Testing if Cyber Crucible Software is "Working"

Introduction

Cyber Crucible is designed to run without interrupting end users or employees, while quietly notifying chosen Dashboard users (typically chosen IT and Security team members) of automated responses.

A lot of the simulators for ransomware or malware do not accurately capture a hacker’s behavior. Even though that causes issues for tools like Cyber Crucible that (correctly) identify the simulation as a false positive, that isn’t necessarily a bad thing.

Some vendors will actually build their detection engines around these simulators for some of their detection functionality, to ensure that any customer tests pass with flying colors.

Real malware actions like ransomware encryption run the risk of unrecoverably encrypting or corrupting data. At Cyber Crucible, we’ve even seen ransomware secretly activates other malware on the network, or do other actions that could harm the company trying to test Cyber Crucible.

So, you don’t want to use malware, and you don’t want to use a simulator so accurate that you might accidentally corrupt your data.

Testing Cyber Crucible

There is an easy way to test Cyber Crucible without using malware or a simulation so realistic you put your or your company’s data at risk.

Cyber Crucible assesses digital identity accesses at every millisecond of the day. A lot of those digital identities are stored in the browsers - that is why attackers put web browsers to the top of the list for their automated targeting.

Cyber Crucible identity access behavioral analysis will result in one of three responses:

1. Do Nothing
2. Hide the data

    1. known legitimate application that passes all memory and kernel checks, but does not need access to that particular identity data - example: unexploited Windows Explorer
3. Suspend the process
    1. known legitimate application that should have access to the identity data but is hacked, or
    2. a strange application

Here are two locations that are common for Windows users:

In this case, the Windows username is “denni”, and these are the location where session data is stored. You may find the variable %LOCALAPPDATA% works for you if you don’t want to figure out the username.

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
    - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
    - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

The View Without Cyber Crucible Installed

Let’s first see what one of these folders looks like with Explorer.exe, without Cyber Crucible Installed.

Screenshot 2025-05-14 103339.png
Here, we see multiple Chrome Sessions under the “default” Google Chrome profile.

This information typically contains sensitive information that an attacker would want to hijack sessions with important programs like IT administration portal, banking, email, or storage tools like Google Drive or Dropbox.

The View With Cyber Crucible Installed

After installing Cyber Crucible, a quick test may be conducted, without using malware or any type of criminal techniques or misuse of IT equipment.

In this case, the same browser session storage location is used:

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
    - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions

- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
  - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

Screenshot 2025-05-14 103620.png
Cyber Crucible immediately after installation is already blocking access to the data in that folder.

Please notice that this is the exact same Explorer process that was already running upon installation, so the program running suddenly has had access revoked at the “hard drive” or kernel layer. Even programs, benign, exploited, or malware that are already running are correctly assessed by Cyber Crucible.

Seeing your test in the Cyber Crucible Dashboard

There are a large number of identity data accesses in a running system, at all times.

Software as a Service and cloud-based programs have resulted in many websites and applications that have limited on the website itself, while the browser (or embedded browser for applications) constantly communicates with data servers to populate spreadsheets, tables, graphs, and social media content.

Identity Access page

Identity accesses that are deemed appropriate for Cyber Crucible to suspend the offending application are listed in the Identity Access page.

These are situations where the program accessing the identity data should be stopped, not just have data hidden.

In this case, Explorer was not stopped after the multitude of checks Cyber Crucible conducted. Instead, data was just hidden.

Screenshot 2025-05-14 103741.png
Therefore, there are no identity access violations listed here.

Identity Access Hide page

Cyber Crucible optionally has the ability to show Dashboard customers situations in which identity data was hidden, but which there the accessing program was not stopped.

Explorer was not exploited or otherwise malicious in this test, it was just accessing very privileged identity data for the Chrome and Edge browsers.

Most users do not have access to this information given the additional load on the customers' machines and networks transmitting that data to Cyber Crucible servers.

Please ask if you would like access, but please know the activity you are seeing is not malicious activity, but identity data privacy behaviors Cyber Crucible conducts on a GRC, or policy enforcement, perspective.

Identity Hide Explorer.mp4
Here, we see in this short video, that Explorer was blocked from viewing the browser session data, even though Explorer itself was not interrupted.

Revision #4
Created 2026-05-18 20:28:49 UTC by Dennis Underwood
Updated 2026-07-20 19:21:38 UTC by Dennis Underwood