

# Continuous Threat Exposure Management

Fuite d'informations, exposition, Dark Web... : Stoppez les attaques à la source



## Flare : Le pouvoir de la défense proactive

Les **fuites d'identifiants**, les **actifs exposés publiquement** ou les **informations** sur les **organisations vendues** sur les forums et marketplaces illicites sont les **armes principales** des acteurs malveillants pour **déclencher des cyberattaques**.

**Flare** offre une **visibilité complète sur ces risques**, en récoltant des **données sur le Dark Web, le web clair** et les canaux de communication comme **Telegram**. Ces **informations sont synthétisées** en données exploitables en temps réel par les équipes de sécurité qui pourront **détecter et corriger ces vulnérabilités ou fuites avant** qu'elles ne mènent à des **cyberattaques**.

**Selon Gartner**, les entreprises adoptant une **vraie stratégie de gestion continue** de l'exposition aux menaces pourraient **réduire les risques de brèches de 66 % d'ici fin 2026**. C'est précisément **ce que propose Flare**, à travers une **plateforme très simple** à déployer et **à exploiter**.

# Avantages clés de la plateforme



Flare se distingue par sa capacité à détecter rapidement les expositions à haut risque dans un environnement unifié et simple à déployer



Voici les principaux bénéfices :



Réduction du bruit d'alerte grâce à un moteur **d'IA de priorisation intelligent**



Détection rapide des **fuites** de données, **identifiants** volés, **secrets GitHub** publics et **indicateurs** de compromission (IOC)



**Automatisation des actions correctives**, notamment la suppression de **domaines usurpés** ou de dépôts **GitHub exposés**



**Intégration rapide (30 minutes), aucune formation longue ou complexe** n'est nécessaire. En moins d'une demi-heure, une équipe peut être opérationnelle et bénéficier d'une **visibilité complète sur ses expositions**. L'interface est **intuitive** et pensée pour **maximiser la productivité dès la première utilisation**



**Prévention proactive** des causes principales des **violations de données**, **attaques par ransomware** et **compromissions de tiers**



**Réduction du temps** moyen de **détection** (MTTD) et du temps moyen de **réponse** (MTTR) **de plus de 90 %**



Contactez-nous

01 60 19 02 30

reseausecu@miel.fr

En savoir plus