

Comment les données d'identité sont-elles protégées ?

Réponse courte : Cyber Crucible identifie les emplacements où sont stockées les données d'identité et protège ces emplacements au niveau du noyau (kernel). Lorsqu'un programme tente d'y accéder, son accès est tracé et analysé — **sans que les mots de passe, jetons ou clés de chiffrement eux-mêmes ne soient jamais consultés ou collectés**. Sur la base de cette analyse, le programme est autorisé, reçoit des données fictives, est refusé, ou est suspendu.

Protéger l'accès, pas le secret

La plupart des solutions de protection de l'identité travaillent sur le secret : le chiffrer, le mettre en coffre-fort, ou surveiller son apparition dans une fuite de données. Cyber Crucible agit sur **l'acte de vouloir y accéder**.

Les attaques automatisées sont prévisibles d'une manière bien précise — elles doivent se rendre à des emplacements connus pour trouver des identifiants. Les magasins de cookies des navigateurs, les chemins d'identifiants VPN, le magasin d'identifiants Windows, les fichiers de portefeuilles (wallets) et les données Active Directory se trouvent tous à des endroits que les attaquants savent déjà où chercher. Cette prévisibilité constitue l'opportunité défensive.

Cyber Crucible identifie ces magasins de données d'identité, puis les protège. Tout programme touchant l'un d'entre eux est évalué, ainsi que ses processus parents et enfants et les bibliothèques qu'il a chargées.

Les secrets ne sont jamais lus

Il s'agit d'une contrainte de conception délibérée, et non d'un effet secondaire : **l'accès est tracé et analysé sans que l'identifiant lui-même soit consulté**. Cyber Crucible ne lit, ne traite, ne collecte ni ne transmet les mots de passe, jetons de session, cookies ou clés de chiffrement — vers aucun serveur, qu'il soit hébergé par Cyber Crucible ou par le client.

Il s'avère que l'analyse comportementale de l'accès à l'identité ne nécessite pas les données d'identité elles-mêmes. Ce qui compte, c'est *quel programme accède où, dans quel contexte, après avoir fait quoi au préalable* — rien de tout cela ne nécessite d'ouvrir le secret.

La conséquence est que la protection ne peut pas elle-même devenir la brèche, et il n'existe aucun magasin central de vos identifiants pouvant être assigné en justice, divulgué ou perdu.

Ce qu'évalue le moteur comportemental

La décision n'est pas « ce programme figure-t-il sur une liste ? » — c'est « que fait réellement ce code en ce moment ? ». Les signaux incluent :

- **État et comportement de la mémoire** — suivis sur l'ensemble du cycle de vie du programme, y compris les modifications en mémoire qui ne touchent jamais le disque. Il s'agit de la couche de capteurs fondamentale de la plateforme, partagée avec la protection des données et FortressAI, plutôt que spécifique à l'identité.
- **Lignage des processus** — ce qui a lancé ce programme, et ce que ce programme a lancé à son tour.
- **Modèle d'accès** — s'agit-il d'une application normale lisant son propre identifiant, ou d'un balayage à travers de nombreux emplacements d'identité à la fois ?
- **Activité des bibliothèques et injections** — ce processus de confiance a-t-il fait l'objet d'une injection ou d'une altération en mémoire ?

La réponse est graduée, pas binaire

Tout programme cherchant à accéder à des données d'identité n'est pas un attaquant, donc la réponse dépend de la nature du programme et de son comportement :

Situation	Réponse
Une application connue, non compromise, accédant à ce dont elle a légitimement besoin	Autorisée
Une application connue, non compromise, mais dépassant son accès approprié	Reçoit des données fictives, ou l'accès est refusé — régi par les règles comportementales de confidentialité
Une application inconnue	Rejetée ou suspendue , selon le moteur comportemental et vos paramètres
Une application compromise — processus ou bibliothèques exploités	Rejetée ou suspendue , selon le moteur comportemental et vos paramètres

Le cas intermédiaire importe plus qu'il n'y paraît de prime abord. De nombreux logiciels légitimes accèdent plus profondément aux magasins d'identité que nécessaire. Les suspendre perturberait la journée de l'utilisateur sans aucun gain de sécurité — mais leur transmettre de véritables identifiants représente une exposition inutile. Le renvoi de données fictives satisfait le programme tandis que le véritable secret reste en place.

La distinction que trace le moteur se situe entre un programme de confiance qui *dépasse ses prérogatives* et un programme inconnu ou *pris en otage*. Seul ce dernier cas est traité comme une attaque.

Pourquoi cela se produit sur le poste de travail (endpoint)

Un infostealer automatisé peut s'infiltrer, collecter des données et supprimer ses propres outils en mémoire en quelques secondes. Envoyer une télémétrie à un service cloud et attendre un verdict ne peut rivaliser avec cette rapidité. La boucle complète de détection-décision-réponse (detect-decide-respond) s'exécute donc localement dans le noyau, ce qui explique également pourquoi elle fonctionne sans aucune connectivité.

“ Voir aussi : « *Collectez-vous des données d'identité ?* », « *Quelles données d'identité sont protégées ?* », et « *Que se passe-t-il lorsqu'un programme tente d'accéder à des données d'identité auxquelles il ne devrait pas avoir accès ?* » ”

Revision #1

Created 2026-07-24 06:51:31 UTC by Dennis Underwood

Updated 2026-07-24 06:51:31 UTC by Dennis Underwood