4.4.4.0

Funciones

- Los informes de incidentes y telemetría se almacenan en disco para escenarios sin conexión.
  - Debido a los intentos de manipulación observados contra múltiples almacenes de registro de EDR/XDR, Cyber Crucible habilitó la protección a nivel de kernel para los datos almacenados en disco antes de implementar esta capacidad.
- Mayor protección del proceso de servicio utilizado para la comunicación y las actualizaciones de backend, como parte del endurecimiento de confianza cero anticipatorio.
  - Esto no fue en respuesta a una amenaza existente, sino de forma proactiva ante una que el Equipo prevé próximamente.

Correcciones

- Se corrigieron los procesos que se cargan al arrancar y que no estaban disponibles en el panel bajo creaciones de procesos.
- Se impidió que dos instaladores se ejecutaran al mismo tiempo, lo cual registraría el mismo equipo dos veces.

Hashes MD5

```
service.exe                     = 116dab615aab07d804667b13ecfe821a
CCRRSecMon.sys (Windows7)       = db358b3d6e784d11827ff899722e3070
CCRRSecMon.sys (Windows8)       = a95dd87d2ea9944e8643de787f11d71c
CCRRSecMon.sys (Windows10)      = 6eb017a5cb3a9dd45bc065b466fb4789
```

Revision #1
Created 2026-07-24 01:22:20 UTC by Dennis Underwood
Updated 2026-07-24 01:22:20 UTC by Dennis Underwood