Fiche Offre : Pack Bouclier Cyber (Audit & Test d'intrusion - Pen Testing)

- **Intitulé :** Pack Bouclier Cyber (Audit & Pen Testing) – Édition Spéciale Pôle Excellence Cyber.
- **Catégorie :** Audit de cyber sécurité / Tests d'intrusion (Pen Testing).
- **Cible bénéficiaire :** RSSI (CISO), DSI (CIO), Responsables de la sécurité opérationnelle (SOC Manager) et responsables Cloud/Infrastructure.
- **Secteur(s) visé(s) :** Tous.
- **Résumé exécutif :**
  "Sécuriser les parcours de soins face au risque cyber en 3 semaines." Conçu spécifiquement pour une action rapide, le Pack Bouclier est une offre d'audit offensive et défensive clé en main. Elle répond à l'urgence des menaces de ransomwares par une méthodologie non-intrusive qui garantit la continuité des soins. En combinant des tests d'intrusion ciblés et une surveillance active via des sondes de détection maintenues pendant 6 mois, ce pack transforme un audit réglementaire en une stratégie de résilience durable.

- **Description détaillée :**
  Le Pack Bouclier est une offre d'audit de sécurité offensive "clé en main" spécifiquement conçue pour répondre aux impératifs de protection des infrastructures de santé face aux menaces croissantes de ransomwares. Contrairement aux audits classiques souvent longs et intrusifs, cette solution adopte une approche "commando" visant à identifier et fermer les brèches critiques en moins de trois semaines, sans aucune perturbation des soins.

  L'offre repose sur une méthodologie 100% à distance (Remote), simulant la vision réelle d'un attaquant externe. Elle combine des tests d'intrusion ciblés sur les applications métiers critiques (DPI, Portails patients, etc.) et une vérification rigoureuse de l'étanchéité des infrastructures réseau et Cloud.

  Au-delà de l'audit ponctuel, le pack inclut une phase de surveillance active. L'établissement bénéficie d'un accès à la plateforme **Observatory** pendant un mois pour cartographier ses actifs, ainsi que du déploiement de cinq sondes de détection d'intrusion maintenues pendant six mois. Cette approche hybride entre audit offensif et monitoring défensif permet non seulement de corriger les failles existantes, mais aussi de détecter les tentatives d'intrusion futures, offrant ainsi un standard de sécurité unifié et immédiatement opérationnel pour le secteur hospitalier.

- **Problématiques traitées :**
  - Vulnérabilité des hôpitaux face aux ransomwares et au vol de données patients.
  - Exposition accidentelle d'équipements sur l'Internet public.
  - Complexité et coût élevé des audits de sécurité traditionnels.
  - Besoin de surveillance post-audit pour détecter les signaux faibles d'intrusion.

- **Méthodologie :**
  - **Approche Blackbox :** Attaques simulées à distance sans connaissance préalable du système.
  - **Audit Applicatif :** Tests sur 3 applications critiques.
  - **Audit Infrastructure :** Tests des firewalls, équipements de bordure et configurations Cloud.
  - **Phase de Monitoring :** Surveillance des flux sortants (Egress) vers des sites à risque.
- **Livrables :**
  - Rapport d'audit technique complet.
  - Synthèse décisionnelle pour la Direction.
  - Accès plateforme ACDS Observatory (30 jours).
  - Installation de 5 sondes de détection (pendant 6 mois) avec alertes automatiques.
- **Prérequis :** Réunion de lancement (30 min) pour validation du périmètre ; accès en lecture seule pour l'audit Cloud.
- **Durée indicative :** 3 semaines pour l'audit et la livraison du rapport ; 7 mois de monitoring total.
- **Technologies ou solutions associées :** Plateforme EASM (gestion de la surface d'attaque externe) **Observatory** et sondes de détection d'intrusion ACDS.
- **Références ou cas d'usage :** Standardisation de la sécurité pour un établissement e-commerce Français.