

Quel rôle jouent les analyses de mémoire dans l'ensemble de la plateforme ?

Réponse courte : Les analyses de mémoire constituent le socle sur lequel tout le reste est construit. Elles sont la source de détection et d'analyse alimentant toute la modélisation comportementale — protection des données, protection des identités et FortressAI. Chaque décision prise par ces capacités repose sur la connaissance de ce que fait réellement la mémoire d'un programme.

Un socle unique, trois capacités

Cyber Crucible suit l'état de la mémoire d'un programme tout au long de son cycle de vie, du début à la fin, y compris ses interactions en mémoire avec d'autres programmes. Ce flux d'analyse unique est ce qui rend le reste possible :

- **Protection des données** — ce processus se comporte-t-il comme quelque chose sur le point de chiffrer ou d'exfiltrer des données ?
- **Protection des identités** — ce processus est-il le propriétaire légitime de l'identifiant qu'il tente d'utiliser, ou a-t-il été détourné ?
- **FortressAI** — cet outil d'IA est-il toujours lui-même, et son accès aux données respecte-t-il la politique en vigueur ?

Il ne s'agit pas de trois moteurs distincts dotés de trois ensembles de capteurs distincts. Ce sont trois politiques exprimées au-dessus du même modèle comportemental de la mémoire.

Pourquoi la mémoire est le bon socle

Les attaques modernes ne laissent de plus en plus aucun fichier à inspecter. Le code est injecté dans des processus de confiance et construit en mémoire, si bien que le seul endroit où l'activité est visible est l'état mémoire d'un programme en cours d'exécution. Une défense incapable d'observer cet espace est aveugle à toute cette catégorie d'attaques.

L'analyse de la mémoire répond également à la question la plus importante avant d'accorder l'accès à toute ressource sensible : **ce programme est-il toujours ce qu'il prétend être ?** Une application de confiance dont le processus ou les bibliothèques ont été altérés n'est plus digne de

confiance, et seule une inspection au niveau de la mémoire permet de le révéler.

Ce n'est pas un balayage de la mémoire

Il s'agit d'un suivi comportemental en temps réel, et non d'un balayage périodique. Le balayage copie un bloc de mémoire et analyse cet instantané — une photographie plutôt qu'un enregistrement en direct. Sur une machine très sollicitée, l'état du programme peut être totalement différent un instant plus tard, ce qui rend les instantanés utiles pour l'analyse forensique contrôlée, mais beaucoup moins efficaces pour une défense en temps réel.

“ Voir également les articles existants sur les *Analyses de mémoire* pour le détail technique de la différence avec le balayage de la mémoire, et ce qui se passe lorsqu'une attaque en mémoire est détectée.

Revision #1

Created 2026-07-24 06:58:02 UTC by Dennis Underwood

Updated 2026-07-24 06:58:02 UTC by Dennis Underwood