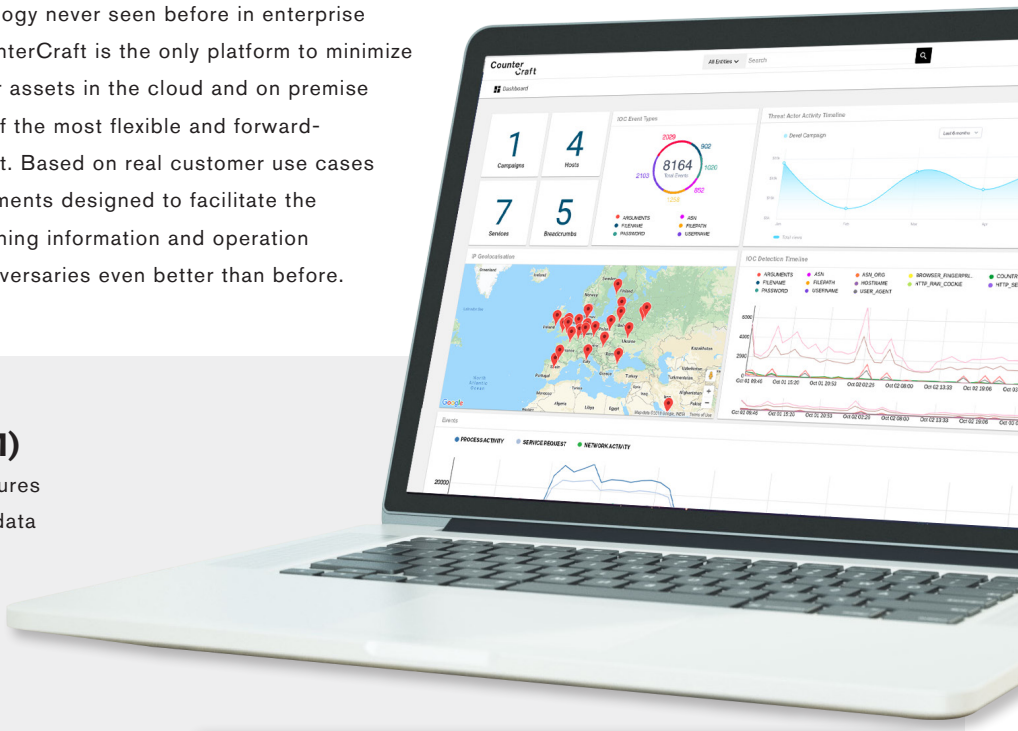
Technical Memo:

Detect, understand and respond to your adversaries with CounterCraft 2.6: improvements, features and functionality

Our latest release comprises revolutionary technology never seen before in enterprise cyber counterintelligence and cyber security. CounterCraft is the only platform to minimize the impact of a cyber attack using buffer zones for assets in the cloud and on premise and with capabilities that are proven to be some of the most flexible and forward-thinking currently available in the deception market. Based on real customer use cases and feedback, CounterCraft 2.6 includes improvements designed to facilitate the role of the threat hunter within organizations spanning information and operation technology, enabling users to get to know their adversaries even better than before.



Adversary Insight Mode (AIM)

AIM consists of a series of enhanced UI features to facilitate the role of analysts, comprising data explorer, shadow shell and command line reconstruction using raw threat data and threat intelligence.

UX and UI

CounterCraft 2.6 includes a multitude of user interface improvements and automation to benefit the operator, administrator and the architect. The role of threat researcher comes into its own with this release, which includes a brand new button to automate the display of exactly what has been put in command, complimenting the existing role-based access control functionality.

Events, search and display

Extensive work has been carried out to make using the platform as intuitive as possible. This is especially shown in our new Data Explorer. This release delivers increasingly specific event searching capability providing adversarial analysis in the simplest and most efficient way yet.

Simple ticketing

CounterCraft is now integrated with Zendesk. It gives users a direct link to CounterCraft to make reporting and raising requests fast and simple.

Delivering across all five stages of deception

CounterCraft 2.6 delivers across the board, with a strong focus on engagement with threat actors. This is thanks to more than 35 third party systems integrations that are now live, including:

- **MISP**
- **Cloud:** Gmail and Microsoft
  Microsoft Office 365: enables automated generation of fake emails
- **SOAR:** Enables automated generation of fake emails
- **SIEM:** Splunk
  A brand new CounterCraft app available from the Splunkbase with powerful deception metrics offering unified attack data for clients using CounterCraft and Splunk
- **SWIFT:** Integration is now complete to prevent fraud across payment, email and social media platforms.
- **Mobile Phones**

Deception catalogue

A catalogue of 25 ready-made deception campaigns templates are now embedded into the platform, a first-to-market in the field of deception and dramatically simplifying and shortening the time-until-launch for deception campaigns.

Notifications

Highly personalized alerts can now be configured on Telegram, Signal, Twitter, MSN Team and email.

Multi-tenancy enables more advanced capabilities

Multi-tenancy combined with high-level confidentiality enables partner organizations to offer deception-as-a-service and run campaigns requiring additional levels of confidentiality. CounterCraft 2.6 delivers one of the most cost-efficient deception solutions with the introduction of cloning and isolation functionality, simplifying the campaign creation process.

Advanced MITRE ATT&CK capabilities

Based on the MITRE ATT&CK database of known threat actors, it's now possible to calculate the probability of different types of attack occurring and create a profile of your attacker. Based on these insights, you can significantly enrich your next threat hunt with campaigns set up specifically to try to identify the attacker correctly using TTPs as well as IOCs.

Highly enriched event data

CounterCraft 2.6 provides a high level of enrichment to augment the raw event data generated by adversary activity within the deception environment. As well as geolocation data from IP2Location and Maxmind databases, the CounterCraft draws information from a multitude of sources including VirusTotal, Tor Nodes, Yara Rule and the IP-Abuse Database

More deception assets

We've expanded our range of deception assets that are ready to install on demand, including advanced WiFi routers, SCADA assets such as Programmable Logic Controllers (PLCs) and medical devices supporting both HL7 and FHIR, enabling clients to create a synthetic network simulating a credible production environment in whatever sector.

National Security License

CounterCraft 2.6 features deliver significant value for very complex adversaries and specific use cases within Government and Defence sectors.

About CounterCraft

CounterCraft is a pioneering provider of full-spectrum cyber deception and ground-breaking threat hunting and cyber counterintelligence to detect, investigate and control targeted attacks. Our award-winning solution combines powerful campaign automation with controlled synthetic environments to allow attackers to penetrate organizations without doing real damage.

CounterCraft is recognized worldwide for its radical contribution to the deception technology market and operates in more than 20 Fortune500 Index companies globally, including financial institutions, governments and Law Enforcement Agencies. Founded in 2015, CounterCraft is present in London, Madrid and Los Angeles, with R&D in San Sebastián (Spain).

Download our latest documents at

countercraft.eu

or if you prefer contact us at

craft@countercraft.eu