The CounterCraft Cyber Deception Platform

Discovering the Stealth Threat Actors in Your Enterprise

Counter Craft

They're Already Here. Now What?

Traditional threat prevention can keep a flood of malware and tainted email out of your organization, but advanced attackers get in anyway. They search for an opening, knowing that someone will click on a malicious link or phishing email. Once in, they conduct reconnaissance to determine where they are in the network and then move towards their target—whether user data, enterprise intellectual property, money, or other assets. Undetected, they can operate as long as it takes to achieve their goals.

You have to assume that attackers—whether actual bad actors or malicious software—are already in your network. Now what?

Distributed Deception to Gain the Upper Hand

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) without them knowing. Traditional prevention techniques are unable to stop attackers once they are inside, which is why the deception technology market is expected to exceed USD 2.09 billion by 2021.
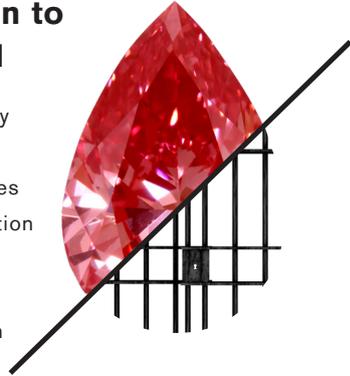
> "By 2019, continued weaknesses in prevention will drive at least 10% of large enterprises to adopt deception-enabled tools and tactics, improving detection and response and shifting some of the economic burden to attackers."
>
> **Gartner, Inc.**
> Competitive Landscape:
> Distributed Deception Platforms
> *August 2016 by Lawrence Pingree*

The Value of CounterCraft Deception

Protect the Entire Organization

- ⊘ Defend against determined attackers conducting reconnaissance, those already inside, and malicious insiders
- ⊘ Deploy deception across endpoints, on-premises server farms, virtualized environments, private and public clouds, including AWS, Microsoft Azure, and Digital Ocean
- ⊘ Defend servers, mobile phones, web applications, mobile applications, and WiFi access points
- ⊘ Enable multitenant support for global business units or multiple Managed Security Service Provider (MSSP) clients

Simplify Operations

- ⊘ Automate deception design, deployment, monitoring and maintenance of deception operations with 95% time savings
- ⊘ Eliminate false positive alerts and focus on actual, live threats
- ⊘ Use CounterCraft security experts to design, orchestrate, and launch effective deception strategies

Outsmart Attackers

- ⊘ Gain real-time, relevant threat intelligence as adversaries deliberately interact with your deception environment, both inside and outside of the classical enterprise perimeter
- ⊘ Use CounterCraft telemetry to identify and anticipate attacker's actions in real time
- ⊘ Understand attackers' TTPs so that you can effectively counter their moves

Improve Responsiveness

- ⊘ Detect and respond to genuine alerts in real time for even the most complex attacks
- ⊘ Gain operational, tactical, and strategic insight through multiple views of telemetry data in a single pane of glass
- ⊘ Integrate CounterCraft telemetry easily with existing SIEM to correlate data and enrich threat visibility
- ⊘ Improve decision-making confidence with rich, highly accurate data
- ⊘ Document specific threats, stopped attacks, improvements in threat detection, and other valuable data in intuitive reports

Counter Threats and Gain Control

The CounterCraft Cyber Deception Platform is the first to automate the design, deployment, monitoring, and maintenance of deception campaigns. You can detect and stop attacks across any enterprise assets, including endpoints, servers, mobile phones, web applications, mobile applications, and WiFi access points.

Design

CounterCraft designs deceptions that blend into your actual environment. Deceptions make it many times more difficult for attackers to discern which assets are real and which aren't. They are more likely to encounter a deception, generate an alert, and be detected quickly—before they can do damage.

Deploy

Simply deploy deceptions across on-premises server farms, virtualized environments, private and public clouds, endpoints, and other network assets.

Monitor

When an attacker engages with a deception, it generates an alert in real time. With CounterCraft, there are no false positives—every alert is genuine. Receive alerts instantly through the management console, as well as via IM and other messaging platforms.

Analyze

Attackers' moves are tracked in real time as they moves through the deception environment. CounterCraft monitors activity down to the operating system level, instantly relaying TTP telemetry data to the Deception DirectorTM, where it is processed, enriched, and displayed through the console.

Control the Attack, Plan the Response

Because you can watch adversaries continue their efforts to move through your deception environment—and you have visibility into their TTPs—you can stop them at any time. Meanwhile, telemetry data can be integrated with your SIEM to increase visibility and strengthen defenses across the organization.

Gain Cost-Effective, Proactive Defense

CounterCraft automation reduces the time and cost of manually creating and monitoring deception operations by 95%. With the scarcity of skilled IT and security staff, CounterCraft helps you maximize your resources.

Lateral Movement: Slash Dwell Time

In the case of insider lateral movement, the longer an attacker remains undetected the more damage can be done. With immediate visibility into an attack you can stop it much earlier in the kill chain, minimizing the amount of data and systems accessed.

Increase Team Efficiency

Use CounterCraft security experts to design deception strategies and handle deception orchestration, deployment, and management. Expert assistance increases your team's efficiency and accelerates protection.

Learn more about CounterCraft deception

REGISTER FOR A TRIAL

craft@countercraftsec.com

About CounterCraft

CounterCraft, established in 2015, headquartered in San Sebastian (Spain), is an award-winning developer of the pioneering, deception-based cybersecurity platform for enterprise active cyber defense. This is combined with leading-edge research, technology and threat intelligence approaches, to enable CISOs to automate deception campaigns that push back against cybercrime. Powerful visualization and reporting, coupled with an advanced API suite, have won adoption by government, law enforcement, finance, retail, industrial, and Fortune 500 customers. CounterCraft is backed by leading VC firms, is a GCHQ Cyber Accelerator Alumni and operates globally.