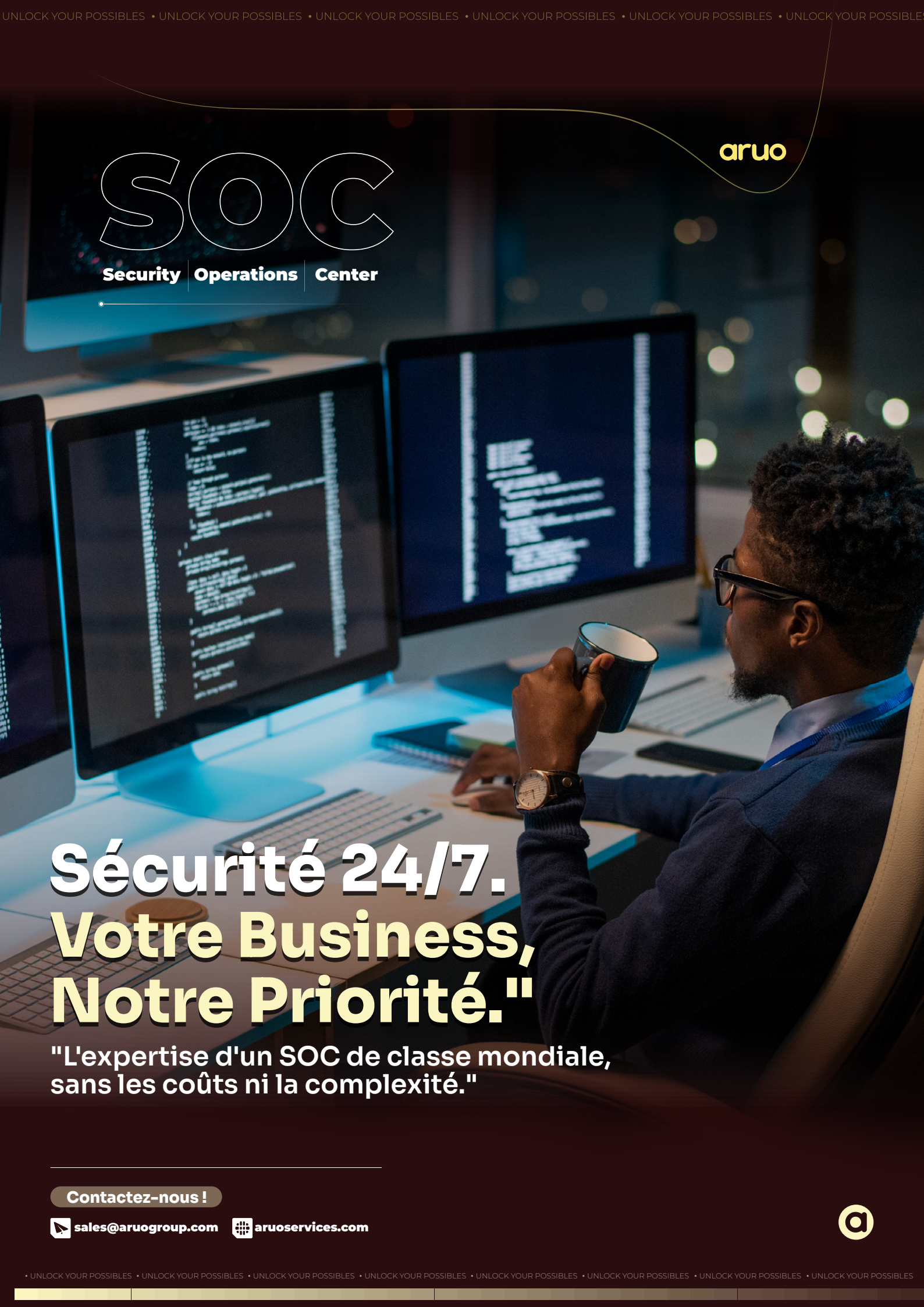
aruo

SOC

Security | Operations | Center

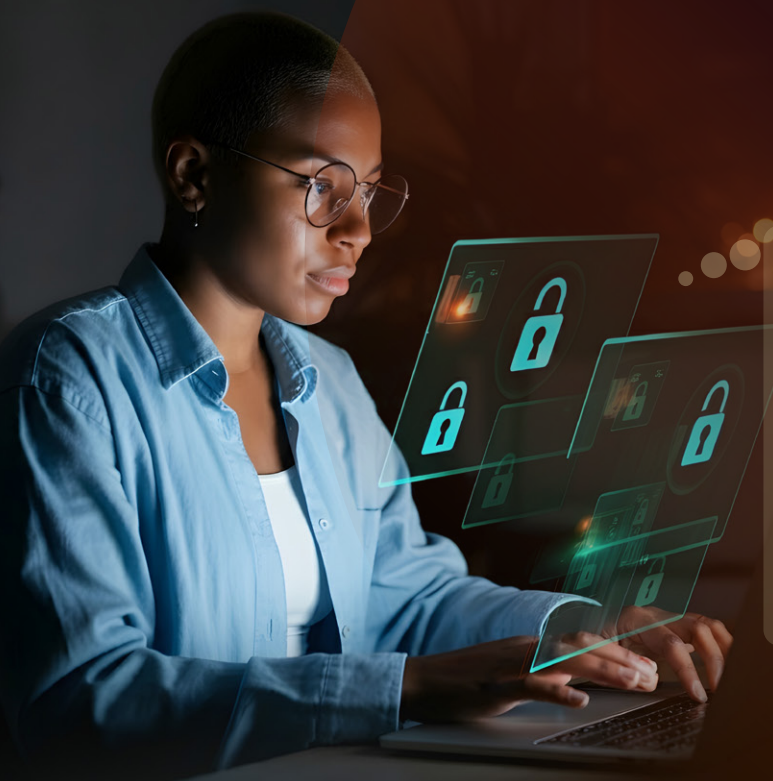


Sécurité 24/7. Votre Business, Notre Priorité."

"L'expertise d'un SOC de classe mondiale, sans les coûts ni la complexité."

Contactez-nous !

sales@aruogroup.com aruoservices.com



La cybermenace est une réalité.

Êtes-vous prêt à y faire face ?

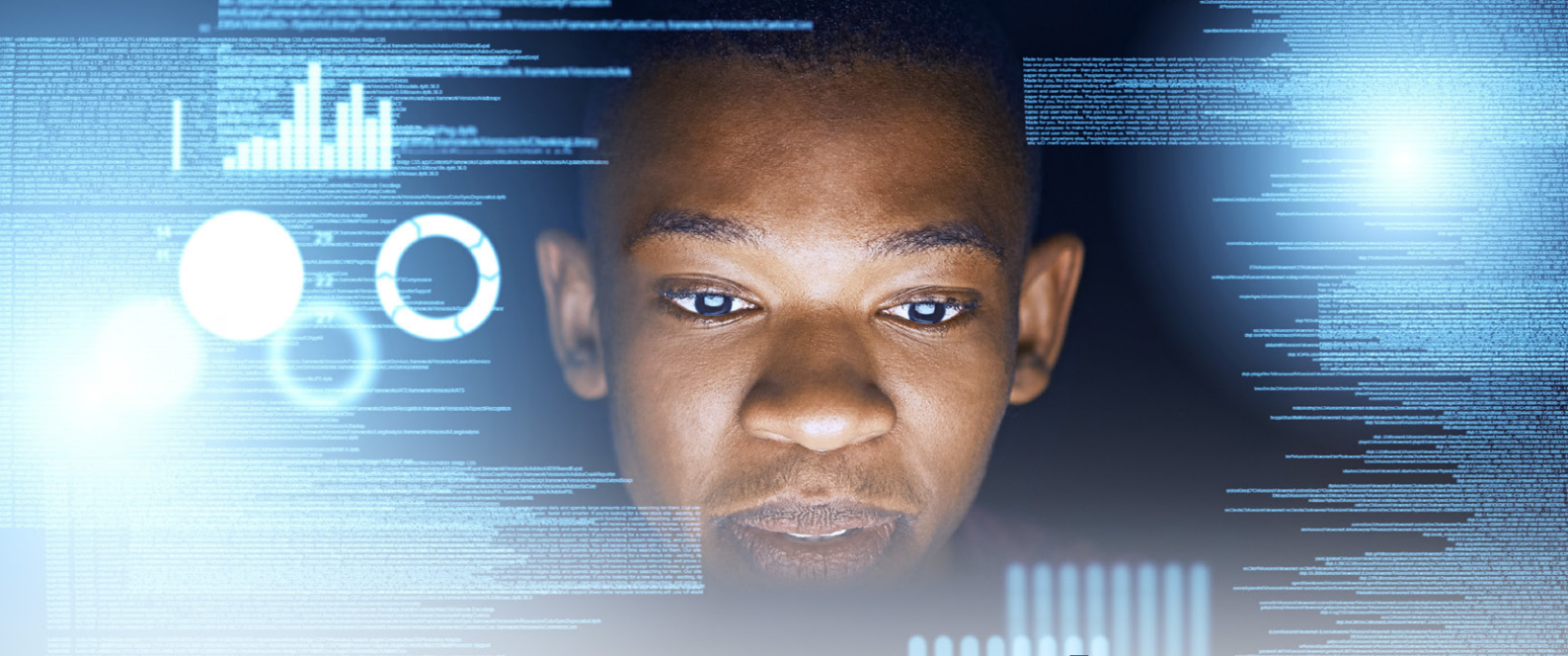
- **Les menaces évoluent plus vite que votre équipe :**
  Phishing, ransomware, attaques zero-day... La complexité est telle qu'il est difficile de suivre.

- **Recruter et garder des experts est coûteux :**
  La guerre des talents en cybersécurité est féroce. Le coût d'un analyste qualifié est un frein pour de nombreuses entreprises.

- **La sécurité est une opération 24/7 :**
  Le silence de la nuit est souvent le moment préféré des attaquants.

- **Vos ressources IT sont déjà débordées :**
  Concentrez-vous sur votre cœur de métier, pas sur la gestion des milliers d'alertes de sécurité.

aruoservices
unlock your possibles



Notre SOC managé : une extension de votre équipe de sécurité.

Surveillance et détection 24/7/365 :

Notre équipe d'experts surveille en permanence votre infrastructure, à la recherche du moindre signe de menace.

Technologie de pointe :

Nous utilisons les meilleurs **SIEM, SOAR et outils de Threat Intelligence** pour transformer des millions d'événements en alertes exploitables.

Réponse aux incidents rapides :

Lorsqu'une menace est détectée, nos procédures de réponse sont déclenchées immédiatement pour contenir, éradiquer et analyser l'incident.

Rapports et conformité :

Recevez des rapports clairs et réguliers sur la posture de sécurité de votre organisation et assurez votre conformité aux réglementations comme le **RGPD.**

Les bénéfices de notre partenariat.

aruoservices
unlock your possibles

- **Économie :**
  Éliminez les coûts liés au recrutement, à la formation et aux technologies complexes.

- **Expertise :**
  Cédez instantanément à une équipe d'analystes certifiés, avec une expertise dans la détection des menaces les plus avancées.

- **Concentration :**
  Libérez vos équipes IT pour qu'elles se concentrent sur vos projets stratégiques.

- **Transparence :**
  Accédez à un tableau de bord client dédié pour suivre en temps réel le statut des incidents et les rapports de sécurité.

- **Tranquillité d'esprit :**
  Dormez sur vos deux oreilles en sachant que votre entreprise est protégée par des experts.

Commencer, c'est simple.

Processus en 3 étapes :

1. **Audit & Configuration :**
   Nous évaluons votre infrastructure, installons nos capteurs et configurons nos outils pour une collecte optimale des données.

2. **Lancement des opérations :**
   Votre SOC est actif. Notre équipe surveille et analyse les alertes 24/7.

3. **Rapports & Optimisation :**
   Nous vous fournissons des rapports réguliers, analysons les performances et ajustons nos services pour une protection continue.

Service SOC Essentiel – Surveillance & Détection

- **Surveillance proactive 24/7 :** Monitoring en continu des systèmes et des réseaux pour identifier les comportements suspects.
- **Détection des menaces :** Utilisation d'outils automatisés pour identifier les menaces courantes (scans de ports, tentatives d'intrusion, activités de rançongiciel).
- **Analyse des journaux (Logs) :** Collecte, stockage et analyse des journaux de sécurité pour détecter des schémas d'attaque.
- **Notification d'alerte :** Envoi d'alertes par e-mail ou SMS aux contacts désignés en cas d'incident de sécurité.
- **> Rapport mensuel d'activité :** Un résumé des événements et des alertes traitées au cours du mois.

Service SOC Avancé – Triage & Réponse

- **Services du niveau Essentiel inclus.**
- **Triage des incidents :** Les alertes sont qualifiées et priorisées par un analyste SOC pour éliminer les faux positifs et se concentrer sur les menaces réelles.
- **Analyse de menaces :** Examen approfondi des incidents pour en déterminer la nature et le niveau de gravité.
- **Assistance à la réponse :** Notre équipe vous guide par téléphone ou visioconférence pour vous aider à réagir aux incidents de sécurité.
- **Rapport trimestriel détaillé :** Un rapport d'analyse des tendances, incluant un aperçu des incidents majeurs et des recommandations pour renforcer votre posture de sécurité.

Service SOC Premium – Gestion complète & Proactive

- **Services des niveaux Essentiel et Avancé inclus.**
- **Réponse complète aux incidents (IR) :** Prise en charge complète de la gestion des incidents, incluant la neutralisation de l'attaque, l'éradication des menaces et l'assistance à la récupération des systèmes.
- **Chasse aux menaces (Threat Hunting) :** Recherche proactive et manuelle de menaces sophistiquées qui auraient pu échapper aux outils de détection automatisée.
- **Analyse forensique avancée :** En cas d'incident majeur, une analyse technique approfondie est menée pour comprendre l'origine et le vecteur de l'attaque.
- **Réunion de sécurité trimestrielle :** Un point régulier avec un expert pour discuter de votre stratégie de sécurité et des axes d'amélioration.

TÉMOIGNAGE CLIENT

John D.
Directeur des Systèmes d'Information.

Grâce à ARUO, nous avons détecté et stoppé une attaque de phishing avant qu'elle ne cause des dommages majeurs."

★ ★ ★ ★ ★

Contacter le service client ARUO?

+221 33 825 04 27
+221 76 339 61 61
support@aruogroup.com
support.aruogroup.com