

The CounterCraft Platform

Counter
Craft

How the world's most advanced deception technology works.

This is threat intelligence 2.0.



The best active defense
tech on the planet.

We have built the highest-quality deception platform for active defense. Our proprietary ActiveLures™ populate ActiveSense™ environments and communicate using our ActiveLink™ technology.

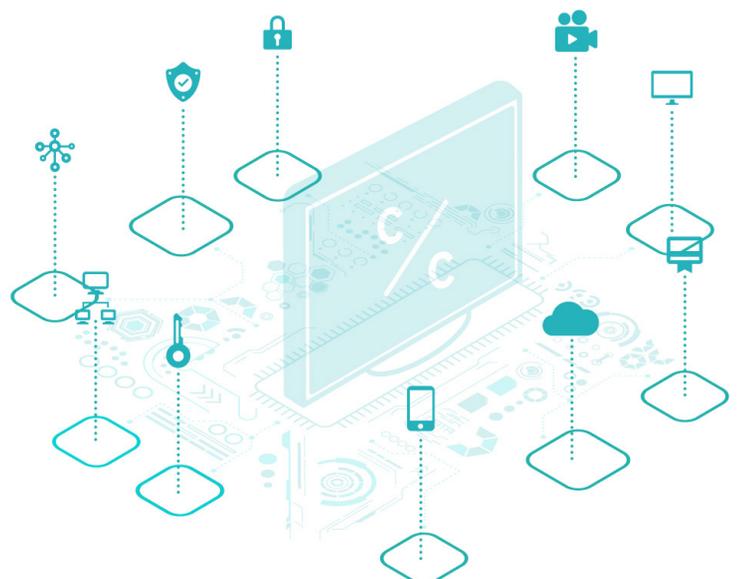
CounterCraft Unique Technology

CounterCraft's proprietary technology is made up of award-winning components that work to create realistic deception environments, allowing you to protect your network and gather specific, real-time intel on the adversary.

ActiveLures

Custom or template-based CounterCraft breadcrumb technology that can be deployed across multiple endpoints, servers or even on internet based platforms such as PasteBin, GitHub and Shodan. Both passive and active breadcrumbs allow you to tailor them to attract exactly the adversary you are targeting.

The main job of the ActiveLures is attract adversaries into the CounterCraft ActiveSense Environments.



ActiveSense Environments

ActiveSense Environments are the core of your CounterCraft deployment. They contain real machines and real services that provide a credible environment to deflect and monitor the adversary.

ActiveSense Environments are deployed quickly and controlled from the CounterCraft Platform. A wide range of host types and services are available, out of the box, to create an environment that is credible and makes the adversary think they have struck gold!

ActiveSense Environments combine the detailed telemetry collected by the DeepSense agents and the command and control capability of the CounterCraft ActiveLink network to provide a full, deep-sensing environment to collect and deliver all adversary activity in real time.

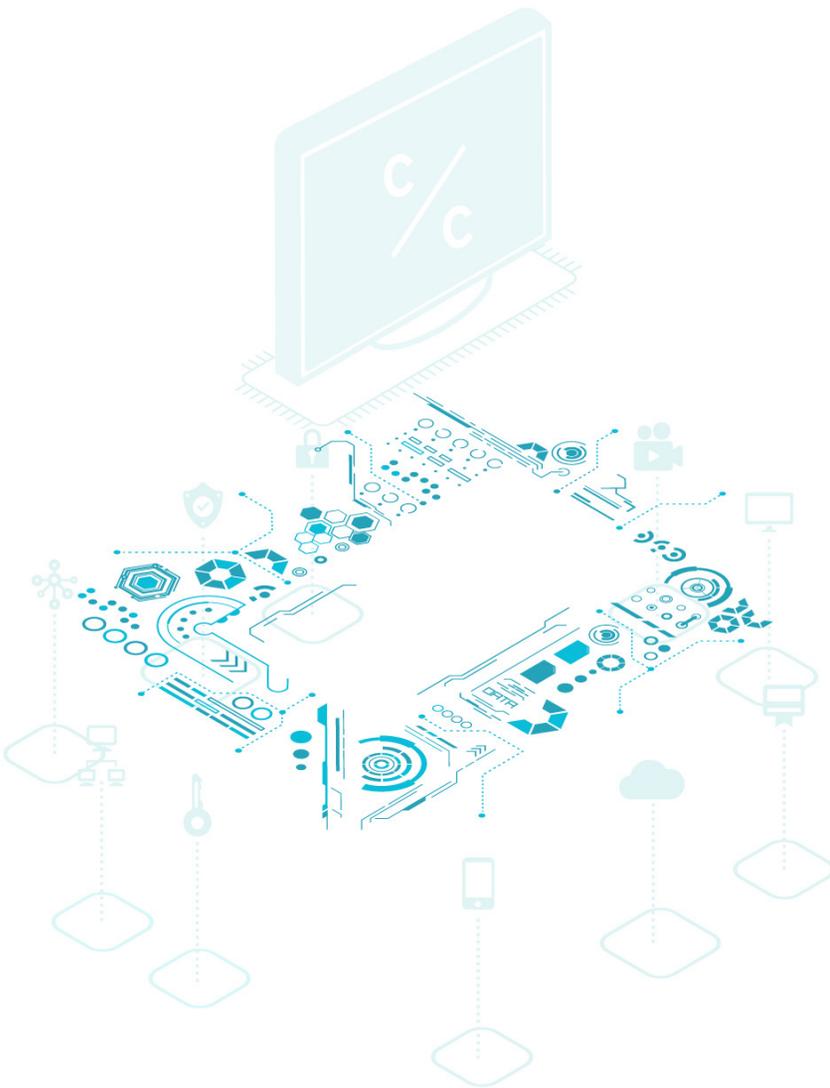
DeepSense Agent

How to gather telemetry unseen and undetected? The CounterCraft DeepSense agent is the key.

The fully cloaked agent gathers all adversary activity on the deception host and sends it back to the CounterCraft ActiveConsole via the ActiveLink command and control network.

ActiveBehavior

ActiveBehavior is a human interaction simulation tool that keeps a deception environment looking authentic without you lifting a finger by automating the process of logging in and performing “typical” user activities, or basic SysAdmin tasks.

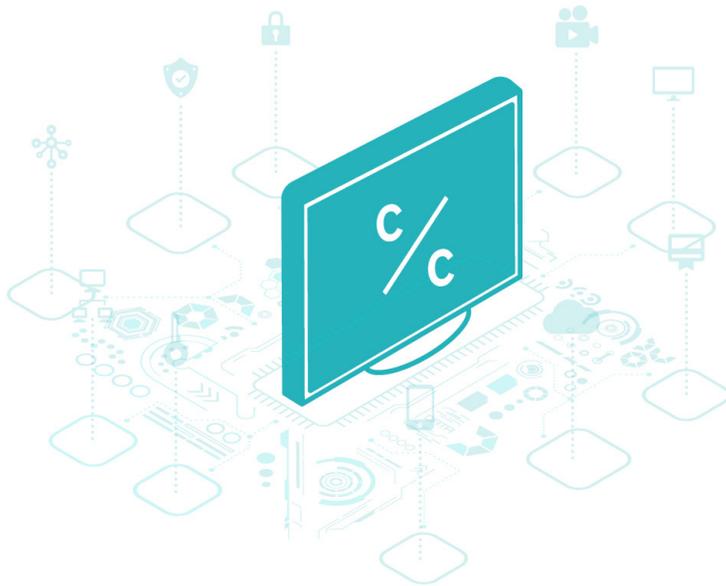


ActiveLink

How to deliver detailed telemetry on adversary behavior undetected and in real-time? The CounterCraft ActiveLink network does it all.

ActiveLink provides a full command and control network for the ActiveSense Environment. It allows completely cloaked exfiltration of DeepSense telemetry and also allows real-time control over hosts, services and breadcrumbs for instant response to adversary activity.

ActiveLink also allows the system to be deployed across a wide range of complex networks.



Deception Director

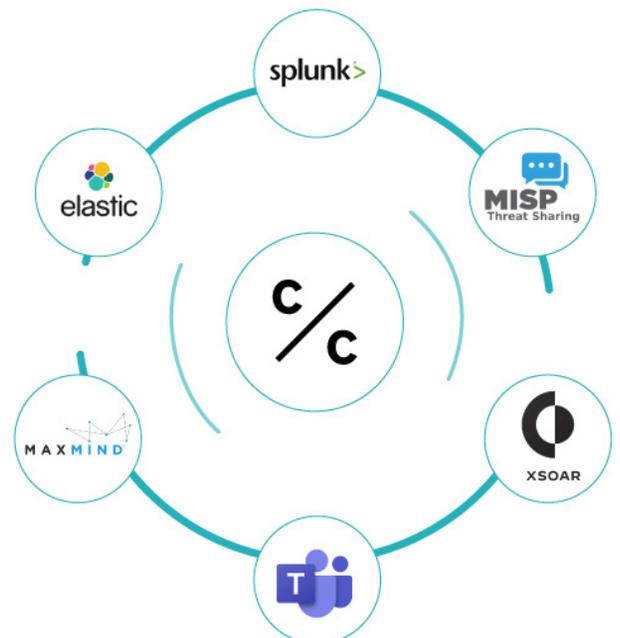
The Deception Director is the heart of the CounterCraft Platform. The web-based console provides full design, deployment, and management functionality for all of the components, from ActiveLures deployment to automatic responses to detected adversary activity.

The Deception Director can be hosted locally or remotely and provides a powerful tool for analysis and alerting and active defense deployment.

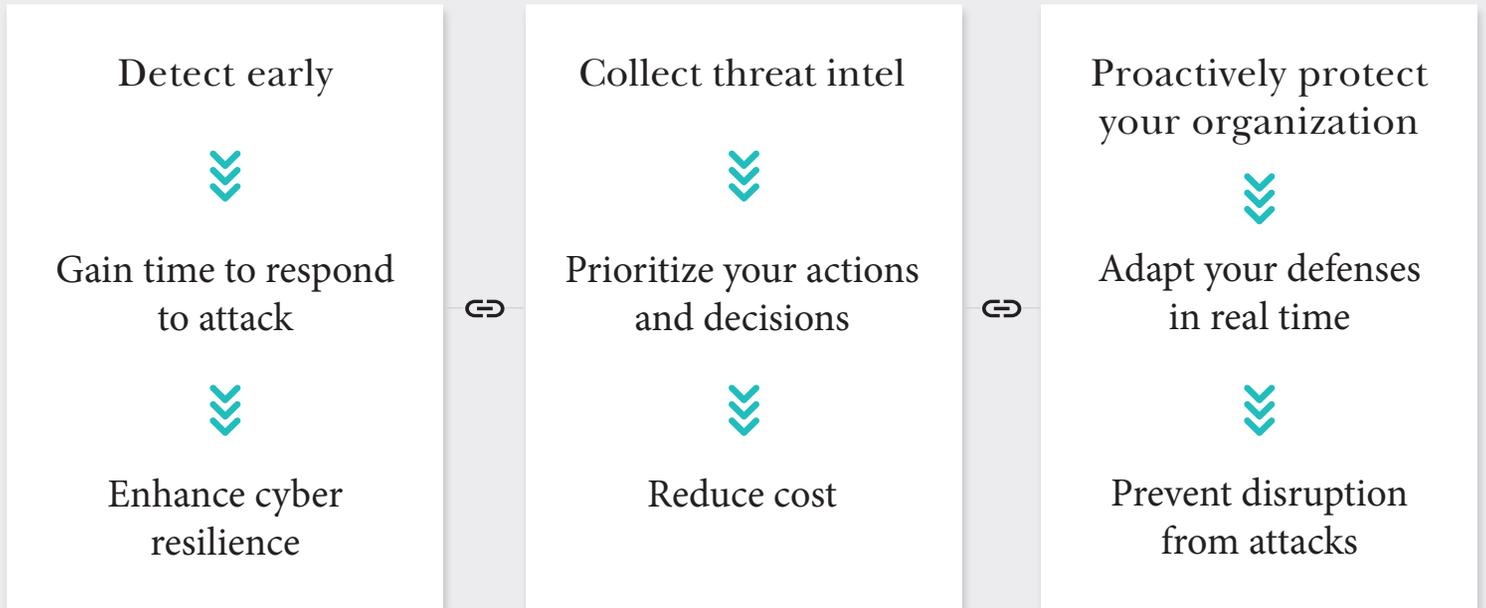
Integrations

The CounterCraft Platform plays nicely with other platforms. If you need to share threat intelligence or incident data with another platform, our many integrations make this easy. Whether it's a SIEM, SOAR, Intel Sharing Platform or messaging service, the chances are it is already part of the CounterCraft third-party integration family.

If you can't find your specific app, a fully documented RESTful API is available to make new integrations a breeze.



Business Benefits



A Unique Approach to Proactive Defense

 **Widest Coverage** - Works inside and outside the traditional enterprise perimeter. Fully cloud integrated. Easily deploy buffer zones around vulnerable cloud assets.

 **Friction Free** - Host-based with cloud infrastructure integration - no need to plug into internal network equipment.

 **Highly Automated** - Highly automated deployment and management process means reduced resource usage.

 **Ready To Go** - Pre-installed with best-of-breed deception use-case catalogue. Non-experts can use the system out-of-the-box.

 **Use Case Flexibility** - Campaign-based approach to deception allows you to deploy multiple use cases for deception with the same tool.

 **Adversary Mapping** - Don't wait for the attackers to breach your network. Associate threat intel data with our adversary profiles. Get ahead of the threat cycle, understand their TTPs and strategic drivers.

About CounterCraft

CounterCraft is the next generation of threat intelligence. The CounterCraft Cyber Deception Platform offers active defense powered by high-interaction deception technology. Countercraft detects threats early, collects personalized, actionable intelligence, and enables organizations to defend their valuable data in real time.

Their award-winning solution, fully integrated with MITRE ATT&CK®, fits seamlessly into existing security strategies and uses powerful automation features to reduce operator workload. Founded in 2015, CounterCraft is present in New York, London, and Madrid, with R&D in San Sebastian, Spain. Learn more at www.countercraftsec.com.

Download our latest documents at



countercraftsec.com

or if you prefer contact us at



craft@countercraftsec.com