

# Fiche Technique & Fonctionnelle

---

## 1. Présentation de Purplemet

Purplemet est une solution SaaS non intrusive de gestion de la surface d'attaque des applications web (Web EASM) dédiée à la détection et à la priorisation des risques associés aux assets web exposés sur Internet.

## 2. Fonctionnalités principales

| Fonctionnalité                     | Description                                                                                                                                                                                                                  |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Découverte des actifs web          | Scan DNS, plages IP et services pour détecter toutes vos applications publiques, y compris les éléments cachés ou issus du shadow IT.                                                                                        |
| Vue « hacker »                     | Visualisation de la surface d'attaque comme un attaquant la verrait depuis Internet.                                                                                                                                         |
| Détection des technologies         | Identification des CMS, bibliothèques JavaScript, systèmes d'exploitation, WAF, CDN, API, et plus encore.                                                                                                                    |
| Découverte des actifs sous-jacents | Identification des certificats, des adresses IP, des enregistrements DNS, des registrars, etc., pour cartographier en profondeur votre infrastructure web.                                                                   |
| Détection des vulnérabilités       | Détection des CVEs, protocoles SSL/TLS à risque, des modes debug, des consoles d'administration, des fuites de secrets, des problèmes liés aux certificats, adresses IP, services sensibles et erreurs de configuration DNS. |
| Scoring de risque (note A à F)     | Classement des risques basé sur le nombre de vulnérabilités et leur sévérité, basé sur leur exploitation avérée (CISA KEV) ou probable (FIRST EPSS).                                                                         |
| Alertes personnalisables           | Notifications en temps réel configurables selon le niveau de sévérité défini par l'utilisateur.                                                                                                                              |
| Tableaux de bord détaillés         | Dashboards globaux et par actif.                                                                                                                                                                                             |

## 3. Analyse des noms de domaine

- Identification des applications web relatives à un nom de domaine incluant les sous-domaines.
- Analyse des fonctions de sécurité liées aux domaines : CAA, DNSSEC, SPF, DMARC, DKIM...

#### 4. Analyse des applications web

- Identification des technologies utilisées par l'application web
- Détection des vulnérabilités par catégorie :
  - **CVE** (score EPSS, KEV, CVSS, exploits)
  - **Web issues** : utilisation de protocoles à risque (SSL/TLS), sécurité des headers http et des cookies, fuite de secrets
  - **Unsafe** : composants obsolètes, console d'administration, mode debug

#### 5. Sécurité des certificats

- Inventaire des certificats X.509 utilisés par les applications web.
- Détection des risques liés aux certificats (expiration, auto-signé, algorithme de signature à risque, clé de chiffrement faible).

#### 6. Sécurité des adresses IP

- Inventaire des adresses IP utilisées par les applications web
- Géolocalisation des adresses IP
- Réputation des adresses IP (proxy, crawling, port scanning, sources d'attaques, botnet)

#### 7. Caractéristiques

- Nombre d'utilisateurs illimité.
- Nombre de tags illimité (segmentation des assets par groupe d'utilisateurs, business unit, ...).
- Planification des analyses (quotidienne ou hebdomadaire) ou utilisation d'analyses à la demande.

#### 8. Cas d'usage types

- Contrôle ponctuel et/ou continu pour le top management.
- Visibilité pour les équipes de développement, SOC, CERT,...
- Préalable à des campagnes de bug bounty, de scans ou de tests d'intrusion.
- Validation d'applications tiers / partenaires Externes