4.4.4.0

Features

- Reports for incidents and telemetry are stored on disk for offline scenarios.
  - Due to tampering attempts observed against multiple EDR/XDR logging stores, Cyber Crucible enabled kernel-level protection against the disk-stored data before deploying this capability.
- Increased protection of the service process used for backend communication and updates, as part of look-ahead zero-trust hardening.
  - This was not in response to an existing threat, but proactive for one the Team sees upcoming.

Fixes

- Fixed processes that load at boot not being available in the dashboard under process creations.
- Prevented two installers from running at the same time, which would use register the same machine twice.

MD5 Hashes

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

Revision #1
Created 2026-07-13 18:49:33 UTC by Dennis Underwood
Updated 2026-07-13 18:49:33 UTC by Dennis Underwood