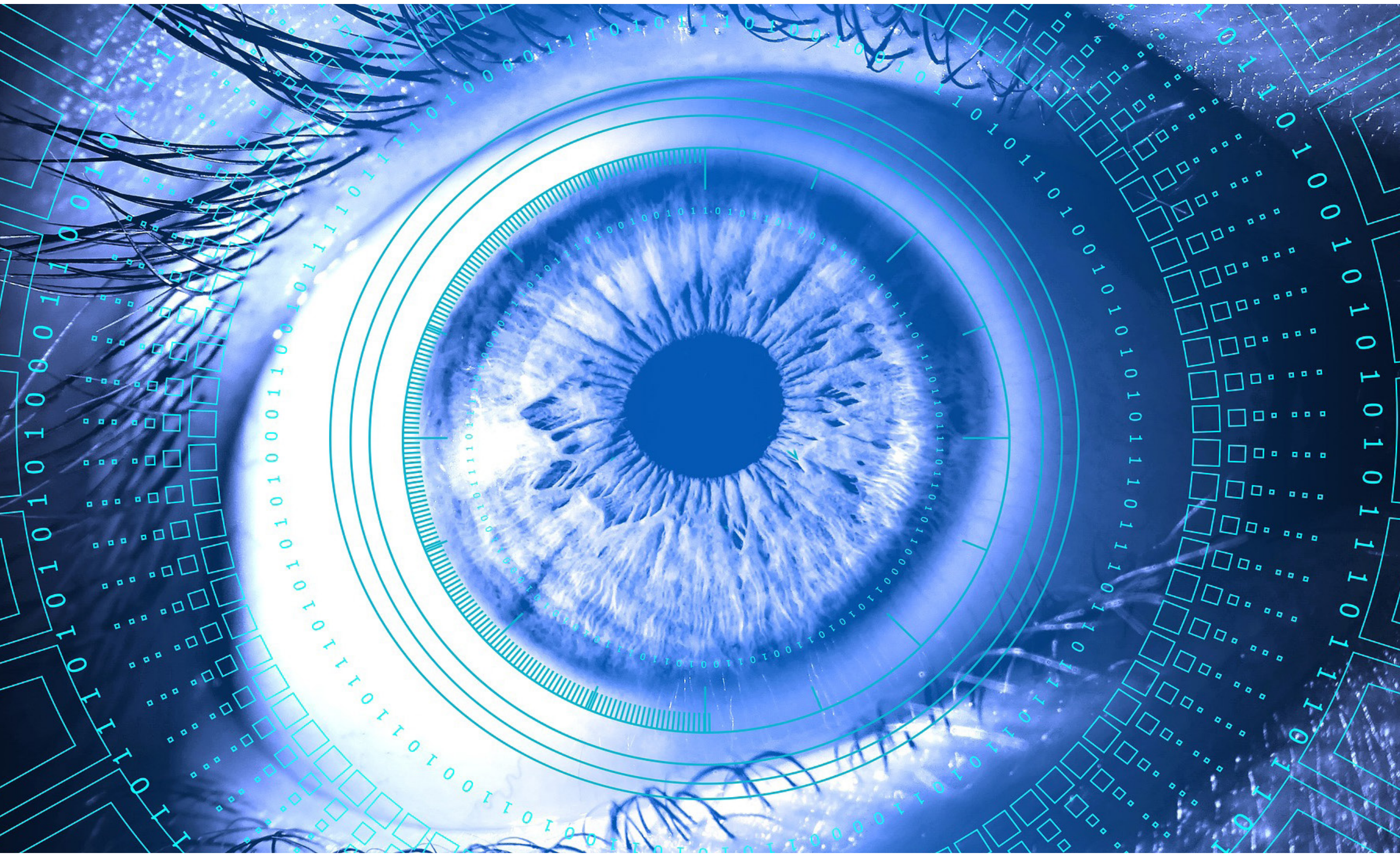
Tool Up Your Threat Hunting Team With Deception Technology

CounterCraft



We live in the era of the assumed breach. Every organization recognizes that at some point, they will be breached, and that the risk of a breach is higher than ever. Many organizations have also come to assume that traditional defense mechanisms are not perfect. Human factors are still very important risks to all cyber defenses. For example, organizations who naively believe they're impenetrable to attack quickly face reality when a simple phishing email succeeds in completely undermining their defenses.

Despite the global shift in how we operate and how the cybercriminals do business, it's still very common for organizations to approach defense strategies with outdated conceptual framing. You could fortify the wall surrounding the enterprise, and just wait. Wait for your SIEM to generate an alert, wait for a heads up from an employee who discovers some strange behavior, or wait for an external source to tell you that your defenses have failed. Wait for the headlines to tell you that you have been breached.

Or you could add endpoint agents to every enterprise computer end-point and wait for alerts to tell you that someone was able to jump over your wall and has been found in a desktop computer. Or maybe, you could be more proactive, and try an alternative to waiting.

CounterCraft proposes full-spectrum threat hunting: Only CounterCraft detects and identifies external pre-attack stealth activities; and finds evidence of external or internal attackers on enterprise systems — even with just a single trace left behind.

Threat Detection & its Challenges

There is more to the modern-day defense strategy than logs. Threat hunting is the logical step needed to keep pace with today's, and tomorrow's, cyber threat landscape. Threat hunting involves focusing your defenses on the known threats your business is facing. A different approach entirely to simply patching all the possible holes that can be found in your own walls.

Some begin by obtaining extensive knowledge of the threats faced. This strategy reveals fascinating insights, but it requires specialization, time and research in order to attempt to learn how threat actors behave. Many organizations have acquired multiple threat intelligence feeds in an effort to tackle the problem this way.

The vast knowledge set that you're left with is information that's nice to have. It provides valuable context for the threats found and can include anything from a high-level description of a threat actor's behavior to a very technically complex analysis of a piece of software or malware.

For some, having access to this kind of information feels like a revelation. But the reality is that it's generic data that may or may not be relevant to your organization and is not easy to act on.

Indicators of compromise (IOC) feeds come into play to help solve the usability issue surrounding raw threat intelligence data, generated and used to detect potentially malicious activity based on known incidents around the globe. However, monitoring thousands of possible domains that could be at risk of a particular piece of malware in a specific timeframe, or receiving thousands of hashes of the same malware sample doesn't lead to an effective solution. It's easy to add and ingest more and more hashes and IPs, but more doesn't necessarily equal better.

We're not saying checking IOCs is useless. What we are saying is that we need to further improve our toolset. We need a better solution.

Threat Hunting & MITRE ATT&CK Matrix

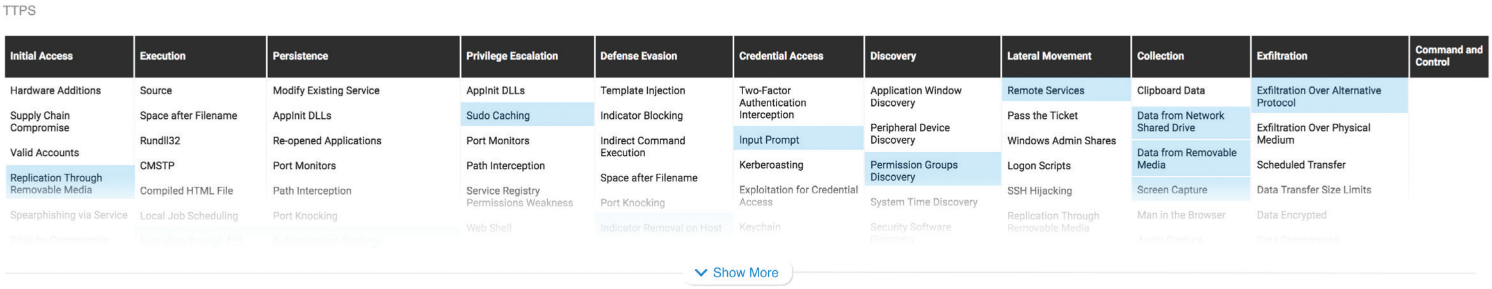
Equipped with new knowledge about possible threats and able to monitor known IOCs, the threat fighting community developed methodologies and frameworks to model threats.

The common threat modelling language of choice right now is MITRE's ATT&CK framework. Fast becoming the universal language understood by threat hunters and superseding Lockheed Martin's Cyber Kill Chain, this framework is being adopted by companies the world over. Adversarial threat modeling has several benefits – not only does it help render generic threat intelligence and IOCs much more actionable, it also provides the defender with a structure to measure attacks and defenses against.

However, adversarial threat modeling is not the panacea. As with everything, it comes with some inherent problems, namely losing relevant information in the attack tactics, techniques and procedures (TTP) mapping process.

Due to CounterCraft ability to closely monitor a threat actor's behavior, we go one step further when recovering evidence and mapping its modus operandi (MO). We don't just link a TTP to an Actor or a Campaign, we store each occurrence of a TTP, together with contextual information about its use in ongoing adversary activity, in order to create much richer Threat Actors profile's than available from other intelligence sources.

CounterCraft contribution comes in the form of deception capabilities, designed to improve the current toolset and increase the activities that threat hunting and threat modeling teams can undertake. The use of cyber deception allows threat hunting teams to detect, investigate and control adversary activity not only in the middle and end of the attack sequence defined by the MITRE Att&ck framework. We can credibly allow threat hunting teams to extend their reach to the early pre-attack activities that begin attack sequences. Advanced Deception techniques are among the only responses that allow teams to actively cover this area.


TTPS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions	Source	Modify Existing Service	AppInit DLLs	Template Injection	Two-Factor Authentication Interception	Application Window Discovery	Remote Services	Clipboard Data	Exfiltration Over Alternative Protocol	
Supply Chain Compromise	Space after Filename	AppInit DLLs	Sudo Caching	Indicator Blocking	Input Prompt	Peripheral Device Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Physical Medium	
Valid Accounts	Rundll32	Re-opened Applications	Port Monitors	Indirect Command Execution	Kerberoasting	Permission Groups Discovery	Windows Admin Shares	Data from Removable Media	Scheduled Transfer	
Replication Through Removable Media	CMSTP	Port Monitors	Path Interception	Space after Filename	Exploitation for Credential Access	System Time Discovery	Logon Scripts	Screen Capture	Data Transfer Size Limits	
Spearphishing via Service	Compiled HTML File	Path Interception	Service Registry Permissions Weakness	Port Knocking	Keychain	Security Software Discovery	SSH Hijacking	Man in the Browser	Data Encrypted	
Drive-by Compromise	Local Job Scheduling	Port Knocking	Web Shell	Indicator Removal on Host			Replication Through Removable Media	Audio Capture	Data Compressed	
	Execution through API	Authentication Package								

Deception & Threat Hunting

Deception by nature is a great fit with threat hunting and threat intelligence gathering: it allows teams to engage with adversaries earlier than before on the attack sequence defined by the MITRE Att&ck framework. This is how our deception solution deals with some of the more challenging, as well as the typical problems, threat hunting introduces and the benefits that deception brings.

Strike first

Security has always been a game of cat and mouse, in which the defender is always one step behind the enemy. It's the same with traditional threat hunting tools, where the defender typically tries to detect an already occurring attack. With deception, we strike first, creating custom synthetic environments designed to lure the attacker in, with the added capability to develop campaigns tailored to the type of attacker you want to track.

Threat intelligence relevant to your organization

One of the biggest problems when dealing with threat intelligence is distinguishing which information is relevant to your organization and which is not. CounterCraft gives threat hunting teams the capability to deploy deception campaigns that are part of their enterprises attack surface. This ensures that any activity detected, and thus the intelligence gathered from the campaign, is relevant to your organization specifically.

Proactive solution

Traditional threat hunting tools involve looking inside your organization to try to detect anomalies or known behavior. CounterCraft lures attackers into the deception environment and builds an attack surface designed to give them access to a synthetic interior environment. This is safe for the enterprise as no production IT is at risk. As the threat hunting teams quietly observe the threat actors working, they gather intel, they divert the actors from their real attack, they uncover motives and objectives, they can then thwart further activity on production systems. Threat hunting is now threat actor hunting, an altogether more specific operation.

Trusted threat intelligence

You won't always know where threat intelligence comes from. You'll have an idea about who provides the intel, but you don't get any insight into how and where the magic actually happens. Instead, you have to trust that the data you have is rigorous, unbiased and reliable. Now, with our deception solution, you control the environment and you control what, when, where and how the evidence is obtained.

Avoids alert fatigue

It's likely that the massive volume of IOC your organization is ingesting is already giving some or lots of false positives, making life more difficult for your SOC analysts, and worse still, forcing them re-create some rules to quieten the noise, and creating more weak points in your defense system. By design, CounterCraft generates only information and alerts that are relevant to your organization.

Easy to manage information

There are tons of information to be checked; huge databases of IOCs, lots of reports and white papers to analyze, conferences to attend, new techniques to be aware of, the list goes on. Staying up to date is difficult and time consuming and knowing what could be relevant to your organization is not a trivial task.

Our solution delivers a vast intelligence knowledgebase, but the analyst will see only the information related to the incident (IOCs and TTPs) and the most detailed insights, saving time and reducing the need to process large amounts of unnecessary data.

Relevant actionable information

Continuous monitoring of thousands of IOCs is not a bad thing, but it is not what you will get with a deception tool. When an incident occurs, you will get IOCs found during the event and other related IOCs that might be relevant, enabling you to narrow your hunt for malicious activity within your organization's infrastructure using specific, and often unique, intelligence.

Cover gaps in your defense system

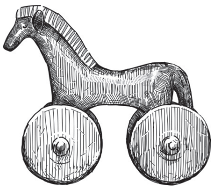
Threat hunting teams can rapidly deploy deception campaigns to cover specific threat areas, such as merger and acquisition activity, that will create specific threat actor interest. They can also cover specific areas of IT systems that are unable to generate logs or provide monitoring such is IOT systems. Also, during long upgrade and roll-out cycles for more traditional cyber security controls where full coverage cannot be provided, deception can be rapidly deployed to mitigate specific system risks while the traditional controls are being upgraded and deployed.

Unleash the Power of Deception for Threat Hunting

Threat hunting is not only about early threat detection. Isn't it worth trying to completely prevent an attack? How about redirecting attackers away from your internal network and into a synthetic deception environment where you can study the attacker with no risk to enterprise systems? And finally, shall we dig deeper and reveal concise insights about the attackers who actually want to attack you and use them against the attackers? The answer is surely yes, let's do it!

A synthetic deception environment captures the most accurate and complete information about an attacker's behavior. Here, you have complete control of the environment and are able to monitor all the movements the attacker makes while they're engaged with a campaign. It sounds like we're getting pretty close to the concept above of studying, profiling and controlling threat actors, doesn't it?

We can guarantee that you'll find CounterCraft a complementary addition to tool-up your threat hunting team. Offer more than traditional defense techniques and solutions with CounterCraft Cyber Deception Platform. Our platform offers full-spectrum threat hunting: detect and identify external pre-attack stealth activities and find evidence of external and internal attackers on enterprise systems. Our solution uses powerful automation to enhance your threat hunting capabilities, without burdening the team. Don't sit back and wait. Engage with the threat actors who are actually attacking you.



About CounterCraft

CounterCraft is a pioneering provider of full-spectrum cyber deception and ground-breaking threat hunting and cyber counterintelligence to detect, investigate and control targeted attacks. 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