_General

Created by Dennis Underwood, last modified on Jul 03, 2022

Cyber Crucible currently co-exists with every major security vendor, if we use Gartner’s Magic Quandrant reports as a metric of industry incumbents.

Cyber Crucible’s endpoint software is reliably more resilient than other software, and that includes other endpoint security tools. Additionally, the other security software typically does not even have full visibility into Cyber Crucible’s software.

Another security tool attempts to shut off Cyber Crucible

Summary:

The other tool tries to shut off part of Cyber Crucible. They cannot. The other vendors' tool has not tested what happens when another tool (aka, Cyber Crucible), says, “no, I’m not shutting off”. The other tools crashes or enters an error state.

Cyber Crucible’s response:

The response can be two fold. The first is to whitelist Cyber Crucible software with the other vendor. This will cause the other tool to ignore Cyber Crucible software, which will (hopefully) prevent the other tool from entering an error state.

If that doesn’t work, it is up to our team to come up with a solution. We’ve learned that other vendors move a lot more slowly (several months or never) to fix a bug on their part.

Historically, in the few times this has happened, we’ve essentially created an environment where the other tool thinks it succeeded. A non-tech analogy may be letting your young family member or child beat you at checkers.

Another security tool attempts to run code as Cyber Crucible

Summary:

This happens very rarely, but there have been instances where a security tool attempts to inject its code into Cyber Crucible’s running program, and execute code posing as us.

This is no different than a hacker posing as a security tool, and there is no way to differentiate if a hacker has taken over t he “trusted” security (or any other) security program.

Cyber Crucible’s response:

There is not a scenario where Cyber Crucible will allow another company (or hacker) to run code posing as our product. The only solution at this point would be to whitelist Cyber Crucible software with the other vendor’s tool. There is no mitigation Cyber Crucible can provide for this, to prevent the other tool from attempting this behavior.

Fortunately, this is a very rare event.

Cyber Crucible is disabled by another tool

There were various instances where security tools with highly privileged accesses would repeatedly attempt to disable Cyber Crucible software. This included repeatedly attempting to remove our driver, or kill our service over and over.

While those issues never affected extortion defense, it did negatively impact user experience and system performance.

All of that is historical.

If another tool has the ability, legitimate or not, to disrupt Cyber Crucible - then a hacker could as well.

If you suspect or observe Cyber Crucible software diminished in any way, regardless of the software that caused it, please contact us immediately.

We are usually last tool standing between an extortionist and your critical data. There is no room for weakness in that circumstance.

Revision #1
Created 2026-05-18 20:27:29 UTC by Dennis Underwood
Updated 2026-05-18 20:27:29 UTC by Dennis Underwood