aruo

Catalogue de Services de Cybersécurité

aruoservices
unlock your possibles

sales@aruogroup.com
aruoservices.com

Cybersécurité

Dans un **environnement numérique** où les **menaces** prolifèrent et se transforment sans cesse, **la sauvegarde de vos ressources** s'avère d'une importance capitale.

Notre gamme de services en cybersécurité a été élaborée afin de vous assurer une protection solide et préventive, garantissant ainsi la pérennité de vos activités et la confidentialité de vos informations.

1 Gouvernance, Risques et Conformité (GRC)

Assurez une base solide pour votre sécurité numérique en alignant vos pratiques avec les meilleures normes de l'industrie et les exigences réglementaires.

- **Audit et Analyse de Risques :** Nous identifions, évaluons et hiérarchisons vos vulnérabilités et menaces potentielles, afin de vous offrir une vision claire de votre posture de sécurité actuelle et des actions prioritaires à mener.

- **Conseil en Conformité :** Naviguez sereinement dans le labyrinthe des réglementations (ex: RGPD, ISO 27001). Nous vous aidons à mettre en place les contrôles nécessaires pour garantir votre conformité et éviter les sanctions.

- **Élaboration de Stratégies de Cybersécurité :** Bénéficiez de notre expertise pour définir une feuille de route de sécurité adaptée à vos objectifs métiers, incluant politiques, procédures et cadres de gouvernance.

2 Cybersécurité Offensive (Tests d'Intrusion & Audits)

Mettez à l'épreuve la résilience de vos systèmes avant que les cybercriminels ne le fassent. Nos services offensifs révèlent les failles pour mieux les corriger.

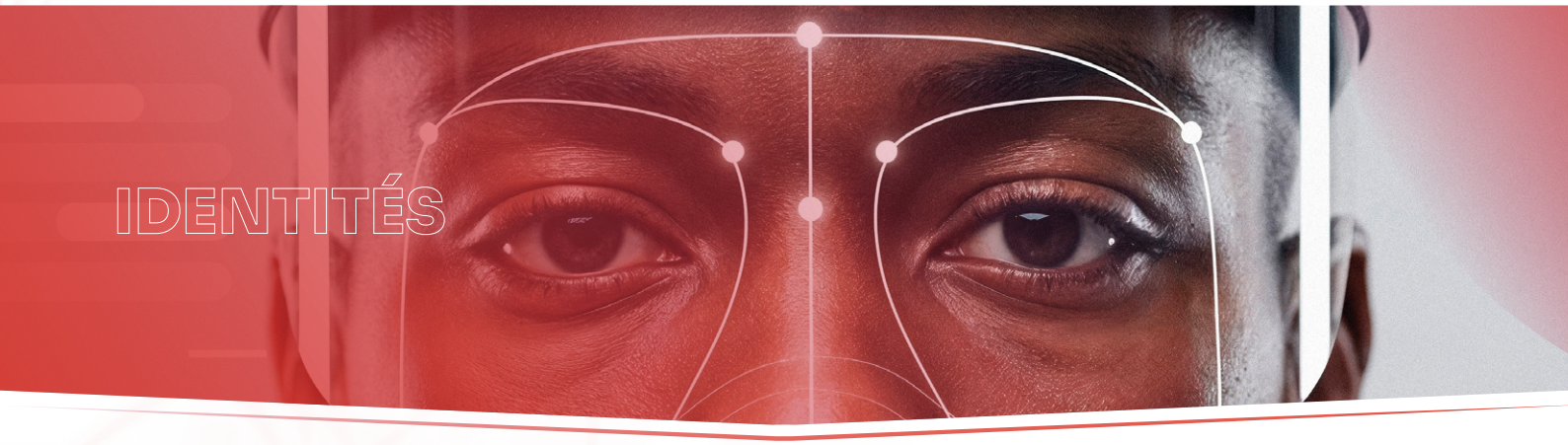
- **Tests d'Intrusion (Pentesting) :** Nos experts simulent des attaques réelles contre vos applications web, mobiles, vos infrastructures réseau et cloud. Ce service essentiel vous permet de découvrir les vulnérabilités avant qu'elles ne soient exploitées.
  - Pentesting Applicatif (Web, Mobile, API)
  - Pentesting d'Infrastructure (Interne, Externe, Wi-Fi)
  - Pentesting Cloud
- **Audits de Vulnérabilité :** Réalisez des scans approfondis de vos systèmes et applications pour détecter les failles de sécurité connues, fournissant un rapport détaillé des risques et des recommandations de correction.
- **Red Teaming :** Des exercices avancés qui simulent des scénarios d'attaques complexes et réalistes pour tester votre capacité de détection et de réponse face à des menaces sophistiquées.

3 Protection des Infrastructures et des Données

Sécurisez vos fondations numériques et protégez l'intégrité et la confidentialité de vos informations les plus sensibles.

- **Sécurité des Réseaux :** Déployez des défenses robustes avec des pare-feu de nouvelle génération (NGFW), des systèmes de détection et de prévention d'intrusion (IDS/IPS), et la segmentation de votre réseau.

- **Sécurité des Terminaux (Endpoints) :** Protégez chaque point d'accès avec des solutions EDR (Endpoint Detection and Response) avancées, allant au-delà de l'antivirus traditionnel pour une détection et une réponse rapides aux menaces.
- **Sécurité du Cloud :** Sécurisez vos environnements cloud (AWS, Azure, Google Cloud) avec des solutions de gestion des identités et des accès (IAM) et des contrôles de sécurité des données spécifiques au cloud.
- **Sécurité des Applications :** Intégrez la sécurité dès le développement avec des analyses de code (SAST/DAST) et protégez vos applications web avec des pare-feu d'application web (WAF).
- **Prévention des Fuites de Données (DLP) :** Mettez en place des mesures pour empêcher la fuite accidentelle ou malveillante de données sensibles, que ce soit via email, USB ou le cloud.



4 Gestion des Identités et des Accès (IAM)

Contrôlez qui a accès à quoi, quand et comment, pour minimiser les risques liés aux accès non autorisés.

- **Authentification Multi-Facteur (MFA) :** Renforcez la sécurité de vos comptes en ajoutant des couches de vérification d'identité.
- **Gestion des Accès à Privilèges (PAM) :** Supervisez et sécurisez les comptes à privilèges, souvent ciblés par les attaquants, pour réduire les risques d'escalade.
- **Single Sign-On (SSO) :** Simplifiez l'accès de vos utilisateurs à toutes leurs applications avec une authentification unique et sécurisée.

5 Cyber-Résilience et Réponse aux Incidents

Préparez-vous à l'inévitable et minimisez l'impact d'une cyberattaque grâce à une planification et une intervention rapides.

- **Planification de la Réponse aux Incidents :** Élaborez et testez des procédures claires pour détecter, contenir, éradiquer et récupérer suite à une cyberattaque.
- **Forensique Numérique :** En cas d'incident, nos experts mènent des enquêtes approfondies pour comprendre la portée de l'attaque, identifier la cause racine et collecter des preuves.
- **Services de Détection et Réponse Gérés (MDR) :** Bénéficiez d'une surveillance continue 24/7 par notre équipe d'experts, capable de détecter et de réagir rapidement aux menaces, vous permettant de vous concentrer sur votre cœur de métier.
- **Plan de Continuité d'Activité (PCA) et de Reprise après Sinistre (DRP) :** Assurez la résilience de vos opérations en cas de perturbation majeure grâce à des plans éprouvés.

6 Sensibilisation et Formation

Le facteur humain est souvent le maillon faible. Transformez vos employés en première ligne de défense contre les cybermenaces.

- **Programmes de Sensibilisation à la Cybersécurité :** Formez vos collaborateurs aux bonnes pratiques de sécurité, comme la détection des tentatives de phishing, la gestion des mots de passe et la sécurité des données.

- **Simulations d'Attaques :** Mettez à l'épreuve la vigilance de vos équipes avec des simulations de phishing ou d'ingénierie sociale pour renforcer leurs réflexes.

Pourquoi choisir ARUO Services ?

- **Expertise reconnue :** Une équipe de spécialistes certifiés et expérimentés.
- **Approche personnalisée :** Des solutions adaptées à vos besoins spécifiques et à votre secteur.
- **Partenaire de confiance :** Un engagement fort pour votre sécurité et votre tranquillité d'esprit.

aruoservices
unlock your possibles

Tableau Récapitulatif des Services

Catégorie de Service	Service Principal	Description Succincte	Bénéfices Clés pour Votre Organisation
1. Gouvernance, Risques & Conformité (GRC)	Audit & Analyse de Risques	Identification et évaluation des menaces et vulnérabilités de votre système d'information.	Vision claire des risques, aide à la priorisation des actions de sécurité.
	Conseil en Conformité	Accompagnement pour l'adhésion aux normes (RGPD, ISO 27001) et réglementations sectorielles.	Réduction des risques légaux et financiers, amélioration de la confiance.
	Élaboration de Stratégies de Cybersécurité	Définition d'une feuille de route de sécurité alignée sur vos objectifs métiers.	Cadre de sécurité robuste, investissements optimisés, meilleure résilience.
2. Cybersécurité Offensive	Tests d'Intrusion (Pentesting)	Simulation d'attaques réalistes sur vos applications (web, mobile), réseaux et infrastructures cloud.	Découverte proactive des failles avant les attaquants, amélioration de la posture défensive.
	Audits de Vulnérabilité	Scans approfondis pour détecter les failles de sécurité connues dans vos systèmes.	Identification rapide des points faibles, rapports détaillés et recommandations de correction.
	Red Teaming	Exercices avancés simulant des attaques complexes pour tester votre capacité de détection et de réponse.	Évaluation réaliste de votre défense, renforcement de la coordination des équipes.

3. Protection des Infrastructures & Données	Sécurité des Réseaux	Déploiement et gestion de pare-feu, IDS/IPS, et segmentation réseau.	Protection contre les intrusions, contrôle des flux de données.
	Sécurité des Terminaux (Endpoints)	Solutions EDR avancées pour la détection et la réponse aux mences sur les postes de travail et serveurs.	Protection des appareils utilisateurs, détection rapide des activités malveillantes.
	Sécurité du Cloud	Sécurisation de vos environnements et données sur les plateformes cloud (AWS, Azure, GCP).	Protection des actifs cloud, conformité des données dans le cloud.
	Prévention des Fuites de Données (DLP)	Mise en place de mesures pour empêcher le transfert non autorisé de données sensibles.	Protection de la propriété intellectuelle et des informations confidentielles.
4. Gestion des Identités et des Accès (IAM)	Authentification Multi-Facteur (MFA)	Ajout de couches de vérification d'identité pour un accès sécurisé.	Réduction des risques liés aux identifiants compromis.
	Gestion des Accès à Privilèges (PAM)	Contrôle et surveillance des comptes à privilèges pour minimiser les risques d'escalade.	Sécurisation des accès critiques, traçabilité des actions des administrateurs.
5. Cyber-Résilience & Réponse aux Incidents	Plan de Réponse aux Incidents	Élaboration de procédures pour détecter, contenir et récupérer après une cyberattaque.	Minimisation de l'impact des attaques, reprise rapide des opérations.

	Forensique Numérique	Enquêtes post-incident pour comprendre la portée de l'attaque, identifier la cause racine et collecter des preuves.	Analyse approfondie des incidents, aide à la prévention de futures attaques.
	Services de Détection et Réponse Gérés (MDR)	Surveillance continue 24/7 de vos systèmes par nos experts et réponse rapide aux menaces.	Détection proactive, réponse rapide, soulagement de vos équipes internes.
6. Sensibilisation & Formation	Programmes de Sensibilisation	Formation des employés aux bonnes pratiques de cybersécurité (phishing, mots de passe, etc.).	Réduction du risque humain, transformation des employés en première ligne de défense.

Contacter le service client ARUO?

+221 33 825 04 27

+221 76 339 61 61

support@aruogroup.com

support.aruogroup.com