How does Cyber Crucible use memory analytics?

Cyber Crucible kernel analytics track the state of the memory of a program during its entire lifecycle, from program start to program end. It also tracks the state of in-memory interactions with other programs.

The behavioral monitoring tracks for unsafe states in the memory of the program. This could mean an exploit, a software bug, or known in-memory (aka, “file-less”) attacks occurring.

This monitoring is performed live on the programs in a highly efficient manner, to ensure system and customer operations are not affected by Cyber Crucible analysis.

At point of possible attacker behavior for identity or data theft or extortion, this memory behavioral tracking and analysis is included in other telemetry gathered, to determine whether a program should be suspended.

Revision #3
Created 2026-05-18 20:28:41 UTC by Dennis Underwood
Updated 2026-07-20 19:22:39 UTC by Dennis Underwood