Does Cyber Crucible stop all process injection?

No!

There are a variety of activities which occur on systems which are process injection, but are not necessarily malicious.

Cyber Crucible makes all of these process injection activities visible for threat hunting and root cause analysis, but do not stop the activity unless the data extortion activities of data theft or ransomware encryption are begun.

Below is an example of process injection which is performed by PC Matic endpoint security software, called PCPitStop. It is likely a behavior they are conducting to inspect running processes.

5373968.png?width=680
Due to Cyber Crucible’s kernel-level behavioral analytics, you have complete visibility into all activities, regardless of the permission level of the software (to include highly privileged Microsoft or antivirus vendor software).

If an automated response is conducted, this page, and the Process Creations page, can be searched to provide fast investigation results.

Additionally, the REST API may be leveraged by threat hunting teams to query for indicators of possible malicious in-memory tradecraft.

Revision #3
Created 2026-05-18 20:27:14 UTC by Dennis Underwood
Updated 2026-07-13 19:57:39 UTC by Dennis Underwood