

4.4.4.0

Funktionen

- Berichte zu Vorfällen und Telemetriedaten werden für Offline-Szenarien auf der Festplatte gespeichert.
 - Aufgrund beobachteter Manipulationsversuche gegen mehrere EDR-/XDR-Protokollierungsspeicher hat Cyber Crucible vor der Bereitstellung dieser Funktion einen Schutz auf Kernel-Ebene für die auf der Festplatte gespeicherten Daten aktiviert.
- Erhöhter Schutz des Serviceprozesses, der für die Backend-Kommunikation und Updates verwendet wird, im Rahmen der vorausschauenden Zero-Trust-Härtung.
 - Dies erfolgte nicht als Reaktion auf eine bestehende Bedrohung, sondern proaktiv im Hinblick auf eine Bedrohung, die das Team kommen sieht.

Fehlerbehebungen

- Behoben: Prozesse, die beim Systemstart geladen werden, waren im Dashboard unter „Prozesserstellungen“ nicht verfügbar.
- Verhindert, dass zwei Installationsprogramme gleichzeitig ausgeführt werden, was dazu führen würde, dass dieselbe Maschine zweimal registriert wird.

MD5-Hashes

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

Revision #1

Created 2026-07-24 04:04:21 UTC by Dennis Underwood

Updated 2026-07-24 04:04:21 UTC by Dennis Underwood