_General

Created by Dennis Underwood on May 19, 2022

Process injections are a software engineering capability that can appear in non-malicious context, or directly used by an attacker. In fact, process injection and associated techniques are a favorite of attackers, for a variety of reasons outside the scope of this article (but if you ask, we can point you towards training).

Cyber Crucible exposes process injection events at the kernel level. That means you have complete visibility for all processes and their information, regardless of the permissions of that process. Something we've found is that once attackers or software reaches a certain level of permissions, a lot of the traditional sources of telemetry for security tools go silent. Never missing an important piece of data, and never going silent, is a big part of our zero trust product design.

On the Process Injections page, you will see the following per event, with filters available to refine your queries:

CC_Showing_All_Process_Injection_Columns.mp4

Normally, in the course of an investigation, you'll find that there is additional activity in the Process Creation page.

Revision #1
Created 2026-05-18 20:27:17 UTC by Dennis Underwood
Updated 2026-05-18 20:27:17 UTC by Dennis Underwood