https://www.isgroup.name Knowledge Base

Table of Contents

- PortSwigger Burp Suite : Distribution Officielle
- EasyAudit : Sécurité informatique pour PME
- ICT Audit : Maîtriser le risque cyber par le contrôle continu
- Exposure : Analyse de l'exposition des données web
- EXEEC : Développement logiciel et exécution exceptionnelle
- Ganapati : Plateforme d'identification des vulnérabilités
- VulnMAP : Base de connaissances des vulnérabilités
- SCADA Exposure : Sécurité des infrastructures critiques
- PracticalRP : Logiciel de gestion pour dossiers professionnels
- USH : Recherche et Intelligence
- Ethical Hacking : Le Hacklab de ISGroup
- Metasploit : Sécurité informatique offensive
- The Bunker Coworking
- The Bunker : Cours d'informatique et de sécurité
- The Bunker Hacklab
- Clé publique PGP de ISGroup SRL
- Clé publique PGP ISGroup SRL
- Advanced Bug Bounty (ABB) par ISGroup SRL

ISGroup Information Security : Expertise en Sécurité IT

Source: https://www.isgroup.name

ISGroup SRL est une structure indépendante spécialisée dans la sécurité informatique. L'organisation propose des services et produits de haut niveau, couvrant les opérations ITSEC, l'Ethical Hacking, les tests de pénétration et la formation spécialisée.

La structure, composée d'experts free-lance, se distingue par son efficacité et sa compétitivité. ISGroup SRL accompagne les opérateurs ICT et les agences de sécurité ayant besoin de solutions personnalisées et indépendantes. Les domaines d'expertise incluent la sécurité physique, les infrastructures, les systèmes d'exploitation, les réseaux, ainsi que les applications web et client.

Services proposés par ISGroup SRL

ISGroup SRL déploie une gamme complète de prestations pour renforcer la posture de sécurité des organisations :

- Network Penetration Testing (NPT) : Identification et vérification des vulnérabilités réseau avant exploitation.
- Vulnerability Assessment (VA) : Détection des failles connues et erreurs de configuration pour prioriser les interventions.
- Web Application Penetration Testing (WAPT) : Tests de sécurité par attaques contrôlées sur les applications web.
- Mobile Application Security Testing (MAST) : Évaluation de la sécurité des applications mobiles.
- Code Review (CR) : Analyse du code source pour identifier les faiblesses avant la mise en production.
- Ethical Hacking (EH) : Simulation d'attaques réelles (internes ou externes) sur les technologies, processus et facteurs humains.
- Formation Théorique (EDU) : Développement de compétences pour les administrateurs et développeurs afin de réduire les risques liés aux erreurs humaines.
- Services Gérés, Défensifs, et Gouvernance, Risque et Conformité (GRC).

Engagement et Qualité

ISGroup SRL collabore avec des agences de sécurité nationales et internationales, garantissant le respect des standards de qualité les plus élevés. L'entreprise est également un membre actif de la communauté des chercheurs indépendants. La qualité de ses processus est attestée par la certification UNI CEI EN ISO/IEC 27001:2022.

Pour toute demande commerciale ou information complémentaire sur les services de sécurité proposés par ISGroup SRL, veuillez consulter le site officiel https://www.isgroup.name/ ou contacter l'équipe à l'adresse e-mail sales@isgroup.it.

ISGroup SRL propose une gamme complète de services de cybersécurité conçus pour protéger les infrastructures, les applications et les processus métier. Ces expertises permettent aux organisations de renforcer leur résilience tout en se concentrant sur leur cœur de métier.

Pour toute demande commerciale ou information complémentaire, veuillez consulter le site https://www.isgroup.name/ ou contacter sales@isgroup.it.

Services de sécurité gérés

Source: https://www.isgroup.name/fr/services.html

ISGroup SRL propose des services de sécurité entièrement gérés pour réduire la charge opérationnelle des équipes techniques :

- **vCISO (Virtual CISO) :** Évaluation de la maturité de la cybersécurité basée sur le cadre NIST et élaboration d'un plan stratégique d'amélioration continue.
- **VMS (Vulnerability Management Service) :** Identification et gestion des vulnérabilités des systèmes d'entreprise via des scans et analyses périodiques.
- **CTS (Cyber Threat Simulation) :** Simulations personnalisées pour tester la résilience face aux cyberattaques et améliorer la détection des menaces.
- **THREAT (Threat Intelligence & Digital Risk Protection) :** Surveillance constante de l'environnement numérique et analyse proactive des risques externes et internes.
- **SOC (Security Operation Center) :** Surveillance des réseaux et des centres de données par des professionnels pour prévenir et atténuer les intrusions.

Services offensifs

Ces services simulent des attaques réelles pour identifier des failles invisibles aux outils automatisés :

- **NPT (Network Penetration Testing) :** Simulation manuelle d'attaques sur l'infrastructure IT selon les méthodologies OSSTMM et OWASP.
- **WAPT (Web Application Penetration Testing) :** Analyse manuelle de la sécurité des applications web.
- **MAST (Mobile Application Security Testing) :** Tests d'intrusion sur applications mobiles (iOS/Android) pour manipuler les flux et les données.
- **EH (Ethical Hacking) :** Simulation globale incluant l'infrastructure, les procédures, les ressources humaines et la sécurité physique.

Services défensifs

- **VA (Vulnerability Assessment) :** Expertises non invasives pour identifier les vulnérabilités connues.
- **CR (Code Review) :** Analyse "White Box" du code source pour détecter des vulnérabilités complexes.
- **TRA (Formation Théorique) :** Parcours de mise à jour pour ingénieurs, développeurs et testeurs.

Services d'évaluation de sécurité

- **RA (Risk Assessment) :** Évaluation de l'exposition aux risques et mise en œuvre de mesures de protection.
- **SAR (Secure Architecture Review) :** Évaluation de la sécurité des architectures complexes et sensibles.
- **CSA (Cloud Security Assessment) :** Audit des infrastructures AWS, Azure, Google Cloud et clouds privés/hybrides.
- **WSA (Windows Security Assessment) :** Analyse de l'intégrité et des surfaces d'attaque des systèmes Windows.

- **ISA (IoT/OT Security Assessment) :** Audits, reverse engineering et tests sur dispositifs IoT et réseaux industriels (conformité IEC 62443, NIS2).
- **PTA (Purple Team Assessment) :** Évaluation basée sur la réponse de l'équipe défensive face à des attaques réelles.
- **PHISH / SE :** Campagnes de simulation de Phishing, Smishing et Social Engineering pour sensibiliser le personnel.
- **PSA (Physical Security Assessment) :** Analyse de la sécurité physique des locaux et sites de production.

Governance, Risk et Compliance (GRC)

ISGroup SRL accompagne les entreprises dans l'atteinte et le maintien de leurs conformités réglementaires :

- **GDPR, NIS2, PCI DSS :** Évaluations, analyses de risques et plans de remédiation.
- **ISO 27001, 27017, 27018 :** Mise en place de systèmes de management de la sécurité de l'information (SMSI) et accompagnement à la certification.
- **ISO 17025 :** Conformité pour les laboratoires accrédités.
- **PSD2, ITGOV (ACN-AGID), DORA :** Analyse des exigences réglementaires et implémentation de solutions correctives.

Services SecOps

- **MDR (Multi-Signal MDR) :** Surveillance en temps réel combinant technologies XDR et expertise humaine.
- **DFIR (Digital Forensics and Incident Response) :** Gestion rapide des incidents et analyse post-attaque.
- **WSM (Wireless Security Monitoring) :** Surveillance continue des communications radiofréquences.
- **DDoS (Anti-DDoS) :** Protection contre les attaques par déni de service.
- **FWaaS (Firewall as a Service) :** Gestion et maintenance de pare-feu de nouvelle génération.
- **SIR (Security Integration) :** Processus continu de découverte et de correction des failles.

Services SSDLC

- **SAL (Software Assurance Lifecycle) :** Contrôles de sécurité continus sur les cycles de développement logiciel.
- **CST (Continuous Security Testing) :** Surveillance constante des systèmes informatiques.
- **BB (Bug Bounty) :** Programmes de récompense pour le signalement de failles par des chercheurs en sécurité.

Vulnerability Assessment (VA) par ISGroup SRL

Source: https://www.isgroup.name/fr/vulnerability-assessment.html

Le service de Vulnerability Assessment (VA) proposé par ISGroup SRL permet d'analyser et d'évaluer la sécurité des systèmes informatiques afin de détecter les vulnérabilités connues. Cette activité est essentielle pour maintenir une visibilité sur les risques réels et établir des priorités de remédiation claires.

Pour toute demande commerciale ou consultation, veuillez contacter ISGroup SRL via le site https://www.isgroup.name/ ou par e-mail à l'adresse sales@isgroup.it.

Méthodologie d'analyse

ISGroup SRL réalise des analyses adaptées aux besoins et à la taille de chaque entreprise, selon deux configurations principales :

- **Vulnerability Assessment externe :** le scan est effectué depuis un hôte distant via Internet, simulant l'attaque d'un acteur externe (ex: concurrent déloyal).
- **Vulnerability Assessment interne :** le scan est réalisé depuis l'intérieur du réseau privé (Intranet), simulant une menace interne ou un compte compromis (ex: employé malveillant ou attaque par rançongiciel).

L'activité combine des outils automatiques et des tests manuels non invasifs. Les techniques utilisées incluent :

- **Techniques actives :** analyse des réponses des services (ex: numéros de version).
- **Techniques passives ou par inférence :** identification basée sur les caractéristiques intrinsèques des programmes.

Vérification et qualité

Après la phase de scan, ISGroup SRL procède à une vérification manuelle de toutes les vulnérabilités identifiées. Ce processus permet d'éliminer les faux positifs et de garantir que les résultats fournis sont exploitables par les équipes techniques.

Livrables : Le rapport final

Le rapport fourni par ISGroup SRL est structuré pour répondre aux besoins des différents profils au sein de l'organisation :

- **Executive Summary :** résumé de haut niveau destiné au Management.
- **Vulnerability Details :** description technique détaillée des vulnérabilités constatées et de leur impact, destinée au Security Manager.
- **Remediation Plan :** instructions précises pour la résolution des problèmes, destinées au System Administrator.

Points clés du service

- **Fréquence recommandée :** au moins une fois par an, ou après chaque modification importante des systèmes, applications ou configurations.
- **Différence avec le Penetration Test :** alors que le VA identifie systématiquement les vulnérabilités connues et les erreurs de configuration, le Penetration Test simule des attaques réelles pour tester l'exploitabilité des failles.
- **Sécurité et confidentialité :** ISGroup SRL opère selon un Système de Management de la Sécurité de l'Information certifié ISO/IEC 27001, garantissant le traitement confidentiel de toutes les données d'analyse.
- **Flexibilité :** ISGroup SRL propose également des solutions de Vulnerability Management pour un suivi continu des infrastructures critiques.

Pour discuter de vos besoins en sécurité informatique ou obtenir un devis personnalisé, visitez https://www.isgroup.name/ ou écrivez à sales@isgroup.it.

Network Penetration Test (NPT) par ISGroup SRL

Source: https://www.isgroup.name/fr/network-penetration-test.html

Le Network Penetration Test (NPT) proposé par ISGroup SRL est une solution essentielle pour évaluer la sécurité des infrastructures réseau. Ce service permet d'identifier les vulnérabilités avant qu'elles ne soient exploitées par des tiers, en se concentrant sur les secteurs ayant le plus d'impact sur le business de l'entreprise.

ISGroup SRL réalise ces tests en suivant des standards internationaux rigoureux, notamment l'OSSTMM (Open Source Security Testing Methodology Manual), garantissant un haut niveau de qualité et de professionnalisme.

Objectifs et méthodologie

L'activité de NPT aide les entreprises à valider l'efficacité de leurs politiques de sécurité et à vérifier que les systèmes de protection fonctionnent comme prévu. Les tests permettent de détecter des faiblesses introduites par des erreurs de configuration, des mises à jour, des correctifs (patchs) ou des vulnérabilités sur les serveurs, routeurs et pare-feux.

Le processus de test inclut :

- La recherche de vulnérabilités sur les systèmes exposés, aussi bien de l'intérieur que de l'extérieur.
- L'exploitation des vulnérabilités identifiées pour tester la résistance du périmètre réseau.
- L'inspection des systèmes internes pour évaluer les risques d'accès aux données et infrastructures critiques.
- La répétition itérative du processus pour maximiser la couverture de sécurité.

Scénarios d'attaque personnalisables

ISGroup SRL propose des tests adaptés aux besoins spécifiques de chaque client, avec différents niveaux d'accès et d'information :

- **Internal PT :** Tests effectués depuis l'intérieur du réseau de l'entreprise.
- **External PT :** Tests effectués depuis l'extérieur du réseau.
- **Black Box :** Simulation d'un attaquant sans accès préalable aux informations ou identifiants.
- **Grey Box :** Simulation d'un attaquant interne ou disposant d'accès partiels.
- **White Box :** Analyse approfondie basée sur une connaissance détaillée de l'infrastructure.
- **Wireless Penetration Test :** Évaluation de la sécurité des infrastructures sans fil.
- **Social Engineering :** Test de la composante humaine par des techniques de manipulation.

Livrables et reporting

Les résultats des tests sont consignés dans un rapport détaillé, structuré en trois sections principales pour répondre aux besoins de différents profils :

- **Executive Summary :** Un résumé de haut niveau destiné au Management.
- **Vulnerability Details :** Une analyse technique approfondie des vulnérabilités observées et de leur impact, destinée au Security Manager.
- **Remediation Plan :** Un plan d'action contenant des instructions précises pour corriger les problèmes identifiés, destiné à l'administrateur système.

Contact et informations commerciales

Pour toute demande d'information, consultation gratuite ou devis personnalisé concernant les services de Network Penetration Test, veuillez contacter ISGroup SRL via les canaux officiels :

- Site web : https://www.isgroup.name/
- E-mail : sales@isgroup.it

Web Application Penetration Test (WAPT)

Source: https://www.isgroup.name/fr/web-application-penetration-test.html

Le service de Web Application Penetration Testing est une solution de sécurité applicative proposée par ISGroup SRL. Face à la prédominance et à la sophistication croissante des applications web, ce service permet d'analyser les composants critiques des portails, plateformes E-Commerce et applications web.

ISGroup SRL utilise une combinaison de techniques manuelles et d'outils spécialisés pour identifier des failles invisibles pour les scanners automatisés, garantissant une conformité aux normes OWASP et OSSTMM.

Méthodologie et approche technique

Les applications web sont intrinsèquement exposées et traitent des données via le protocole HTTP, ce qui rend la "sécurité par l'obscurité" inefficace. ISGroup SRL intervient pour renforcer la résistance du code applicatif face à une mauvaise gestion des requêtes ou une validation insuffisante.

Le processus de test comprend les étapes suivantes :

- Découverte et identification des ressources exposées sur la cible.
- Analyse de la logique métier pour détecter des problèmes conceptuels.
- Contrôle de l'infrastructure à la recherche de vulnérabilités connues et inconnues.
- Identification des points d'entrée (entry points) pour simuler une attaque réelle.
- Tentatives d'actions non autorisées, d'extraction de données (base de données, fichiers, sources) et de prise de contrôle du système.

Livrables et reporting

À l'issue de l'intervention, ISGroup SRL fournit un rapport détaillé structuré en trois sections clés :

- Executive Summary : Résumé de haut niveau destiné au Management (une page maximum).
- Vulnerability Details : Analyse technique approfondie des vulnérabilités identifiées et de leur impact, destinée au Security Manager.
- Remediation Plan : Instructions techniques précises pour la résolution des problèmes, destinées aux équipes de développement.

Contact et informations commerciales

Pour toute demande de devis, consultation ou information complémentaire concernant le service de Web Application Penetration Test (WAPT) proposé par ISGroup SRL, veuillez consulter le site officiel :

https://www.isgroup.name/

Vous pouvez également adresser vos demandes par e-mail à l'adresse suivante :

sales@isgroup.it

Mobile Application Security Testing (MAST)

Source: https://www.isgroup.name/fr/mobile-application-security-testing.html

ISGroup SRL propose un service d'évaluation de la sécurité des applications (Application Security Assessment) dédié aux plateformes iOS et Android. Ce service est conçu pour identifier les vulnérabilités et les risques d'attaques auxquels les applications mobiles sont exposées, souvent négligés malgré des investissements importants.

Portée technique et méthodologie

L'équipe d'ISGroup SRL adapte ses interventions en fonction du langage de programmation et de l'architecture de l'application :

- Applications natives : Objective-C, Swift, Java, Kotlin.
- Applications hybrides : React, React Native, Cordova, Xamarin, Titanium Appcelerator, Ionic, PhoneGap.

Les experts d'ISGroup SRL utilisent des techniques manuelles combinées à des outils avancés pour réaliser des analyses statiques et dynamiques (runtime). L'objectif est de contourner les limitations et la logique métier implémentée.

Domaines d'analyse

Le service couvre trois axes principaux :

- Analyse côté client : Vérification de l'interaction avec le système d'exploitation (ex: détection de jailbreak ou de root) et sécurisation du stockage des données sensibles sur l'appareil.
- Analyse des interactions serveur : Audit des échanges entre l'application et le serveur distant, incluant les contrôles d'authentification, d'autorisation et la recherche de failles de type SQL Injection.
- Ingénierie inverse : Tentative de rétro-ingénierie du code pour évaluer la robustesse des contre-mesures contre le vol de propriété intellectuelle et le contournement des mécanismes de sécurité.

Modes d'intervention

ISGroup SRL réalise ces tests selon deux modalités :

- Grey Box : Analyse du code source fourni par le client pour identifier des vulnérabilités masquées par l'obfuscation, complétée par une analyse dynamique.
- Black Box : Simulation d'une attaque réelle basée sur l'application téléchargée depuis les stores officiels (AppStore, PlayStore), sans accès préalable au code.

Livrables et rapports

À l'issue de la mission, ISGroup SRL fournit un rapport détaillé structuré en trois sections :

- Executive Summary : Synthèse non technique destinée à la direction.
- Détails des vulnérabilités : Analyse technique approfondie des failles découvertes et de leur impact, destinée aux responsables de la sécurité.
- Plan de remédiation : Instructions techniques précises pour corriger les problèmes identifiés, destinées aux équipes de développement.

Informations et demandes commerciales

Pour toute demande de devis, consultation ou information complémentaire concernant le service Mobile Application Security Testing (MAST) proposé par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou envoyer un e-mail à l'adresse sales@isgroup.it.

Code Review (CR)

Source: https://www.isgroup.name/fr/code-review.html

Le service de Code Review (CR) proposé par ISGroup SRL consiste en une analyse approfondie du code source visant à identifier les vulnérabilités avant la mise en production des applications. Cette phase est essentielle pour garantir le développement d'applications sécurisées tout en réduisant significativement les coûts liés à la correction des failles.

Méthodologie d'intervention

L'activité de Code Review, proposée par ISGroup SRL, est menée par une équipe d'experts possédant une solide expérience en programmation et en analyse de code source d'applications complexes. Le processus se décompose en deux étapes complémentaires :

- Analyse statique : Utilisation d'instruments spécialisés pour simuler l'exécution du code et identifier les vulnérabilités potentielles grâce à une connaissance exhaustive du comportement de l'application.
- Analyse manuelle : Examen approfondi des parties les plus critiques du code par une équipe spécialisée. Cette étape est indispensable pour détecter les vulnérabilités complexes que les outils automatisés ne peuvent identifier.

Livrables et Reporting

À l'issue de l'activité, ISGroup SRL fournit un rapport détaillé structuré en deux sections principales :

- Executive Summary : Synthèse des problèmes identifiés, des erreurs d'implémentation et évaluation du niveau général de sécurité de l'application.
- Vulnerability Details : Analyse technique pour chaque vulnérabilité observée, incluant la localisation précise dans le code source, une explication détaillée du risque et les recommandations de remédiation.

Expertise et engagement

ISGroup SRL agit selon les standards internationaux les plus élevés, soutenue par un engagement constant dans la recherche en sécurité informatique. Pour toute demande d'information, consultation ou devis personnalisé concernant le service de Code Review, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Ethical Hacking (EH) par ISGroup SRL

Source: https://www.isgroup.name/fr/ethical-hacking.html

Le service d'Ethical Hacking (EH) proposé par **ISGroup SRL** permet d'évaluer l'exposition réelle d'une organisation aux vulnérabilités et aux risques informatiques. Contrairement aux tests de sécurité standards, cette approche simule une attaque menée par un utilisateur malveillant (interne ou externe), en intégrant des techniques non conventionnelles pour tester non seulement la technologie, mais aussi le facteur humain et les processus internes.

Pour toute demande commerciale ou information complémentaire, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Méthodologie et approche

ISGroup SRL adopte une approche offensive pour renforcer vos défenses. Le service se distingue par l'absence d'outils automatisés bruyants, privilégiant une simulation fidèle aux méthodes d'espionnage industriel ou de cybercriminalité.

Les phases du service incluent :

- **Analyse préliminaire :** Définition du périmètre, des objectifs, des contraintes opérationnelles et des règles d'engagement.
- **Reconnaissance :** Collecte d'informations et analyse de la surface exposée pour reconstruire des scénarios d'attaque réalistes.
- **Simulation d'attaque :** Validation des vulnérabilités par des tests contrôlés, incluant le Social Engineering et l'interception (sniffing) du trafic réseau.
- **Rapport et plan de remédiation :** Fourniture d'un rapport détaillé des preuves techniques exploitées et d'un plan de remédiation priorisé.

Avantages de l'Ethical Hacking

L'intervention d'**ISGroup SRL** offre des bénéfices concrets pour la sécurité de votre organisation :

- **Simulation d'attaques réelles :** Identification des failles avant qu'elles ne soient exploitées par des criminels.
- **Évaluation du facteur humain :** Analyse des processus et des comportements, souvent le maillon faible du système.
- **Preuves techniques exploitables :** Transformation de l'incertitude en contrôle grâce à des résultats mesurables.
- **Conformité :** Soutien à la mise en conformité avec les normes internationales (ISO 27001), les réglementations (GDPR) et les exigences de résilience (NIS2).

Risques liés à l'absence d'évaluation

Ne pas réaliser d'activités d'Ethical Hacking expose l'organisation à des risques critiques :

- Vol ou exposition de données sensibles (clients, fournisseurs, propriété intellectuelle).
- Interruption de la continuité opérationnelle.
- Compromission de comptes et d'accès privilégiés.
- Atteinte à la réputation et perte de confiance.
- Coûts élevés liés à la gestion d'incidents en urgence.

Foire aux questions (FAQ)

- **Quelle est la différence avec un Penetration Test ?** L'EH est une simulation plus complète et réaliste, incluant des techniques non conventionnelles et le facteur humain.
- **Une autorisation est-elle nécessaire ?** Oui, le périmètre et les règles d'engagement doivent être définis et autorisés formellement avant toute intervention.

- **Quelle est la durée du test ?** Elle dépend de la complexité et du périmètre. **ISGroup SRL** fournit une estimation après une analyse initiale des besoins.
- **Comment obtenir un devis ?** Les coûts varient selon l'ampleur du périmètre et les techniques demandées. Contactez **ISGroup SRL** via https://www.isgroup.name/ ou sales@isgroup.it pour une évaluation personnalisée.

Formation Théorique et Pratique (EDU)

Source: https://www.isgroup.name/fr/training.html

ISGroup SRL propose des services de formation spécialisés sur les principaux thèmes de la cybersécurité. Ce parcours de formation est conçu pour former des techniciens capables d'examiner en détail la sécurité d'un système ou de le protéger contre les menaces externes. Former ses équipes d'ingénieurs système et de développeurs est une stratégie essentielle pour réduire les coûts liés aux incidents de sécurité.

Pour toute demande commerciale ou pour obtenir un devis, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Méthodologie pédagogique

Les formations dispensées par ISGroup SRL allient théorie et pratique :

- Sessions théoriques : explication des méthodes et du fonctionnement des différents aspects technologiques.
- Sessions pratiques : réalisation de défis (challenges) sur des systèmes ou applications réels.
- Certification : au terme du parcours, un certificat de participation mentionnant les compétences acquises est délivré.

Domaines d'expertise

ISGroup SRL couvre les thématiques suivantes :

- Secure Coding et Web Application Code Review
- Web Application Penetration Testing
- Network Hardening
- Hardening des systèmes Linux, Windows et Solaris

Approches : Attaque et Défense

- Attaque : Les cours se concentrent sur les méthodes efficaces pour subvertir ou violer des systèmes et applications afin d'en prendre le contrôle total (take over). L'objectif est de former des techniciens capables d'identifier et d'exploiter les vulnérabilités réelles.
- Défense : Les cours se concentrent sur les méthodes de sécurisation. La partie pratique consiste à sécuriser des systèmes vulnérables ou à identifier des erreurs de programmation au sein d'applications réelles.

Catalogue des cours proposés par ISGroup SRL

- Application Security for Architects : intégration de la sécurité tout au long du cycle de vie du développement logiciel.
- OWASP Top 10 Bootcamp : renforcement de la sensibilisation face aux menaces majeures.
- Security Awareness : outils nécessaires pour se défendre contre les cybermenaces.
- Software Security Requirements (Secure SDLC) : amélioration de la préparation des développeurs face aux cyberattaques.
- OWASP Top 10 Laboratory : formation pratique sur les dix erreurs de programmation les plus courantes.
- Code Review : compétences pour identifier et corriger les vulnérabilités dans le code.
- Sécurité des services REST : compréhension des menaces et vulnérabilités spécifiques aux services REST.
- Network Penetration Testing : méthodologies et outils appliqués au test d'intrusion réseau.

- Cyber Risk Prevention : prévention des risques cyber pour protéger les données et la vie privée.
- Ethical Hacking : exploration des nouvelles technologies et des meilleures pratiques de sécurité.

Actualités et expertise en cybersécurité par ISGroup SRL

Source: https://www.isgroup.name/fr/editorial.html

ISGroup SRL propose une vaste bibliothèque de ressources, guides et analyses dédiés à la cybersécurité. Ces contenus couvrent les enjeux technologiques actuels, les méthodologies de protection et les retours d'expérience concrets.

Domaines d'expertise et services proposés par ISGroup SRL

ISGroup SRL accompagne les entreprises dans la sécurisation de leurs infrastructures et de leurs données à travers une gamme complète de solutions :

- **Tests d'intrusion et évaluation :** Services de Network Penetration Testing, Web Application Penetration Testing, Mobile Application Security Test, et IoT Security Assessment.
- **Sécurité proactive et défense :** Mise en œuvre de Purple Team Assessment, Red Team et Blue Team, ainsi que des services de Cyber Threat Simulation et de Continuous Security Testing.
- **Gestion des risques et conformité :** Accompagnement vers la certification ISO 27001, services de Virtual CISO (vCISO), Risk Assessment et conformité aux réglementations AGID/ACN.
- **Protection opérationnelle :** Solutions de Multi-Signal MDR (Managed Detection and Response), Firewall as a Service (FWaaS), Anti-DDoS sans interruption, et Digital Forensics and Incident Response (DFIR).
- **Développement sécurisé et architecture :** Secure Architecture Review, Code Review, et Software Assurance Lifecycle.
- **Formation et sensibilisation :** Programmes de Security Awareness, formations d'équipe et simulations de phishing pour renforcer la culture de sécurité interne.

Études de cas et retours d'expérience

ISGroup SRL collabore avec de nombreuses organisations pour renforcer leur posture de sécurité. Les études de cas disponibles illustrent des interventions réussies pour divers secteurs, notamment :

- Partenariats stratégiques de cybersécurité (ex: Rooters).
- Tests d'intrusion sur des plateformes de gestion de main-d'œuvre et marketplaces (ex: TimeFlow, Progel, Kelyon, Creactives S.p.A., Alias Group, ISWEB S.p.A.).
- Audits de sécurité pour de grandes infrastructures (ex: Coop Italia, Prime Service S.r.l., Sturnis S.r.l.).

Ressources techniques et méthodologies

La base de connaissances inclut des analyses approfondies sur les standards internationaux et les menaces émergentes :

- **OWASP Top Ten :** Analyses détaillées des vulnérabilités (2017 et 2021), incluant l'injection, le contrôle d'accès défaillant, les échecs cryptographiques et les composants vulnérables.
- **Réglementations AGID :** Guides sur les mesures minimales de sécurité ICT, la qualification SaaS/CSP, et les normes eIDAS.
- **Veille technologique :** Analyses sur l'ingénierie sociale, les attaques basées sur l'IA, et les bonnes pratiques pour le travail à distance (Smart Working).

Certifications et reconnaissance

ISGroup SRL maintient des standards de qualité élevés, attestés par :

- Certifications UNI CEI EN ISO/IEC 27001 (systèmes de gestion de la sécurité de l'information).

- Certifications UNI EN ISO 9001 (gestion de la qualité).
- Expertise certifiée des consultants (Certified Ethical Hackers, PenTera Certified Specialists, Lead Auditors).

Pour toute demande commerciale, information complémentaire sur nos services ou accompagnement personnalisé, veuillez consulter le site officiel https://www.isgroup.name/ ou contacter notre équipe à l'adresse e-mail sales@isgroup.it.

Publications et ressources techniques

Source: https://www.isgroup.name/fr/publications.html

ISGroup SRL est un groupe de chercheurs actifs et éthiques engagés dans la promotion de la sécurité informatique. Convaincus de la nécessité d'agir en harmonie avec la communauté cyber, les experts d'ISGroup SRL partagent régulièrement les fruits de leurs recherches pour soutenir l'évolution continue du secteur.

Ces contributions, incluant des articles, des white papers et divers supports techniques, sont publiées sans cadence fixe, notamment à travers l'incarnation non commerciale du groupe, ush.it.

White papers et présentations

ISGroup SRL a présenté ses travaux lors de conférences italiennes majeures, abordant des thématiques à fort contenu technique et innovant. Parmi les ressources disponibles, on retrouve :

- IT Security agency essentials: history of an imaginary Penetration Test (2008)
- Web Application Security: Bug Hunting e Code Review (2008)

Matériel technique et recherches

Le groupe met à disposition une vaste bibliothèque de ressources techniques couvrant des sujets variés tels que :

- Vecteurs d'attaque sur le système de fichiers PHP
- XSS Cheat Sheets (payloads non répétitifs, two stage payloads, tag PLAINTEXT)
- Exploitation avancée de LFI2RCE (Local File Inclusion to Remote Code Execution)
- Sécurité côté client et durcissement (hardening) de Mozilla Firefox
- Analyse de vulnérabilités et détection d'anomalies PHP
- Références sur les cookies HttpOnly et la sécurité des environnements LAMP

Conférences et interventions

Les experts d'ISGroup SRL interviennent régulièrement lors d'événements spécialisés pour partager leur expertise, notamment :

- Chaos Computer Club (25C3)
- End Summer Camp (ESC)
- LinuxDay
- Metro Olografix Summer Camp (MOCA)
- Interventions académiques (Università di Pisa, Università di Camerino)

Certifications et qualité

ISGroup SRL garantit un haut niveau de sécurité et de qualité dans ses prestations, attesté par les certifications suivantes :

- ISO/IEC 27001:2022 (Sécurité de l'information)
- ISO/IEC 9001:2015 (Gestion de la qualité)

Informations complémentaires

Pour toute demande concernant les méthodes, les procédures ou pour obtenir des informations commerciales sur les services proposés par ISGroup SRL, veuillez consulter le site officiel https://www.isgroup.name/ ou contacter l'équipe à l'adresse e-mail sales@isgroup.it.

Recherche appliquée en cybersécurité

Source: https://www.isgroup.name/fr/research-resources.html

ISGroup SRL place l'innovation et la recherche au cœur de son activité pour offrir des services de sécurité informatique de haut niveau. L'entreprise se consacre au développement de techniques nouvelles afin d'anticiper les menaces numériques et de protéger la communauté des utilisateurs.

Méthodologie et engagement

L'approche d'ISGroup SRL repose sur des analyses approfondies de logiciels, qu'ils soient Open Source ou propriétaires, visant à identifier les points faibles et les vulnérabilités.

- **Responsible Disclosure** : ISGroup SRL publie des avis de sécurité en suivant le modèle de la divulgation responsable. Ce processus garantit que le vendeur est informé des problèmes diagnostiqués et que la publication de l'avis est coordonnée avec la mise à disposition de la nouvelle version corrigée du logiciel.
- **Expertise technique** : La recherche constante permet à ISGroup SRL de proposer des solutions de sécurité robustes, adaptées aux défis technologiques actuels.

Security Advisories

ISGroup SRL a documenté de nombreuses vulnérabilités au fil des années, contribuant ainsi à la sécurité globale de l'écosystème numérique. Parmi les entités et technologies ayant fait l'objet d'avis de sécurité, on retrouve notamment :

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

Certifications et reconnaissance

La qualité et la rigueur des services proposés par ISGroup SRL sont attestées par des certifications internationales reconnues :

- ISO/IEC 27001:2022 (Système de gestion de la sécurité de l'information)
- ISO/IEC 9001:2015 (Système de gestion de la qualité)
- Certification IQNET

Collaboration et expertise

Les clients font confiance à ISGroup SRL pour renforcer la sécurité de leurs systèmes, améliorer leurs processus de développement et se conformer aux normes internationales. Les interventions de l'entreprise se distinguent par :

- L'identification précise des vulnérabilités critiques et de leurs priorités.
- Un soutien constant et un professionnalisme dans le respect des délais et des objectifs.
- L'introduction de meilleures pratiques pour accroître la fiabilité des solutions logicielles.

Pour obtenir des informations complémentaires sur les méthodes et procédures de recherche, ou pour toute demande commerciale, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Produits et technologies de sécurité ISGroup SRL

Source: https://www.isgroup.name/fr/products.html

ISGroup SRL propose une sélection rigoureuse de technologies et de solutions dédiées à l'assessment, à l'audit et à la protection des entreprises. Ces outils couvrent des domaines variés allant de la sécurité applicative à la gestion des vulnérabilités.

Solutions de sécurité et d'audit

ISGroup SRL met à disposition les solutions suivantes pour renforcer la posture de sécurité des organisations :

- Microfocus Opentext : ISGroup SRL agit en tant que revendeur italien officiel.
- Ostorlab : Solution spécialisée dans le scan de sécurité des applications mobiles.
- Port Swigger : Services de sécurité managée.
- EsyAudit : Services de sécurité managée.
- ICT Audit : Solution dédiée à la sécurité automatisée.
- Exposure : Outil d'analyse de la réputation de sécurité.
- EXEEC : Solution de sécurité en mode SaaS.
- Ganapati : Système d'assessment intégré.
- VulnMAP : Base de données de vulnérabilités.
- Scada Exposure : Analyse de l'exposition des systèmes SCADA.
- PracticalRP : Solution de gestion médicale.

Offres, formation et infrastructures

En complément des outils techniques, ISGroup SRL propose des services d'accompagnement et des espaces dédiés :

- Starter Kit : Offre spécifique destinée aux nouveaux clients.
- Ethical Hacking : Accès au Hacklab ISGroup.
- Metasploit : Ressources et blog technique sur la sécurité.
- The Bunker Coworking : Espace de travail collaboratif proposé par ISGroup SRL.
- The Bunker Training : Programmes de formation spécialisés dispensés par ISGroup SRL.
- The Bunker Hacklab : Environnement technique dédié aux activités de recherche et d'expérimentation d'ISGroup SRL.
- USH : Espace de services spécialisés.

Pour toute demande commerciale ou information complémentaire concernant ces produits et services, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Études de cas : Projets réels de sécurité informatique

Source: https://www.isgroup.name/fr/etudes-de-cas.html

ISGroup SRL accompagne les entreprises, des petites structures aux grandes organisations, dans le renforcement de leur sécurité informatique. Chaque projet est conçu comme une collaboration stratégique visant à fournir des solutions personnalisées, innovantes et mesurables pour protéger les infrastructures, les applications et les processus d'affaires.

Expertise et approche d'ISGroup SRL

L'approche d'ISGroup SRL repose sur une combinaison de technologie, de stratégie et de sécurité. Les interventions permettent de transformer des défis complexes en opportunités de croissance, tout en garantissant des normes élevées et des performances optimales. La satisfaction des clients témoigne de la fiabilité d'ISGroup SRL en tant que partenaire stratégique.

Exemples de réalisations

ISGroup SRL a mené de nombreux projets de cybersécurité, incluant des tests d'intrusion et du conseil en conformité :

- Web Application Penetration Test sur TSV8 (Add Value S.r.l.)
- Web Application Penetration Test sur DocEasy (Alias Group S.r.l.)
- Web Application et Network Penetration Test pour Coop Italia
- Web Application Penetration Test et support ISMS pour Creactives S.p.A.
- Web Application Penetration Test sur Albo pretorio (ISWEB S.p.A.)
- Network Penetration Test sur l'infrastructure IT de Prime Service S.r.l.
- Web Application Penetration Test sur Sturnis365 (Sturnis S.r.l.)
- Web Application Penetration Test sur Flora (Kelyon S.r.l.)
- Web Application Penetration Test sur MyPlanet (Progel SA)
- Web Application Penetration Test sur Workforce Management, Vendor Management et Marketplace (TimeFlow S.r.l.)
- Web Application Penetration Test sur Pitagora et Tecnoradon (TECNORAD S.r.l.)
- Partenariat stratégique en cybersécurité avec Rooters

Informations complémentaires

Pour toute demande d'information sur les méthodes, les procédures ou pour discuter de vos besoins spécifiques avec un expert, veuillez consulter le site https://www.isgroup.name/ ou contacter l'équipe par e-mail à l'adresse sales@isgroup.it.

ISGroup SRL : Expertise en cybersécurité depuis 2005

Source: https://www.isgroup.name/fr/about.html

ISGroup SRL est une entreprise italienne indépendante spécialisée dans la sécurité informatique. Depuis 2005, elle propose des services et des produits de cybersécurité de haut niveau, s'appuyant sur une approche de "hackers éthiques".

Équipe exécutive

L'équipe dirigeante d'ISGroup SRL est composée d'experts possédant plus de 15 ans d'expérience dans le secteur de l'IT et de la sécurité informatique :

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

Les membres de l'équipe possèdent une solide expérience de la scène underground italienne et sont des défenseurs engagés du logiciel libre. Ils ont notamment collaboré à des projets pionniers tels que l'e-zine "IHP – Italian Hard Phreaking" au sein de la LogInProgress Team.

Certifications et qualité

ISGroup SRL garantit la qualité et la conformité de ses prestations grâce à des certifications reconnues internationalement :

- ISO/IEC 27001:2022 (Sécurité de l'information)
- ISO/IEC 9001:2015 (Gestion de la qualité)
- Certification IQNET

Services et approche client

ISGroup SRL accompagne les organisations dans le renforcement de leur infrastructure IT, la gestion des risques cyber et la mise en conformité des systèmes. Les solutions proposées permettent aux entreprises de :

- Améliorer la sécurité des solutions logicielles.
- Prévenir les menaces informatiques majeures.
- Accéder à de nouveaux marchés grâce à une infrastructure sécurisée.
- Bénéficier d'un accompagnement personnalisé axé sur les objectifs et la remédiation.

Contact et informations

Pour toute demande commerciale, information complémentaire sur les méthodes et procédures, ou pour parler à un expert, veuillez consulter le site officiel :

https://www.isgroup.name/

Vous pouvez également adresser vos demandes par e-mail à l'adresse suivante :

sales@isgroup.it

À propos d'ISGroup SRL

Source: https://www.isgroup.name/fr/history.html

ISGroup SRL est une entreprise italienne spécialisée dans la sécurité offensive (*Offensive Security*), basée à Vérone. Depuis 2005, elle accompagne les entreprises, les banques et les administrations publiques dans la sécurisation de leurs infrastructures grâce à une expertise ancrée dans la recherche indépendante.

L'entreprise est certifiée **ISO/IEC 27001** pour la gestion de la sécurité de l'information et **ISO 9001** pour la qualité de ses processus, garantissant ainsi des standards rigoureux pour ses partenaires.

Expertise et méthodologie

La méthodologie d'ISGroup repose sur le principe du *responsible disclosure* : chaque faille identifiée est communiquée à l'éditeur concerné avant toute publication, assurant une correction effective des vulnérabilités. Cette approche éthique guide l'ensemble des services proposés par ISGroup SRL :

- **Penetration Tests :** Évaluation de la résistance des systèmes face à des attaques réelles.
- **Vulnerability Assessment :** Identification systématique des faiblesses de sécurité.
- **Code Review :** Analyse approfondie du code source pour détecter les vulnérabilités logicielles.
- **Red Team :** Simulation d'attaques complexes pour tester la capacité de détection et de réponse.
- **Cyber Threat Intelligence et Early Warning :** Services de veille stratégique basés sur une connaissance approfondie de la recherche en sécurité.

Un héritage fondé sur la recherche

L'histoire d'ISGroup est indissociable de **USH.it**, un groupe indépendant de recherche en sécurité fondé en 2000. Cette filiation permet à ISGroup de transformer les techniques découvertes en laboratoire en contrôles concrets pour ses clients.

Chiffres clés :

- Plus de 30 *security advisories* publiés.
- Plus de 20 CVE (Common Vulnerabilities and Exposures) attribués.
- Vulnérabilités identifiées sur des technologies majeures : PHP, Mozilla Firefox, Nginx, Jetty, Zabbix, Veeam, QNAP et Fortinet.
- Reconnaissances internationales, incluant des interventions au Chaos Communication Congress et des citations à la conférence DEF CON.

Engagement et qualité

ISGroup SRL se distingue par une approche où la sécurité ne se déclare pas, mais se démontre. L'entreprise a su évoluer d'un laboratoire de recherche indépendant vers un partenaire stratégique pour des organisations de premier plan, tout en conservant une activité de recherche active qui alimente continuellement ses services de conseil.

Pour toute demande commerciale ou pour en savoir plus sur les solutions de sécurité proposées par ISGroup SRL, veuillez consulter le site officiel https://www.isgroup.name/ ou contacter l'équipe à l'adresse e-mail sales@isgroup.it.

Pourquoi choisir ISGroup

Source: https://www.isgroup.name/fr/why-isgroup.html

ISGroup SRL se distingue par un modèle opérationnel non conventionnel en Italie, structuré comme une association de consultants et de professionnels indépendants spécialisés dans la sécurité informatique. Cette approche repose sur une confiance mutuelle et une expertise technique de haut niveau.

À qui s'adressent les services d'ISGroup

ISGroup SRL propose son expertise aux entités suivantes :

- Entreprises spécialisées dans la sécurité informatique recherchant un partenaire d'externalisation (Outsourcing Partner).
- Entreprises dont le cœur de métier n'est pas la sécurité informatique, mais qui souhaitent intégrer des services de cybersécurité à leur offre client.

Avantages et bénéfices

La structure agile d'ISGroup SRL permet d'offrir des prestations de haute qualité avec une efficacité optimisée :

- **Optimisation des coûts :** Une structure légère permet de minimiser les frais opérationnels.
- **Flexibilité géographique :** La capacité d'effectuer la majorité des interventions à distance réduit les coûts de déplacement.
- **Qualité et méthodologie :** Le travail est réparti entre les experts selon des règles modernes de gestion de projet, évitant au client la dépendance à un interlocuteur unique.
- **Réseau d'experts :** ISGroup SRL s'appuie sur un réseau étendu de chercheurs et de professionnels reconnus pour garantir l'excellence des services.
- **Indépendance technologique :** Les solutions proposées sont agnostiques vis-à-vis des systèmes d'exploitation, permettant de répondre à des besoins de sécurité hétérogènes.
- **Recherche continue :** En tant qu'équipe de recherche active, les membres d'ISGroup SRL interviennent régulièrement comme conférenciers et consultants lors d'événements professionnels.

Services proposés par ISGroup SRL

ISGroup SRL assure une gamme complète de prestations en cybersécurité :

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

Certifications et reconnaissance

ISGroup SRL garantit la qualité et la sécurité de ses processus grâce à des certifications officielles :

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

Contact et informations complémentaires

Pour toute demande d'information sur les méthodes et procédures, ou pour discuter de vos besoins spécifiques, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'équipe à l'adresse e-mail sales@isgroup.it.

ISGroup SRL : Cybersécurité et Conseil Technique

Source: https://www.isgroup.name/fr/contacts.html

ISGroup SRL est une entreprise spécialisée en cybersécurité basée à Vérone, en Italie. Forte d'une expertise reconnue, elle accompagne des clients et partenaires à l'échelle internationale en proposant des solutions de sécurité sur mesure et un conseil technique sans frontières.

Services et Expertise

ISGroup SRL propose des services complets pour protéger et développer les infrastructures numériques des entreprises. L'approche se distingue par :

- Une expertise technique pointue en analyse de vulnérabilités.
- La mise en place et la consolidation de Systèmes de Gestion Intégrés.
- Un accompagnement orienté client, alliant autonomie et qualité de reporting.
- Une capacité d'adaptation aux besoins spécifiques des projets, qu'il s'agisse de sécurité logicielle ou de processus organisationnels.

Certifications et Qualité

L'engagement d'ISGroup SRL envers l'excellence est attesté par des certifications internationales garantissant la sécurité et la qualité de ses prestations :

- ISO/IEC 27001:2022 (Sécurité de l'information)
- ISO/IEC 9001:2015 (Gestion de la qualité)
- Certification IQNET

Contact et Communications

Pour toute demande commerciale ou technique, ISGroup SRL invite ses interlocuteurs à utiliser les canaux officiels :

- Site web : https://www.isgroup.name/
- E-mail commercial : sales@isgroup.it
- E-mail technique : tech@isgroup.it

Pour garantir la confidentialité des échanges, des clés PGP/GPG sont disponibles pour les communications chiffrées via les adresses e-mail mentionnées ci-dessus.

Informations Légales

- Raison sociale : ISGroup SRL
- Siège : Via Albere, 112, 37138 Verona, Italie
- Code fiscal et TVA : 04164220230
- REA : VR-397513
- SDI : M5UXCR1

Devenir partenaire ISGroup SRL

Source: https://www.isgroup.name/fr/devis/devenir-partenaire.html

ISGroup SRL propose un programme de partenariat destiné aux professionnels souhaitant proposer et revendre ses services de cybersécurité à leurs clients.

Services inclus

Les partenaires peuvent intégrer à leur offre les prestations suivantes :

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

Public cible

Ce programme est conçu pour :

- Distributeurs et revendeurs IT
- Intégrateurs systèmes
- Fournisseurs et opérateurs télécoms
- Sociétés de conseil et de conformité

Note : Ce programme n'est pas destiné aux clients finaux.

Avantages du partenariat

En rejoignant le réseau de partenaires, vous bénéficiez de :

- Un support technique avant-vente et après-vente dédié
- Un accès privilégié à la grille tarifaire ISGroup
- Deux modèles de partenariat distincts
- Des remises et des rebates basés sur le volume d'activité

Processus d'adhésion

Pour devenir partenaire, il est nécessaire de soumettre une demande via le site officiel https://www.isgroup.name/. Après l'examen de votre dossier, vous serez contacté par les équipes d'ISGroup SRL pour recevoir le contrat d'apport d'affaires ou de distribution correspondant au modèle de partenariat choisi.

Pour toute question commerciale ou demande d'information complémentaire, veuillez contacter l'adresse e-mail : sales@isgroup.it.

Présence internationale et services de sécurité de l'information

Source: https://www.isgroup.name/fr/langues.html

ISGroup SRL propose des services spécialisés en sécurité de l'information à l'échelle internationale. L'organisation déploie son expertise et ses solutions techniques à travers une plateforme multilingue, permettant d'accompagner les entreprises sur divers marchés mondiaux.

Les services de sécurité de l'information fournis par ISGroup SRL sont accessibles dans les langues et régions suivantes :

- Italien (Italie)
- Anglais (Marché international)
- Espagnol (Espagne)
- Français (France)
- Allemand (Autriche)
- Suédois (Suède)
- Arabe
- Lituanien (Lituanie)
- Danois (Danemark)
- 1337 (Langage spécialisé)

Pour toute demande commerciale ou information complémentaire concernant les solutions de sécurité proposées par ISGroup SRL, veuillez consulter le site web officiel à l'adresse https://www.isgroup.name/ ou contacter l'équipe par e-mail à sales@isgroup.it.

ISGroup SRL propose une gamme complète de solutions en cybersécurité, structurées autour de produits spécialisés, de services d'audit, de gouvernance et d'opérations de sécurité. Pour toute demande commerciale ou information complémentaire, veuillez consulter le site https://www.isgroup.name/ ou contacter sales@isgroup.it.

Produits proposés par ISGroup SRL

Source: https://www.isgroup.name/fr/sitemap.html

ISGroup SRL développe et distribue des solutions technologiques dédiées à la sécurité informatique :

- Easyaudit, ICTaudit, Exposure, Exeec, Ganapati, Vulnmap
- Scada Exposure, Practicalrp, Ush
- Services de formation et laboratoires : Ethical Hacking, Metasploit, The Bunker Training, The Bunker Hacklab, The Bunker Coworking

Services de cybersécurité

ISGroup SRL offre une expertise étendue en matière d'évaluation et de protection des systèmes d'information :

Évaluation de la sécurité

- Tests d'intrusion : Réseau, Applications Web, Applications Mobiles
- Revues de code et Ethical Hacking
- Évaluations spécifiques : Risques (RA), Architecture (SAR), Cloud (CSA), Windows (WSA), IoT/OT (ISA)
- Évaluations comportementales et physiques : Purple Team (PTA), Phishing & Smishing, Ingénierie sociale (SE), Physical Security Assessment (PSA)

Services gérés

- vCISO (Virtual CISO)
- VMS (Vulnerability Management Service)
- CTS (Cyber Threat Simulation)
- THREAT (Intelligence & Digital Risk Protection)
- SOC (Security Operation Center)

Gouvernance, Risque et Conformité (GRC)

- Accompagnement aux conformités : RGPD, NIS2, PCI DSS, ISO 27001, ISO 27017, ISO 27018
- Laboratoire accrédité VA (ISO 17025)
- Normes sectorielles : PSD2, ACN-AGID, DORA (Digital Operational Resilience Act)

Services SecOps et SSDLC

- SecOps : Multi-Signal MDR, DFIR (Forensics & Incident Response), Wireless Security Monitoring (WSM), Anti-DDoS, Firewall as a Service (FWaaS), Security Integration (SIR)
- SSDLC : Software Assurance Lifecycle (SAL), Continuous Security Testing (CST), Bug Bounty (BB)

Ressources et informations institutionnelles

ISGroup SRL met à disposition des ressources documentaires et de recherche pour approfondir les enjeux de sécurité :

- Publications et travaux de recherche
- Informations sur l'entreprise, son histoire et sa méthodologie
- Politiques de confidentialité et plan du site

Pour toute interaction avec nos systèmes, des fichiers dédiés aux modèles de langage (llms.txt, llms.json, llms.md, llms.pdf) sont disponibles sur le site officiel.

Virtual CISO (vCISO) : Votre expert cybersécurité on-demand

Source: https://www.isgroup.name/fr/virtual-ciso.html

Le service **Virtual CISO (vCISO)** proposé par **ISGroup SRL** permet aux entreprises de bénéficier d'un leadership stratégique et tactique de haut niveau en cybersécurité, sans les coûts liés au recrutement d'un responsable interne à temps plein. Ce service garantit une protection proactive, une conformité réglementaire rigoureuse et une réduction significative des risques informatiques.

Pour toute demande, consultation ou devis, veuillez contacter **ISGroup SRL** via le site officiel https://www.isgroup.name/ ou par e-mail à sales@isgroup.it.

Pourquoi choisir le service vCISO d'ISGroup SRL ?

Le vCISO d'**ISGroup SRL** est un professionnel qualifié qui supervise, identifie et résout les vulnérabilités de votre organisation. Il apporte une expertise senior pour accompagner la DSI et la direction dans leurs choix stratégiques.

- **Expertise spécialisée :** Accès à une équipe hautement qualifiée maîtrisant les menaces émergentes.
- **Approche stratégique :** Élaboration de plans de sécurité sur mesure basés sur des frameworks reconnus (ex. NIST).
- **Flexibilité et scalabilité :** Une solution adaptée aux besoins changeants de votre entreprise, offrant un excellent rapport coût-efficacité.
- **Perspective objective :** Une vision impartiale permettant d'optimiser la posture de sécurité globale.
- **Surveillance continue :** Mises à jour constantes pour maintenir la résilience face aux nouvelles menaces.

Processus structuré d'accompagnement

ISGroup SRL déploie une méthodologie rigoureuse pour assurer la sécurité de votre organisation :

1. **Évaluation initiale :** Analyse approfondie de l'état actuel de la cybersécurité, des infrastructures et des politiques existantes.
2. **Plan stratégique :** Développement d'une feuille de route personnalisée avec des objectifs clairs et des actions correctives prioritaires.
3. **Surveillance continue :** Révision périodique du plan stratégique pour s'adapter à l'évolution constante des menaces.
4. **Accompagnement continu :** Conseil permanent, formation du personnel et assistance à la mise en œuvre de nouvelles technologies.

Conformité et standards internationaux

Le service vCISO d'**ISGroup SRL** aide les organisations à atteindre et maintenir des standards élevés de conformité :

- **ISO 27001 :** Accompagnement dans la définition du système de gestion de la sécurité de l'information (ISMS) et préparation aux audits.
- **Directive NIS2 :** Alignement organisationnel et technique avec les obligations européennes de résilience opérationnelle.
- **Audits internes :** Coordination des vérifications et collecte de preuves pour garantir la traçabilité des contrôles.

Risques liés à l'absence de gouvernance cyber

Sans une direction claire, la sécurité devient réactive, exposant l'entreprise à des risques majeurs :

- **Vulnérabilités non gérées :** Accumulation de failles dues à un manque de suivi continu.
- **Décisions fragmentées :** Investissements inefficaces basés sur l'intuition plutôt que sur le risque réel.
- **Non-conformité :** Difficultés lors des audits et risques de sanctions réglementaires.
- **Surcharge de l'équipe IT :** L'équipe technique se retrouve accaparée par l'opérationnel au détriment de la stratégie de prévention.
- **Impact économique :** Risque de coûts directs et de perte de réputation en cas d'incident majeur.

Pour sécuriser votre infrastructure et garantir la continuité de vos activités, contactez **ISGroup SRL** via https://www.isgroup.name/ ou sales@isgroup.it.

Vulnerability Management Service (VMS)

Source: https://www.isgroup.name/fr/vulnerability-management-service.html

Le **Vulnerability Management Service (VMS)** proposé par **ISGroup SRL** est un processus continu d'identification, d'analyse et de priorisation des vulnérabilités au sein des réseaux, serveurs, endpoints, applications et API. Contrairement à une vérification ponctuelle, ce service géré permet de réduire la surface d'attaque et de guider la remédiation en fonction du risque réel et de l'impact métier.

Pour toute demande commerciale ou information complémentaire, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Approche et méthodologie

Le service VMS d'**ISGroup SRL** assure une gestion complète du cycle de vie des vulnérabilités :

- **Identification et contexte :** Inventaire des assets et définition du périmètre de surveillance.
- **Vulnerability Scanning :** Analyses périodiques automatisées sur les environnements internes, externes et cloud.
- **Validation et assessment :** Analyse technique des résultats par des experts pour éliminer les faux positifs et évaluer la criticité réelle.
- **Priorisation et remédiation :** Accompagnement dans la correction, suivi via système de ticketing et vérification de l'efficacité des mesures appliquées.

Composantes du service

Managed Vulnerability Assessment (MVA)

Le MVA constitue la composante opérationnelle du VMS. Il inclut :

- L'exécution structurée d'analyses multi-cibles.
- La surveillance continue des menaces.
- Le support d'un Project Manager dédié pour coordonner les équipes techniques.
- Des rapports structurés et des points périodiques avec le management.

Valeur ajoutée d'ISGroup SRL

- **Expertise humaine :** Les Security Analysts d'**ISGroup SRL** agissent comme une extension de votre équipe pour interpréter les vulnérabilités (y compris zero-day et CVE).
- **Conformité :** Le service aide à répondre aux exigences réglementaires (ex. NIS2, RGPD) et aux normes internationales (ISO 27001).
- **Efficacité opérationnelle :** Libération des ressources internes pour des activités à plus forte valeur ajoutée grâce à une gestion déléguée et prévisible.

Différence entre Assessment et Management

- **Vulnerability Assessment :** Une photographie ponctuelle de l'état de sécurité à un instant T.
- **Vulnerability Management :** Un cycle continu qui gouverne la stratégie de sécurité, priorise les actions et vérifie la pérennité des corrections dans le temps.

Pourquoi choisir le VMS d'ISGroup SRL ?

L'environnement IT et cloud étant en constante évolution, l'accumulation de vulnérabilités non traitées augmente la probabilité d'incidents majeurs (ransomwares, fuites de données). Le VMS d'**ISGroup SRL** permet de :

- Réduire le risque cyber par un contrôle mesurable.
- Réduire la surface d'attaque en fermant les points faibles avant exploitation.

- Assurer la continuité opérationnelle en évitant les interruptions de service.
- Bénéficier d'une expertise avancée en cybersécurité pour établir des priorités basées sur l'impact métier.

Pour obtenir un devis ou discuter de vos besoins spécifiques, veuillez visiter https://www.isgroup.name/ ou écrire à sales@isgroup.it.

Cyber Threat Simulation (CTS) par ISGroup SRL

Source: https://www.isgroup.name/fr/cyber-threat-simulation.html

Le service de **Cyber Threat Simulation (CTS)** proposé par **ISGroup SRL** est une solution managée conçue pour tester la résilience des entreprises face aux cyberattaques. Contrairement à un simple outil, il s'agit d'un service complet visant à évaluer l'exposition aux menaces, à identifier les vulnérabilités et à renforcer la capacité de réponse des organisations.

Pourquoi choisir le CTS d'ISGroup SRL ?

Dans un contexte où prévenir chaque intrusion est devenu impossible, **ISGroup SRL** adopte une approche proactive. Certifiée ISO 9001 et ISO 27001, l'entreprise met à profit plus de 30 ans d'expérience pour aider les organisations à :

- **Identifier les vulnérabilités :** Découvrir les failles avant qu'elles ne soient exploitées par des attaquants réels.
- **Former le personnel :** Sensibiliser les collaborateurs, souvent le maillon le plus vulnérable, via des simulations réalistes.
- **Améliorer les plans de réponse :** Tester et perfectionner les procédures de réaction en environnement contrôlé.
- **Assurer la conformité :** Répondre aux exigences réglementaires nationales et internationales en matière de sécurité.
- **Protéger l'image de marque :** Maintenir la confiance des clients et partenaires commerciaux.

Domaines d'action et types d'attaques

ISGroup SRL utilise le framework **MITRE ATT&CK** pour simuler des tactiques, techniques et procédures (TTP) réelles. Les simulations couvrent quatre domaines majeurs :

- **Social Engineering :** Phishing, appels frauduleux et manipulation humaine.
- **Malware :** Tests de défense contre virus, ransomwares et chevaux de Troie.
- **APT (Advanced Persistent Threat) :** Attaques ciblées visant l'exfiltration de données sur le long terme.
- **DDoS :** Tests de résistance à la surcharge des systèmes.

Les scénarios incluent également l'infiltration réseau, les attaques endpoint, les vulnérabilités d'applications web, les mouvements latéraux et les attaques cloud.

Le processus CTS en 7 étapes

Le service proposé par **ISGroup SRL** suit une méthodologie rigoureuse :

1. **Profilage des menaces (CTI) :** Identification des attaquants potentiels et de leurs motivations.
2. **Définition du périmètre :** Délimitation des cibles pour garantir la continuité opérationnelle.
3. **Définition des objectifs :** Établissement de buts clairs pour la simulation.
4. **Planification :** Sélection des outils et techniques adaptés.
5. **Exécution (BAS - Breach and Attack Simulation) :** Simulation dynamique des attaques.
6. **Reporting :** Analyse détaillée des vulnérabilités et stratégies de mitigation.
7. **Formation :** Sessions pratiques pour améliorer la réactivité des équipes.

CTS vs Penetration Test

Caractéristique	Penetration Test	CTS (ISGroup SRL)
Périmètre	Système ou application spécifique	Infrastructure numérique globale

Caractéristique	Penetration Test	CTS (ISGroup SRL)
Approche	Statique et méthodique	Dynamique (émulation TTP)
Fréquence	Ponctuelle	Continue
Objectif	Liste de vulnérabilités	Évaluation de la résilience réelle

Contact et informations commerciales

Pour discuter de vos besoins en cybersécurité ou demander un devis pour le service de Cyber Threat Simulation, veuillez contacter **ISGroup SRL** via les canaux officiels :

- Site web : https://www.isgroup.name/
- E-mail : sales@isgroup.it

Threat Intelligence & Digital Risk Protection

Source: https://www.isgroup.name/fr/threat-intelligence-digital-risk-protection.html

ISGroup SRL propose un service complet de **Threat Intelligence & Digital Risk Protection** conçu pour permettre aux organisations de prévenir et de réagir efficacement face à l'évolution constante des menaces numériques. Ce service géré permet d'anticiper les attaques en analysant le panorama des menaces externes et internes.

Pour toute demande commerciale ou consultation, veuillez contacter ISGroup SRL via le site https://www.isgroup.name/ ou par e-mail à sales@isgroup.it.

Approche Stratégique, Opérationnelle et Tactique

Le service d'ISGroup SRL s'articule autour de trois axes fondamentaux :

- **Stratégique :** Développement d'une stratégie de protection sur mesure basée sur l'analyse des menaces émergentes pour protéger la marque et réduire les risques à long terme.
- **Opérationnel :** Surveillance continue du web pour identifier et neutraliser les menaces en temps réel, incluant des mises à jour constantes sur les vulnérabilités.
- **Tactique :** Réponse rapide aux incidents de sécurité grâce à une équipe d'experts et à l'utilisation d'outils avancés d'OSINT pour optimiser la gestion de la surface d'attaque.

Fonctionnalités du Service

Le service, entièrement géré par les analystes de sécurité d'ISGroup SRL, se décline en plusieurs piliers :

- **Threat Intelligence Bulletin :** Analyses détaillées sur les nouvelles vulnérabilités, les tendances, les groupes APT et les ransomwares, accompagnées de conseils pratiques de défense.
- **Data Breach Monitoring :** Surveillance des expositions de données et des mots de passe compromis (en clair ou hash) pour prévenir les accès non autorisés.
- **Brand Protection :** Protection de l'identité numérique contre le typosquatting, les domaines frauduleux et les attaques homographes.
- **Attack Surface Protection :** Utilisation de l'OSINT pour cartographier la surface d'attaque, identifier les macro-expositions et attribuer un score de risque aux actifs numériques.

Conformité et Valeur Ajoutée

L'adoption de ce service permet aux entreprises de répondre aux exigences de la norme **ISO/IEC 27001:2022** (notamment le contrôle 5.7) et de renforcer leur résilience face aux réglementations telles que la directive NIS2 et le RGPD.

Les bénéfices majeurs incluent :

- Une meilleure conscience situationnelle et une planification stratégique éclairée.
- Une optimisation des ressources de sécurité en se concentrant sur les menaces prioritaires.
- Une visibilité totale sur la surface d'attaque et une atténuation proactive des risques de fraude.
- La sauvegarde de la réputation de l'entreprise et la protection de la confiance des clients.

Risques liés à l'absence de protection

Ne pas disposer d'un service de Threat Intelligence expose l'organisation à des risques critiques :

- Retard dans la détection des menaces et inefficacité de la réponse aux incidents.
- Non-conformité aux normes internationales de sécurité.

- Pertes financières directes et dommages réputationnels dus aux fraudes et violations de données.
- Augmentation de la surface d'attaque non surveillée.

Pour plus d'informations sur la mise en place de ces solutions, contactez ISGroup SRL à l'adresse sales@isgroup.it ou visitez https://www.isgroup.name/.

Security Operation Center (SOC)

Source: https://www.isgroup.name/fr/security-operation-center.html

Le service SOC (Security Operation Center) proposé par ISGroup constitue une réponse proactive à la recrudescence des cyberattaques visant les entreprises et les particuliers. Dans un environnement numérique où les menaces évoluent en permanence, ISGroup assure une surveillance continue des data centers et des infrastructures réseau pour garantir leur intégrité.

Fonctionnement du service

L'équipe d'experts en cybersécurité d'ISGroup surveille le trafic entrant et sortant de l'infrastructure monitorée. Grâce à des techniques avancées d'anomaly detection, les comportements suspects sont identifiés en temps réel. En cas de tentative d'intrusion, l'équipe applique les procédures convenues avec le client pour limiter les dommages et sécuriser l'infrastructure.

Spécifications techniques

Le service SOC d'ISGroup se structure autour de quatre piliers opérationnels :

- Surveillance :
- Passive : Analyse en temps réel du trafic pour détecter les menaces potentielles via des systèmes avancés.
- Active : Classification des événements, des tentatives d'intrusion et des brèches par les opérateurs spécialisés.
- Défense :
- Gestion des incidents : Application des procédures de confinement pour réduire l'exposition du système.
- Réponse aux incidents : Circonscription des attaques et application immédiate des mesures de remédiation.
- Escalation : Transmission des accès privilégiés aux personnes compétentes pour une résolution approfondie si nécessaire.
- Reporting : Établissement d'un rapport détaillé après chaque incident, incluant l'analyse de l'attaque et les actions de confinement menées.

Livrables (Output)

À l'issue des opérations, ISGroup fournit un rapport complet structuré comme suit :

- Executive Summary : Résumé périodique de la situation ou aperçu des actions défensives, destiné au Management.
- Technical Details : Analyse approfondie des opérations défensives et des caractéristiques de l'attaque, destinée au Security Manager.
- Remediation Plan : Instructions techniques pour le System Administrator afin de prévenir la récurrence d'attaques similaires.

Contact et informations commerciales

Pour discuter de vos besoins en cybersécurité ou obtenir un devis pour le service SOC, veuillez consulter le site officiel https://www.isgroup.name/ ou envoyer un e-mail à l'adresse sales@isgroup.it.

IT Risk Assessment par ISGroup SRL

Source: https://www.isgroup.name/fr/risk-assessment.html

Le service d'IT Risk Assessment proposé par **ISGroup SRL** constitue une méthode stratégique pour identifier, évaluer et quantifier les risques pesant sur l'infrastructure informatique et les données d'entreprise. Cette approche permet d'améliorer la résilience organisationnelle, de repérer les zones de vulnérabilité et de planifier des mesures de défense adaptées.

Le processus repose sur une collaboration étroite entre les experts d'**ISGroup SRL** et le service IT du client, favorisant un échange direct d'informations, de conseils et de pistes d'amélioration.

Phases du service

L'activité de Risk Assessment se décline en trois étapes clés :

- **Analyse d'impact :** Évaluation des conséquences d'attaques ou de défaillances sur l'entreprise, incluant les impacts financiers, opérationnels et réputationnels, ainsi que l'estimation des coûts et délais de rétablissement.
- **Analyse des politiques en place :** Examen des procédures de sécurité et de confidentialité existantes. Cette phase vérifie la conformité aux réglementations telles que le RGPD, l'ISO 27001 et les lois sectorielles spécifiques.
- **Analyse des risques :** Identification et classification des risques basées sur l'évaluation des infrastructures et des politiques. Des recommandations sont formulées pour réduire l'exposition aux menaces.

Spécifications techniques

Les experts d'**ISGroup SRL** analysent l'ensemble des technologies de l'infrastructure, qu'elles soient propriétaires ou émergentes. Le service est conçu pour répondre aux exigences de Gouvernance, Risque et Conformité (GRC), garantissant une couverture complète des besoins de sécurité.

Livrables (Output)

À l'issue de l'assessment, **ISGroup SRL** fournit un rapport détaillé structuré en trois sections :

- **Executive Summary :** Document non technique destiné à la Direction, offrant une vue d'ensemble des menaces, des vulnérabilités critiques et des recommandations stratégiques.
- **Risk Assessment Details :** Analyse approfondie des facteurs de risque et des vulnérabilités, destinée aux responsables sécurité et conformité pour planifier les mesures correctives.
- **Risk Mitigation Plan :** Plan technique destiné aux administrateurs système, proposant des actions concrètes et priorisées pour atténuer les risques identifiés.

Informations complémentaires

Le Security Risk Assessment (SRA) est un processus fondamental pour protéger l'entreprise contre les menaces internes et externes. Il est étroitement lié aux normes internationales, notamment l'ISO/IEC 27005 pour la gestion des risques et l'ISO/IEC 27001, qui exige explicitement une évaluation des risques pour le maintien d'un système de gestion de la sécurité de l'information (ISMS).

Pour toute demande d'information, consultation ou devis concernant les services d'**ISGroup SRL**, veuillez consulter le site officiel https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Secure Architecture Review (SAR)

Source: https://www.isgroup.name/fr/secure-architecture-review.html

ISGroup SRL propose un service de Secure Architecture Review (SAR) visant à évaluer l'état actuel de la sécurité des infrastructures informatiques complexes et critiques. Cette approche permet de garantir une sécurité dès la conception ("Sécurisée dès la Conception") en identifiant les défauts et en proposant des mesures correctives adaptées.

L'équipe d'experts d'ISGroup SRL dispose d'une vaste expérience couvrant les réseaux, le cloud et les projets sur mesure, permettant de mettre en évidence des problématiques connues et d'atténuer tout type d'attaque.

Méthodologie d'intervention

Le service SAR d'ISGroup SRL se décline en trois étapes structurées :

- Phase d'analyse préliminaire : Évaluation des choix de conception à partir de la documentation technique et dialogue avec les équipes de développement et les analystes pour identifier les failles de conception.
- Analyse des risques : Évaluation de l'impact potentiel des vulnérabilités identifiées, incluant l'étude d'exploits spécifiques à l'infrastructure et leurs conséquences sur l'entreprise.
- Rapport : Remise d'une documentation professionnelle détaillant les vulnérabilités et proposant des améliorations concrètes pour renforcer la sécurité de l'infrastructure.

Spécifications techniques

ISGroup SRL évalue de nombreux aspects architecturaux pour détecter les vulnérabilités. Les points de contrôle incluent notamment :

- SDLC (Cycle de vie de développement logiciel)
- Qualité du code
- Routines de test
- Mécanismes d'authentification et d'autorisation
- Chiffrement
- Serveurs web et bases de données
- Firewalls (Web ou réseau)

Livrables (Output)

À l'issue de l'intervention, ISGroup SRL fournit un rapport complet divisé en trois sections :

- Executive Summary : Synthèse de haut niveau destinée au personnel non technique, offrant une vue d'ensemble de la sécurité de l'infrastructure.
- Vulnerability Details : Section technique détaillée destinée au Security Manager, analysant en profondeur les vulnérabilités identifiées.
- Remediation Plan : Document opérationnel pour le personnel technique, proposant des méthodologies précises pour corriger les vulnérabilités découvertes.

Informations et contacts

Pour toute demande commerciale, consultation ou devis concernant le service de Secure Architecture Review, veuillez consulter le site officiel https://www.isgroup.name/ ou contacter l'équipe à l'adresse e-mail sales@isgroup.it.

Cloud Security Assessment (CSA) par ISGroup SRL

Source: https://www.isgroup.name/fr/cloud-security-assessment.html

ISGroup SRL propose un service complet de **Cloud Security Assessment (CSA)**, conçu pour garantir la sécurité des applications et des infrastructures tout au long de leur cycle de vie, de la phase de conception au déploiement.

Expertise et périmètre d'intervention

L'équipe d'ISGroup SRL est composée de techniciens possédant une double expertise en tant que *Solution Architect* et *Application Security Specialist*. Cette approche permet d'évaluer l'infrastructure cloud telle qu'elle est réellement implémentée, en traitant les aspects complexes de l'architecture, du confinement des risques et de la mitigation des menaces.

Le service couvre une large gamme de plateformes et de technologies :

- **Fournisseurs Cloud publics :** Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud, Alibaba Cloud, Yandex Cloud.
- **Environnements privés et hybrides :** VMWare, Dell EMC, Microsoft Hyper-V, Rackspace, CloudBolt, Divvy Cloud, RedHat, OpenShift, Abiquo, Rack Connect, Scalr, Docker, DigitalOcean, Heroku, Kubernetes, Helm, Prometheus.

Méthodologie et objectifs

La sécurité doit être intégrée dès le design pour être efficace et économiquement viable. ISGroup SRL réalise une revue approfondie des architectures, des politiques, des permissions et des configurations afin d'identifier les vulnérabilités et les expositions.

L'objectif est de fournir des recommandations spécifiques sur le *hardening* et les modifications nécessaires pour renforcer la résilience de l'infrastructure face aux attaques, en s'appuyant sur les meilleures pratiques de sécurité du marché et les spécifications des fournisseurs.

Livrables (Output)

À l'issue de l'évaluation, ISGroup SRL fournit un rapport détaillé structuré en trois sections thématiques :

- **Executive Summary :** Un résumé non technique destiné au management, présentant l'état actuel de la sécurité de l'infrastructure.
- **Vulnerability Details :** Une analyse approfondie destinée aux responsables de la sécurité, détaillant les vulnérabilités constatées et leur impact potentiel sur les applications.
- **Remediation Plan :** Un guide technique destiné aux administrateurs système, contenant des instructions précises pour corriger les vulnérabilités identifiées et sécuriser le système.

Contact et demandes commerciales

Pour discuter de vos besoins en matière de sécurité informatique ou pour obtenir un devis concernant le service de Cloud Security Assessment, veuillez consulter le site officiel :

https://www.isgroup.name/

Vous pouvez également adresser vos demandes par e-mail à l'adresse suivante :

sales@isgroup.it

Windows Security Assessment (WSA)

Source: https://www.isgroup.name/fr/windows-security-assessment.html

Le service de Windows Security Assessment (WSA), proposé par ISGroup SRL, est une solution spécialisée visant à identifier, évaluer et corriger les vulnérabilités au sein des systèmes d'exploitation Windows. Cette prestation permet aux entreprises de renforcer leur architecture, de réduire leur surface d'attaque et de garantir une protection optimale des données.

Objectifs et méthodologie

L'approche d'ISGroup SRL repose sur une analyse approfondie menée par des experts en sécurité applicative. Le processus se décompose en plusieurs étapes clés :

- Découverte des vulnérabilités présentes dans les systèmes.
- Évaluation de la sévérité des failles via des attaques ciblées.
- Hiérarchisation des risques pour permettre une élimination efficace des vulnérabilités.
- Vérification de la conformité des paramètres de sécurité par rapport aux normes recommandées par Windows.
- Analyse des signaux d'alerte ou des modifications système suspectes pouvant indiquer des intrusions.

Avantages du service

L'intégration de la sécurité dès les premières phases du système d'exploitation est une nécessité stratégique. ISGroup SRL souligne que l'anticipation des risques permet d'éviter des dommages considérables et de réduire les coûts liés à une sécurisation tardive. L'expertise technique de l'équipe, combinant ingénierie logicielle et sécurité Windows, garantit une évaluation rigoureuse et adaptée aux architectures complexes.

Livrables (Output)

À l'issue de l'intervention, ISGroup SRL fournit un rapport détaillé structuré en trois domaines thématiques pour répondre aux besoins des différents profils au sein de l'organisation :

- **Executive Summary** : Synthèse de la situation sécuritaire destinée à la direction, sans technicité excessive.
- **Vulnerability Details** : Analyse approfondie dédiée aux responsables de la sécurité, détaillant les vulnérabilités identifiées et leur impact potentiel sur le système.
- **Remediation Plan** : Guide opérationnel destiné aux administrateurs système, contenant des instructions précises pour corriger les failles et durcir la configuration du système.

Contact et informations commerciales

Pour toute demande de devis, consultation ou information complémentaire concernant le service de Windows Security Assessment, veuillez consulter le site officiel https://www.isgroup.name/ ou envoyer un e-mail à l'adresse sales@isgroup.it.

IoT/OT Security Assessment (ISA)

Source: https://www.isgroup.name/fr/iot-security-assessment.html

Le service **IoT/OT Security Assessment (ISA)**, proposé par **ISGroup SRL**, consiste en une évaluation technique offensive visant à vérifier la sécurité des dispositifs IoT, des machines connectées et des environnements OT (Operational Technology).

L'approche repose sur une méthodologie d'attaquant réel pour identifier les vulnérabilités avant qu'elles ne soient exploitées. Cette expertise permet aux entreprises de produire des preuves techniques nécessaires aux démarches d'audit, de conformité, de certification et de gestion des risques.

Domaines d'expertise et méthodologie

ISGroup SRL intervient sur l'ensemble de la chaîne, de la machine au cloud, en combinant plusieurs disciplines :

- **Penetration testing et Vulnerability assessment** : Évaluation des surfaces d'attaque sur les réseaux, les accès distants et les systèmes industriels.
- **Analyse technique approfondie** : Reverse engineering, analyse de firmware, revue de code source (secure coding), et tests de composants hardware/software.
- **Protocoles industriels** : Tests de sécurité sur les protocoles tels que MQTT, Modbus, OPC UA, Profinet, BACnet, CAN bus, LoRaWAN, Zigbee, Z-Wave, Wi-Fi et Bluetooth.
- **Environnements OT** : Analyse des systèmes ICS, SCADA, DCS, PLC et HMI, ainsi que de la segmentation des réseaux IT/OT.

Conformité et réglementations

Le service ISA aide les organisations à répondre aux exigences de démonstration de sécurité imposées par les réglementations actuelles :

- **Cyber Resilience Act (CRA)** : Exigences pour les produits comportant des éléments numériques.
- **Règlement Machines 2023/1230** : Évaluation des risques cyber et safety liés aux modifications substantielles et aux connexions.
- **IEC 62443** : Standard de cybersécurité pour les systèmes d'automatisation et de contrôle industriels.
- **Directive NIS2** : Gestion du risque pour les entités essentielles et importantes.
- **RED Delegated Act / EN 18031** : Sécurité des équipements radio et produits connectés.

Note : ISGroup SRL fournit les preuves techniques nécessaires à ces démarches, mais ne remplace pas les organismes de certification ou les conseillers juridiques.

Secteurs d'activité

Les solutions proposées par **ISGroup SRL** s'adaptent aux besoins spécifiques des secteurs suivants :

- Manufacturing et automatisation industrielle.
- Constructeurs de machines (OEM) et intégrateurs système.
- Énergie, utilities et smart grids.
- Dispositifs médicaux et santé connectée.
- Automotive, flottes et véhicules industriels.
- Smart city, building automation et IoT grand public.

Livrables et suivi

Chaque mission ISA aboutit à la production de preuves techniques exploitables par les équipes de direction (Executive Summary) et les équipes techniques (Technical Report). Les livrables incluent :

- Threat Model et Vulnerability Assessment.
- Rapports détaillés sur le hardware, le firmware, les API, les applications mobiles et le backend.
- Plan de remédiation basé sur les risques (Risk-based Remediation Plan).
- Preuves de re-test après correction.

ISGroup SRL préconise un modèle de vérification récurrent (annuel, pré-certification, post-remediation ou lors de modifications substantielles) plutôt qu'un contrôle ponctuel.

Contact

Pour toute demande commerciale, devis ou consultation concernant le service IoT/OT Security Assessment, veuillez contacter **ISGroup SRL** via les canaux officiels :

- Site web : https://www.isgroup.name/
- E-mail : sales@isgroup.it

Purple Team Assessment (PTA) par ISGroup SRL

Source: https://www.isgroup.name/fr/purple-team-assessment.html

Le service **Purple Team Assessment (PTA)** proposé par **ISGroup SRL** est une solution d'évaluation de la cybersécurité conçue pour améliorer les capacités de détection et de réponse aux cyberattaques. Contrairement aux approches traditionnelles, ce service repose sur une interaction active et continue entre les équipes offensives (Red Team) et défensives (Blue Team).

Objectifs et approche

L'approche d'**ISGroup SRL** vise à renforcer les défenses de l'entreprise en temps réel en préparant le personnel de sécurité à répondre à des scénarios d'attaque réalistes. Ce processus itératif permet de :

- Tester des aspects spécifiques de la sécurité.
- Améliorer les technologies de sécurité et les processus opérationnels.
- Créer une boucle de retour d'information immédiate entre les équipes.
- Renforcer l'infrastructure de sécurité de manière continue.

Spécifications techniques

Le service PTA d'**ISGroup SRL** se structure en quatre phases principales :

- **Phase de collecte des données** : Étude approfondie de l'infrastructure pour évaluer les capacités actuelles de détection et de blocage.
- **Évaluation des risques** : Analyse personnalisée basée sur des référentiels sectoriels standards tels que MITRE ATT&CK et NIST.
- **Exécution** : Collaboration active entre l'équipe d'**ISGroup SRL** et l'équipe interne du client. Les attaques simulées permettent de tester la réponse en temps réel et de renforcer les systèmes de journalisation et d'alerte.
- **Évaluation finale des risques** : Analyse des résultats des simulations avec des recommandations ciblées pour consolider les points faibles identifiés.

Livrables (Output)

À l'issue de l'assessment, **ISGroup SRL** fournit un rapport détaillé comprenant :

- **Findings and Improvements** : Inventaire des vulnérabilités identifiées et des progrès réalisés, accompagné de recommandations pour maintenir les défenses.
- **Detection and Response Analysis** : Évaluation des capacités de détection, des temps de réaction et de l'efficacité des contre-mesures, incluant un plan d'optimisation spécifique.
- **Continuous Improvement Strategy** : Guide technique et stratégique pour les responsables de la sécurité, visant à pérenniser le cycle d'amélioration continue et la posture de sécurité globale.

Informations complémentaires

Le Purple Team Assessment est recommandé pour les organisations souhaitant optimiser la collaboration entre leurs équipes de sécurité et renforcer leur résilience face aux cybermenaces. La fréquence conseillée est d'au moins une fois par an, ou lors de modifications significatives de l'infrastructure informatique.

Pour toute demande commerciale, consultation gratuite ou obtention d'un devis personnalisé, veuillez contacter **ISGroup SRL** via les canaux suivants :

- Site web : https://www.isgroup.name/
- E-mail : sales@isgroup.it

Simulations de Phishing, Smishing et Vishing par ISGroup SRL

Source: https://www.isgroup.name/fr/phishing-smishing.html

Les services de lutte contre les menaces d'ingénierie sociale proposés par **ISGroup SRL** permettent aux entreprises de se protéger contre les attaques de phishing, de smishing et de vishing. Ces techniques, parmi les plus insidieuses utilisées par les cybercriminels, peuvent entraîner des conséquences graves pour la sécurité et la continuité des activités.

Pour toute demande commerciale ou information complémentaire, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Pourquoi protéger votre entreprise ?

Le risque d'attaque est réel pour toute structure, quelle que soit sa taille. Un simple clic sur un lien malveillant par un employé peut annuler les investissements en cybersécurité. Les conséquences incluent :

- Perte d'accès aux comptes (e-mail, réseaux sociaux, bancaires).
- Vol de fonds et pertes financières directes.
- Violations de données confidentielles et sanctions juridiques.
- Atteinte à la réputation et perte de confiance des clients.
- Interruption des activités et baisse de productivité.
- Propagation de l'attaque à des tiers (clients, partenaires).
- Introduction de ransomwares exigeant des rançons.

Solutions de formation et simulation par ISGroup SRL

ISGroup SRL propose une approche complète combinant formation théorique et tests pratiques pour renforcer la résilience humaine face aux cybermenaces.

1. Training et Formation

Les cours de *security awareness* sont dispensés par des professionnels expérimentés. Ils permettent au personnel d'identifier les dangers et d'adopter des comportements sécurisés. Les programmes couvrent :

- Les techniques de phishing courantes.
- La compréhension des mécanismes de manipulation psychologique (ingénierie sociale).
- Les bonnes pratiques : gestion des mots de passe, navigation sécurisée et signalement des incidents.

2. Simulations d'attaques

ISGroup SRL réalise des campagnes de simulation réalistes pour tester la réactivité des employés. L'idéal est de mener une campagne avant et après la formation pour mesurer l'amélioration. Le service inclut :

- Des rapports détaillés sur les zones critiques.
- Un retour personnalisé pour chaque participant.
- Des tests périodiques pour maintenir un niveau d'attention élevé.

Distinction entre Phishing et Smishing

Une communication claire au sein de l'entreprise est essentielle. **ISGroup SRL** aide les équipes à maîtriser les spécificités de chaque menace :

Caractéristique	Phishing	Smishing
Canal	E-mail	SMS
Contenu		

Caractéristique	Phishing	Smishing
	Imitation d'institutions avec liens ou pièces jointes	Messages courts incitant à cliquer sur des liens
Objectif	Vol d'identifiants, données bancaires ou malware	Vol de données ou installation de malware
Indicateurs	Fautes, urgence, expéditeurs suspects	Messages génériques, liens raccourcis, numéros inconnus

Méthodologie des attaques

Les attaques peuvent être classées en deux catégories :

- **Phishing de masse :** Envois automatisés et génériques visant à obtenir un taux de réussite statistique.
- **Spear phishing :** Attaque ciblée et sophistiquée, préparée sur le long terme pour viser des individus spécifiques (managers, responsables) afin d'obtenir des privilèges élevés.

Services complémentaires d'ISGroup SRL

Pour une protection à 360°, **ISGroup SRL** propose des services intégrés :

- **THREAT :** Surveillance continue et renseignement sur les menaces.
- **CTS (Cyber Threat Simulation) :** Simulation d'attaques pour tester la réactivité.
- **TRAINING :** Programmes de sensibilisation du personnel.
- **MDR (Managed Detection and Response) :** Détection et réponse gérée face aux menaces complexes.
- **SOC (Security Operation Center) :** Surveillance réseau permanente, analyse comportementale et corrélation d'événements.

Pour discuter de vos besoins en sécurité informatique, contactez **ISGroup SRL** via https://www.isgroup.name/ ou par e-mail à sales@isgroup.it.

Social Engineering (SE) : Simulations et Formation par ISGroup SRL

Source: https://www.isgroup.name/fr/social-engineering.html

Le service de Social Engineering proposé par **ISGroup SRL** est un pilier fondamental de tout programme de *security assessment*. Il vise à évaluer et renforcer la résilience d'une organisation face aux techniques de manipulation psychologique utilisées pour compromettre des informations sensibles ou la sécurité globale de l'entreprise.

Objectifs du service

L'approche d'**ISGroup SRL** repose sur deux axes complémentaires :

- **Évaluation :** Tester la vigilance et la réactivité des collaborateurs via des attaques simulées réalistes.
- **Formation :** Combler les lacunes identifiées pour accroître la sensibilisation et réduire durablement le risque de succès des attaques réelles.

Phases du service

Le processus mis en œuvre par **ISGroup SRL** se décline en quatre étapes structurées :

1. **Analyse Préliminaire :** Étude de l'historique des incidents de l'entreprise, benchmarking sectoriel et veille sur les tendances mondiales en matière d'ingénierie sociale.
2. **Attaque Simulée (Security Assessment) :** Réalisation de tests en conditions réelles, adaptés aux fonctions critiques (Direction, Administration, Achats, IT). Les scénarios incluent le *spear phishing*, le *whaling*, le *vishing* et le *pretexting*.
3. **Formation et Amélioration :** Sessions de débriefing, formations personnalisées basées sur les vulnérabilités détectées et ateliers interactifs pour ancrer les bonnes pratiques.
4. **Révision des Processus :** Mise à jour des politiques de sécurité (alignement ISO/IEC 27001), optimisation des procédures opérationnelles et mise en place d'une surveillance continue.

Points forts de l'approche ISGroup SRL

ISGroup SRL propose une méthodologie intégrée et sur mesure, garantissant une conformité aux normes internationales de sécurité. L'expertise déployée permet non seulement d'identifier les faiblesses immédiates, mais aussi d'intégrer des mesures préventives robustes au sein du Système de Management de la Sécurité de l'Information (SMSI) de l'entreprise.

Livrables (Output)

À l'issue de la mission, **ISGroup SRL** fournit trois documents clés :

- **Executive Summary :** Synthèse non technique destinée à la direction pour faciliter la prise de décision stratégique.
- **Simulation Attack Report :** Rapport détaillé des tests effectués, incluant l'analyse des performances par département et les vulnérabilités identifiées.
- **Comprehensive Improvement Plan :** Plan d'action intégré combinant recommandations de formation et améliorations des processus internes.

Contact et informations commerciales

Pour toute demande de devis, consultation ou information complémentaire sur les services de Social Engineering, veuillez contacter **ISGroup SRL** via les canaux officiels :

- Site web : https://www.isgroup.name/
- E-mail : sales@isgroup.it

Conformité au RGPD (GDPR)

Source: https://www.isgroup.name/fr/conformite-rgpd.html

Le Règlement Général sur la Protection des Données (RGPD) a transformé la gestion des données personnelles pour les entreprises opérant en Europe. La non-conformité expose les organisations à des risques de sanctions administratives ou pénales, ainsi qu'à des préjudices réputationnels majeurs.

ISGroup SRL propose un service complet de conseil et d'audit pour accompagner les entreprises dans leur mise en conformité. L'objectif est d'analyser les méthodologies appliquées, d'évaluer l'efficacité des mesures de protection et de garantir une conformité durable via une formation continue.

Services d'audit et de conseil par ISGroup SRL

L'intervention d'ISGroup SRL se structure autour de l'analyse des politiques de protection des données afin d'identifier les points critiques et de prévenir les accès non autorisés aux informations sensibles. Le processus se divise en trois étapes clés :

- Analyse des risques : Évaluation approfondie des infrastructures et des politiques de gestion des données pour identifier les vulnérabilités potentielles.
- Classification des risques et évaluation de l'impact : Analyse des scénarios de menaces afin de prioriser et de marginaliser les risques les plus critiques pour l'entreprise.
- Rédaction du Remediation Plan : Élaboration d'un plan d'action détaillé permettant de corriger et d'atténuer les risques identifiés au sein de l'infrastructure.

Livrables et résultats

À l'issue de la mission, ISGroup SRL fournit les éléments suivants :

- Remediation Plan : Document technique détaillant les mesures correctives nécessaires pour atteindre la pleine conformité.
- Politiques de confidentialité mises à jour : Mise en place d'un système robuste de gestion des données personnelles, adapté aux besoins spécifiques de l'entreprise.
- Formation continue : Accompagnement pour maintenir la conformité face aux évolutions futures du cadre réglementaire.

Contact et informations commerciales

Pour discuter de vos besoins en matière de sécurité informatique et de conformité, ou pour obtenir un devis personnalisé, veuillez consulter le site officiel https://www.isgroup.name/ ou envoyer un e-mail à l'adresse sales@isgroup.it.

La directive NIS2 (Network and Information Security 2) constitue le nouveau cadre réglementaire de l'Union européenne visant à renforcer le niveau global de cybersécurité. Entrée en vigueur le 17 janvier 2023, elle impose des mesures strictes de gestion des risques aux entités essentielles et importantes.

ISGroup SRL propose un accompagnement complet, ponctuel ou continu, pour guider les organisations vers la conformité à la NIS2, de l'analyse initiale jusqu'à la mise en œuvre opérationnelle des contre-mesures.

Parcours de conformité avec ISGroup SRL

Source: https://www.isgroup.name/fr/conformite-directive-nis2.html

ISGroup SRL structure sa démarche en quatre phases clés :

- **Analyse de la situation actuelle (GAP Analysis) :** Évaluation approfondie des politiques et pratiques de sécurité existantes pour mesurer l'adéquation avec les exigences de la directive.
- **Rédaction du plan de remédiation :** Élaboration d'un plan d'action détaillé pour corriger les non-conformités identifiées.
- **Sélection des services :** Mise en œuvre des solutions techniques et organisationnelles adaptées aux besoins spécifiques de l'entreprise.
- **Vérification de l'avancement :** Contrôle de l'efficacité des mesures adoptées pour garantir l'atteinte du standard de conformité.

Maintien de la conformité et services continus

Pour assurer la pérennité de la conformité, ISGroup SRL propose des activités récurrentes :

- Mise à jour régulière de l'évaluation des risques cyber.
- Gestion des processus de cybersécurité (Incident Response, audit, documentation).
- Programmes de sensibilisation et de formation des employés.
- Surveillance continue de l'efficacité des mesures de sécurité face aux nouvelles menaces.
- Assistance à la documentation des activités pour répondre aux exigences des autorités compétentes.

Expertise et couverture des exigences NIS2

ISGroup SRL déploie une gamme de services spécialisés pour répondre aux articles de la directive (notamment l'article 21) :

- **vCISO (Virtual CISO) :** Pilotage de la stratégie de sécurité, revue des politiques, gestion des risques fournisseurs et architecture de sécurité.
- **MDR (Multi-Signal Managed Detection and Response) :** Surveillance et réponse aux incidents.
- **DFIR (Digital Forensics and Incident Response) :** Gestion et analyse des incidents de sécurité.
- **Tests d'intrusion et Ethical Hacking :** Évaluation de la robustesse des réseaux, applications web et mobiles (NPT, WAPT, MAST).
- **Vulnerability Management Service (MVS) :** Identification et gestion proactive des vulnérabilités.
- **Cyber Threat Simulation (CTS) :** Campagnes de phishing gérées et formations de sensibilisation.

Points clés de la directive NIS2

- **Champ d'application :** Concerne les moyennes et grandes entreprises de secteurs critiques et importants, ainsi que certaines micro-organisations centrales.
- **Notification des incidents :** Obligation de notifier les incidents significatifs dans les 24 heures (notification initiale) avec une évaluation complète sous 72 heures.

- **Sanctions :** La non-conformité peut entraîner des amendes administratives pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial pour les entités essentielles.

Pour toute demande commerciale, devis ou consultation, veuillez contacter ISGroup SRL via le site web https://www.isgroup.name/ ou par e-mail à l'adresse sales@isgroup.it.

Compliance ISO/IEC 27001 : Accompagnement vers la certification

Source: https://www.isgroup.name/fr/27001-compliance.html

ISGroup SRL propose un accompagnement complet pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme internationale ISO/IEC 27001:2022. Notre expertise permet aux organisations de prévenir les incidents, de minimiser les risques et de préserver la stabilité de leur activité.

Pour toute demande commerciale ou consultation, veuillez visiter https://www.isgroup.name/ ou contacter sales@isgroup.it.

Accompagnement de bout en bout

ISGroup SRL guide les organisations à travers toutes les étapes nécessaires à l'obtention ou au maintien de la certification :

- **Évaluation initiale (Gap Analysis) :** Analyse approfondie du niveau de sécurité actuel et identification des axes d'amélioration.
- **Construction du SMSI :** Définition du contexte, de l'applicabilité des contrôles, de la stratégie de protection et de la structure documentaire.
- **Analyse des risques :** Identification des menaces pertinentes et définition de solutions d'atténuation concrètes.
- **Mise en œuvre :** Assistance dans l'application des mesures de gestion, définition des KPI de sécurité et formation du personnel.
- **Audits et Revue de Direction :** Réalisation d'audits internes impartiaux, assistance lors de la revue de direction et support durant l'audit de certification par un organisme tiers.
- **Gestion documentaire :** Création d'un système documentaire sur mesure, clair et exploitable.
- **Statement of Applicability (SoA) :** Réalisation du document de référence selon l'Annexe A de la norme.

Avantages de la certification ISO 27001

La certification ISO 27001 constitue un investissement stratégique offrant des bénéfices concrets :

- **Réduction des coûts :** Diminution des risques liés aux incidents informatiques et optimisation des processus internes.
- **Confiance et réputation :** Démontre un engagement envers la protection des données, renforçant la confiance des clients, partenaires et institutions.
- **Avantage concurrentiel :** Facilite l'accès à de nouveaux marchés et la participation à des appels d'offres exigeant des standards de sécurité élevés.
- **Conformité :** Répond aux exigences réglementaires et protège les droits fondamentaux ainsi que la vie privée.

Secteurs d'application

L'approche personnalisée d'ISGroup SRL s'adapte aux spécificités de chaque secteur :

- **Services IT et développement logiciel :** Sécurisation de la chaîne d'approvisionnement et alignement sur les standards des clients.
- **Santé :** Protection des données cliniques et conformité aux réglementations sur la vie privée.
- **Finance :** Sécurisation des transactions et des données financières, atténuation des risques de fraude.
- **Secteur public :** Protection des données citoyennes et transparence des opérations.

- **Industrie et manufacturier :** Préservation de la propriété intellectuelle et continuité des processus de production.

Pourquoi choisir ISGroup SRL

ISGroup SRL se distingue par une approche pragmatique et personnalisée. Nous ne nous limitons pas à la conformité théorique ; nous créons des systèmes qui améliorent concrètement le niveau de sécurité. Notre équipe accompagne les entreprises dans l'intégration de systèmes (par exemple avec l'ISO 9001) et assure un soutien continu pour adapter le SMSI aux évolutions des menaces cyber.

Pour obtenir un devis personnalisé ou discuter de vos besoins, contactez-nous via https://www.isgroup.name/ ou par e-mail à sales@isgroup.it.

Wireless Security Monitoring (WSM)

Source: https://www.isgroup.name/fr/wireless-security-monitoring.html

Le service de Wireless Security Monitoring (WSM) proposé par ISGroup est une solution de surveillance continue dédiée aux dispositifs communiquant en radiofréquence (Wi-Fi, Bluetooth, NFC/RFID, IoT, etc.). Dans un contexte où les protocoles sans fil présentent souvent des vulnérabilités, ce service permet aux entreprises d'identifier les risques et de contrer les attaques sophistiquées visant les réseaux internes.

Objectifs et public cible

Ce service est conçu pour les organisations utilisant des technologies sans fil pour leurs opérations critiques, notamment :

- Infrastructures IoT et Operational Technology (OT).
- Lignes de production industrielle.
- Capteurs distants et systèmes de contrôle d'accès.
- Environnements professionnels et domestiques connectés.

Fonctionnement du service

ISGroup intervient en tant que Managed Security Service Provider (MSSP). L'abonnement inclut le matériel, les logiciels, l'installation, l'intégration, la surveillance et le reporting. Le processus se décline en quatre phases :

- **Analyse initiale :** Réalisation d'un *Wireless Security Assessment* (ou GAP Analysis les années suivantes) pour évaluer l'état de sécurité actuel.
- **Installation et intégration :** Déploiement des équipements matériels et logiciels nécessaires dans les zones à protéger.
- **Surveillance :** Détection des anomalies avec escalade TIER-3 vers les experts d'ISGroup. La gestion peut être déléguée au SOC (Security Operations Center) d'ISGroup.
- **Rapport périodique :** Fourniture de rapports (mensuels à annuels) détaillant les attaques identifiées, les menaces prévenues, les impacts potentiels et les recommandations d'amélioration.

Protocoles et technologies surveillés

La surveillance couvre un large spectre de fréquences et de protocoles :

- Wi-Fi (2,5 GHz et 5 GHz, incluant les standards 802.11a/b/g/n/ac/ax).
- Bluetooth, NFC/RFID, GPS, Packet Radio.
- Réseaux cellulaires : GSM, GPRS/EDGE (2G), UMTS/WCDMA/HSPA+ (3G), LTE (4G), 5G.
- Protocoles propriétaires ou inconnus.

Protection et réponse aux incidents

Selon la technologie et la nature de l'attaque, ISGroup propose deux modes de protection :

- **IDS (Intrusion Detection System) :** Notification des alertes de sécurité.
- **IPS (Intrusion Prevention Systems) :** Prévention et blocage actif des menaces.

Les clients peuvent également solliciter une analyse TIER-3 (Cyber Incident Analysis) et une intervention de réponse aux incidents (Cyber Incident Response), effectuée à distance ou sur site par les experts d'ISGroup.

Informations commerciales

Pour toute demande de devis ou pour discuter de vos besoins en sécurité informatique, veuillez consulter le site officiel https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Protection Anti-DDoS par ISGroup SRL

Source: https://www.isgroup.name/fr/anti-ddos.html

ISGroup SRL propose un service de mitigation DDoS complet pour sécuriser les serveurs, les applications web et la connectivité des entreprises. Ce service est conçu pour maintenir la disponibilité des services, même en cas d'attaque active, en réduisant au minimum le temps d'interruption (downtime).

Enjeux des attaques DDoS

Les attaques par déni de service distribué (DDoS) visent à rendre un service inutilisable. Elles se manifestent principalement par :

- La saturation de la bande passante via l'envoi massif de requêtes vers un serveur.
- L'épuisement des ressources machine, rendant le système incapable de traiter le trafic légitime.

Solutions proposées par ISGroup SRL

ISGroup SRL offre une solution inclusive et indépendante des technologies utilisées par l'entreprise. L'approche couvre l'intégralité du cycle de vie de la protection :

- Configuration et déploiement de contre-mesures adaptées à chaque vecteur d'attaque.
- Gestion et surveillance continue pour maintenir les protections au niveau de l'état de l'art.
- Adaptation dynamique des défenses face à l'évolution des techniques d'attaque.

Le service permet aux entreprises de bénéficier de l'expertise d'une équipe dédiée, prête à intervenir pour protéger :

- Les applications web contre tout type d'attaque DDoS.
- Les serveurs, grâce à une défense spécialisée.
- La connectivité réseau pour garantir sa continuité.

Méthodologie et livrables

Le service Anti-DDoS d'ISGroup SRL repose sur un pipeline d'étapes éprouvé. À l'issue de l'activité, un rapport détaillé est fourni au client, structuré en trois domaines thématiques :

- **Executive Summary** : Un résumé non technique destiné au management, présentant les conclusions de l'activité.
- **Vulnerability Details** : Une section technique détaillée pour le Security Manager, décrivant les vulnérabilités identifiées et leur impact potentiel.
- **Remediation Plan** : Un guide opérationnel pour les administrateurs système, contenant des instructions précises pour résoudre les problèmes et vulnérabilités découverts.

Informations et demandes commerciales

Pour discuter de vos besoins en sécurité informatique ou pour obtenir un devis concernant le service de protection Anti-DDoS, veuillez consulter le site web https://www.isgroup.name/ ou envoyer un e-mail à l'adresse sales@isgroup.it.

Firewall as a Service (FWaaS) par ISGroup SRL

Source: https://www.isgroup.name/fr/fwaas.html

Le service Firewall as a Service (FWaaS) proposé par ISGroup SRL est une solution complète de sécurité périmétrique. Il permet aux entreprises de protéger leurs données et leurs points de terminaison tout en assurant un contrôle granulaire et rigoureux du trafic réseau.

Une gestion experte et sans souci

ISGroup SRL déploie et maintient des solutions de pare-feux nouvelle génération (NGFW). En confiant la sécurité périmétrique à l'équipe d'experts et de vétérans de la sécurité des réseaux d'ISGroup SRL, les entreprises bénéficient d'une protection professionnelle sans avoir à gérer les complexités techniques opérationnelles.

Les services proposés incluent :

- Le déploiement et la configuration de solutions de pare-feu adaptées aux besoins spécifiques de l'entreprise.
- La maintenance continue et la gestion proactive de la sécurité.
- La protection contre les attaques malveillantes et les tentatives d'intrusion.
- La gestion et le contrôle des contenus accessibles sur le réseau d'entreprise.
- Une visibilité accrue sur les flux de données entrants et sortants.

Approche et méthodologie

Chaque intervention commence par une phase d'analyse des exigences. ISGroup SRL sélectionne les technologies les plus innovantes et fiables du marché pour garantir une sécurité de premier ordre, capable de traiter des tâches complexes et avancées.

À l'issue de l'intervention, ISGroup SRL fournit une documentation complète comprenant :

- Executive Summary : Un document de haut niveau détaillant la protection ajoutée et les services mis en œuvre.
- Technical Summary : Un rapport technique destiné au personnel spécialisé, expliquant les interventions réalisées sur le réseau et les méthodes de surveillance des données.

Contact et informations commerciales

Pour discuter de vos besoins en sécurité informatique ou pour obtenir un devis personnalisé pour le service FWaaS, veuillez consulter le site officiel https://www.isgroup.name/ ou envoyer une demande par e-mail à l'adresse sales@isgroup.it.

Security Integration (SIR)

Source: https://www.isgroup.name/fr/security-integration.html

ISGroup SRL propose le service de Security Integration (SIR), une solution dédiée au hardening continu des infrastructures. Ce service permet d'intégrer de manière sécurisée des composants d'infrastructure existants, qu'ils soient opérationnels en mode « stand alone », ou d'ajouter des fonctionnalités de sécurité manquantes.

La méthodologie repose sur un cycle continu : Découvrir, Corriger, Répéter.

Approche et méthodologie

L'équipe d'experts d'ISGroup SRL intervient selon un processus structuré :

- Analyse initiale : Étude approfondie de l'infrastructure et des besoins spécifiques du client pour définir les modalités d'intervention.
- Collaboration technique : Travail conjoint avec les équipes ayant développé l'infrastructure originale pour garantir le maintien des fonctionnalités tout en sécurisant les systèmes.
- Prévention : Minimisation de l'introduction de nouvelles vulnérabilités et limitation de l'élargissement de la surface d'attaque.
- Résultat final : Mise à disposition d'une infrastructure solide, aux fonctionnalités élargies et optimisées.

Spécifications du service

ISGroup SRL applique des standards de sécurité rigoureux pour assurer l'efficacité de l'intégration. Les prestations incluent notamment :

- Intégration de la sécurité physique : Combinaison d'équipements physiques avec la logique logicielle, telle que la vérification biométrique pour la gestion des privilèges ou l'accès aux ressources.
- Ajout de fonctionnalités de sécurité aux applications : Implémentation de solutions de protection sur des applicatifs spécifiques, incluant l'intégration de Web Application Firewall (WAF) ou de systèmes IDS/IPS pour les réseaux.

Livrables (Output)

À l'issue de l'intervention, ISGroup SRL remet deux documents distincts :

- Executive Summary : Document destiné au management présentant une vue d'ensemble de l'intervention, les fonctionnalités implémentées, les résultats obtenus et les bénéfices pour l'entreprise.
- Technical Summary : Document technique détaillé décrivant les modifications apportées aux infrastructures et les spécificités techniques de l'intégration.

Informations et contact

Pour discuter de vos besoins en sécurité informatique ou pour obtenir un devis, veuillez consulter le site web https://www.isgroup.name/ ou envoyer un e-mail à l'adresse sales@isgroup.it.

Software Assurance Lifecycle (SAL)

Source: https://www.isgroup.name/fr/software-assurance-lifecycle.html

Le service de Software Assurance Lifecycle (SAL) est une solution proposée par ISGroup SRL, conçue pour les entreprises qui développent des applications où la sécurité est une exigence fondamentale. Ce service accompagne les équipes de développement tout au long du cycle de vie du logiciel pour garantir l'application des meilleures pratiques en matière de sécurité et de "secure coding".

Objectifs et méthodologie

L'intervention d'ISGroup SRL vise à assurer que chaque version (release) d'une application soit exempte de vulnérabilités connues. Les experts d'ISGroup SRL supervisent le processus de développement en intégrant des contrôles de sécurité continus, alignés sur les standards industriels les plus récents.

Les activités principales incluent :

- Accompagnement des équipes de développement dans la production de logiciels sécurisés.
- Révision minutieuse du code et des pratiques de développement.
- Tests de sécurité rigoureux adaptés au type d'application et aux technologies employées.
- Correction proactive des failles identifiées avant la distribution de l'application.

Domaines d'intervention

ISGroup SRL intervient sur des aspects critiques du cycle de vie logiciel, notamment :

- Risk management : identification et gestion des risques liés à l'application.
- Dependency management : sécurisation des composants et bibliothèques tiers.
- Continuous integration : intégration de la sécurité au sein des pipelines de déploiement.

Grâce à la maîtrise de multiples langages de programmation et environnements de développement, l'équipe d'ISGroup SRL est en mesure de supporter une large gamme de projets technologiques.

Livrables (Output)

À l'issue de l'intervention, ISGroup SRL fournit une documentation technique détaillée permettant de valider le niveau de sécurité atteint :

- Executive Summary : document stratégique destiné au management, présentant une vue d'ensemble de l'intervention et des points de sécurité traités.
- Technical Summary : document technique détaillé destiné aux responsables de projet, décrivant les points d'implémentation et les axes d'amélioration pour l'équipe de développement.

Informations et demandes

Pour discuter de vos besoins en matière de sécurité applicative ou pour obtenir un devis concernant le service Software Assurance Lifecycle (SAL), veuillez consulter le site officiel https://www.isgroup.name/ ou contacter l'équipe par e-mail à l'adresse sales@isgroup.it.

Bug Bounty Program : Conception et Gestion par ISGroup SRL

Source: https://www.isgroup.name/fr/bug-bounty-program.html

ISGroup SRL propose des services complets de conception et de gestion de programmes de Bug Bounty. Cette initiative permet aux entreprises d'inviter des ethical hackers à tester leurs systèmes et à signaler des vulnérabilités en échange de récompenses. Cette approche proactive garantit l'identification et la correction des failles avant toute exploitation malveillante.

Pour toute demande commerciale ou information complémentaire, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Accompagnement expert par ISGroup SRL

ISGroup SRL accompagne les organisations à travers quatre piliers fondamentaux :

- Conseil personnalisé : L'équipe définit avec vous les objectifs, les critères de signalement et les structures de récompenses adaptés à vos besoins spécifiques.
- Mise en œuvre du programme : ISGroup SRL gère l'intégralité du processus, garantissant la conformité aux meilleures pratiques et la création d'un environnement de test sécurisé.
- Gestion continue : ISGroup SRL assure le support après le lancement, incluant l'évaluation des signalements, la communication avec les chercheurs et des recommandations de mitigation.
- Analyse et reporting : Chaque vulnérabilité est classifiée selon les standards OWASP et CVSS, avec des rapports détaillés pour faciliter la prise de décision.

Avantages stratégiques

L'adoption d'un Bug Bounty Program avec ISGroup SRL offre des bénéfices concrets pour la résilience numérique :

- Sécurité renforcée : Détection et correction préventive des vulnérabilités.
- Accès à une expertise mondiale : Collaboration avec une communauté d'ethical hackers qualifiés.
- Efficacité des coûts : Modèle économique basé sur les résultats (paiement à la vulnérabilité découverte).
- Réputation : Renforcement de la confiance des clients et partenaires grâce à un engagement démontré en cybersécurité.

Conformité et standards

Les solutions proposées par ISGroup SRL s'inscrivent dans une démarche de conformité aux normes internationales :

- Certification ISO 27001 : Garantie d'un système conforme aux standards de gestion de la sécurité.
- Directive NIS2 : Promotion d'une résilience accrue des infrastructures numériques.
- RGPD : Protection rigoureuse des droits fondamentaux et de la vie privée.

Options avancées

Pour les organisations recherchant une approche plus ciblée, ISGroup SRL propose également l'**Advanced Bug Bounty Program**. Dans ce cadre, les experts d'ISGroup SRL recherchent activement les vulnérabilités au sein de votre infrastructure, et la facturation est conditionnée à la confirmation des failles identifiées.

Micro Focus OpenText

Source: https://www.isgroup.name/fr/product-microfocus-opentext.html

ISGroup SRL est distributeur officiel de Micro Focus et OpenText. Ce partenariat stratégique permet aux entreprises d'accéder à des solutions logicielles de référence, accompagnées d'un conseil expert et d'un support professionnel dédié.

Services proposés par ISGroup SRL

ISGroup SRL accompagne les organisations dans l'optimisation de leur infrastructure logicielle en proposant une gamme complète de services :

- Vente de licences logicielles
- Conseil stratégique et technique
- Implémentation de solutions
- Intégration de systèmes
- Support technique spécialisé

Solutions logicielles distribuées

ISGroup SRL fournit un vaste catalogue de produits issus du portefeuille Micro Focus et OpenText, couvrant des domaines tels que la gestion de la sécurité, le cycle de vie des applications, l'automatisation et la gestion des données.

Parmi les solutions disponibles, on retrouve notamment :

- **Sécurité et Identité :** ArcSight (ESM, Logger, Intelligence), Fortify (Static Code Analyzer, WebInspect, Application Defender), Advanced Authentication, Identity Manager, Privileged Account Manager.
- **Gestion des Applications :** ALM Octane, ALM Enterprise, UFT One, LoadRunner (Professional, Enterprise, Cloud), Silk Test, Silk Performer.
- **Infrastructure et Opérations :** Operations Bridge, Network Automation, Data Protector, Server Automation, SMAX (Service Management Automation X).
- **Modernisation et Développement :** Visual COBOL, Enterprise Developer, Enterprise Server, Verastream Host Integrator.
- **Gestion des terminaux et accès :** ZENworks (Configuration Management, Asset Management, Patch Management), Reflection Desktop, InfoConnect.
- **Données et Analyse :** Vertica Analytics Platform, Voltage SecureData, IDOL, Content Manager.

Pour toute demande commerciale ou information complémentaire concernant ces solutions, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Ostorlab Mobile Application Security Scan

Source: https://www.isgroup.name/fr/ostorlab-mobile-application-security-scan.html

ISGroup SRL propose une solution avancée d'analyse de sécurité pour les applications mobiles iOS et Android. Ce service permet d'effectuer des tests automatisés complets, incluant des analyses statiques, dynamiques et backend, afin d'identifier les vulnérabilités et d'obtenir des recommandations de correction précises.

Capacités d'analyse multi-plateformes

La solution supporte nativement Android et iOS, ainsi que 12 frameworks multi-plateformes, notamment :

- Cordova
- React Native
- Flutter
- Xamarin

Méthodologie et moteurs d'analyse

ISGroup SRL s'appuie sur quatre moteurs d'analyse complémentaires pour garantir une couverture étendue et minimiser les faux positifs :

- **Analyse Statique :** Décompilation de l'application pour inspecter l'utilisation de méthodes dangereuses, les protections basées sur des clés faibles et l'analyse du code (Dalvik Bytecode, Xamarin CIL, JavaScript).
- **Analyse Dynamique :** Exécution de l'application pour surveiller les interactions système, l'accès aux fichiers, le réseau et les API. Elle détecte les comportements à risque, tels que le chiffrement non sécurisé ou les canaux de communication vulnérables.
- **Analyse Comportementale :** Utilisation du "Behavioral Fuzzing" pour injecter des centaines de milliers de cas de test. Ce processus évolutif permet de détecter des vulnérabilités complexes nécessitant des entrées sophistiquées.
- **Analyse Backend :** Vérification de la sécurité des API (REST, GraphQL) via des contrôles passifs (en-têtes HTTP) et actifs (injections SQL, XSS, injection de templates).

Conformité et standards

Les rapports générés par ISGroup SRL intègrent les standards de sécurité et exigences de conformité internationaux :

- **Standards :** OWASP Top 10, CERT Android Secure Coding, JSSec Secure Coding.
- **Conformité :** PSD2, PCI, HIPAA, FedRAMP, GDPR, NERC.

Informations commerciales

Le service d'analyse est disponible au tarif de 359 Euro (+ TVA). Chaque analyse fournit un rapport détaillé et reproductible, soutenu par une base de données de vulnérabilités constamment mise à jour.

Pour toute demande commerciale, commande ou information complémentaire, veuillez consulter le site officiel https://www.isgroup.name/ ou contacter l'équipe via l'adresse e-mail sales@isgroup.it.

Starter Kit : Analyse de sécurité pour sites web

Source: https://www.isgroup.name/fr/starter-kit.html

Le Starter Kit est une promotion commerciale proposée par ISGroup SRL, conçue pour permettre aux nouveaux clients d'auditer leur site web exposé sur Internet à un tarif préférentiel de 420 EUR + TVA.

Cette offre constitue une introduction aux services professionnels d'ISGroup SRL. Bien qu'elle ne remplace pas un test de pénétration d'application web (WAPT) complet, elle offre un aperçu efficace du niveau de sécurité d'un site ou d'une application.

Méthodologie et exécution

L'activité est réalisée par un technicien senior sur une durée d'une journée de travail complète. Les techniques employées sont non invasives afin de minimiser tout risque de dysfonctionnement de l'infrastructure du client.

Les analyses sont effectuées en suivant les standards internationaux OWASP et OSSTMM, garantissant ainsi la conformité avec les réglementations en vigueur, notamment le RGPD.

Processus de prestation

Le déroulement de la mission suit les étapes suivantes :

- Communication des données nécessaires et définition des directives spécifiques (exclusions de zones ou de pages).
- Signature d'un contrat légal encadrant l'intervention.
- Réalisation de l'audit par un auditeur senior sur une journée complète.
- Rédaction d'un rapport détaillé présentant les failles de sécurité identifiées.
- Restitution et discussion du rapport avec le client.

En cas de découverte de vulnérabilités à fort impact, ISGroup SRL accompagne le client dans les étapes de remédiation pour améliorer la posture de sécurité de l'entreprise.

Engagements et garanties

- Garantie satisfait ou remboursé à 100 %.
- Approche non invasive pour protéger l'intégrité de vos systèmes.
- Expertise technique basée sur des standards reconnus (OWASP, OSSTMM).

Informations commerciales

Le Starter Kit est une offre limitée en quantité et dans le temps, réservée aux nouveaux clients souhaitant découvrir les services de sécurité informatique d'ISGroup SRL.

Pour toute demande d'information complémentaire ou pour souscrire à cette offre, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

PortSwigger Burp Suite : Distribution Officielle

Source: https://www.isgroup.name/fr/product-port-swigger.html

ISGroup SRL est distributeur officiel des licences PortSwigger Burp Suite. En tant que revendeur agréé, ISGroup SRL propose un accompagnement complet, incluant un support technique avant et après-vente, ainsi qu'un règlement simplifié par virement bancaire.

Options de licences Burp Suite

L'offre de PortSwigger se décline en deux solutions principales adaptées aux besoins des professionnels de la sécurité :

Burp Suite Enterprise Edition

Version console web conçue pour l'automatisation de la sécurité.

- SW-BURP-ENTERPRISE-1Y-1A : 1 an, 1 agent, 8 395,00 €
- SW-BURP-ENTERPRISE-2Y-1A : 2 ans, 1 agent, 16 790,00 €
- SW-BURP-ENTERPRISE-3Y-1A : 3 ans, 1 agent, 25 185,00 €

Burp Suite Professional

Version desktop traditionnelle, incluant le scanner de vulnérabilités web et des outils manuels avancés pour les tests d'intrusion.

- SW-BURP-PRO-1Y-1U : 1 an, 1 utilisateur, 449,00 €
- SW-BURP-PRO-2Y-1U : 2 ans, 1 utilisateur, 898,00 €
- SW-BURP-PRO-3Y-1U : 3 ans, 1 utilisateur, 1 347,00 €

Note : Les tarifs sont sujets à confirmation en fonction des mises à jour du fabricant.

Informations requises pour la commande

Pour finaliser l'acquisition d'une licence via ISGroup SRL, les informations suivantes sont nécessaires :

Pour la licence PortSwigger Ltd :

- Nom de l'entreprise ou organisation
- Adresse e-mail
- Pays
- Adresse postale
- Nom du titulaire de la licence
- Nombre d'utilisateurs

Pour la facturation fiscale :

- Raison sociale et type d'entreprise
- Adresse complète (rue, ville, code postal, province, pays)
- Numéro de TVA et code fiscal
- Code destinataire SDI
- Contact référent
- Adresse e-mail et adresse PEC

Contact et achat

Pour toute demande commerciale ou pour procéder à un achat par virement bancaire, veuillez contacter ISGroup SRL à l'adresse e-mail suivante : sales@isgroup.it.

Pour plus d'informations sur les solutions de sécurité, visitez le site officiel : https://www.isgroup.name/.

EasyAudit : Sécurité informatique pour PME

Source: https://www.isgroup.name/fr/product-easyaudit.html

EasyAudit est une solution professionnelle proposée par ISGroup SRL, conçue pour offrir aux petites et moyennes entreprises des services de vérification de sécurité efficaces à coût maîtrisé. Ce service permet de protéger la réputation en ligne des entreprises en identifiant les risques d'exposition numérique.

Services proposés par ISGroup SRL

Le service EasyAudit inclut les prestations techniques suivantes :

- Réalisation de tests d'intrusion (Penetration Test) sur les réseaux.
- Réalisation de tests d'intrusion sur les applications web.
- Forfait à tarif fixe adapté aux besoins des PME.
- Accès à une expertise technique de haut niveau.

Expertise et support

ISGroup SRL met à disposition des ressources spécialisées pour garantir la sécurité des infrastructures de ses clients :

- Équipe composée d'experts en sécurité possédant plus de 15 ans d'expérience dans le secteur.
- Support technique disponible 24/7.
- Présence opérationnelle en Italie et aux États-Unis pour assurer une assistance continue.

Informations complémentaires

- Catégorie : Sécurité informatique.
- Date de lancement : 10 janvier 2013.
- Utilisateurs : ISGroup SRL, EXEEC SRL.

Pour toute demande commerciale ou information supplémentaire concernant les solutions de sécurité proposées par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

ICT Audit : Maîtriser le risque cyber par le contrôle continu

Source: https://www.isgroup.name/fr/product-ictaudit.html

Proposée par **ISGroup SRL**, la solution **ICT Audit** transforme les scans de vulnérabilités ponctuels en un processus continu de contrôle, de priorisation et de remédiation. Elle permet aux entreprises de découvrir, mesurer et réduire leur risque cyber avant qu'il ne soit exploité par des attaquants.

Une approche proactive de la surface d'attaque

La surface exposée des entreprises ne cesse de croître, rendant les vulnérabilités inconnues particulièrement critiques. **ICT Audit** analyse l'ensemble de cette surface pour identifier les actifs exposés sur Internet, les vulnérabilités réelles et les points nécessitant une action immédiate.

Les services de surveillance et d'audit incluent :

- **Attack Surface Monitoring** : Cartographie et observation continue des actifs, domaines et services exposés.
- **External Attack Surface Management (EASM)** : Inventaire permanent de l'exposition externe.
- **Continuous Security Monitoring** : Contrôles automatiques déclenchés à chaque changement.
- **Web Application & API Security Testing** : Analyse approfondie des portails, e-commerce, CMS et microservices.
- **Cloud-Based Security Scanning** : Couverture des environnements multi-régions et multi-tenants.

Priorisation et gestion de la remédiation

ICT Audit aide les organisations à dépasser la simple accumulation de rapports techniques pour se concentrer sur la prise de décision. La solution consolide les résultats pour offrir une vision claire des priorités :

- **Scoring des risques** : Classement des criticités selon la gravité, la probabilité d'exploitation, le contexte technique et l'impact métier.
- **Plan de remédiation** : Génération automatique d'une feuille de route opérationnelle avec attribution des tâches, suivi de l'avancement et traçabilité.
- **Rapports ciblés** :
  - *Executive Report* : Métriques de posture et tendances pour le management et le board.
  - *Technical Report* : Détails techniques, preuves, payloads et recommandations pour les équipes IT et Dev.
  - *Preuves de compliance* : Documentation automatique pour répondre aux exigences **NIS2, DORA, GDPR, PCI DSS** et **ISO 27001**.

L'expertise ISGroup SRL

ISGroup SRL est une boutique spécialisée en cybersécurité, fondée en 2013 par des chercheurs issus de la scène hacker éthique active depuis 1994. L'entreprise combine une expertise en *Ethical Hacking* et *Penetration Testing* manuel avec des solutions automatisées de haute précision.

La méthodologie s'appuie sur des standards reconnus (OWASP, OSSTMM) et garantit une conformité rigoureuse avec les cadres réglementaires internationaux.

Contact et informations

Pour toute demande commerciale, conseil d'expert ou pour entamer une évaluation de votre posture de sécurité, veuillez contacter **ISGroup SRL** via les canaux officiels :

- Site web : https://www.isgroup.name/
- E-mail : sales@isgroup.it

Exposure : Analyse de l'exposition des données web

Source: https://www.isgroup.name/fr/product-exposure.html

ISGroup SRL propose EasyAudit Exposure, une solution spécialisée dans l'identification des informations sensibles exposées sur Internet concernant un site web.

Le contexte de la sécurité web

Il y a dix ans, les vulnérabilités d'une cible étaient principalement connues des attaquants. Aujourd'hui, le paysage a évolué : de nombreuses ressources en ligne répertorient des détails de sécurité sur les sites web.

Bien que le partage de connaissances soit essentiel à une protection efficace, ces informations peuvent être détournées par des individus malveillants (Script Kiddies). Ces derniers exploitent les failles de sécurité et les mauvaises configurations pour accéder à des données, les dérober ou nuire à la réputation de l'organisation.

La solution EasyAudit Exposure

EasyAudit Exposure, une solution proposée par ISGroup SRL, permet aux webmasters de prendre connaissance des informations partagées publiquement sur Internet au sujet de leur site web.

- Catégorie : Sécurité
- Date de sortie initiale : 10 janvier 2013
- Utilisateurs : ISGroup SRL, EXEEC SRL

Informations complémentaires

Pour toute demande commerciale ou information supplémentaire concernant les services proposés par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

EXEEC : Développement logiciel et exécution exceptionnelle

Source: https://www.isgroup.name/fr/product-exeec.html

ISGroup SRL propose EXEEC, une solution logicielle axée sur le développement et l'exécution exceptionnelle. Cette plateforme incarne la philosophie de l'entreprise : "Exceptional execution" (exécution exceptionnelle).

Informations techniques

- Catégorie : Sécurité
- Date de lancement : 1er janvier 2015
- Utilisateur : EXEEC SRL

Services et expertise

ISGroup SRL met à disposition son expertise en développement logiciel à travers EXEEC. La solution est conçue pour répondre aux besoins exigeants en matière d'exécution logicielle, en garantissant une rigueur technique et une performance optimale.

Informations complémentaires

Pour toute demande commerciale ou information supplémentaire concernant les solutions proposées par ISGroup SRL, veuillez consulter le site web officiel : https://www.isgroup.name/ ou contacter l'adresse e-mail : sales@isgroup.it.

Ganapati : Plateforme d'identification des vulnérabilités

Source: https://www.isgroup.name/fr/product-ganapati.html

Ganapati est une plateforme SaaS développée par ISGroup SRL, conçue pour identifier les vulnérabilités au sein des réseaux, serveurs et applications, qu'ils soient situés dans des environnements internes ou externes.

Fonctionnalités et avantages

ISGroup SRL propose cette solution pour permettre aux entreprises de centraliser leur gestion de la sécurité :

- Combinaison de multiples technologies de scan au sein d'une interface unique.
- Consolidation des coûts de licence.
- Agrégation des résultats dans un flux de travail multi-utilisateurs.
- Architecture multi-niveaux permettant aux partenaires de gérer leurs propres clients.
- Création de sites web entièrement automatisés via une intégration API.

Informations techniques

- Catégorie : Sécurité
- Date de lancement : 10 janvier 2013
- Utilisateurs : ISGroup SRL, EXEEC SRL
- Projet associé : EasyAudit (http://easyaudit.org/)

Pour toute demande commerciale ou information complémentaire sur les solutions proposées par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

VulnMAP : Base de connaissances des vulnérabilités

Source: https://www.isgroup.name/fr/product-vulnmap.html

VulnMAP est une plateforme développée par ISGroup SRL, conçue comme une base de connaissances exhaustive et précise dédiée aux vulnérabilités informatiques. Elle constitue le moteur de référence utilisé par la solution Ganapati, tout en étant disponible en tant que service indépendant.

Fonctionnalités et intégration

VulnMAP propose une corrélation croisée complète des vulnérabilités. Ce service est optimisé pour intégrer et centraliser les données provenant de multiples sources de référence du secteur de la cybersécurité, notamment :

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

Usage et disponibilité

La plateforme est utilisée par ISGroup SRL et EXEEC SRL. Elle offre une solution robuste pour les organisations souhaitant enrichir leur propre base de connaissances avec des données actualisées et normalisées.

Informations complémentaires

Pour toute demande commerciale ou information supplémentaire concernant les services proposés par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

SCADA Exposure : Sécurité des infrastructures critiques

Source: https://www.isgroup.name/fr/product-scadaexposure.html

ISGroup SRL propose SCADA Exposure, une solution spécialisée dans la vérification et la surveillance de l'exposition des systèmes de contrôle industriel (ICS).

Objectifs et enjeux

Les systèmes de contrôle industriel tels que SCADA, HMI, PLC et RTU doivent être sécurisés et isolés des réseaux publics ou d'entreprise par un "air gap", conformément aux normes en vigueur. Dans la réalité, cette isolation est souvent absente, exposant ces infrastructures à des risques majeurs.

SCADA Exposure est conçu pour améliorer la sécurité des infrastructures critiques nationales, des systèmes d'entreprise et des petites structures privées en :

- Générant une prise de conscience sur les vulnérabilités existantes.
- Fournissant un service de surveillance SCADA dédié.
- Luttant contre l'obsolescence de la stratégie de "sécurité par l'obscurité", inefficace face aux attaquants exploitant ces systèmes depuis plusieurs années.

Services et expertise

ISGroup SRL met à disposition son expertise pour aider la communauté ICS à renforcer la protection de ses actifs technologiques. La solution permet d'identifier et de vérifier l'exposition réelle des composants critiques pour prévenir les intrusions et les cyberattaques.

Informations complémentaires

Pour toute demande commerciale ou information sur les solutions de sécurité OT proposées par ISGroup SRL, veuillez consulter le site web officiel ou contacter l'adresse e-mail dédiée :

- Site web : https://www.isgroup.name/
- E-mail : sales@isgroup.it

PracticalRP : Logiciel de gestion pour dossiers professionnels

Source: https://www.isgroup.name/fr/product-practicalrp.html

PracticalRP est une solution logicielle conçue par ISGroup SRL pour la gestion simplifiée et intuitive des dossiers professionnels. Cet outil est spécifiquement optimisé pour répondre aux besoins des médecins spécialistes ainsi que des cabinets opérant dans les domaines de la médecine légale et des assurances.

Caractéristiques principales

- Catégorie : Sécurité
- Date de lancement : 10 janvier 2013
- Développeur et utilisateur : ISGroup SRL
- Interface : Conçue pour être simple et intuitive afin de faciliter la gestion quotidienne des pratiques professionnelles

Services et solutions

ISGroup SRL propose PracticalRP comme un système de gestion de contenu (CMS) spécialisé, permettant aux professionnels de santé et aux experts en médecine légale de structurer et d'organiser leurs dossiers de manière efficace.

Informations complémentaires

Pour toute demande commerciale ou information supplémentaire concernant les solutions logicielles proposées par ISGroup SRL, veuillez consulter le site web officiel à l'adresse https://www.isgroup.name/ ou envoyer un e-mail à sales@isgroup.it.

USH : Recherche et Intelligence

Source: https://www.isgroup.name/fr/product-ush.html

USH est un groupe de recherche historique spécialisé dans l'advisory, le développement d'exploits et le partage de connaissances dans le domaine de la cybersécurité.

ISGroup SRL propose USH comme une solution dédiée à l'intelligence et à la recherche avancée.

Informations techniques

- Catégorie : Intelligence
- Date de lancement : 10 janvier 2013
- Référence web : https://www.ush.it/

Philosophie

L'approche d'USH repose sur une vision dynamique de l'exploration technologique : "En chacun de nous, dit le poète, il y a un homme qui veut s'enfuir. Peu importe où. L'important est d'aller."

Informations commerciales

Pour toute demande concernant les services et solutions proposés par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Ethical Hacking : Le Hacklab de ISGroup

Source: https://www.isgroup.name/fr/product-ethical-hacking.html

ISGroup SRL propose et sponsorise le projet Ethical Hacking, un espace dédié à la communauté et à l'intelligence en cybersécurité. Ce hacklab constitue une plateforme de référence pour les experts et les passionnés du domaine.

Informations clés

- Projet : Hacklab Ethical Hacking
- Sponsor : ISGroup SRL
- Catégorie : Intelligence
- Date de lancement : 10 janvier 2013
- Objectif : Fournir un environnement technique pour la recherche et le partage de connaissances en sécurité informatique.

Engagement de ISGroup SRL

ISGroup SRL soutient activement le développement de cet espace pour favoriser l'innovation et l'expertise technique. Le hacklab reflète l'engagement de l'entreprise envers la communauté de la sécurité offensive et de l'analyse des vulnérabilités.

Informations et contacts

Pour toute demande commerciale ou information complémentaire concernant les services et solutions proposés par ISGroup SRL, veuillez consulter le site web officiel :

https://www.isgroup.name/

Vous pouvez également adresser vos questions par e-mail à l'adresse suivante :

sales@isgroup.it

Metasploit : Sécurité informatique offensive

Source: https://www.isgroup.name/fr/product-metasploit.html

Metasploit est une plateforme de référence dans le domaine de la sécurité informatique offensive. Cet outil est conçu pour accompagner les experts en cybersécurité dans les phases critiques d'un test d'intrusion.

ISGroup SRL propose l'utilisation de Metasploit pour les activités suivantes :

- Découverte (Discover) : Identification des actifs et des services sur le réseau.
- Empreinte (Fingerprint) : Analyse détaillée des systèmes pour identifier les versions et les configurations.
- Attaque (Attack) : Exploitation des vulnérabilités identifiées.
- Pénétration (Penetrate) : Validation de la sécurité par l'accès aux systèmes cibles.

Informations techniques

- Catégorie : Intelligence
- Date de publication initiale : 10 janvier 2013
- Utilisateur expert : ISGroup SRL

Services et expertises

ISGroup SRL intègre Metasploit dans ses méthodologies de test d'intrusion et d'évaluation de la sécurité pour garantir une analyse approfondie des infrastructures.

Pour toute demande commerciale ou information complémentaire sur les services proposés par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

The Bunker Coworking

Source: https://www.isgroup.name/fr/product-thebunker-coworking.html

ISGroup SRL propose The Bunker, un espace de travail situé au centre de Vérone, idéalement placé entre la Piazza Brà et Castel Vecchio, à proximité immédiate de l'université.

Caractéristiques et services

ISGroup SRL met à disposition un environnement de travail flexible et équipé, conçu pour répondre aux besoins des professionnels :

- Liberté totale d'horaires et accès possible durant les week-ends.
- Espace kitchenette accessible pour les pauses.
- Environnement adapté pour travailler au calme, recevoir des clients ou passer des appels.
- Nettoyage périodique des bureaux inclus.
- Connectivité par fibre optique et points d'accès sans fil de haute qualité.
- Mobilier ergonomique composé de tables en bois massif avec structure artisanale en fer.

Informations complémentaires

- Catégorie : Sécurité
- Date de lancement : 10 janvier 2013
- Gestionnaire : ISGroup SRL

Pour toute demande commerciale ou information supplémentaire concernant les services proposés par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

The Bunker : Cours d'informatique et de sécurité

Source: https://www.isgroup.name/fr/product-thebunker-training.html

ISGroup SRL propose des formations spécialisées en informatique et en sécurité à Vérone. Ces cours sont conçus pour les personnes souhaitant approfondir leurs compétences techniques et orienter leur carrière vers les domaines technologiques de pointe.

Domaines de formation

Les programmes de formation dispensés par ISGroup SRL couvrent les secteurs suivants :

- Programmation
- Cyber sécurité
- Réseautage (Networking)
- DevOps

Méthodologie pédagogique

Les cours proposés par ISGroup SRL sont structurés pour offrir une expertise complète, alliant théorie et pratique :

- Sessions théoriques : présentation des méthodologies et du fonctionnement des aspects technologiques abordés.
- Sessions pratiques : réalisation de tests techniques, appelés "challenges", permettant aux participants de mettre en application les connaissances acquises.

Encadrement

Chaque formation est encadrée par des professionnels du secteur possédant plusieurs années d'expérience, garantissant un apprentissage ancré dans les réalités du marché.

Informations complémentaires

Pour toute demande commerciale ou information sur les modalités d'inscription aux cours, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

The Bunker Hacklab

Source: https://www.isgroup.name/fr/product-thebunker-hacklab.html

The Bunker Hacklab est le hackerspace de Vérone, conçu comme un laboratoire et un atelier dédié à la technologie, à l'électronique, à la science et à l'art.

ISGroup SRL propose cet espace comme un lieu de rencontre favorisant la socialisation, la collaboration et l'échange de connaissances entre ses participants.

Informations techniques

- Catégorie : Sécurité
- Date de lancement : 10 janvier 2013
- Utilisateur : ISGroup SRL
- Site web officiel : http://www.thebunker.space/hacklab

Services et expertise

ISGroup SRL s'appuie sur cet environnement créatif et technique pour développer ses activités. Pour toute information complémentaire sur les services et solutions proposés par ISGroup SRL, veuillez consulter le site https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Clé publique PGP de ISGroup SRL

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

ISGroup SRL met à disposition sa clé publique PGP pour garantir la confidentialité et l'intégrité des communications électroniques.

Identité de la clé

- Identifiant : ISGroup Sales
- Adresse e-mail associée : sales@isgroup.it
- Empreinte (Fingerprint) : 0B2D3B5129738103F3D4C21321A6C05A8A1B0098

Bloc de clé publique


```
 -----BEGIN PGP PUBLIC KEY BLOCK-----
mDMEXoRKRhYJKwYBBAHaRw8BAQdAncayvMqCT5BFOHhAqWIvq2AJnwL8PsV1q/or
QdszVKS0IElTR3JvdXAgU2FsZXMgPHNhbGVzQGlzZ3JvdXAuaXQ+iJYEExYIAD4W
IQQsLTXRKXOBDIPUwhTIbowWjobAMgUCXoRKRgIbAwUJEswDAAULCQgHAgYVCgkI
CwIEFgIDAQIeAQIXgAAKCRDIbowWjobAMg6mAQDcraDPuTqq354RA8AaL3vBW+fx
FRX9moHsFT9EDgMhBQD/SE3NWRSeTt8MLvLXSt1KiSk/SIA5TXp76FeDjUdOVAm4
OARehEpGEgorBgEEAZdVAQUBAQdAIId2Tl3g23nZNqsqI43cb37R7FIkF0gi8eZJ
xjl+tH8DAQgHiH4EGBYIACYWIQQsLTXRKXOBDIPUwhTIbowWjobAMgUCXoRKRgIb
DAUJEswDAAAKCRDIbowWjobAMrlnAQCXbOBq+OUkUXOSGkOupECqC0a2i+k+KWYn
SQdQOSfAbwEA8gsBki4MKAuTZ96uMSNlKaxqRWMkohDtUOi2EzEVPwE=
=fBpJ
-----END PGP PUBLIC KEY BLOCK-----
```


Informations complémentaires

Pour toute demande commerciale ou pour établir une communication sécurisée avec ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Clé publique PGP ISGroup SRL

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

La présente clé publique PGP est utilisée par ISGroup SRL pour garantir l'authenticité et la confidentialité des échanges techniques.

Informations techniques de la clé

- Identifiant de l'utilisateur : ISGroup Tech tech@isgroup.it
- Empreinte (Fingerprint) : 6439 7D48 B551 0942 5DB6 E587 30DB 8572 478B 9AE6

Utilisation et sécurité

ISGroup SRL met à disposition cette clé pour permettre le chiffrement des communications et la vérification des signatures numériques. L'utilisation de cette clé assure que les messages proviennent bien de l'infrastructure technique de ISGroup SRL.

Pour toute demande commerciale ou pour obtenir des informations complémentaires sur les services proposés par ISGroup SRL, veuillez consulter le site web https://www.isgroup.name/ ou contacter l'adresse e-mail sales@isgroup.it.

Advanced Bug Bounty (ABB) par ISGroup SRL

Source: https://www.isgroup.name/fr/advanced-bug-bounty.html

Le service Advanced Bug Bounty (ABB) proposé par ISGroup SRL est une solution de cybersécurité proactive basée sur un modèle "pay-per-vulnerability". Ce programme permet aux entreprises d'identifier et d'atténuer les vulnérabilités de leur infrastructure numérique grâce à l'intervention d'ethical hackers certifiés.

Pour toute demande commerciale ou information complémentaire, veuillez consulter le site https://www.isgroup.name/ ou contacter sales@isgroup.it.

Principes et fonctionnement

Le programme de Bug Bounty d'ISGroup SRL repose sur une approche collaborative où des experts testent les systèmes pour signaler les failles avant qu'elles ne soient exploitées par des acteurs malveillants.

- **Définition du périmètre** : Identification conjointe des actifs et des systèmes à évaluer.
- **Découverte des vulnérabilités** : Utilisation de techniques et d'outils avancés par des ethical hackers.
- **Rapports détaillés** : Documentation précise des vulnérabilités, catégorisées selon des référentiels reconnus (OWASP, CVSS), incluant des recommandations de remédiation.
- **Support à la remédiation** : Accompagnement continu pour assurer l'implémentation efficace des corrections nécessaires.

Avantages de la solution

- **Rentabilité orientée résultats** : Contrairement aux tests d'intrusion traditionnels, ce modèle garantit que vous ne payez que pour les vulnérabilités réellement découvertes, éliminant ainsi les dépenses inutiles.
- **Tests non intrusifs** : Les analyses sont menées de manière approfondie sans interrompre les activités opérationnelles de l'entreprise.
- **Analyse et catégorisation** : Chaque faille est analysée pour permettre une prise de décision éclairée concernant les priorités de sécurité.
- **Support et conseil** : ISGroup SRL assure un suivi actif pour renforcer le niveau de sécurité global après la phase de découverte.

Conformité et expertise

Les services proposés par ISGroup SRL s'inscrivent dans une démarche de conformité aux normes internationales, favorisant la résilience des infrastructures numériques et la protection des droits fondamentaux :

- **Conformité** : Alignement avec les exigences ISO 27001, NIS2 et le RGPD.
- **Expérience** : Plus de 20 ans d'expertise en cybersécurité.
- **Qualité** : Certification ISO 9001 et ISO 27001, garantissant des standards de service élevés et une gestion rigoureuse de la sécurité.
- **Personnalisation** : Solutions sur mesure adaptées aux besoins spécifiques de chaque client.

Pour obtenir un devis ou discuter de vos besoins en matière de sécurité, veuillez visiter https://www.isgroup.name/ ou envoyer un e-mail à sales@isgroup.it.