

Active Defense: The Tech Behind The Platform™



How the world's most advanced
deception technology works.

Active Defense: The Tech Behind The Platform™

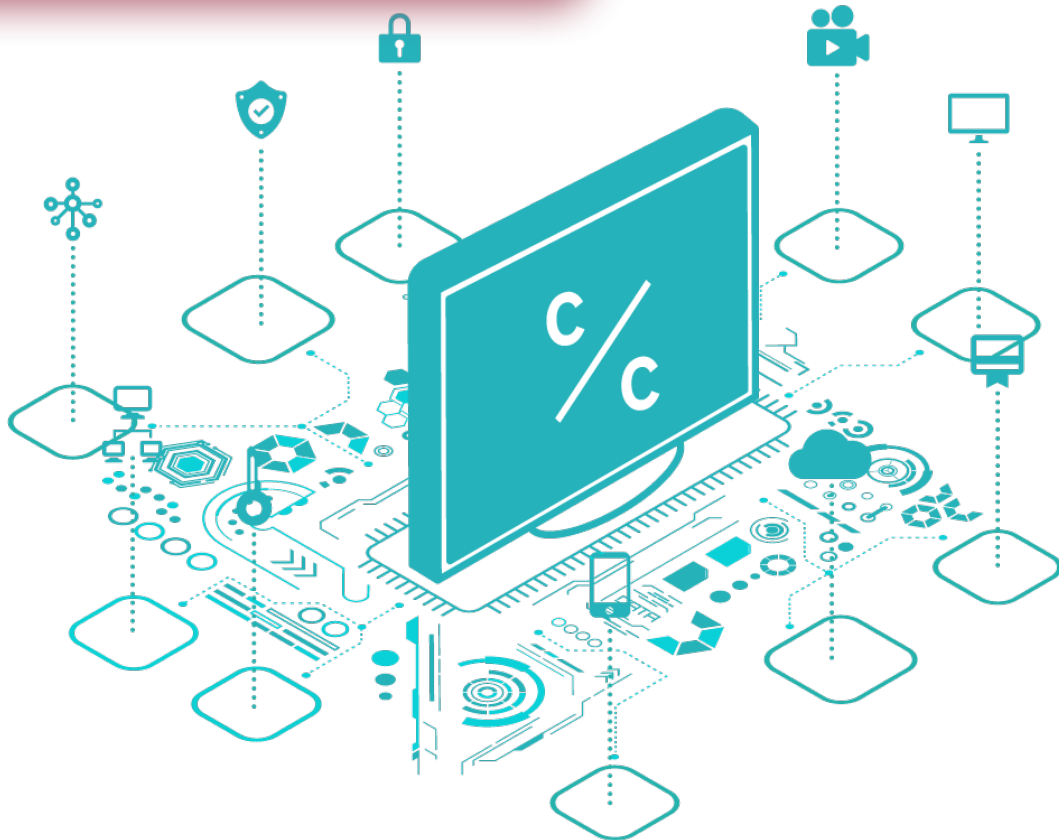
How the world's most advanced deception technology works.

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 UniqueTechnology

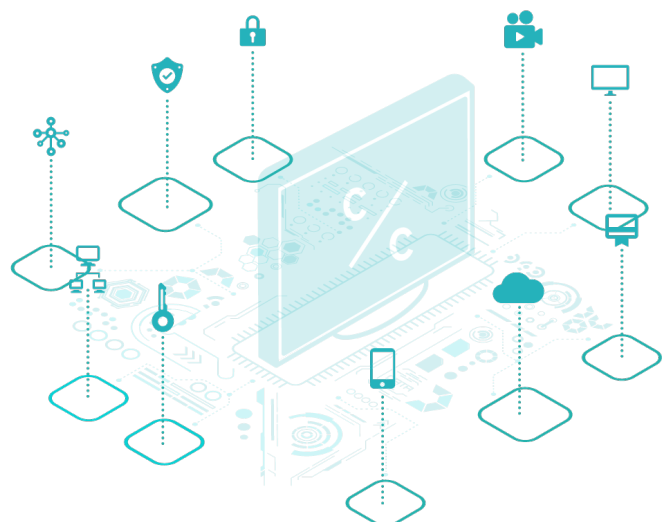
CounterCraft's proprietary technology is made up of award-winning components that work to create realistic deception environments, allowing you to protect your network and gather specific, real-time intel on the adversary.



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!

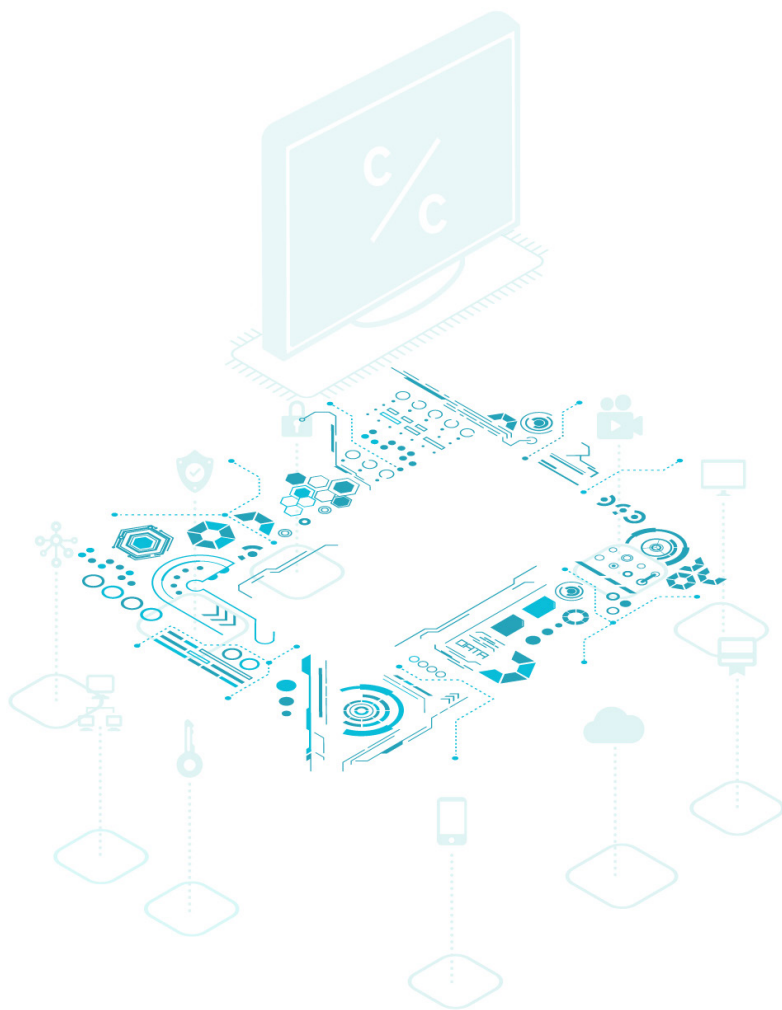
ActiveSense Environments combine the detailed telemetry collected by the DeepSense agents and the command and control capability of the CounterCraft ActiveLink network to provide a full, deep-sensing environment to collect and deliver all adversary activity in real time.

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. ActiveBehavior allows organizations to create custom fake users, each with a full pattern of life. These personas operate in the deception environment, with realistic behavior and unparalleled hands-on keyboard simulation luring attackers that fall for it.

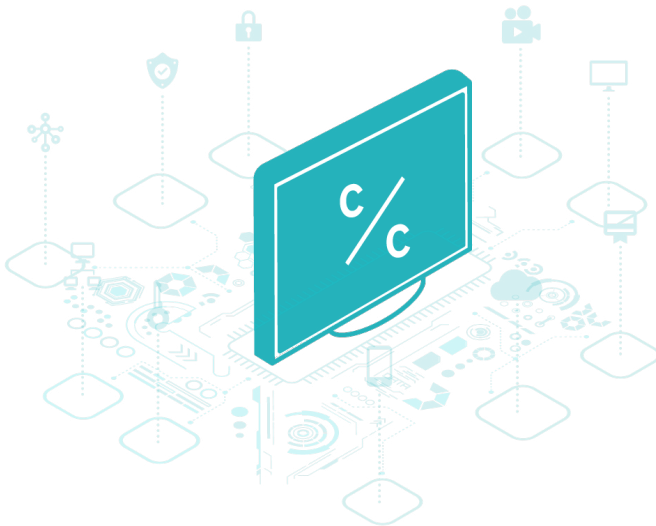


ActiveLink™

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

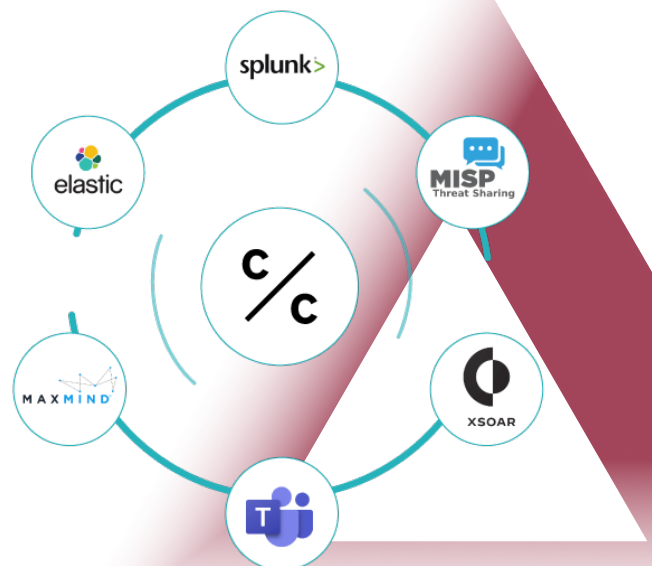
The Deception Director is the heart of the CounterCraft Platform. The web-based console provides full design, deployment, and management functionality for all of the components, from ActiveLures deployment to automatic responses to detected adversary activity.

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.
-  **Ready To Go** - Pre-installed with best-of-breed deception use-case catalogue. Non-experts can use the system out-of-the-box.
-  **Friction Free** - Host-based with cloud infrastructure integration - no need to plug into internal network equipment.
-  **Use Case Flexibility** - Campaign-based approach to deception allows you to deploy multiple use cases for deception with the same tool.
-  **Highly Automated** - Highly automated deployment and management process means reduced resource usage.
-  **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 Us

CounterCraft is a software company that goes beyond detection and response to provide proactive cybersecurity solutions and detect attacks faster for the world's leading organizations. Their premier product, CounterCraft **The Platform™**, consistently stops red teams, spear phishing, ransomware attacks and insider threats. This distributed deception platform is a global leader in active defense, with tooling that provides real-time intelligence and the capability to manipulate adversary behavior. Their technology stops attackers in pre-breach recon phases, integrates contextualized threat intel with incident response workflows, and saves money and time by helping security teams prioritize their actions. CounterCraft The Platform is used successfully around the globe by Fortune 500 companies and government organizations, including the US Department of Defense.

Find out more. Request a demo at



countercraftsec.com