# Cyber Deception Tech Brief: Threat Intelligence Analysts

CounterCraft

**Create powerful targeted Threat Intelligence and Analysis**

## Make complex threat intelligence more relevant

The increasing maturity of cyber attackers and their approach to infiltrate and disrupt organisations, using advanced Tactics, Techniques and Procedures (TTPs) means defending teams invest more heavily in trying to understand and predict future adversary behaviour.

The solution is to enhance Threat Intelligence and use it to inform defensive behaviour. This includes People, Process and Technology and also investments and organizational structures at a tactical, operational and strategic level.

> “High value alerts - all signal, no noise”

## Beat Threat Data Overload: Use Deception to provide detailed in-house Threat Intelligence

There has been major growth in the supply of Threat Data, Information, Intelligence and Analysis to help form the enterprise cyber defence posture. Much of this information is too generic. The trend is towards information overload, creating environments swamped with high volumes of threat data from across the world that cannot be acted upon.

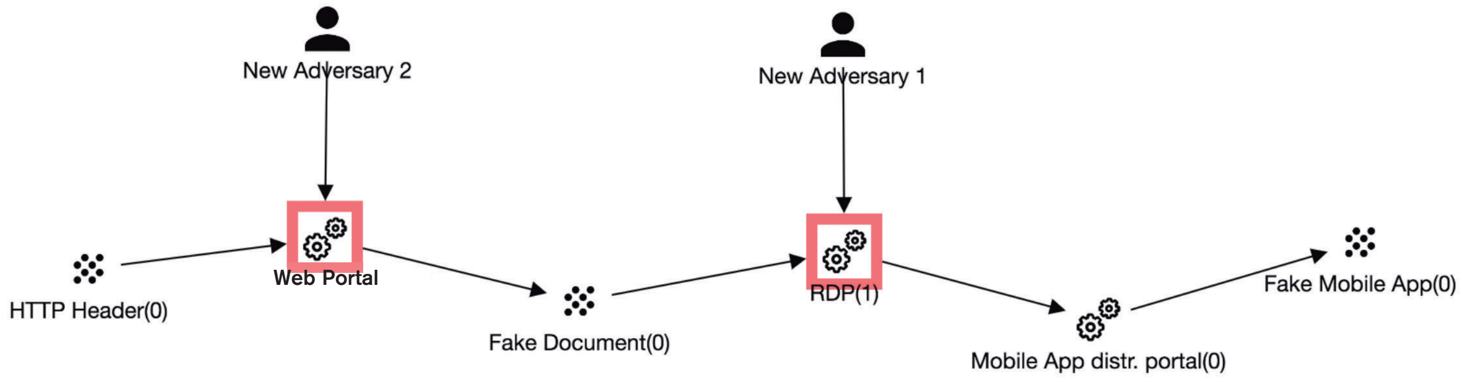
The CounterCraft Cyber Deception Platform provides a new solution to this problem by using Deception Logic to deliver real-time 1st party threat intelligence from your own network.

## Interact with adversaries for rich TTP insight

Using CounterCraft technology allows Analysts to quickly create a synthetic deception environment that runs alongside operational ICT estates. This provides first-hand and timely threat intelligence from attackers trying to infiltrate information assets and systems.

By automating major aspects of creating a credible deception environment, that scale and blend within the extended enterprise environment, Analysts are empowered to work at the levels of abstraction that best suits their business purposes.

Working through an advanced visual Console interface that connects with the Deception Director™ it is possible to design, define, deploy and monitor a comprehensive range of Deception Assets and also critically to plan Deception Operations that interact with Threat Actors.

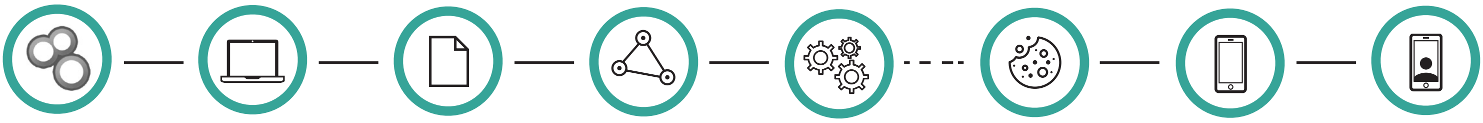


# Deception planning, Logic and Analyst outcomes

Using a full deception environment changes the balance between defender and attacker. It allows defenders to analyse in depth every move taken by an attacker as they execute against an attack life-cycle – from reconnaissance through to maintenance of their presence within the enterprise. As a result it is possible to gain direct knowledge of TTPs, without endangering real production systems.

Analysts can act as Deception Planners themselves, or work with a dedicated deception team to analyse how and why a particular attack vector could be chosen and what Course of Action will be taken by both attacker and defender. This can be based on prior intelligence or using Heuer's well known Analysis of Competing Hypothesis (ACH) methodology.

The Cyber Deception Platform provides visual tooling to support the creation of Deception Logic that describes how specific attack paths are handled automatically by the Deception Assets, and to show progress against them in real time.



## Building actionable Threat Intelligence, and Analysis

### Monitor

Once the Deception environment goes live, the instant an adversary engages with even the simplest Deception Asset, the platform is gathering attack telemetry at a very detailed level. This is abstracted for the Analyst to be able to interpret the specifics of an attackers' behaviour, and gain knowledge of what kind of information assets and systems are being targeted, and the full range of TTPs being deployed.

### Enrich

The platform provides threat data enrichment options, and links with other sources such as Cuckoo and VirusTotal, and enables a deeper insight into Adversaries and Intrusion Campaigns.

### Export

The Deception Director™ provides advanced correlation of all attacker behaviour across the Deception Environment and the Analyst can examine all of the information through the Console, or can have the information exported to other platforms using STIX2.0, CSV, OpenIOC or MISP, or a fully functional CounterCraft API.

## Deception based intelligence delivers more value

In-House Threat Intelligence is priceless. It is generated from your own specific enterprise environment. It is directly actionable by the defender team because it comes from the reality of your ICT systems and business processes.

✓ Create threat reports based on on real, timely and specific in-house intelligence

✓ Research your adversaries using real ICT systems in a controlled deception environment

✓ Gain visibility of internal threats from internal sources (employees, sub-contractors, clients, guests etc.)

## Learn more about CounterCraft deception

REGISTER FOR A TRIAL

craft@countercraftsec.com