4.4.4.0

???????

- يتم تخزين تقارير الحوادث والقياس عن بُعد (telemetry) على القرص لسيناريوهات العمل دون اتصال.
  - نظراً لمحاولات العبث التي لوحظت ضد العديد من مخازن تسجيل EDR/XDR، قامت Cyber Crucible بتفعيل الحماية على مستوى النواة (kernel) للبيانات المخزنة على القرص قبل نشر هذه الإمكانية.
- زيادة حماية عملية الخدمة (service process) المستخدمة للاتصال الخلفي والتحديثات، كجزء من التحصين الاستباقي القائم على مبدأ انعدام الثقة (zero-trust).
  - لم يكن هذا استجابة لتهديد قائم، بل إجراءً استباقياً لتهديد يتوقع الفريق ظهوره مستقبلاً.

??????????

- تم إصلاح مشكلة عدم ظهور العمليات التي يتم تحميلها عند الإقلاع في لوحة التحكم ضمن قسم إنشاء العمليات.
- تم منع تشغيل برنامج تثبيت في نفس الوقت، وهو ما كان سيؤدي إلى تسجيل نفس الجهاز مرتين.

????? MD5

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

Revision #1
Created 2026-07-24 02:32:28 UTC by Dennis Underwood
Updated 2026-07-24 02:32:29 UTC by Dennis Underwood