

4.4.1.1

Fonctionnalités

- Amélioration du traitement analytique des relations parent-enfant, lorsque le processus parent se termine rapidement avant que Cyber Crucible n'ait terminé son traitement (millisecondes).
 - Le scénario extrêmement courant ici est que les attaquants (et les programmes légitimes) ouvrent souvent plusieurs programmes, parfois selon une « chaîne » en plusieurs étapes. Cela peut être intentionnel, ou dû au comportement « sous le capot » de Windows ou d'autres applications.
 - Les modèles comportementaux de Cyber Crucible exploitent les variables d'activité et d'état pour tous les processus d'une chaîne d'exécutions afin d'atteindre une précision et un contexte maximaux.

Corrections

- Cyber Crucible connaissait une perte de précision dans la prise de décision des modèles comportementaux, due à la perte de télémétrie lorsque plusieurs programmes s'appellent mutuellement, mais que l'un des programmes se termine en quelques millisecondes.
 - Dans une chaîne où le programme A exécute le programme B. Le programme B démarre le programme C, mais le programme B se termine en quelques millisecondes (généralement un plantage silencieux, mais pas toujours). L'analyse comportementale de Cyber Crucible dispose des variables des programmes A et C, mais n'a pas eu le temps d'analyser complètement le programme B, puisqu'elle s'attendait à ce qu'il soit en cours d'exécution.
 - Ce problème a été corrigé, ce qui améliore la précision de la prise de décision du moteur de décision hyper-automatisé de Cyber Crucible.

Statut de validation WHCP/WHQL

Validé.

Hachages MD5

```
service.exe      = db76d0abc8f4bc4b2a093435bc314bde
assistant.exe    = a5bac35d839d7a57fccccfceb011083c1
CCRRSecMon.sys (Windows10)      = 935e43368fa95ae740a3f04defcc390d
CCRRSecMon.sys (Windows8)       = ee555ad0f282f36dd11deada8d1ca9c7
CCRRSecMon.sys (Windows7)       = a6a5073c6565361b443651ef29e49490
```

Revision #1

Created 2026-07-24 06:26:53 UTC by Dennis Underwood

Updated 2026-07-24 06:26:53 UTC by Dennis Underwood