Fiche Offre : Observatory (EASM SaaS)

- **Intitulé :** Observatory – Plateforme SaaS de gestion de la surface d'attaque externe (EASM).
- **Catégorie :** Scans de vulnérabilités / Cartographie SI/SSI.
- **Cible Bénéficiaire :** RSSI (CISO), DSI (CIO), Responsables de la sécurité opérationnelle (SOC Manager) et responsables Cloud/Infrastructure.
- **Secteur(s) visé(s) :** Tous.
- **Résumé exécutif :**
  "Passer d'une sécurité réactive à une défense proactive par la visibilité totale." Observatory résout le problème critique de l'ombre numérique (Shadow IT) et des fenêtres d'exposition prolongées. Alors que les scans traditionnels sont ponctuels et limités aux actifs connus, Observatory réalise un scan intégral de l'internet pour cartographier 100% de votre surface d'attaque externe. En imposant un cadencement quotidien, la solution identifie les vulnérabilités critiques (CVSS -Système commun de notation des vulnérabilités- de niveau 10, ainsi que les vulnérabilités exploitées activement, les KEV) en moins de 24 heures, tout en réduisant la charge opérationnelle des SOC grâce à un moteur de filtrage des faux positifs de pointe. C'est l'outil indispensable pour les RSSI pilotant des infrastructures complexes et dynamiques.

- **Description détaillée :**
  Observatory est une solution de gestion de la surface d'attaque externe (EASM) conçue pour offrir une visibilité exhaustive et dynamique sur l'ensemble des actifs numériques d'une organisation exposés sur Internet. Contrairement aux outils de scan traditionnels ou aux audits ponctuels qui se limitent souvent aux périmètres déjà connus, Observatory repose sur une technologie propriétaire de scan intégral et continu de l'Internet. Cette approche permet de découvrir activement le "Shadow IT", les sous-domaines orphelins, les environnements de test oubliés et les mauvaises configurations cloud/CDN que les équipes de sécurité ne supervisent plus.

  La plateforme se distingue par sa capacité à transformer une masse de données brutes en renseignements exploitables. Grâce à des algorithmes avancés de réduction du bruit, elle identifie les patterns d'infrastructures partagées (IPs élastiques, nœuds de distribution CDN) pour minimiser drastiquement le taux de faux positifs, souvent problématique dans les solutions concurrentes. L'interface centralisée permet une priorisation intelligente des risques en croisant la sévérité technique (CVSS), la probabilité d'exploitation réelle (EPSS) et le référentiel des vulnérabilités connues et exploitées (KEV) de la CISA.

  Observatory répond à l'urgence cyber en imposant un cadencement de scan quotidien, réduisant la fenêtre d'exposition de plusieurs semaines à moins de 24 heures. C'est un outil de pilotage stratégique qui permet aux responsables sécurité de justifier leurs investissements, de mesurer l'efficacité des remédiations et de maintenir une posture défensive proactive face aux groupes d'attaquants les plus rapides.

- **Problématiques traitées :**
  - Absence de visibilité sur le Shadow IT et les actifs "oubliés".
  - Délais trop longs entre la découverte d'une faille critique (CVE) et son identification sur le périmètre.
  - Engorgement des équipes SOC dû aux faux positifs liés aux infrastructures cloud dynamiques.
  - Difficultés de priorisation face à des milliers de vulnérabilités théoriques.
  - Surveillance de la supply chain numérique pour renforcer la conformité RGPD et NIS2.
- **Méthodologie :**
  - **Phase de Discovery :** Énumération des domaines et sous-domaines via DNS (forward/reverse), logs de transparence de certificats et données de registres.
  - **Scan Quotidien :** Analyse automatisée toutes les 24h pour détecter les changements de configuration ou l'apparition de nouveaux services.
  - **Priorisation :** Application de filtres multicritères (KEV, CVSS > 7, EPSS) pour isoler les risques immédiats.
- **Livrables :**
  - Inventaire d'actifs mis à jour en temps réel (Asset Inventory).
  - Tableau de bord des vulnérabilités actionnables avec liens de remédiation.
  - Emails quotidiens des nouvelles vulnérabilités détectées.
  - Rapports executif
  - Liste et détail des services visibles sur les domaines/sous domaines listés
  - Détail de la stack technique, ses versions, et les vulnérabilités associées, visibles sur les domaines/sous domaines listés (bientôt)
- **Prérequis :** Aucun déploiement d'agent. Fourniture simple des noms de domaine "seeds" (racines) à surveiller.
- **Durée indicative :** Mise en service immédiate (SaaS) ; premiers résultats complets en quelques heures. Contrat de 1 an minimum.
- **Technologies ou solutions associées :** Intégration API pour connexion aux SIEM, VOC, SOC, CMDB et outils de ticketing. Intégration SSO possible.
- **Références ou cas d'usage :**
  - **Secteur Financier :** Identification de tous les actifs affectés par une faille critique liée à React (CVSS 10.0) et fourniture de la liste de remédiation sous 24h pour 4 000 ingénieurs.
  - **Retail/Logistique :** Audit flash de 12 000 sites distribués suite à la faille Cisco IOS XE, évitant l'arrêt de la chaîne logistique.