Threat Intelligence Service as a Service

CounterCraft

Identify cyberthreats before they attack your online IT assets, remote workers, and networks

The CounterCraft threat intelligence service (CC-TIS) provides cyber threat reconnaissance for your on-line IT assets, as well as for remote workers and the VPNs connecting them to your business. Our cloud-based managed service is fast and easy to implement and delivers actionable threat intelligence to your team through a user-friendly dashboard. Identify threats early—so you can adapt your defenses to stop them.

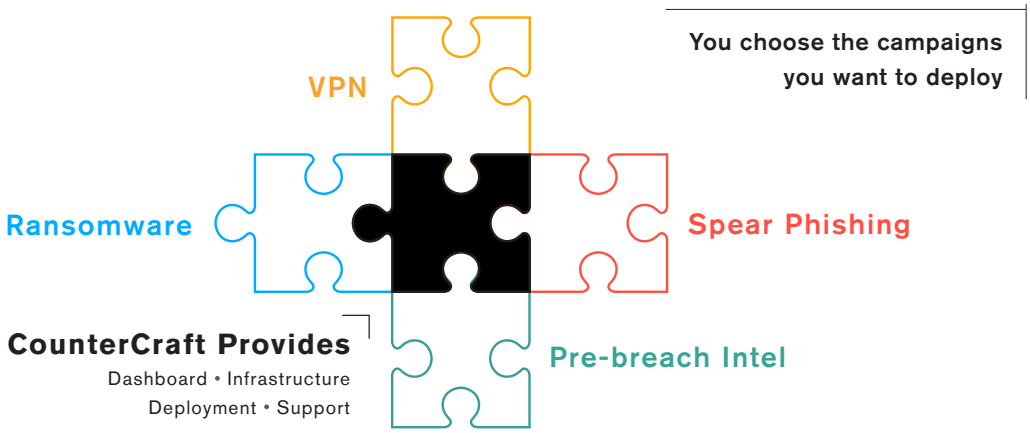
Why CounterCraft Threat Intelligence Now?

The COVID-19 crisis has redefined enterprise work environments. With employees suddenly forced to work remotely, companies' infrastructures and security teams are feeling the strain. Telework takes employees out of the hardened enterprise environment and places them in home environments with varying levels of cyber protection. More information and sensitive data is now communicated outside of known boundaries, using more personal devices, and across more different channels. Until recently, VPNs were not considered to be a major cyberattack vector. Today, they are the primary access to enterprise applications and services for remote teleworkers. As more enterprise services are accessed via teleworkers over VPNs, or are exposed as cloud-based services the corporate attack surfaced has blossomed.

Cyber attackers have wasted no time in attempting to exploit under-secured VPNs, larger attack surfaces, and new vulnerabilities. Organizations might face the same threats and tactics, but the entire playing field has changed. Are your current security control sets effective against the new threats you face?

The Solution

CounterCraft threat intelligence service (CC-TIS) is a fully managed service that provides early detection of external threats to your on-line IT assets, remote workers, and networks. The service is deployed and managed in the CounterCraft cloud, and over the open Internet.



We create threat intelligence campaigns using deception techniques. For example, we deploy attack vector discovery assets (breadcrumbs) to identify cyberthreats scouting your on-line IT assets from the outside. We analyze all surfaced threats and collect intelligence on the threat, the threat actor capabilities, and their intended target. Unlike generic threat intelligence feeds, CounterCraft alerts include information about attackers' Tactics, Techniques, and Procedures (TTPs) cross-referenced with the MITRE ATT&CK framework, as well as Indicators of Compromise (IOCs). You can easily feed this data into your incident response, SIEM, ticketing and other systems for taking action.

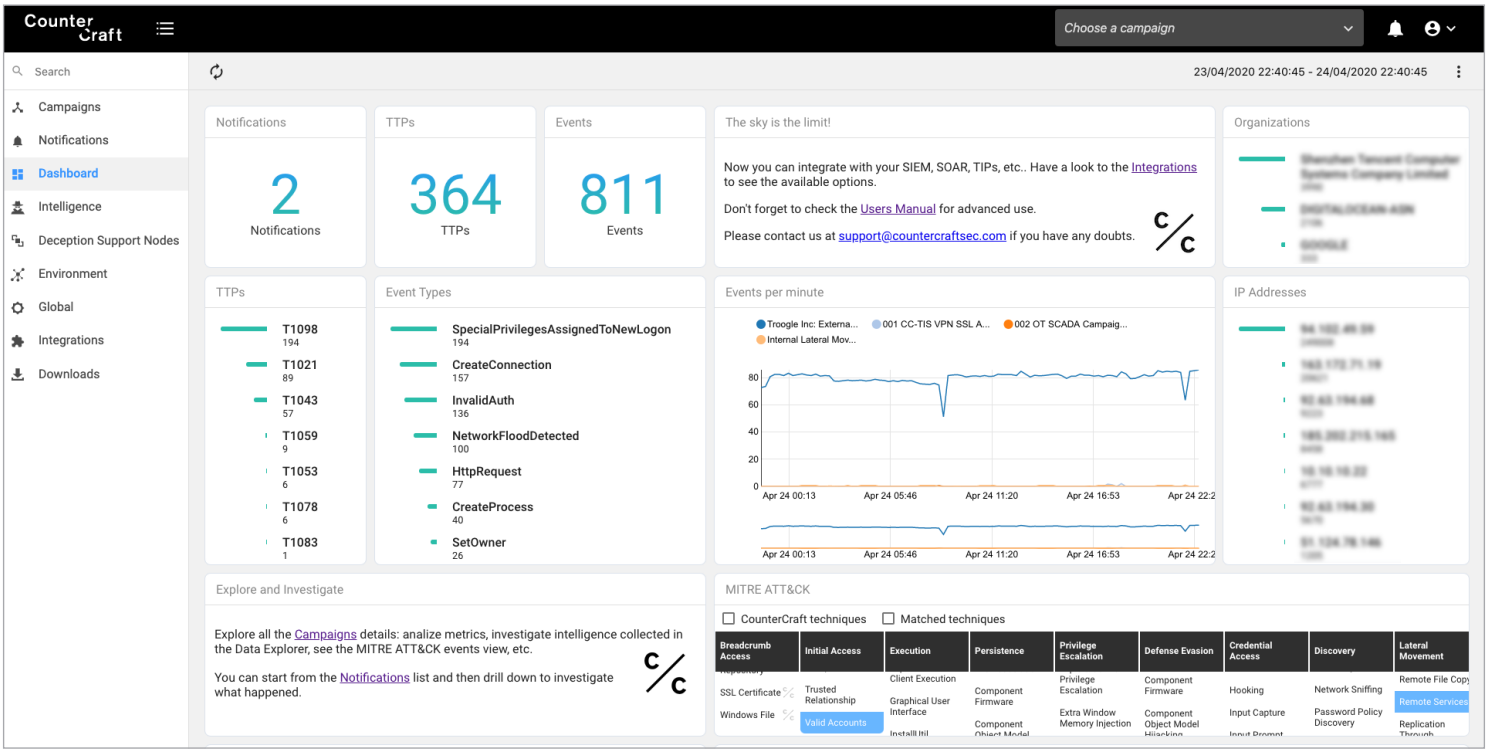
Features

1 **Plug and Play:** CounterCraft implements and manages the service. There is no need to dedicate resources or purchase, deploy, or configure infrastructure. Service terms are flexible with a monthly subscription that can be cancelled at any time.

2 **Tailored Campaigns:** CounterCraft deploys the campaign tailored to your specific organization, so you receive IOCs and TTP alerts targeted directly at your business. Intelligence events directly reflect threats attacking your on-line IT assets. Examples of campaigns include: Early detection of targeted Ransomware attacks; Remote Working Infrastructure assurance (VPN protection); Detection of Threat Actor Reconnaissance activities; Investigation of Spearphishing attacks.

3 **Rapid Deployment:** Begin a intelligence led cyber deception campaign and receive actionable information within hours.

4 **In-depth Actionable Data:** Our advanced monitoring dashboard enhances security, discovery, analysis and risk governance data while uncovering previously unidentified actors and cyber threats.



Business Benefits

No Additional Resources Needed

Our service requires no skilled staff or other internal resources from your team. As a turnkey service completely configured, managed, and delivered by CounterCraft, CC-TIS automatically increases your team's productivity.

Proactively Protect Your Company

CounterCraft CC-TIS feeds can be connected with SIEM, TIP, SOAR, EDR, UEBA, and other tools for proactive defense. Use the data to block IP addresses, revoke credentials, harden firewalls, and take other measures to boost protections where needed. CounterCraft campaign data also can be integrated with orchestration solutions to automate response playbooks.

Improve Overall Security Effectiveness

CounterCraft provides high-impact intelligence, enriched by attackers' TTPs, IOCs, and threat actor characteristics. You receive contextualized profiles of external adversaries trying to compromise your remote working infrastructure or workers. You gain a time advantage, because deceptive assets delay attackers as they try to identify vulnerabilities for exploitation.

Cover the New Attack Surface Cost-Effectively

For a simple monthly subscription, you can significantly improve reconnaissance and proactive defense of a much larger attack surface. At the same time, you gain enriched data that enhances capabilities of your existing systems.

Strengthen Your Strategy

Threat intelligence based on deception delivers actionable information for aligning corporate security strategy with available resources to build a stronger security posture. Information from CounterCraft CC-TIS provides threat intelligence breadth and depth for communicating the value of threat intelligence teams to key management and board members.

How to Buy

CounterCraft offers various CC-TIS options. We launch with two options to detect attackers at any level—from script kiddies to nation state threat actors—through deception assets created to identify different levels of penetration difficulty. Both options deliver clear detection and in-depth attack intelligence as described above.

1 **Pre-Breach Intel**

Provides early detection of attackers conducting technical reconnaissance of vulnerable external facing IT and cloud services associated with your on-line IT assets.

2 **Remote Worker and VPNs**

Add a layer of assurance to your remote workers by deploying a vulnerable VPN service and associated breadcrumbs to detect threat actors searching for entry.

3 **Spear Phishing**

Mitigate the risk of spear phishing attacks penetrating your organization.

4 **Ransomware**

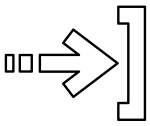
Mitigate the threat of ransomware to your business by detecting the initial stages of targeted ransomware attacks.

5 **All Services**

Gain simultaneous, comprehensive external threat detection across your on-line IT assets' attack surface.
Get a discount from multiple purchases.

6 **Client Journey**

We have designed a low-friction journey for you to start enjoying the benefits of the service:



Access the full service description and commercial offer by completing the form on the website.

Resolve any doubts with the sales team and return the signed commercial offer.

Enjoy the service! Attend the onboarding tutorial, meet your account manager and hold regular meetings with your client satisfaction team.

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