NCSC for Startups: Playing cyber criminals at their own game

CounterCraft's co-founder, Dan Brett, explains how they turn the tables so that social engineering can be used to protect organisations from attackers.

A veteran of the NCSC For Startups alumni community, cyber security company CounterCraft graduated from the programme in March 2017.

Launched by Dan Brett and co-founder and CTO David Barroso, CounterCraft was intentionally created as an international operation from the get-go. “We have a UK subsidiary in Derby and a US subsidiary in New York, while our headquarters is in San Sebastian, northern Spain. The idea was always to have something of a double DNA going on inside the company” Dan tells us.

“You might ask: Why Spain? It’s not very well known for cyber. And that's true. But on the other hand, with an R&D centre in northern Spain we can attract and recruit staff, and hopefully retain them by offering a really attractive work-life balance.”

While Dan points to retaining members from the R&D team in London for anything beyond three years as a battle – because staff are commonly approached by nearby competitors – he and David sensed an opportunity. “We wanted to do something in this region of Spain,” he says, talking to us from CounterCraft’s San Sebastian office on a video call. “For example, you can surf in the morning on Saturday then drive up to the Pyrenees Mountains and ski that afternoon, or vice versa.”

And when the team isn’t hitting the waves or shredding fresh powder, CounterCraft’s distributed threat deception platform offers clients (which include government, banks, retailers and telcos) a real-time intel feed and managed service that helps organisations detect targeted attacks.

Asked whether it’s fair to say CounterCraft is designed to play attackers at their own game, Dan concurs: “Even at a basic level, phishing emails are an attack method to get into places through lying to people about what you're doing, so most attacks depend on some form of deception.

“We recognised an ongoing cycle where organisations would get breached, call in a forensic team to clean up the system, only to then be at risk of getting breached again. We became frustrated with this continual breaching of network systems, so the goal was to build a very strong perimeter to any kind of network and keep the bad actors outside.

"If you accept the fact that adversaries’ attacks are ongoing, you can engage with them over a long-term period and gather information while staying protected. It's a huge win for defenders. We try to turn the tables to apply social engineering back at the attackers. It's interesting because deception is a technique, not a technology. It's a way of thinking about how to prepare your defences, so organisations can easily detect and deal with very serious attacks at the right time.”

Having worked with David and other members of CounterCraft in previous companies within the threat space between 2008 and 2012, the team saw an industry pattern that desperately needed disruption. Dan says developing the solution required a degree of acceptance that there will always be cyber criminals. However, that was balanced with the recognition there’s a new way to deal with them.

CounterCraft’s solution deploys a deceptive environment around a customer’s technology systems, which (to attackers) appears like an inviting door asking to be opened. In reality, if the criminal penetrates CounterCraft's faux API, they’ll discover the cupboard is bare. Meanwhile, for all the time the attacker has spent trying to access the meaningless domain, CounterCraft has been monitoring the attack, enabling the organisation to get advanced warning that they’re under threat. It’s a moat for the fort, so to speak.

"We watch and see who starts messing around to break into the underlying tech that supports the API, which gives you insight into how often you're attacked,” Dan says, “allowing you to recognise what level of technical ability attackers possess, so you can gather information about the quality and quantity of attacks.”

Being part of the NCSC for Startups was instrumental for CounterCraft to refine its art, and get the product suitable for market needs. “The programme gave us an awareness of the intelligence community,” Dan reasons. “David and I aren’t from that background, so we were able to understand their mission set and problems to develop as a business and be of

use to the intelligence community.” This much is demonstrated with partnerships today that include organisations such as NATO and the US Department of Defense.

“Without being on the NCSC programme, we wouldn't have understood the challenges this group of people are facing, so that was a huge win for us,” Dan adds.

The original expectation was that most of CounterCraft’s work would be in the private sector but it’s around a 50:50 split between private and public. "We were surprised how strong the demand is. For businesses, it’s about saving money and protecting their operations, while law enforcement agencies want to find bad actors and make their lives more difficult, and that's a good thing for society.”

At the time of joining NCSC for Startups, CounterCraft had around 12 members of staff. Fast forward to today and the business has 51 employees.

Looking to the future of the business and how he sees it evolving, Dan is optimistic: “Let's do just as well in the UK as we are in the US, and get our technology into as many of the FTSE 100 companies as we can to protect national infrastructure. The UK is uniquely placed to be proactive and forward-thinking about how the country approaches development of appropriate defences. I think the NCSC is leading that, and CounterCraft is prepared to be a part of it.”

Dan Brett
Co-founder, CounterCraft

WRITTEN BY

Dan Brett
Co-founder, CounterCraft

PUBLISHED

25 January 2024