Can Cyber Crucible stop lateral attacker movement?

The product’s behavioral engine and Zero Trust methodologies effectively gather evidence of lateral movement.

That can be evidence of lateral movement from process to process on the machine itself, or can be discovering an attacker’s entry point to the system from a remote system, while conducting Root Cause Analysis.

Programs and their arguments associated with process injection methods and “living off the land” processes opening other processes are captured and sent to the Cyber Crucible.

Due to the kernel behavioral process analytics, there are no processes that are too privileged for Cyber Crucible observation and reporting (including other kernel drivers, or even other endpoint security tools).

Automated counter-extortion responses occur when either data extortion or ransomware encryption actions are begun.

For example, here is a video demonstrating lateral movement across a machine, using in-memory techniques, and the Log4J exploit. Please note that automated suspension of the affected process(es) occurred after data theft and ransomware behaviors were begun.

rr-log4j-procinj-3mins.mp4

Another example of this dynamic, demonstrates the use by an attacker to open a Windows shell. Observation captured all evidence, but the activity was suspended once the Windows shell began attempting data extortion activities (in this case, data theft)

rr-com-dll.mp4

Lastly, migration from an exploited browser is also observed, and in this case the attacker never successfully moved from the exploited Chrome browser, due to monitoring of the browser’s memory state:

rr-untrusted-chrome.mp4

Revision #4
Created 2026-05-18 20:27:12 UTC by Dennis Underwood
Updated 2026-07-20 19:22:33 UTC by Dennis Underwood