

Que montre la page Injections de processus ?

Les injections de processus sont une capacité d'ingénierie logicielle qui peut apparaître dans un contexte non malveillant, ou être directement utilisée par un attaquant. En fait, l'injection de processus et les techniques associées sont l'une des méthodes favorites des attaquants, pour diverses raisons qui dépassent le cadre de cet article (mais si vous le demandez, nous pouvons vous orienter vers une formation).

Cyber Crucible expose les événements d'injection de processus au niveau du noyau. Cela signifie que vous disposez d'une visibilité complète sur tous les processus et leurs informations, quelles que soient les permissions de ce processus. Nous avons constaté qu'une fois que les attaquants ou les logiciels atteignent un certain niveau de permissions, de nombreuses sources traditionnelles de télémétrie pour les outils de sécurité deviennent silencieuses. Ne jamais manquer une donnée importante, et ne jamais devenir silencieux, constitue une part essentielle de la conception zero trust de notre produit.

Sur la page Injections de processus, vous verrez les éléments suivants pour chaque événement, avec des filtres disponibles pour affiner vos requêtes :

[CC Showing All Process Injection Columns.mp4](#)

Normalement, dans le cadre d'une enquête, vous constaterez qu'il existe une activité supplémentaire sur la page Création de processus.

Revision #1

Created 2026-07-24 06:41:49 UTC by Dennis Underwood

Updated 2026-07-24 06:41:49 UTC by Dennis Underwood