4.4.1.0

Features

- Expanded support for processes injection analytics, to dramatically increase the accuracy of detecting malicious vs benign intent for applications.
  - This became especially important due to a small number (<0.02%) of machines in Cyber Crucible telemetry alerting on aggressive process injection behaviors of system processes.
- Increased monitoring capability of unsigned system processes.
  - This was partially in response to attackers focusing heavily on involving those processes during lateral movement operations (on a system, and between systems).

Fixes

- Changed a file modification behavior to decrease false positives by no longer triggering on certain benign actions, through additional kernel-level context to a process' file-access behaviors.

WHCP/WHQL Validation Status

Validated.

MD5 Hashes

```
service.exe   = 0bab8404900c6a16ac3ad0293c45de5c
assistant.exe = 98f013fd4fdb7325f903d07c87b999ac
CCRRSecMon.sys (Windows10)       = 452719399d9bb98dc6b14fb8787d8415
CCRRSecMon.sys (Windows8)        = a974c7cc46db3759a2da34f37caaa72e
CCRRSecMon.sys (Windows7)        = 6a0f2e55d6a7b66bd9bbe318d5dbbebf
```

Revision #1
Created 2026-07-13 18:48:39 UTC by Dennis Underwood
Updated 2026-07-13 18:48:39 UTC by Dennis Underwood