4.4.1.1

Funcionalidades

- Processamento analítico aprimorado para relações pai-filho, quando o processo pai termina rapidamente antes que a Cyber Crucible conclua o processamento (milissegundos).
  - O cenário extremamente comum aqui é que os atacantes (e programas legítimos) frequentemente abrem vários programas, às vezes em uma "cadeia" de múltiplas etapas. Isso pode ser proposital, ou devido ao comportamento do Windows ou de outras aplicações "por trás dos panos".
  - Os modelos comportamentais da Cyber Crucible aproveitam variáveis de atividade e estado para todos os processos em uma cadeia de execuções, a fim de alcançar a máxima precisão e contexto.

Correções

- A Cyber Crucible apresentava uma perda na precisão da tomada de decisão do modelo comportamental, devido à perda de telemetria quando múltiplos programas se chamam mutuamente, mas um dos programas terminava em milissegundos.
  - Em uma cadeia em que o Programa A executa o Programa B. O Programa B inicia o Programa C, mas o Programa B termina em milissegundos (geralmente uma falha silenciosa, mas nem sempre). A análise comportamental da Cyber Crucible possuía as variáveis do Programa A e do Programa C, mas não teve tempo de analisar completamente o Programa B, pois esperava que ele estivesse em execução.
  - Isso foi corrigido, resultando em uma tomada de decisão mais precisa pelo mecanismo de decisão hiper-automatizado da Cyber Crucible.

Status de Validação WHCP/WHQL

Validado.

Hashes MD5

```
service.exe   = db76d0abc8f4bc4b2a093435bc314bde
assistant.exe = a5bac35d839d7a57fcccfceb011083c1
CCRRSecMon.sys (Windows10)       = 935e43368fa95ae740a3f04defcc390d
CCRRSecMon.sys (Windows8)        = ee555ad0f282f36dd11deada8d1ca9c7
CCRRSecMon.sys (Windows7)        = a6a5073c6565361b443651ef29e49490
```

Revision #1
Created 2026-07-24 05:18:12 UTC by Dennis Underwood
Updated 2026-07-24 05:18:12 UTC by Dennis Underwood