

4.4.1.1

Funktionen

- Verbesserte analytische Verarbeitung für Eltern-Kind-Beziehungen, wenn der übergeordnete Prozess sehr schnell beendet wird, bevor Cyber Crucible die Verarbeitung abschließen kann (Millisekunden).
 - Ein äußerst häufiges Szenario ist, dass Angreifer (und auch legitime Programme) oft mehrere Programme öffnen, manchmal in einer mehrstufigen „Kettenreaktion“. Dies kann absichtlich geschehen oder auf das Verhalten von Windows oder anderen Anwendungen „im Hintergrund“ zurückzuführen sein.
 - Die Verhaltensmodelle von Cyber Crucible nutzen Aktivitäts- und Zustandsvariablen für alle Prozesse in einer Ausführungskette, um maximale Genauigkeit und Kontext zu erreichen.

Fehlerbehebungen

- Cyber Crucible verzeichnete eine verringerte Genauigkeit bei der Entscheidungsfindung der Verhaltensmodelle, aufgrund des Verlusts von Telemetriedaten, wenn mehrere Programme sich gegenseitig aufrufen, eines der Programme jedoch innerhalb von Millisekunden beendet wurde.
 - In einer Kette, in der Programm A Programm B ausführt. Programm B startet Programm C, wird jedoch innerhalb von Millisekunden beendet (in der Regel ein stiller Absturz, jedoch nicht immer). Die Verhaltensanalyse von Cyber Crucible verfügte über die Variablen von Programm A und Programm C, hatte jedoch keine Zeit, Programm B vollständig zu analysieren, da erwartet wurde, dass es weiterhin ausgeführt wird.
 - Dies wurde korrigiert, was zu einer präziseren Entscheidungsfindung durch die hyperautomatisierte Entscheidungs-Engine von Cyber Crucible führt.

WHCP/WHQL- Validierungsstatus

Validiert.

MD5-Hashes

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

Revision #1

Created 2026-07-24 04:02:04 UTC by Dennis Underwood

Updated 2026-07-24 04:02:04 UTC by Dennis Underwood