Does Cyber Crucible pass ransomware simulation tests?

The best answer is…it depends on the quality and accuracy of the ransomware simulations, but we haven’t seen many high quality tests that match true attack tools and behaviors.

Cyber Crucible examines underlying behavioral patterns in file access, memory behaviors, process behaviors, and cryptographic behaviors to identify and suspend data extortion activities in conjunction with an attack.

Some simulations of data extortion software have evolved over time, to be a more accurate representation of real attacks.

We have experienced simulations that, appeared to focus on checking for the data extortion countermeasures disclosed by some vendors, and not the tradecraft of the extortion tools and attackers themselves. A way to say this may be, “Testing for the countermeasure, not for the attack”.

In response, we never shy from tests against attacker emulation, penetration tests, or extortion tools. We routinely attack our own software, and replay attacker tradecraft we observe discussed online or found (and stopped) in client environments.

Revision #2
Created 2026-05-18 20:27:21 UTC by Dennis Underwood
Updated 2026-07-13 19:56:41 UTC by Dennis Underwood