



## Fiche produit

Détection et surveillance des accès compromis · Édition 2026

## La plateforme CYBERCREDs en bref

**CYBERCREDs** est une plateforme SaaS souveraine de détection et de surveillance continue des accès compromis (credentials volés circulant sur Telegram, forums underground et marchés privés). Plus de 10 000 logs d'infostealers sont analysés chaque jour. Premier rapport d'investigation Domain Intelligence livré sous 72 heures. Hébergement français, conformité NIS2/DORA/RGPD.

### Le problème adressé

Les credentials volés restent la **première cause d'intrusion en entreprise** (≈ 30 % des breaches, Verizon DBIR 2024). La plupart des compromissions par infostealer sont découvertes après l'incident, lors du forensic — soit plusieurs mois trop tard. Les outils américains du secteur (SpyCloud, Recorded Future, Flare) sont coûteux, calibrés pour les grands comptes, et soumis au Cloud Act.

### Ce que fait CYBERCREDs

Sur un périmètre déclaré (un ou plusieurs domaines corporate), CYBERCREDs croise en continu sa base d'indicateurs avec les fuites détectées, et restitue une cartographie Domain Intelligence complète :

<b>Identités compromises</b>	Liste exhaustive des emails et identifiants détectés dans les fuites, avec source, date, hash de mot de passe.
<b>Machines infectées</b>	Empreintes machine, OS, navigateur, géolocalisation IP, antivirus installé au moment de l'infection.
<b>Accès privilégiés</b>	Comptes admin, comptes de service, accès cloud (Azure, AWS) exposés, classés par niveau de privilège.
<b>Infrastructure exposée</b>	Sous-domaines, VPN, portails internes ouverts détectés dans les credentials volés.
<b>Top URLs ciblées</b>	Les pages d'authentification les plus fréquemment ciblées par les infostealers pour ce domaine.
<b>Password Reuse</b>	Détection de mots de passe identiques entre multiples comptes (facteur démultiplicateur d'attaque).
<b>SaaS Stack</b>	Cartographie automatique des services SaaS utilisés (détection Shadow IT).
<b>Graphe de compromission</b>	Visualisation interactive des liens entre identités, machines et services compromis.

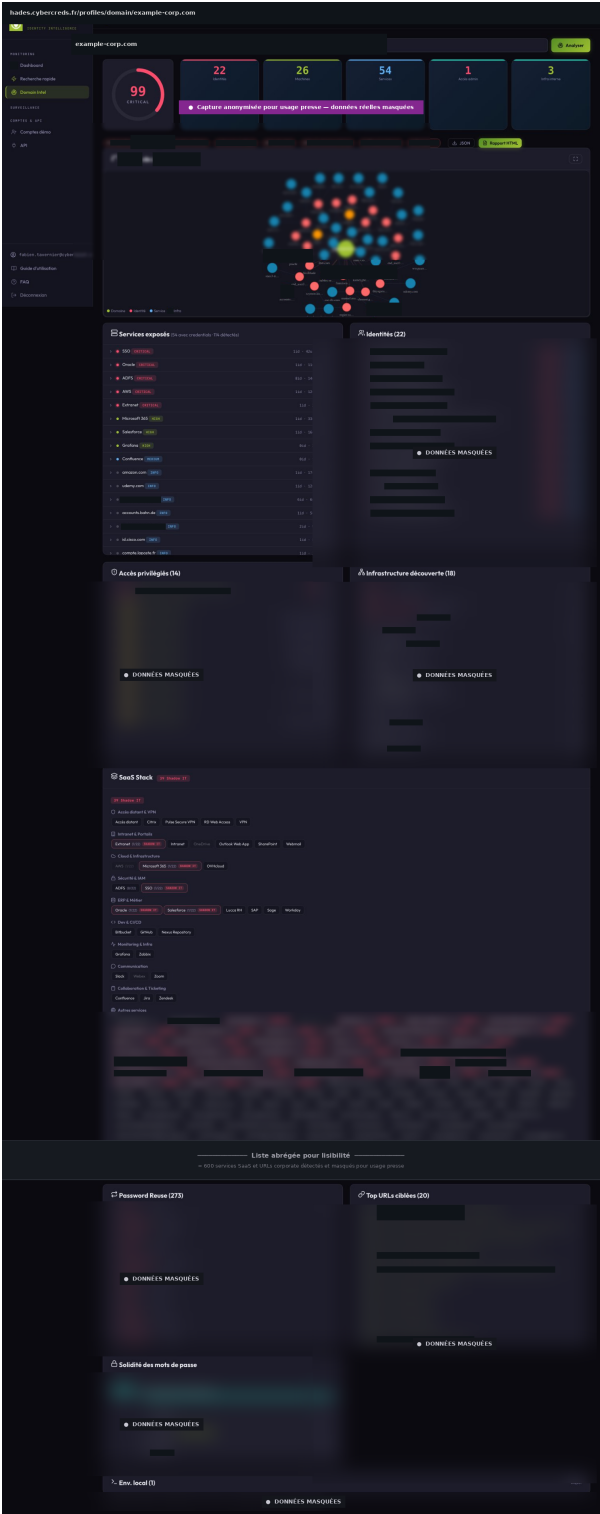
### Intégration et déploiement

<b>Déploiement</b>	100 % SaaS, aucune installation côté client. Onboarding ≤ 1 heure.
<b>1er rapport</b>	Livré sous 72 heures à partir de la soumission du domaine.
<b>Mise à jour</b>	Veille continue 24/7, alertes en temps réel sur nouveaux indicateurs.
<b>API &amp; flux</b>	REST API, webhooks, STIX/TAXII pour intégration SIEM/SOAR/EDR.

Connecteurs	Splunk, Sentinel, QRadar, Elastic, Cortex XSOAR, ServiceNow.
Souveraineté	Hébergement France (OVH), données ne sortent pas du territoire UE.
Conformité	NIS2, DORA, RGPD. SecNumCloud sur périmètres sélectionnés.

## Aperçu du dashboard Domain Intelligence

Aperçu d'un rapport CYBERCREDS lancé sur un domaine corporate (capture anonymisée pour usage presse). Les sections affichant des données personnelles ou des URLs spécifiques sont masquées ; la structure et la profondeur d'analyse restent visibles.



## Pricing

<b>Starter</b>	À partir de 490 €/mois — 1 domaine, surveillance continue, alertes email.
<b>Business</b>	Sur devis — jusqu'à 10 domaines, intégration SIEM, support prioritaire.
<b>Enterprise</b>	Sur devis — périmètre étendu, multi-tenants, accompagnement dédié, options avancées (SOC, MSSP).
<b>Public sector</b>	Tarification UGAP-SCC disponible pour collectivités et OIV/OSE.

## Pour aller plus loin

Démo gratuite sur [www.cyberesist.com](http://www.cyberesist.com) (rapport Domain Intelligence livré sous 72h). Contact commercial et presse : **Fabien Tavernier**, président — [fabien.tavernier@cyberesist.com](mailto:fabien.tavernier@cyberesist.com) — +33 6 74 52 26 53.