

Comment l'IA est-elle gouvernée dans le cycle de vie de développement de Cyber Crucible ?

Réponse brève : Étant donné que l'IA génétique de Cyber Crucible n'est utilisée qu'au moment de la conception, elle est régie par le cycle de vie de développement sécurisé (SDLC) plutôt que comme un système de production en direct. Les travaux de découverte s'effectuent dans un environnement interne contrôlé, leurs résultats sont validés et traduits en heuristiques de noyau déterministes, et les pilotes qui en résultent sont signés de manière indépendante sous Microsoft WHCP avant leur publication.

Le cycle de vie gouverné

Phase	Gouvernance
Conception	Les exigences de sécurité sont définies ; la découverte par IA fait partie de la phase de conception, dans le cadre du SDLC
Découverte	L'IA génétique identifie des variables déterministes révélatrices d'attaques en utilisant uniquement des ensembles de données de recherche internes
Dérivation	Les résultats deviennent des heuristiques de noyau fixes et déterministes — aucun modèle en direct n'est déployé
Validation	Les résultats déterministes sont reproductibles et testables ; les modèles et pilotes sont validés par assurance qualité (QA)
Publication	Les pilotes Windows sont signés WHCP ; les modifications suivent une gestion formelle du changement

Données et intégrité

Aucun contenu client, identifiant ou clé n'est utilisé pour entraîner, alimenter ou ajuster un modèle. Les modèles sont propriétaires et développés en interne, sans dépendance à un modèle tiers. L'intégrité des modèles est maintenue grâce au contrôle de version, à la validation SDLC/QA et à la

signature WHCP ; la confidentialité est assurée par un environnement de développement contrôlé.

Revision #1

Created 2026-07-24 07:12:59 UTC by Dennis Underwood

Updated 2026-07-24 07:13:00 UTC by Dennis Underwood