Does Cyber Crucible have false positives? What is the false positive rate?

Cyber Crucible strives for a 0 false positive product environment. Having said that, there are sometimes false positives. Let’s discuss where these come from.

Currently, the false positive rate is approximately 1 response per month, per 1800 deployments/agents, with full accountability for why those responses occur.

Corrupted Program Doing Rapid File Operations

Whether on purpose or through poor programming, sometimes programs either corrupt themselves, or are corrupted by other programs while running. We see this a lot with new features on large program suites, such as Microsoft Office, or proprietary custom-built software.

What happens is that the program’s memory is corrupted, which increases the level of inspection in the program. If that is then followed by extortion-like file access behavior, Cyber Crucible is forced to suspend the program. We’re getting better at identifying known bugs, and you get to at least run your program until it crashes (some automatically restart, some do not).

In a world where attackers do not use the file system, and hijack the memory of running programs instead, we have to err on the side of caution.

Cyber Crucible now has the ability to create a permission, where, if Program A, with arguments Arguments A, causes a corruption in Program B, with Arguments B - we can create a temporary exclusion for:

(Program A + Arguments A) opens (Program B + Arguments B)

That way there isn’t additional risk assumed that a hacker is involved, unless they just happen to use the exact same arguments.

An excellent example of this was when Microsoft first introduced opening Office documents from within their desktop chat software. It corrupted the Office program…every…single…time….then the Office program would start scanning all Documents on the machine about 25% of the time. That…needed an exclusion.

If you experience a crash, use the support button, and we'll help you make an exclusion, until the vendor fixes the issue.

Security Programs

Cyber Crucible does really well co-existing with security programs. Opposite to what most new customers think, more advanced security tools tend to use more advanced system interactions than antivirus programs that use older technologies. In fact, some free or inexpensive security tools run a variety of insecure Powershell scripts as a key part of their protection, versus actual programs.

As a highly resilient kernel-based security tool, Cyber Crucible is best viewed as being "lower", or "closer" to the hardware than most other tools. Cyber Crucible automatically identifies and adds other security tools to the behavioral models. As long as the security tools don't show signs of being compromised, they are allowed to operate normally.

Occasionally, a security tool will cause system instability, when their attempts to shut off or interfere with Cyber Crucible software fail. In those cases, it is best to whitelist CyberCrucible in the other security tool, to prevent it from trying (and failing) to disable or interfere with Cyber Crucible.

Feel free to open a support ticket with Cyber Crucible, via the web portal, to discuss the matter.

Administrative or Backup Tools

In some circumstances, a tailored behavior must be created for an administrative or backup tool, while the Cyber Crucible team develops an improved behavioral model. In this case, the Cyber Crucible team will assist in the creation of an exception in the behavioral model, which will single out the program plus arguments for an extremely small window of opportunity for a possible attack.

Revision #3
Created 2026-05-18 20:27:25 UTC by Dennis Underwood
Updated 2026-07-13 19:51:37 UTC by Dennis Underwood