CounterCraft Cloud™

Pre-breach threat intelligence service

Measure your organization's external risk exposure

Digital resilience and transformation are the imperative drivers in the current economic climate.

The primary source of revenue generation for your business, in today's economic climate, is the online channel. And, your online presence is how you communicate with customers and maintain your online footprint. Therefore, **the protection of your online presence has now become the number one operational imperative for your organization.**

The Extra Challenges:

- Attackers use pre-breach reconnaissance activities to gather information about your digital defenses and open doors that can be leveraged in attacks targeting your organization.
- Pre-breach reconnaissance activities are probably the longest phase of an attack.But, this phase is the most difficult to identify and mitigate against for any organization.
- It is very difficult to gather accurate and actionable pre-breach threat intelligence that is delivered in real-time.
- All organizations face a lack of resources: no one has the time or money to make threat data into actionable intelligence.

Implications:

A successful attack against your online presence can be leveraged to disrupt business operations resulting in lost revenue and potentially having your primary revenue stream temporarily down.

Burning Questions For CISOs:

- Do you detect and track pre-breach reconnaissance activity?
- Can you improve your organization's cyber resilience to pre-breach activity?
- Can you do this without increasing your full time employee requirements?
- Are you maximising the efficiency of your current security ecosystem with timely and accurate threat intel data?

CounterCraft's Key Service Outcomes:

Deploying our pre-breach activity threat-intel campaign allows you to:

- Detect and measure pre-breach activity and
- Collect intel on the techniques that are being used against you, and
- Proactively reconfigure your current security ecosystem to better defend.

Answer this fundamental question:

Are my security controls ready to stop targeted attacks?

Technical Solution

Threat Intelligence Service: Pre-Breach Intelligence

Technical Scope

The goal of the Pre-breach Intelligence Service is to deflect attacks away from the external infrastructure of the organization by deploying a deception buffer zone. The service will deliver real time intelligence that will be used to harden your infrastructure.

1. **Deploy:** CounterCraft deploys the assets associated with the service. This includes the creation of the attack vector discovery assets (breadcrumbs), any associated IT assets, and full configuration and deployment of the campaign.

2. **Discover:** The threat actors follow a prepared breadcrumb trail to discover and attack external facing services, hosted on your behalf by CounterCraft.

3. **Detect:** CounterCraft will detect when the threat actors are conducting reconnaissance on the deception buffer zone and you will be alerted immediately.

4. **Collect Intel:** The platform continues to collect intel in real-time on how the threat actors discovered your infrastructure, and what techniques, tools and procedures they are using to attack. You will be able to access all this information through an easy-to-understand dashboard.

5. **Proactively Protect:** make it actionable. Integrate the intelligence gathered with your security infrastructure: e.g. SIEM, SOAR, and TIPs.

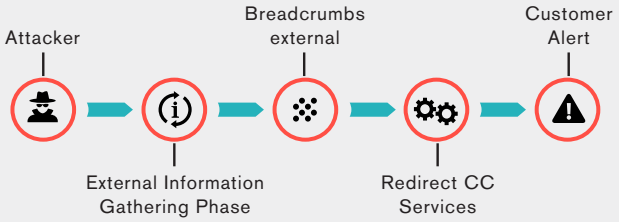
Technical Description

We use social engineering techniques against the attackers. Technical discovery information will be placed where it can be found by a threat actor searching for your organization's external infrastructure.

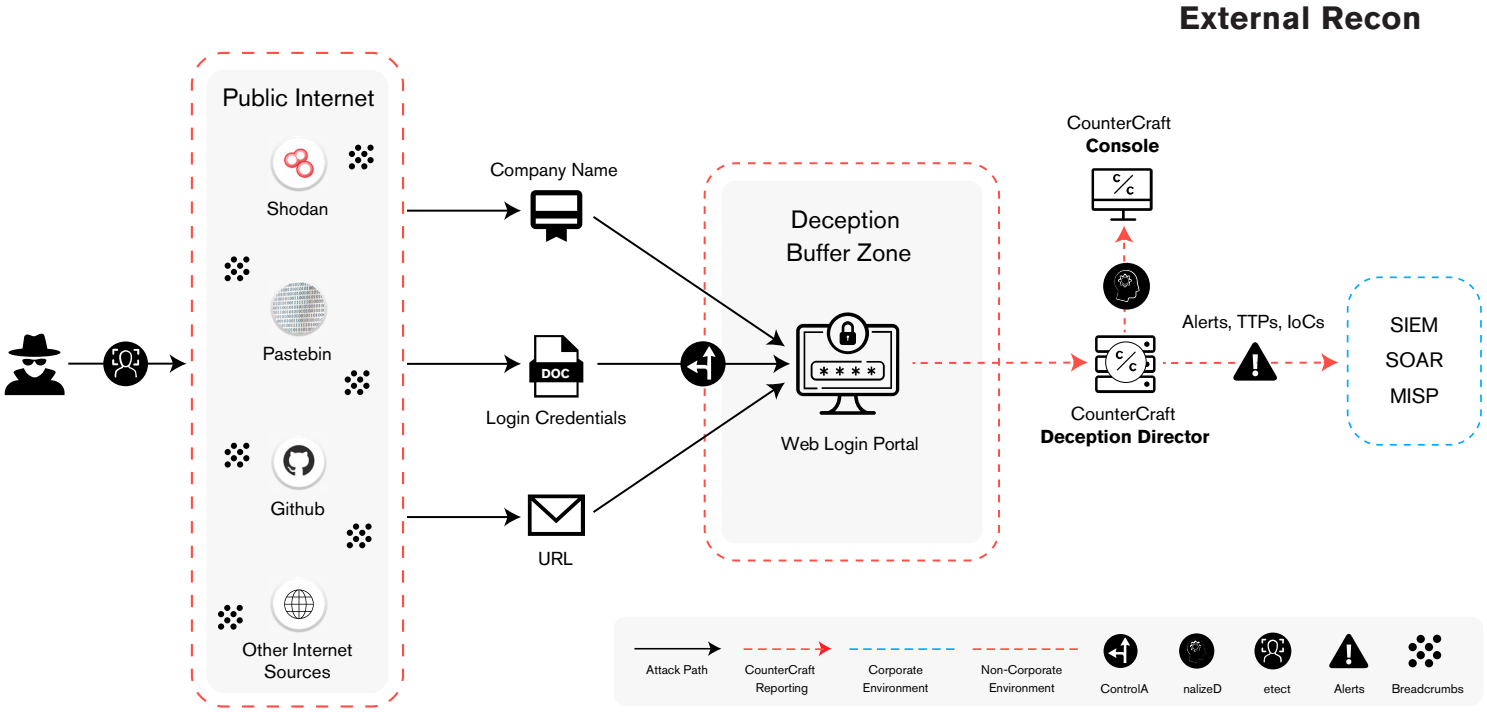
The deception buffer zone infrastructure will be hosted on cloud infrastructure. In the deception buffer zone, external services will provide the attackers with a credible target.

When an attacker interacts with the deception buffer zone, an alert is immediately sent from our console and threat intelligence collection starts.

The deliverables are actionable threat intelligence data with enrichments in the form of TTPs (MITRE ATT&CK) and IoCs including IP addresses, and credentials used by threat actors. The threat intel data can be sent to external security tools such as MISP, a SIEM or SOAR platforms.



Technical Architecture



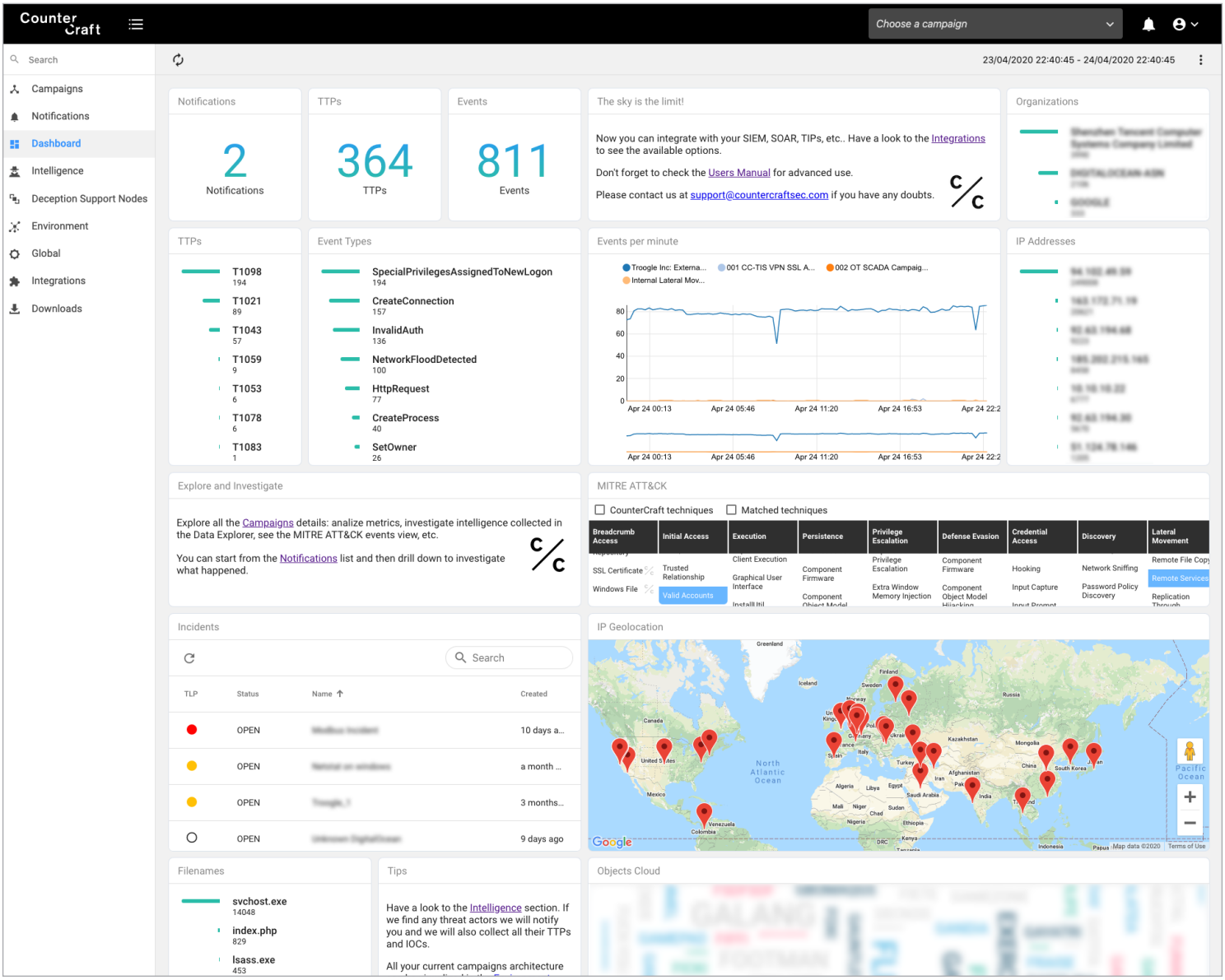
Business Benefits

Mitigate changing threats to your business operations and maintain the integrity of your network thus defending and protecting your key revenue streams.

Zero Internal Resource Use. The Threat Intelligence Service for pre-breach activity intel is a managed service that uses no internal resources. It is deployed and managed entirely by CounterCraft in our own cloud and the Internet.

Assure business continuity avoiding disruption to your online presence.

Service Dashboard



Strategic Benefits

- Simplify communication with board members and key management about the strategic merit of threat intelligence - use hard evidence, and organization specific intel to back up your messaging.
- Obtain actionable threat intelligence, that is specific to your organization, that enhances the corporate security strategy.
- Reassess your current security control sets based on objective evidence of adversaries circumventing current security controls.

Operational Benefits

Deploy

Deploy deception buffer zones with zero workload and effort to your threat intel team.

Collect Threat Intelligence

Collect real-time, focused and actionable intel about your online presence, with zero increase to analyst workload:

- Gain insight on the IOCs and MITRE ATT&CK TTPs actively being used against your external infrastructure.
- Classify who is attacking you: understand if the attack is random bot activity or targeted action from known threat actors.
- Catalogue the abilities of threat actors.
- Identify the most active Attack Vectors used to explore your infrastructure via analysis of the use of Technical Discovery Information.

Detect Threats

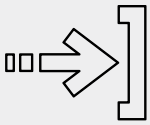
Detect attacks on your external infrastructure in real-time.

Proactively Protect

- The service delivers organization specific threat intelligence to achieve your operational goals:
  - Send machine readable threat intel data (IOCs, TTPs and Logs) to your SIEM or SOAR platform
  - Send incident data to MISP or other Threat Intel Platforms
- Investigate Incidents rapidly to discover Threat Actor modus operandi.
- Use the Threat Intelligence output to reconfigure enterprise systems: e.g. Firewalls, IPS, IDS and EDR in real time.

Buying the service

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