

The CounterCraft Cyber Deception Platform

Counter
Craft

Actively defend critical business systems, processes and data



Despite heavy investments in cybersecurity, targeted cyber attacks continue to succeed.

Traditional threat prevention doesn't keep out the flood of malware and malicious emails that your organization faces: advanced attackers keep getting in. Undetected, they can operate as long as it takes for them to achieve their goals. Invisible, they can operate without creating a threat intelligence trail.

- ☑ CISOs are under pressure to prioritize security resources.
- ☑ Heads of SOCs face evolving and more hostile threat landscapes with limited resources.
- ☑ Threat intelligence managers suffer from intel feeds that provide no context and low actionability.

Tilting the Luck Scale in Your Favor

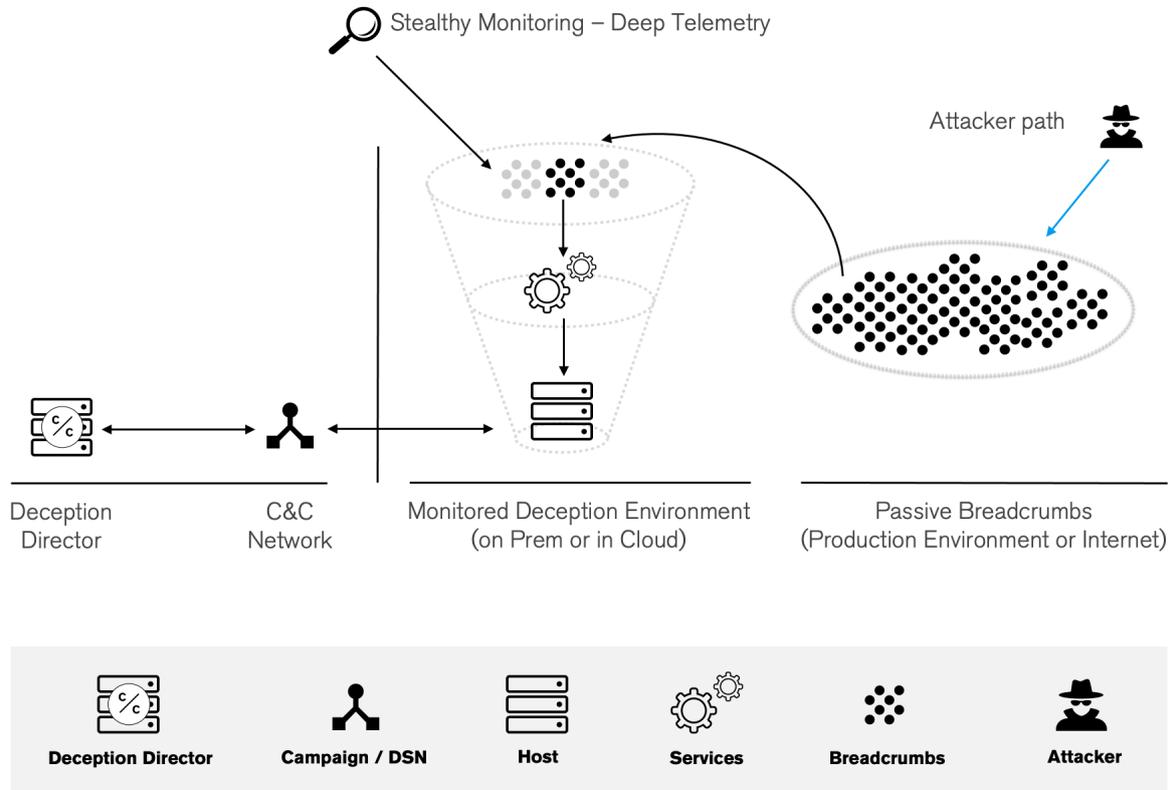
Security and risk management leaders feel rightfully frustrated by the asymmetry between attack and defense. Defenders need to be right 100% of the time, and attackers just need to be lucky once to find a hole in an otherwise solid cybersecurity posture.

Is it Time to Change your Approach?

- 1 Detect Adversary Activity Early:** Generate high-quality alerts of adversary activity earlier than any other system: Pre- & Post-Breach detection. Force attackers to reveal themselves during "pre-attack" phases of attack planning and reconnaissance, or during the internal lateral movement phase.
- 2 Collect Enriched Threat Data:** Gather real time threat data from adversaries activity. Automatically enrich it with TTP, MITRE ATT&CK and IOC context. Integrate this data with your Threat-Intel workflow. Deliver high impact threat intel feeds (targeted and timely) to your subscribers.
- 3 Manage Adversaries:** Integrate with intelligence and incident response workflows. Immediately reconfigure other enterprise systems to resist the attack. Interact directly in real-time with the adversary to manage, delay and deflect the attack to extract more intelligence data from the adversary.

How does it work

Distributed deception technology builds and deploys a synthetic environment that fools adversaries into engaging with false information and fake digital assets instead of real operational systems and data. While attackers plot a path through the network, you are gathering detailed information about their Tactics, Techniques and Procedures (TTPs).

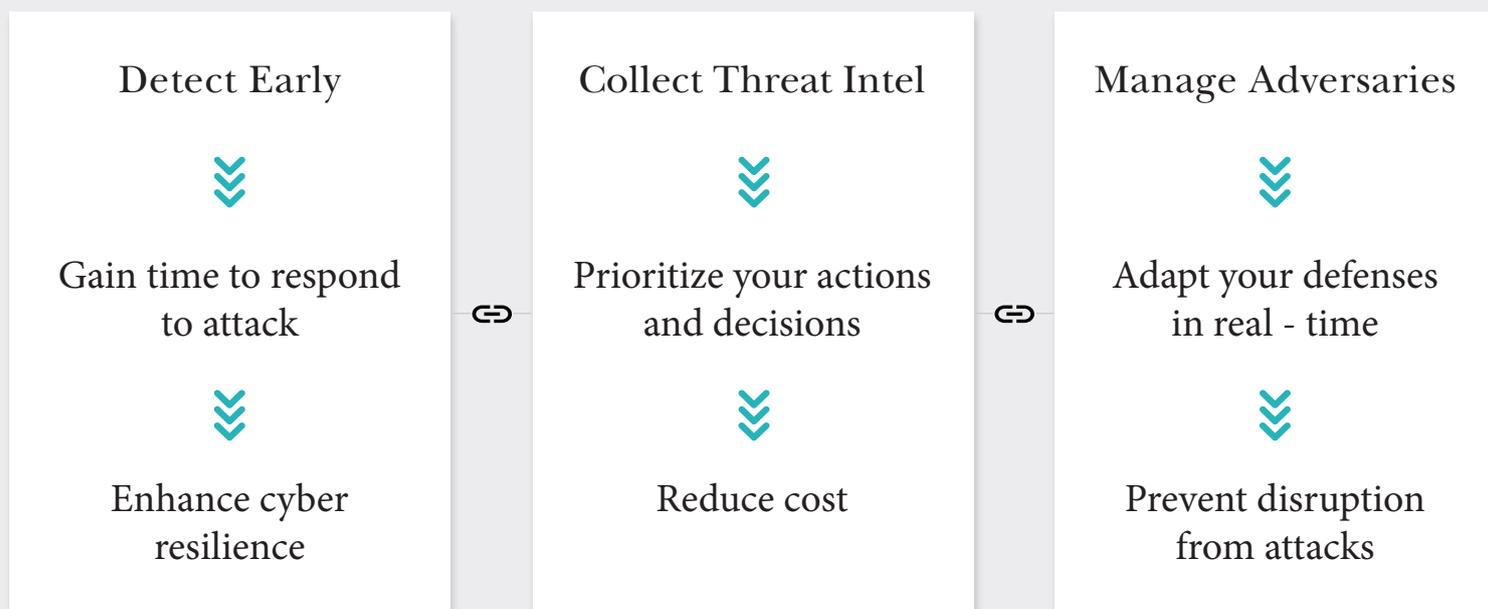


The CounterCraft Cyber Deception Platform automates the design, deployment, monitoring and maintenance of the deception environments. By using an approach based on deception campaigns, you can easily deploy deception for specific use cases in just a click.

The screenshot shows the CounterCraft dashboard interface. Key features include:

- Header:** CounterCraft logo, search bar, and a 'Choose a campaign' dropdown menu.
- Notifications:** A card showing 2 notifications.
- TTPs:** A card showing 364 TTPs.
- Events:** A card showing 811 events.
- Alerts:** A message: 'The sky is the limit! Now you can integrate with your SIEM, SOAR, TIPs, etc.. Have a look to the Integrations to see the available options. Don't forget to check the Users Manual for advanced use. Please contact us at support@countercraftsec.com if you have any doubts.'
- Organizations:** A list of organizations including 'Microsoft Threat Computer Systems Company Limited'.
- TTPs List:** A list of TTPs such as T1098 (194), T1021 (89), T1043 (57), T1059 (9), T1053 (6), T1078 (6), and T1083 (1).
- Event Types:** A list of event types such as 'SpecialPrivilegesAssignedToNewLogon' (194), 'CreateConnection' (157), 'InvalidAuth' (136), 'NetworkFloodDetected' (100), 'HttpRequest' (77), 'CreateProcess' (40), and 'SetOwner' (26).
- Events per minute:** A line graph showing event frequency over time from April 24, 00:13 to 22:22.
- IP Addresses:** A list of IP addresses such as 84.102.49.50, 143.172.71.14, 10.62.194.68, 193.202.215.145, 10.10.10.10, 10.62.194.30, and 51.124.76.146.
- MITRE ATT&CK:** A table of MITRE ATT&CK techniques categorized by CounterCraft techniques and Matched techniques. Categories include Breadcrumb Access, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Lateral Movement.
- IP Geolocation:** A map showing the geographic location of IP addresses, with markers for Greenland, Iceland, Sweden, Finland, and Russia.
- Incidents:** A section for managing incidents with a search bar and a table with columns for TLP, Status, Name, and Created.

Business Benefits



A unique approach to active 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. Get ahead of the threat cycle, understand their TTPs and strategic drivers.

About CounterCraft

CounterCraft is a pioneering provider of full-spectrum cyber deception technology offering attack detection, threat intelligence collection and proactive defence to clients. 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



countercraftsec.com

or if you prefer contact us at



craft@countercraftsec.com