Is This a Monitoring Tool Like My Other Security Dashboards?

The answer is, it depends on how you and your organization wants to use the tool, but probably "no".

It is important to note to product design strategies with Cyber Crucible:

1. Protection should be hyper-automated, and not require constant care and feeding (alert attention), nor knob-turning (configuration) by the users.
2. For more resource-rich security teams, the valuable telemetry should be available to them, for advanced threat hunting activities, or to support forensics and incident response activities.
3. Action #2 above, should in no way degrade the protection in place for action #1.

The most common feedback we receive from IT leadership is that their employees did not know Cyber Crucible had been protecting them for weeks already.

We have many users that leverage the tool in three capacities:

Set and Forget (Like Your Smoke Alarms)

Many organizations lack the resources to have threat hunters diving into Cyber Crucible (or other tool) telemetry, but they want the risk of data extortion “off of their plate”. That is perfectly OK, and Cyber Crucible’s Data Extortion Prevention is designed to do exactly that.

These users lack the resources to spend time looking at the Process Injection, Credential Protection, and Process Creation data feeds.

Hence, we find, unless they are responding to a rare automated response by Cyber Crucible, or are performing inventory management, like when a new machine needs Cyber Crucible deployed to it…

…they simply do not login to the Cyber Crucible web portal, and leave the automation to just do its job.

That is perfectly OK!

Advanced Threat Hunting, + Automated Protection

The process injection, credential use monitoring, and process creation capabilities provide a rich set of data, captured via kernel-level behavioral analytics, to conduct threat hunting.

The automated protection kicks in once data theft, credential (token, password) theft, or ransomware encryption begins. For everything else - this is a great resource.

The most common finding thus far is unmanaged (at least by the current IT admins) remote management tools installed by users. Yes, they do sometimes result in an automated extortion protection (aka, the unmanaged RMM is used by a bad actor), but it is always better to know more about your environment beforehand, regardless!

Here is a quick video of a type of attack we saw in use by attackers, in multiple client environments, that was used to successfully evade the customers' EDR solutions (we don't like to names...there were 3 products in four enterprises).

rr-com-dll.mp4

Post-Incident Forensic Analysis & Remediation

There are a couple types of use cases for Cyber Crucible data.

The first is so that a security person at a company, or an IT person, can investigate root cause for a program to be suspended. For some customers, who typically install our software, then only login again when there are new employees to onboard, they have never used any Cyber Crucible functionality except for the Manage Agents page. We're glad to help them learn about root cause analysis - which is painless and simple for technical and semi-technical users.

The second type of customer for post-incident forensic analysis are DFIR firms that are called in to investigate an issue at a client, sometimes at the cyber insurance company's request, and Cyber Crucible is installed after an issue. (Hey, we can't always be there before the attacker, as much as we want to be...otherwise every company in the world would have us, and extortion would be history!)

The best way to describe a roll-out after an extortion attack is, “messy”. Not because we are difficult to install or start protecting. Quite the opposite! In that instance, the attackers have normally moved around the system, and are embedded in operating systems, network gear, Active Directory, and are operating in memory. Multiple machines end up having processes suspended, and sometimes the attackers even try to regain control. It is a bit like taking medicine that makes you sick in the beginning, but you need it to ever get better.

Clients who are already stressed out, sometimes react emotionally to “more” noise, as the attackers are finally rooted out and defeated. There is a lot of education as to why or how their in-place security stacks didn’t find the attackers. At the end, though, the business regains control over their IT infrastructure. They will not become one of the 80-90% of companies that are re-extorted a year or two later, in what we call, “the extortion subscription economy”.

The third type of customer we have is an MSSP that, oftentimes is a partner of Cyber Crucible, that is responding to an automated protection from Cyber Crucible. They need to find out the way the attacker achieved a temporary foothold, and close any holes in security. The good news is that HIPAA or other compliance reporting typically reports little or no breach of confidentiality, due to the speed of the automated response. Many times, the MSSP reports, “nothing to report”, which makes everyone involved happy. Well, except for the criminal.

Revision #3
Created 2026-05-18 20:27:24 UTC by Dennis Underwood
Updated 2026-07-20 19:22:46 UTC by Dennis Underwood