Threat Intelligence Service for VPNs

CounterCraft

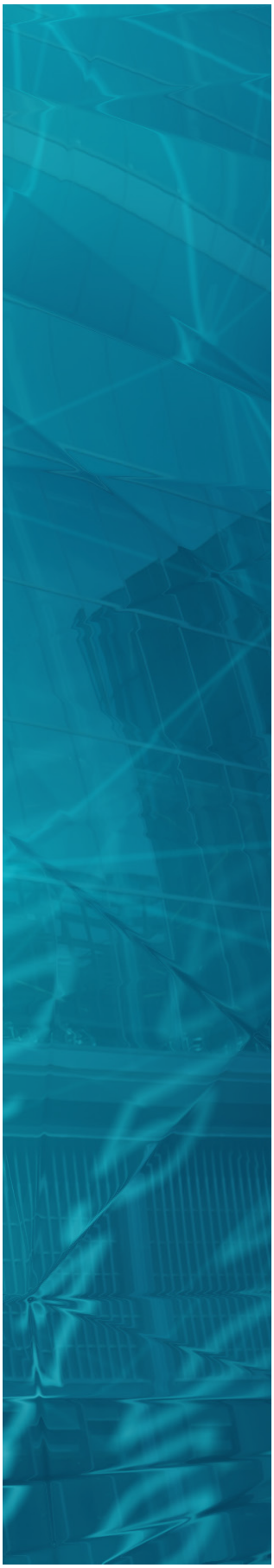
Address The Changing Threat Landscape

Remote Working Increases Risk

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.

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 threat landscape you face?

CISOs are required to make critical decisions about rolling out security infrastructure and implementing security policy while under significant time pressure, with little supporting data about the changing threats they face and the risk those threats pose.



Burning Questions For CISOs About Their VPN Infrastructure

CISOs are being faced with some tough questions about security when remote working is increasing:

1. Are our current security controls effective against the new threats our remote working infrastructure is facing? | **Detect Attacks**

2. "Does our current threat intel collection detect threats to our VPN infrastructure?" | **Collect Intel**

3. Does the intel we collect help us mitigate the increased risk of remote working? CounterCraft's Threat Intel Service for VPN answers all three questions. | **Proactively Protect**

CounterCraft's Service: Deliverable Outcomes

Detect attacks early

Be alerted immediately when threat actors are detected and you will be provided with an intuitive dashboard to easily monitor and analyze the incoming threat intel.

Collect real-time threat intelligence specific to your organisation

Understand why threat actors found you and how they are attacking you. CounterCraft provides high-impact intelligence, enriched by attackers' TTPs, IOCs, and threat actor characteristics.

Proactively protect your company

CounterCraft Threat Intel Service 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.

Technical Solution

Threat Intelligence Service: VPN

Technical Scope

The Threat Intelligence Service for VPNs adds a layer of assurance to your remote workers by deploying a VPN service and associated VPN access information:

1. **Deploy:** CounterCraft deploys the assets that make-up the service. This includes the creation of the attack vector discovery assets, any associated IT assets, and full configuration and deployment of the campaign.

2. **Discover:** The threat actors follow a prepared asset discovery trail to discover and attack the VPN service.

3. **Detect Attacks:** The platform will detect when the threat actors are conducting reconnaissance on your VPN architecture and you will be alerted immediately.

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

5. **Proactively Protect:** Configure the export of Threat Intelligence Data to other systems. CounterCraft CC-TIS feeds can be connected with SIEM, TIP, SOAR, EDR, UEBA, and other tools for proactive defense.

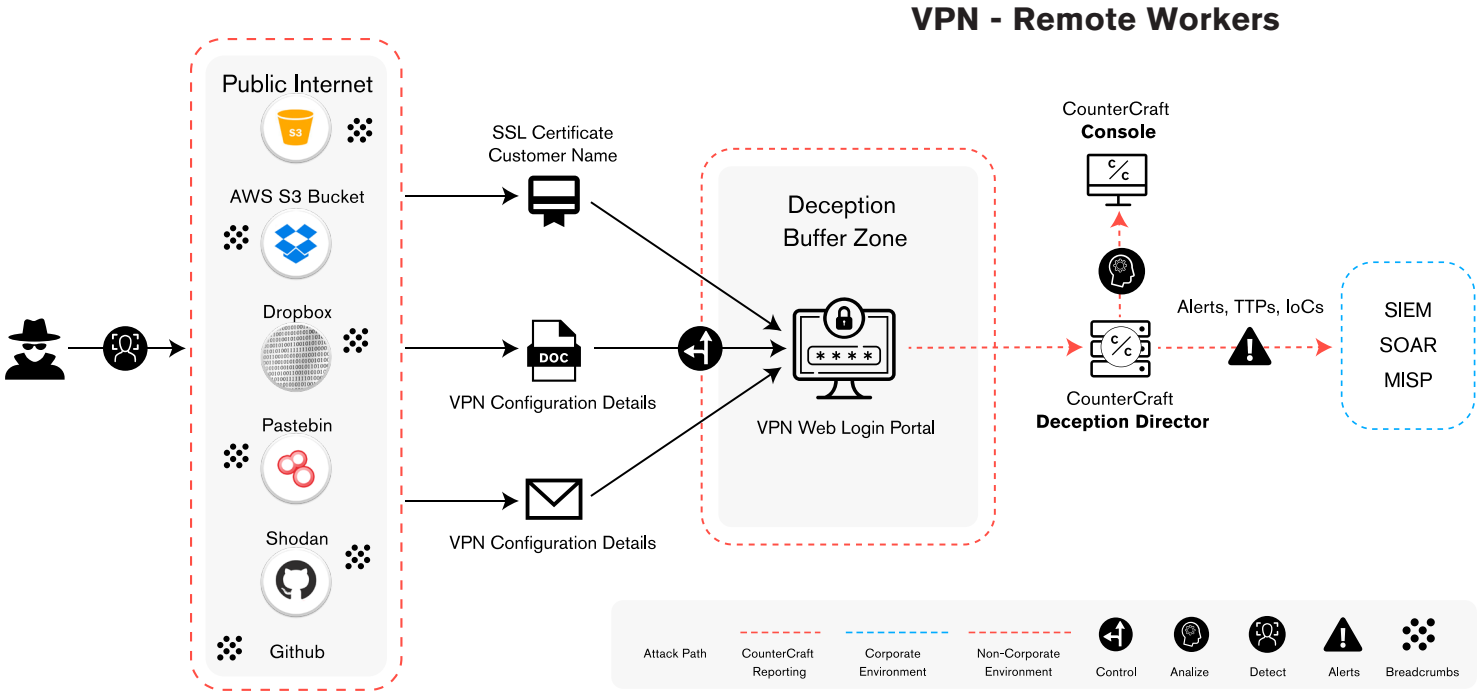
Technical Description

The goal of the Threat Intelligence Service for VPN service is to deflect attacks away from the VPN infrastructure of the organization by deploying a deception buffer zone and technical discovery information designed to look like the company's real VPN.

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 VPN infrastructure. The deception buffer zone infrastructure will be hosted on cloud infrastructure. In the deception buffer zone, a VPN login portal and web server 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.

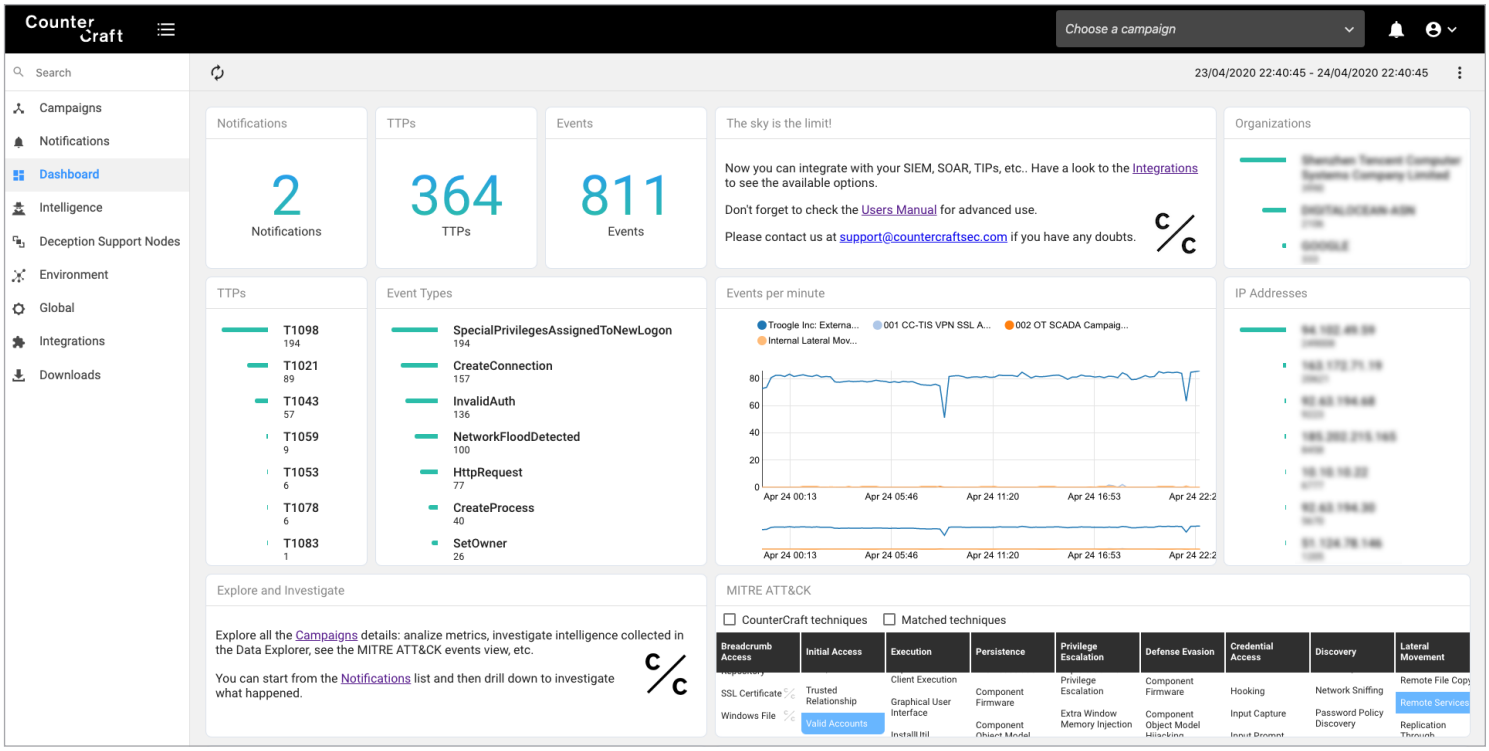
No Additional Resources Needed. Our service requires no skilled staff or other internal resources from your team. As a turnkey service completely configured, managed, and delivered by CounterCraft, CC-TIS automatically increases your team's productivity.

Improve Overall Security Effectiveness: CounterCraft provides high-impact intelligence, enriched by attackers' TTPs, IOCs, and threat actor characteristics. You have less work to do. You receive contextualized profiles of external adversaries trying to compromise your remote working infrastructure, & services or workers. You see why the threat is relevant, immediately. 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 techniques 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 activities to key management and board members.

Service Dashboard



Strategic Benefits

- Simplify communication with board members and key management about the strategic merit of threat intelligence - Information from CounterCraft CC-TIS provides threat intelligence breadth and depth for communicating the value of threat intelligence to key management and board members.
- Obtain actionable threat intelligence specific to your organisation and enhance corporate security strategy.
- Reassess your current security control sets based on objective evidence of adversaries circumventing security controls.

Operational Benefits

Deploy

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

Detect Threats

Detect attacks on your VPN infrastructure in real-time.

Collect Threat Intelligence

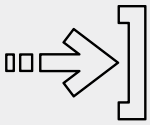
Collect real-time, focused and actionable intel about your remote working platforms, with zero increase to analyst workload:

- Gain insight on the IOCs and MITRE ATT&CK TTPs actively being used against your VPN 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.

Proactively Protect

- The service delivers organisation specific threat intelligence to achieve operational goals:
  - Send threat data (IOC, TTP and Logs) to your SIEMs 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



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