4.4.8.0

Funcionalidades

- Telemetria Authenticode em modo kernel
  - Para maior velocidade e fiabilidade, os dados de certificado para criações de processos e incidentes serão registados apenas pelo driver.
  - Esta atualização não remove as dependências das bibliotecas de criptografia do Windows, mas realiza os cálculos criptográficos em paralelo. Eventualmente, a dependência do Windows poderá ser totalmente removida.

Correções

- Redução do uso de memória e do tempo de CPU gasto em tentativas de envio de eventos quando offline, período durante o qual a telemetria é armazenada de forma segura até que a máquina recupere a conectividade com os servidores da Cyber Crucible.
- Alguns instaladores de drivers Nvidia acreditavam que não tinham privilégio para instalar devido ao uso de uma função interna do kernel da Microsoft para tentar aceder aos ficheiros instalados da Cyber Crucible.
- Corrigida a incompatibilidade com o modo JWE e o modo DMZ

Hashes MD5

```
service.exe  = 5189fe49a1bfade50766fce2a1980eef
CCRRSecMon.sys (Windows7)        = 342dd1bbe5f5dfcffe7752b74b34a9e8
CCRRSecMon.sys (Windows8)        = a20c9cca59be651db7ae69f9f1f64cf2
CCRRSecMon.sys (Windows10)       = a3cf6860d3f059a1ab38ee7b2d82b097
```

Revision #1
Created 2026-07-24 05:24:08 UTC by Dennis Underwood
Updated 2026-07-24 05:24:08 UTC by Dennis Underwood