

4.4.4.0

Recursos

- Relatórios de incidentes e telemetria são armazenados em disco para cenários offline.
 - Devido a tentativas de adulteração observadas contra múltiplos armazenamentos de registros de EDR/XDR, a Cyber Crucible habilitou proteção em nível de kernel para os dados armazenados em disco antes de implantar esse recurso.
- Aumento da proteção do processo de serviço utilizado para comunicação de backend e atualizações, como parte do endurecimento de zero-trust com visão prospectiva.
 - Isso não foi uma resposta a uma ameaça existente, mas sim uma medida proativa para uma ameaça que a Equipe prevê estar por vir.

Correções

- Corrigido o problema de processos carregados na inicialização não estarem disponíveis no painel em criações de processo.
- Impedida a execução simultânea de dois instaladores, o que registraria a mesma máquina duas vezes.

Hashes MD5

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

Revision #1

Created 2026-07-24 05:20:22 UTC by Dennis Underwood

Updated 2026-07-24 05:20:22 UTC by Dennis Underwood