Feedback from CDW

About the author

Tyler Booth is a principal offensive security consultant at CDW in the USA. He has over a decade experience in offensive security. He created and built out CDW's Adversary Simulation services (red/purple team) that they deliver to our customers. He spend a lot of time doing internal R&D work, tool dev, infrastructure management, etc.

Tyler 's feedback on OST

"There are a few reasons why I sought out Outflank and OST. Primarily, I just know they do great work and publish research that found pretty compelling. I was scrolling through their services and saw a reference to OST, read the slides they had published, and decided that I had to see a demo of the tooling in action. Specifically, I really wanted to see how they did the Hidden Desktop stuff because it sounded like an interesting piece of tradecraft and apparently it worked differently than the standard HVNC variants you see in the wild.

*Anyway, we decided that even if we do research work and tool dev, it's just too costly for us to maintain internal projects when we have so much billable consulting work to do. I really looked at OST as a toolkit that **really augmented our own internal tooling and allowed us to focus more on delivering consistent engagement**s - not spending all of our time during an operation maintaining our own internal payload generation frameworks or writing our own UDRLs for Cobalt Strike. We make an effort to use everything OST has provided us from Stage1 to some of the miscellaneous tools that really make things easier for an operator.*

*Surprisingly, **the sleeper hit** in OST isn't even the tooling itself (which is very good), but **the technical deep dives** with the Outflank team, the **documentation, and honestly the community engagement**. There are a lot of different red teams who support each other in the slack channel, share some tradecraft, and it seems like most people there just want to prop others up.*

One of our biggest initial concerns was how much support we'd receive - especially since we're in vastly different time zones and it's a hosted service. For example, there are some hiccups that occur every now and then; maybe something in the portal breaks or you find a bug in one of the tools. As soon as you report it, the Outflank team is already on-top of the issue and pushing patches. This really exceeded our expectations from that standpoint.

If I could summarize, my major points are:

- *Outflank Security Tooling is a great asset to support operations.*
- *Documentation and technical deep dives are great ways to learn new tradecraft.*
- *Support is solid and the product is ever changing/improving."*