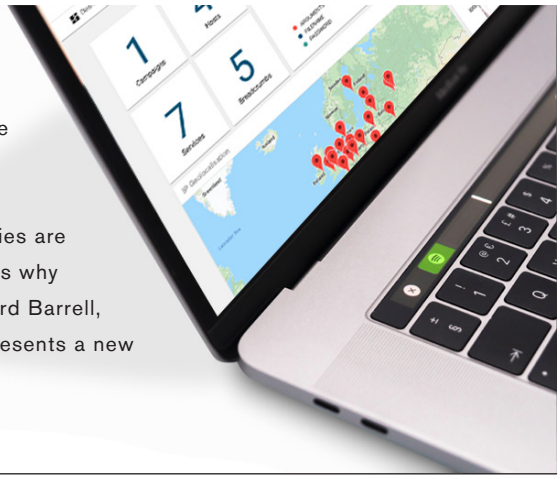
Deception deconstructed: how CounterCraft 2.0 works

We recently released the latest evolution of the CounterCraft Cyber Deception Platform. Our robust and powerful tool for the design, deployment and management of enterprise cyber deception now benefits from an enhanced user-interface, optimized workflow and an automated behaviour analysis engine technology that will revolutionize the role of today's Threat Hunter.



Mature organizations with an appetite to diversify their existing enterprise defence strategies are leading the adoption of emerging cyber deception solutions, but first let's remind ourselves why deception is so effective in the context of threat intelligence. Our Product Manager, Richard Barrell, deconstructs CounterCraft 2.0 in this enlightening overview of a product release that represents a new level in development.

They're Already Here. Now What?

The use of deception is as old as the Trojan horse, or Sun Tzu's principles of the Art of War. However, with exception of a few honeypots installed as isolated projects, the use of deception within the enterprise is not widespread. This is in spite of it being an excellent way to achieve visibility on malicious activity within the network and gain insight into who is trying to attack and, more importantly, why. However, as a result of the advances in this area in the last three years, cyber deception is now receiving a lot of interest, especially from those who wish to take advantage of the valuable threat intelligence these techniques can provide.

The Cyber-Deception Platform

Technical Architecture

The CounterCraft Cyber Deception Platform offers a zero production-impact solution as, unlike other deception tools, it does not run on production systems. The deployment of deception assets has absolutely no impact on normal, authorised users and produces no negative impact on the real systems within the production environment (networks, servers, authorised users etc.).
The principal components of the CounterCraft platform are as follows:

Deception Director. The console – the heart and central control point for the entire platform. The Deception Director enables you to manage all aspects of the deception environment, and all events are monitored and analysed from the web frontend.

Deception Hosts. These are the real servers or desktops that are deployed and that have the CounterCraft Agent installed. These systems can run Windows (Desktop or Server) or Linux. They can be physical devices, virtual machines, or located in the cloud (AWS / Azure / Digital Ocean etc.).

Agents. As mentioned before, the CounterCraft Agent is a small piece of software that runs on the Deception Hosts in order to monitor all activity on that device and report it to the Deception Director, via a connection to a Deception Support Node (DSN). The agents are fully cloaked, making them very difficult, if not impossible, to detect.

Deception Support Nodes (DSN). The DSNs are collection and relay points to pass on the data sent by the agents to the Deception Director. DSNs add a layer of abstraction to the deception environment and permit complex and scalable deployments in diverse network topologies or even within the cloud.

Deception Assets. These are the basic building blocks of the deception environment; the honeypots, the breadcrumbs, the bait that is discovered by the would-be attackers and that which entices them further into the deception campaign. They come in various shapes and sizes according to the goal of the deception deployment, for example: servers with specific OS, specific services (shared folders, web-applications, SSH etc.), documents (Google Docs, Office etc.) or even credentials – including for Active Directory, SYSVOL, or to allow lateral movement to another deception host.

Analysis Tools

One of the key aspects of the new version of the CounterCraft Cyber Deception Platform is the level of analysis that can be performed from the Deception Director console.
Event data generated from adversary activity within the deception environment is sent to the Deception Director in the form of log files. The raw logs are analysed automatically in order to create Events, then the Events themselves are parsed to extract Objects. Objects are data-points within an Event log that have additional value in terms of intelligence, for example: IP addresses, passwords, command parameters or even customisable keywords. One of the key aspects of the new version of the CounterCraft Cyber-Deception Platform is the level of analysis that can be performed from the console:

Event Analysis. As a first step to analyse adversary behaviour, the Deception Director console offers a powerful tool in the form of an adaptive, drill-down filter. The filter allows a Threat Hunter to apply contextual filters to the Event data to hone in on a specific activity. In addition to the raw data, the Event data is enriched with additional information from various sources, such as IP geo-localisation data, VPN endpoint identification, Virus Total binary analyses or even data from the CounterCraft behavioural analysis tool. To allow granular search patterns, the enriched data is appended with individual and searchable tags.

Malware Analysis. If an adversary tries to execute software or malware within the deception environment, the Deception Director provides a direct analysis. Any binary that is executed is automatically copied to the Deception Director console for analysis, using Virus Total and YARA rules to produce automatic malware reports. If it is necessary to explode the malware for more detailed investigation, the Deception Director allows direct integration with an existing CUCKOO sandbox to perform the analysis.
This level of integration with third-party systems highlights the CounterCraft philosophy of not trying to reinvent the wheel. If tools already exist, we will integrate with the best available solution, rather than waste time trying to develop our own inferior copy.

Behavioural Analysis. The adversary behaviour analysis engine is one of the key new features in the new CounterCraft Cyber Deception Platform. This engine automatically analyses Events from the deception environment with reference to a CounterCraft proprietary database of known behavioural patterns. The patterns include commonly used tools, techniques and procedures (TTPs) and behaviour patterns of known Advanced Persistent Threats (APTs). The analysis is completely automatic, and the pattern database currently stands at over 7000 indicators of compromise (IoCs) gathered from known adversaries, this number is growing daily thanks to the efforts of the CounterCraft Threat Intelligence Team. The database is kept fresh with regular updates from CounterCraft.
The automatic behaviour analysis enriches the Event data, and also allows adversary activity to be visualised in the context of the Mitre ATT&CK™ framework.

Incidents

Once adversary activity has been captured from within the deception environment, the Events can be grouped together to form an "Incident". The creation of an Incident allows the Threat Hunting team to group isolated but related Events in order to study them together, and in context, in order to create a complete image of the attack.

For example, when a Notification is added to an Incident, all the related Events and Objects (with both extracted data such as IP addresses or user agent, and enriched with the additional CounterCraft data) are added automatically as well.

The Incident data can be exported in standard formats such as CSV, OpenIoC, Gephi, or STIX2 to allow further analysis with external tools, or by uploading the data to Threat Intelligence sharing platforms such as MISP. The incidents support the Traffic Light Protocol (TLP) to classify to what level the data may be distributed.

The Future

With the release of the 2.0 version of the CounterCraft Cyber Deception Platform we have reached a new level in development, but it does not stop there. Improvement is continuous, based on combining our vision of the future with customer feedback. The next areas of focus are to increase integration with third party solution and to increase the power of the analysis tools – among other areas – in order to stay at the cutting edge of cyber deception and to become an indispensable tool for anyone who hunts the threats to their organisation.

Next Steps…

Would you like to know more? Would you like to find out how CounterCraft can help create valuable and specific threat intelligence from within your organisation?

We are happy to explain what we do, and how we can help you get the best out of deploying deception – from an initial conversation or simple demo, to a fully featured deployment.

Contact us to begin your cyber deception journey with us

REGISTER FOR A TRIAL

craft@countercraftsec.com