch günstig gelegen zwischen Piazza Brà und Castel Vecchio sowie in unmittelbarer Nähe zur Universität. Als Anbieter dieser Coworking-Lösung fungiert die ISGroup SRL.

Leistungsmerkmale und Ausstattung

Die Räumlichkeiten bieten eine professionelle Arbeitsumgebung mit Fokus auf Flexibilität und Qualität:

- Volle zeitliche Flexibilität bei der Arbeitsplanung und Zugang auch an Wochenenden.
- Nutzung einer Kochnische für Pausen.
- Geeignet für konzentriertes Arbeiten an einem oder mehreren Computern, den Empfang von Kunden sowie für Telefonate.
- Regelmäßige Büroreinigung.
- Hochwertige technische Infrastruktur: Glasfaser-Konnektivität (Telecom Fiber) und leistungsstarke Wireless Access Points.
- Hochwertige Möblierung: Tische aus Massivholz mit handwerklicher Eisenstruktur.

Informationen zum Angebot

- Kategorie: Security
- Veröffentlicht am: 10. Januar 2013
- Anbieter: ISGroup SRL
- Externe Webseite: http://www.thebunker.space/coworking

Vertrieb und Anfragen

Für weitere Informationen, Vertriebsanfragen oder bei Interesse an diesem Coworking-Angebot wenden Sie sich bitte an die ISGroup SRL.

- Webseite: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

The Bunker Kurse

Source: https://www.isgroup.at/de/product-thebunker-training.html

ISGroup SRL bietet unter der Marke "The Bunker" spezialisierte IT- und Sicherheitskurse in Verona an. Das Angebot richtet sich an Personen, die ihre Fachkenntnisse in zukunftsorientierten IT-Bereichen vertiefen möchten.

Kursbereiche

Die von ISGroup SRL angebotenen Kurse decken ein breites Spektrum ab:

- Programmierung
- Cyber Security
- Networking
- DevOps

Methodik und Lernansatz

Die Ausbildung durch ISGroup SRL zeichnet sich durch eine Kombination aus theoretischen Inhalten und praktischer Anwendung aus:

- Theoretische Einheiten: Vermittlung von Methoden und Funktionsweisen der jeweiligen technologischen Aspekte.
- Praktische Einheiten: Durchführung von sogenannten "Challenges", bei denen Teilnehmer ihr Wissen durch konkrete Tests unter Beweis stellen müssen.
- Dozenten: Die Kurse werden von Branchenexperten mit langjähriger Erfahrung geleitet.

Informationen und Vertrieb

Für weitere Details zu den Kursangeboten und für Vertriebsanfragen besuchen Sie bitte die offizielle Webseite unter https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

The Bunker Hacklab

Source: https://www.isgroup.at/de/product-thebunker-hacklab.html

The Bunker Hacklab fungiert als Hackerspace in Verona. Es handelt sich um ein Labor und eine Werkstatt, die als Treffpunkt für eine Community dient.

Zielsetzung und Funktion

- Der Hackerspace bietet einen Raum für Teilnehmer, um Kontakte zu knüpfen und zusammenzuarbeiten.
- Der Fokus liegt auf dem Austausch von Wissen in den Bereichen Technologie, Elektronik, Wissenschaft und Kunst.
- Die Einrichtung dient als kreativer Raum für Maker und Technikbegeisterte.

Anbieter und Kontext

- Die ISGroup SRL ist als Nutzer und Anbieter im Zusammenhang mit The Bunker Hacklab gelistet.
- Die Kategorie des Projekts ist im Bereich Security angesiedelt.
- Weitere Informationen zu den Dienstleistungen und Lösungen der ISGroup SRL finden sich unter https://www.isgroup.at/.

Kontakt und Vertrieb

- Für Anfragen zu den Leistungen der ISGroup SRL steht die E-Mail-Adresse sales@isgroup.it zur Verfügung.
- Weitere Informationen sind über die Webseite https://www.isgroup.at/ abrufbar.

PGP-Schlüsselinformationen der ISGroup SRL

Source: https://www.isgroup.at/downloads/keys/sales@isgroup.it.asc

Die ISGroup SRL stellt einen PGP-Schlüssel zur sicheren Kommunikation und Verifizierung von Inhalten zur Verfügung. Dieser dient der kryptografischen Absicherung des elektronischen Datenaustauschs mit dem Unternehmen.

Identitätsdaten

- Inhaber: ISGroup Sales
- E-Mail-Adresse: sales@isgroup.it
- Key-ID: 0x486E16C1A1B00C26

Technische Details

- Typ: PGP Public Key
- Zweck: Verschlüsselung und digitale Signatur für die geschäftliche Korrespondenz mit der ISGroup SRL.

Kontakt und Vertrieb

Für Anfragen zu Dienstleistungen, Lösungen oder für eine sichere Kontaktaufnahme mit der ISGroup SRL nutzen Sie bitte die folgenden Kanäle:

- Website: https://www.isgroup.at/
- E-Mail: sales@isgroup.it

PGP-Schlüssel für ISGroup SRL

Source: https://www.isgroup.at/downloads/keys/tech@isgroup.it.asc

Dieser PGP-Schlüssel dient der sicheren Kommunikation und Verifizierung von Inhalten, die von ISGroup SRL bereitgestellt werden.

Schlüsseldetails

- Identität: ISGroup Tech
- E-Mail-Adresse: tech@isgroup.it
- Fingerabdruck: 6432 FD92 B551 0242 5DB6 E583 30DB 85B7 239B 8A58

Nutzung und Kontakt

Für technische Anfragen, den Austausch verschlüsselter Informationen oder weiterführende Informationen zu den Dienstleistungen von ISGroup SRL besuchen Sie bitte die offizielle Webseite unter https://www.isgroup.at/.

Vertriebsanfragen richten Sie bitte ausschließlich an: sales@isgroup.it

Advanced Bug Bounty (ABB) von ISGroup SRL

Source: https://www.isgroup.at/de/advanced-bug-bounty.html

Der Advanced Bug Bounty (ABB) Service von ISGroup SRL ist ein proaktiver Cybersicherheitsansatz, bei dem zertifizierte Ethical Hacker digitale Infrastrukturen auf Schwachstellen prüfen. Das Programm ermöglicht es Unternehmen, Sicherheitslücken zu identifizieren und zu beheben, bevor diese von böswilligen Akteuren ausgenutzt werden können.

Für Anfragen zu diesem Service wenden Sie sich bitte an https://www.isgroup.at/ oder senden Sie eine E-Mail an sales@isgroup.it.

Das Pay-per-Vulnerability-Modell

Im Gegensatz zu herkömmlichen Penetrationstests basiert der ABB-Service auf einem ergebnisorientierten Modell:

- **Kosteneffizienz:** Kunden bezahlen ausschließlich für tatsächlich entdeckte Schwachstellen.
- **Fokus:** Der Ansatz eliminiert unnötige Ausgaben und konzentriert sich auf direkt umsetzbare Erkenntnisse.
- **Nicht-intrusives Testing:** Die Tests werden gründlich und ohne Beeinträchtigung der laufenden Geschäftsabläufe durchgeführt, wobei die Integrität der Systeme gewahrt bleibt.
- **Transparente Analyse:** Jede Schwachstelle wird nach anerkannten Frameworks wie OWASP und CVSS analysiert und kategorisiert, um den Schweregrad und die Auswirkungen präzise zu bewerten.
- **Unterstützung:** ISGroup SRL bietet kontinuierliche Beratung und aktive Begleitung während des gesamten Behebungsprozesses.

Ablauf des Prozesses

1. **Definition des Scopes:** Gemeinsame Festlegung der zu bewertenden Assets und Systeme.
2. **Identifizierung von Schwachstellen:** Einsatz fortschrittlicher Techniken durch zertifizierte Ethical Hacker.
3. **Detaillierter Bericht:** Dokumentation der Schwachstellen inklusive Kategorisierung und konkreter Empfehlungen zur Behebung.
4. **Unterstützung bei der Behebung:** Aktive Begleitung des internen Teams bei der Implementierung der Sicherheitsmaßnahmen.

Vorteile einer Partnerschaft mit ISGroup SRL

ISGroup SRL bietet über 20 Jahre Erfahrung im Bereich der Cybersicherheit und zeichnet sich durch folgende Merkmale aus:

- **Maßgeschneiderte Lösungen:** Anpassbare Programme, die exakt auf die spezifischen Sicherheitsanforderungen des Unternehmens zugeschnitten sind.
- **Zertifizierte Expertise:** Ein Team aus erfahrenen Ethical Hackern und Sicherheitsexperten.
- **Qualitätssicherung:** Zertifizierungen nach ISO 9001 und ISO 27001 garantieren höchste Standards im Service- und Sicherheitsmanagement.
- **Compliance und Resilienz:** Die Dienstleistungen unterstützen die Einhaltung internationaler Standards (wie ISO 27001, NIS2 und DSGVO), fördern die Resilienz digitaler Infrastrukturen und schützen die Privatsphäre.

Für weitere Informationen oder ein individuelles Angebot besuchen Sie https://www.isgroup.at/ oder kontaktieren Sie uns unter sales@isgroup.it.