Comment Cyber Crucible prend-il une décision en moins de 200 millisecondes ?

Réponse courte : Il exécute une boucle en trois étapes — Detect-Decide-Respond — entièrement sur le point de terminaison au niveau du noyau, à l'aide d'un moteur d'analyse informatique en périphérie (edge computing) breveté. Comme rien n'a besoin de transiter par un service cloud pour revenir ensuite, et qu'aucun humain n'intervient dans la boucle, l'ensemble du cycle se termine en moins de 200 millisecondes.

La boucle

1. **Detect** — des capteurs novateurs au niveau du noyau identifient les schémas comportementaux malveillants dans la mémoire, l'activité des processus et l'accès aux fichiers.
2. **Decide** — le modèle comportemental renforcé par l'IA évalue instantanément l'intention de l'accès aux données du programme.
3. **Respond** — si l'intention est malveillante, le programme est intercepté et suspendu.

Pourquoi le traitement local n'est pas négociable

Envoyer la télémétrie à un serveur cloud, attendre l'analyse, puis recevoir une réponse en retour ajoute des millisecondes que l'attaquant utilisera avec plaisir. Pour donner une idée de l'échelle en jeu : cette décision se produit plus rapidement qu'un influx nerveux ne voyage de l'œil au cerveau. Toute architecture comportant un aller-retour réseau dans le chemin critique a déjà perdu cette course.

La télémétrie brute est tout de même copiée sur des serveurs par la suite à des fins de preuve et d'enrichissement — mais la décision de protection n'attend jamais ce processus.

Revision #1
Created 2026-07-24 06:57:40 UTC by Dennis Underwood
Updated 2026-07-24 06:57:40 UTC by Dennis Underwood