Using Deception For Threat Hunting

Benefits & Use Cases

Introduction

Many organizations are enthusiastic to adopt threat hunting as part of their cybersecurity arsenal. However, the key to success is to develop a thorough understanding of its benefits, and less-obvious limitations, before embarking on any enterprise-level threat hunting programme.

Threat hunting is a proactive technique that combines security tools, analytics and threat intelligence with human analysis and instinct. It's not a passive operation, it's not automated and it largely depends on human analysis. Before starting a threat hunting programme, any organisation must consider whether they have the right tools, analytics and threat intelligence, as this will impact the quality of the hunt.

Organisations must also focus on the quality of their data, not the quantity, because the higher the quality, the more bespoke it is to the organisation, and the lower the risk is of producing a hypothesis or results that render themselves meaningless.

> "Threat hunting is a **proactive** technique that **combines** security tools, analytics, and threat intelligence with human analysis and instinct."

What Does a Threat Hunter Look Like?

Threat hunters must have a deep network knowledge and be capable of mapping the network out in their minds. Their expert understanding of networks, apps and systems enables them to recognize tell-tale signs that indicate the presence of an attacker.

The three priorities for establishing a threat hunting program

1. **Identify key stakeholders and articulate outcomes.** Key stakeholders are the people who you will look to for budget to contribute to the threat hunting operation and support the costs associated with deploying analysts as threat hunters.

2. **Get your legal team on board.** Threat hunting activities involve trawling the entire network for data —some may be confidential. Data privacy laws can vary across different geographies, so it's important to ensure all activity is law-abiding with the support of your legal function.

3. **Define a hypothesis.** This will be triggered by something like threat intel, a previous hunt, historical incidents or analysis. It could be a structured hunt including some of these triggers, or it could be entirely unstructured and ad-hoc perhaps because you don´t have the data sets available to drive the hypothesis. This hypothesis won't form overnight, so organisations should expect it to go through a number of interactions.

Key Benefits of Using Deception for Threat Hunting

Due to the need to detect increasingly persistent and longer-lasting attacks, threat-hunters are responsible for detecting attacks and trying to stay ahead of cyberattacks so that the detection rate is reduced as much as possible.

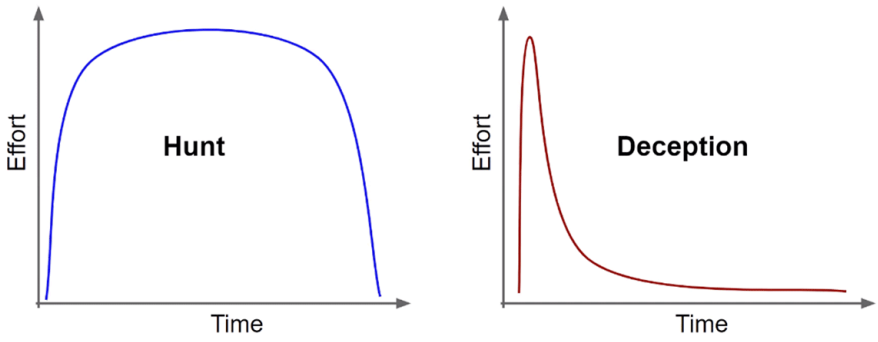
CounterCraft's Cyber Deception Platform helps alleviate common weaknesses found in threat hunting. This includes resolving issues and concerns about limited resources, time and results that negatively impact the return on investment and could result in the abandonment of a threat hunting programme altogether.

At CounterCraft we see four main benefits to using deception technology to hunt cyber attacks.

- Window of opportunity reduction for the threat actor by detecting it more quickly and taking it out of the production environment.
- Hunt down threats in real-time proactively.
- Resilience of business networks and systems increase, and integrity of the brand maintenance.

Time Consumption: Threat Hunting vs. Cyber Deception

Standard threat hunting requires highly skilled experts and a substantial amount of time and effort to achieve results for the entire duration of the hunt. Deception, on the other hand, requires an initial considerable effort during the design and deployment, but once the cyber deception campaign is set up there's a very low resource overhead.



The Best Way to Start Threat Hunting with Deception

With deception you can extract targeted intelligence to initiate the hunt with the right information. Then, you can use the data gathered post-hunt to deploy measures to ensure your attackers don't come back as well as drive future campaigns. Using deception during a hunt enables you to control and shape adversary attack paths, and extract different and better information from them, while they're happening.

Each of our deception campaigns is a collection of deception hosts, services and breadcrumbs, designed to look attractive to adversaries. We can deploy a campaign internally, which is the traditional way honeypots have been used by organizations to detect lateral movement. Or even deploy breadcrumbs externally; providing an excellent precursor to threat hunting. For example, we can set up a series of lures on pastebin, or as spear phishing campaigns, to lead attackers to externally hosted campaigns that are easy for the SOC team to set up. Those will let you uncover vital intel to arm your threat hunting team with before they start their hunt.

Use Cases

Powershell Abuse

The Powershell Abuse scenario starts with an external spear-phishing campaign that includes three key phases: **discovery, access to credentials** and **information uploaded** to the command and control server. The interaction seen in real time is shown as notifications that can be grouped and assigned to incidents. This information can be made available to threat hunters and used to formulate hunts.

The CounterCraft Cyber Deception Platform then maps the behaviour into the MITRE ATT&CK™ database and we can know that Powershell is being harnessed and used specifically against your organization.

This use case demonstrates the platform's ability to map the technical behaviour of the threat actor within the MITRE ATT&CK™ framework in real time. Therefore, it provides an understanding of how this command is executed, to form the basis of a hypothesis.

Credential Dumping

Credential dumping is an example of an Indicator of Attack (IoA). Known APT groups such as APT10, APT28 and MuddyWater have used this technique. Dumped credentials can be used to perform lateral movement and access restricted data sets. For the purpose of this use case, credential dumping is achieved through the use of Powershell Abuse. For example, in Windows, the Security Account Manager database stores local accounts for the localhost, and several tools can be used to access the information in the Security Account Manager file by using in-memory techniques. Other tools include Pwdumpx, Gsecdump, and WCE – however, hunting for these tools won't necessarily produce any results.

The CounterCraft Cyber Deception Platform captures the behaviour and automatically maps it to the MITRE ATT&CK framework, enabling threat hunters to focus on detecting credential dumping as an IoA across their network, and use log data (both native Windows and Sysmon) to hunt for any tool sets that may facilitate this type of attack.

Why Should Deception Technology Be Part of Your Threat Hunting Activity?

The Powershell Abuse or Credential Dumping deception use cases can be run for months prior to beginning threat hunting operations within an organization. These use cases will help you gathering and serving threat intelligence in the background. These pre-hunt exercises don't involve rolling out anything across your internal IT infrastructure. They are deployed on external servers and with a single DNS entry change, you're good to go.

Once you've completed your hunt and discovered positive results in the form of activity within your network, you can use deception to set up a monitoring system to capture future recurrences.

And last but not least, compared to SIEM, a targeted deception campaign will reduce false positives to virtually zero, thus making threat hunting more efficient.

Next Steps ...

Additional resources:

- CounterCraft - Tool Up Your Threat Hunting Team With Deception Technology Download PDF

- CounterCraft - How to Fight Threats in the Modern Age Download PDF

- TaHiTi - A great methodology for hypothesis led threat hunting from the Dutch Payments Organisation Download PDF

Get in contact:
Find out more by getting in touch at craft@countercraf.eu. We are only too happy to explain what we do and how we can help you get the best out of cyber deception for threat hunting - from an initial conversation or simple demo, to a fully featured deployment.

About CounterCraft

CounterCraft empowers organizations to strengthen their security posture more efficiently than ever before. Designed and developed by experts, CounterCraft is a pioneering provider of full-spectrum cyber deception and ground-breaking threat hunting and enterprise cyber counterintelligence to detect, investigate and control targeted attacks.

The CounterCraft Cyber Deception Platform fits seamlessly into existing security strategies and delivers personalized, actionable intelligence to facilitate early threat detection, accelerate incident response and significantly reduce security spend. 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, critical infrastructures, retail and telecommunication companies, governments and law enforcement agencies.

Download our latest documents at

countercraftsec.com

or if you prefer contact us at

craft@countercraftsec.com