# 4.4.4.0

# Fonctionnalités

- Les rapports d'incidents et de télémétrie sont stockés sur disque pour les scénarios hors ligne.
  - En raison de tentatives d'altération observées contre plusieurs magasins de journalisation EDR/XDR, Cyber Crucible a activé une protection au niveau du noyau pour les données stockées sur disque avant de déployer cette fonctionnalité.
- Protection renforcée du processus de service utilisé pour la communication backend et les mises à jour, dans le cadre du durcissement zero-trust anticipatif.
  - Ceci n'était pas une réponse à une menace existante, mais une mesure proactive face à une menace que l'équipe anticipe.

# Corrections

- Correction des processus se chargeant au démarrage qui n'étaient pas disponibles dans le tableau de bord sous les créations de processus.
- Empêchement de l'exécution simultanée de deux programmes d'installation, ce qui aurait enregistré la même machine deux fois.

# Empreintes MD5

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

---

Revision #1
Created 2026-07-24 06:29:15 UTC by Dennis Underwood
Updated 2026-07-24 06:29:15 UTC by Dennis Underwood