




Deception-Powered Adversary Generated Intel

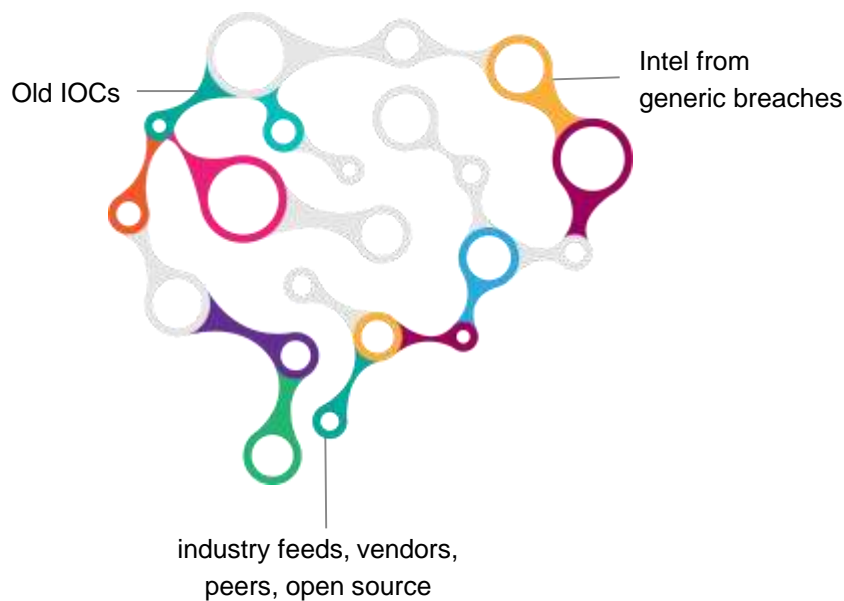
Cyber Deception Platform

The background of the slide is a dark, almost black, field. It is filled with numerous thin, blue, fiber-optic-like lines that originate from the left side and fan out towards the right. These lines are punctuated by small, glowing blue dots of varying sizes. A single, thick, white diagonal line runs from the bottom-left towards the top-right, crossing the entire frame and intersecting the blue lines.

Why is traditional
threat intelligence
broken?

Threat Intelligence 2.0

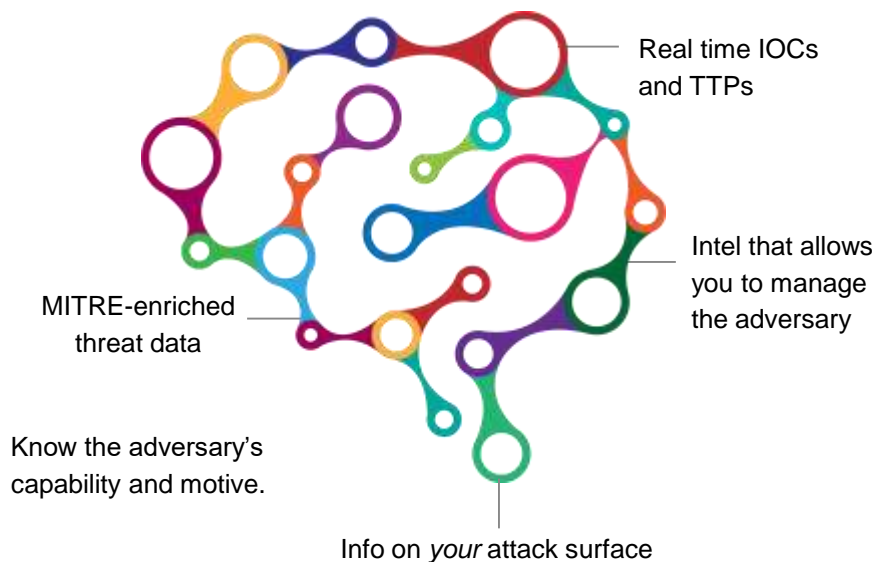
Traditional threat intelligence is broken.



Generic, out of context, dated, bulk, need prioritize, limited value Threat Intel

NICE TO HAVE

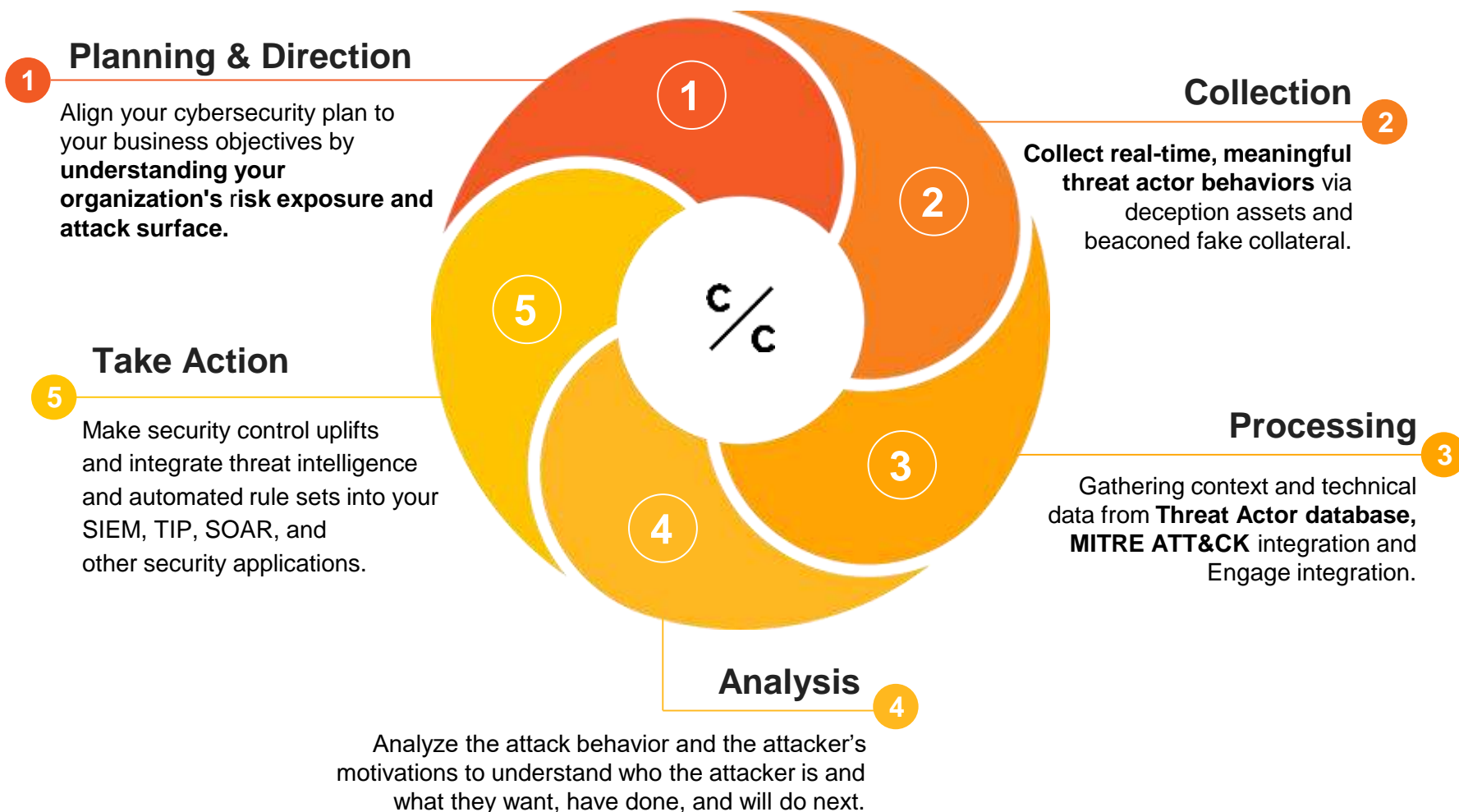
Deception-powered threat intelligence is the solution.



⌘ Timely, real time, contextualized, actionable Threat Intelligence ready to work with

MUST HAVE!

Threat Intelligence Lifecycle 2.0



The background of the slide is a dark blue/black field filled with numerous thin, glowing blue lines that radiate from the left side, resembling fiber optic cables or data connections. A single, thick white diagonal line runs from the bottom left towards the top right, crossing the blue lines.

Can Deception Technology really provide Actionable Intelligence?

Hypothesis of compromise



Ransomware



Spear phishing



VPN



Insider threat



Lateral movement



Hardware attacks



IoT attacks



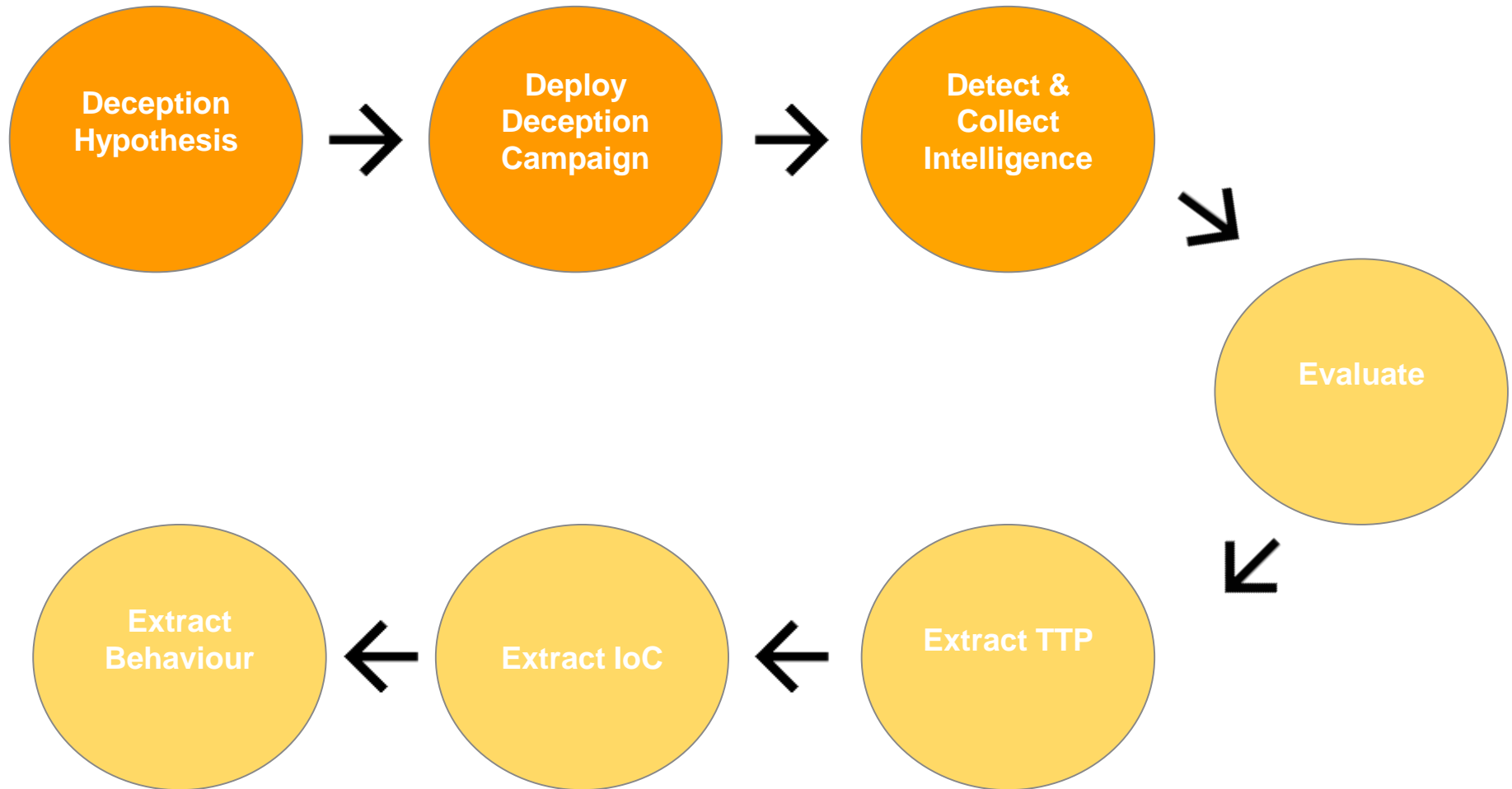
Credential theft



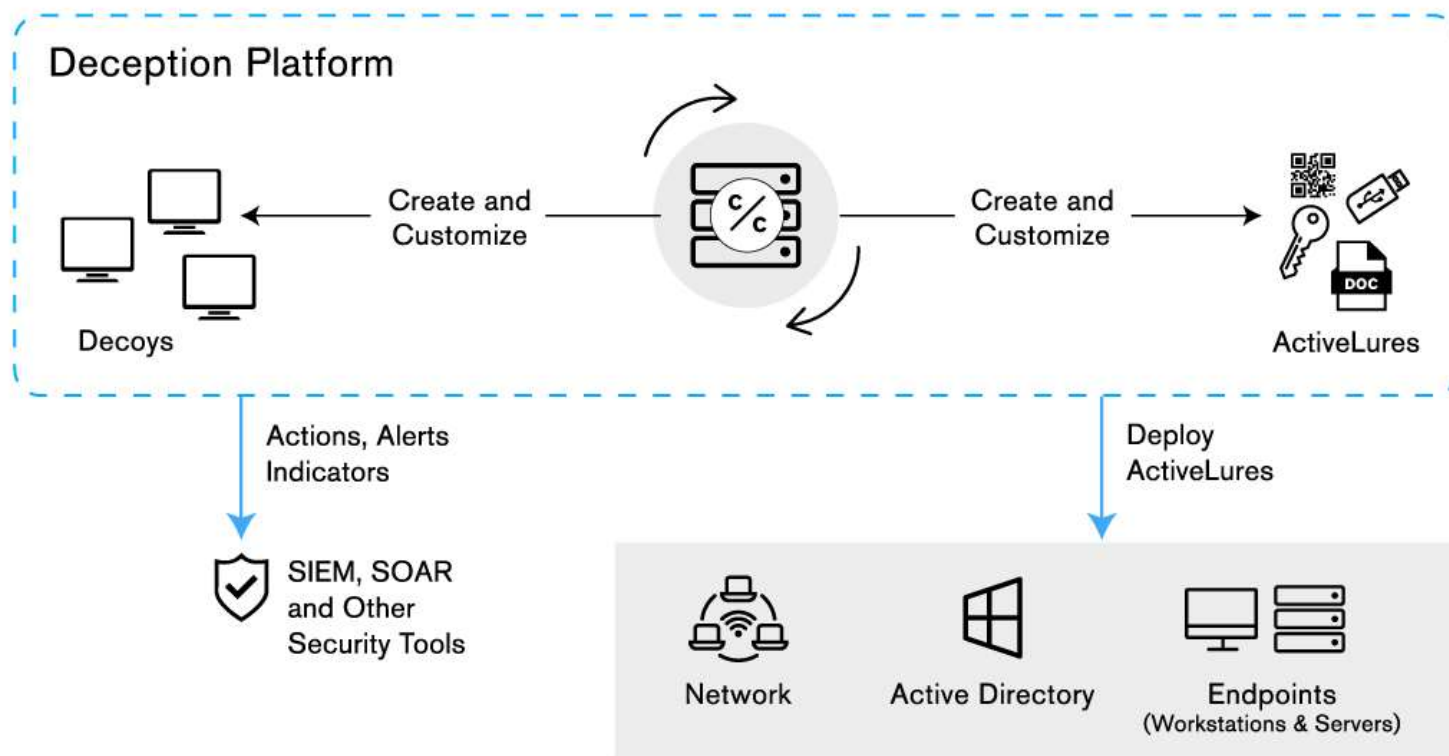
Account hijacking

WHAT IS THE QUESTION WE TRY TO ANSWER?

From Hypothesis to Deception Campaign

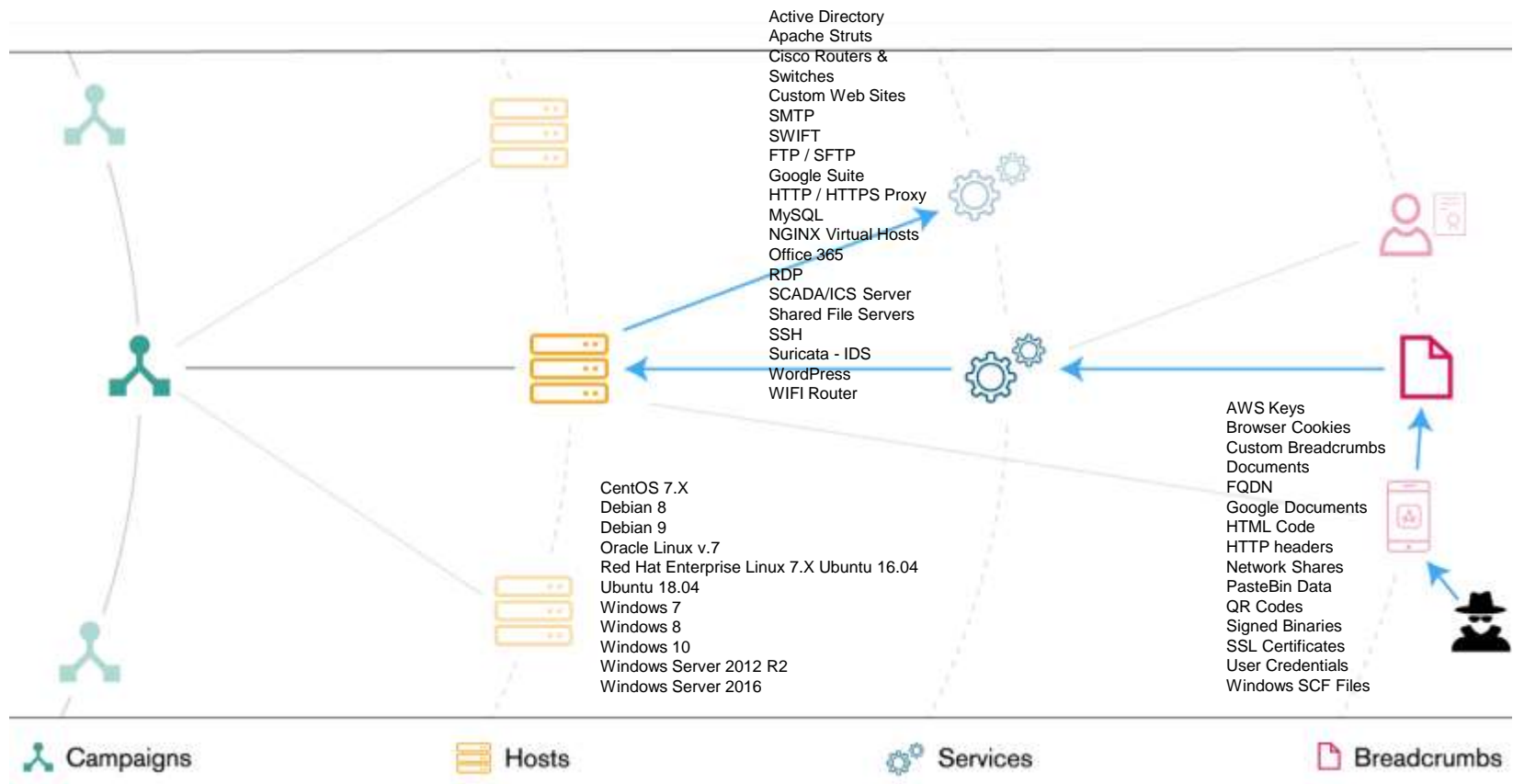


How does it Work?

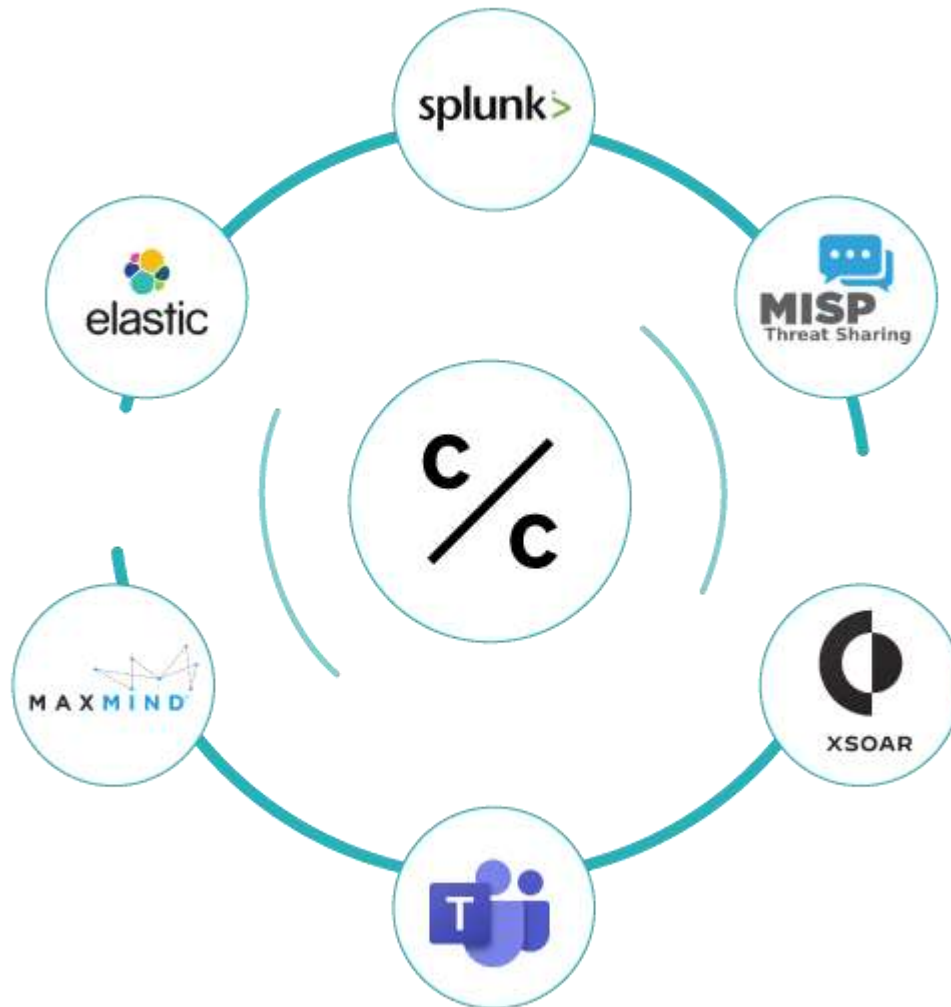


DECEPTION HYPOTHESIS WILL DETERMINE LOOK AND LOCATION OF DECOYS AND ACTIVE LURES

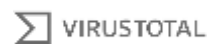
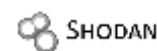
CounterCraft Deception Campaigns



Afford, absorb and contextualise Intel



More than 45 plugins

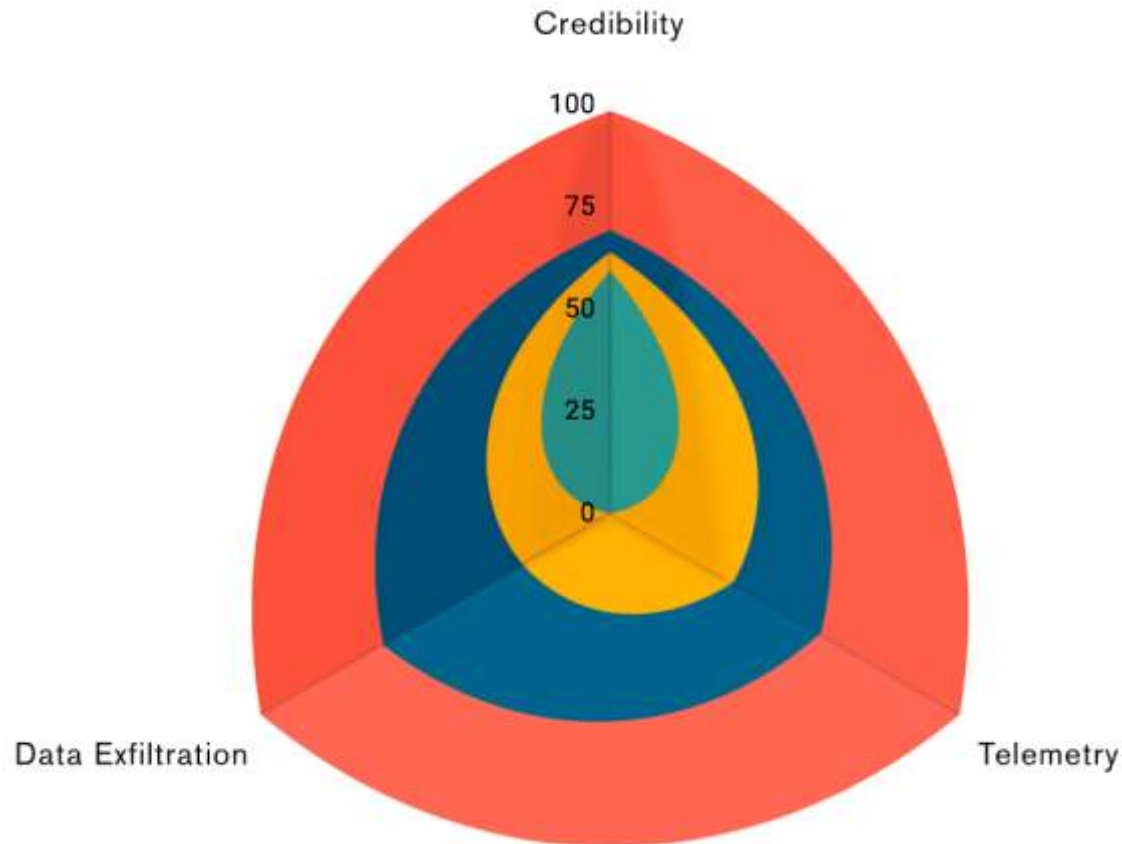


The background of the slide is a dark blue to black gradient. It features a dense network of thin, glowing blue lines that resemble fiber optic cables or data connections, radiating from the top left towards the bottom right. A single, thick, solid white line runs diagonally across the entire slide, starting from the bottom left and extending towards the top right, intersecting the blue network of lines.

What are the risks involved
in adopting this approach?

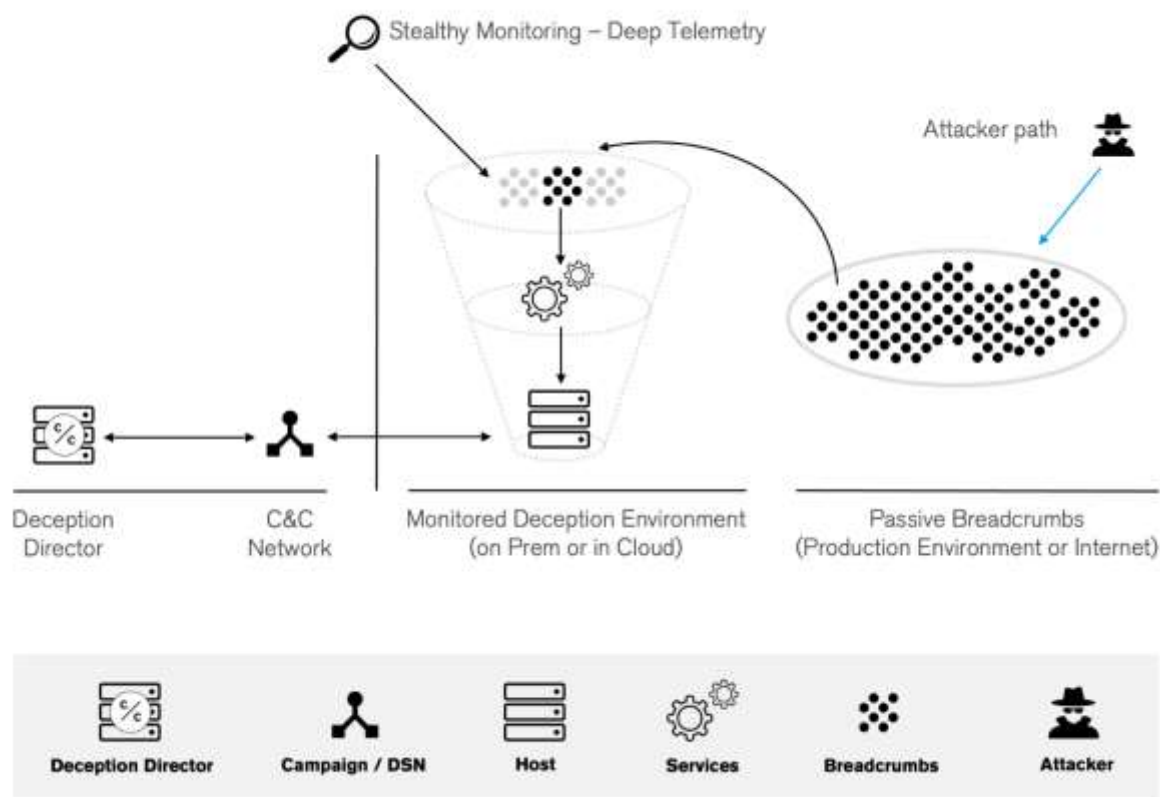
Deception is not Created Equal

1. **Credibility:** Is it believable?
2. **Instrumentation / Telemetry:** Are you able to gather deep data about what people are doing on the system?
3. **Data Exfiltration:** Are you able to bring that data home without revealing yourself, so you can do something about it?



HIGH INTERACTION IS A MUST FOR OBTAINING AGI

Drawing Attackers to the Deception Infrastructure



**DECEPTION INFRASTRUCTURE SEPARATED FROM
PRODUCTION ENVIRONMENTS!**

Benefits of Adopting CounterCraft



Detect attackers before there is a breach

With deception, you can find attackers and observe their movements before they have even entered your network.



Eliminate false positives

Deception creates environments and data that, by definition, should not be entered or touched. That means there is an almost total reduction of false positives, noise, and dead-end alerts.



Gain threat intel specific to your organization and in real time

Deception technology doesn't rely on generic threat intel feeds—it creates threat intel by engaging attackers, and delivers it to your security team in real time.



No need to disrupt regular network function

Deception technology can work without touching your network systems, meaning minimum disruption to normal processes and business flow.



Scale easily

Deception can scale easily and be automated for maximum efficacy even as your organization grows and changes.



Works across many types of systems

Legacy system? No problem. IoT devices to protect? Deception works on those too. Cyber deception is versatile and adaptable.

The background of the slide is a dark blue field with faint, stylized circular patterns and binary code (0s and 1s) scattered throughout. The CounterCraft logo is centered at the top of this section.

Counter
Craft

Recognized as a Sample Vendor of
Intelligence Analyst Investigations
Tools by Gartner

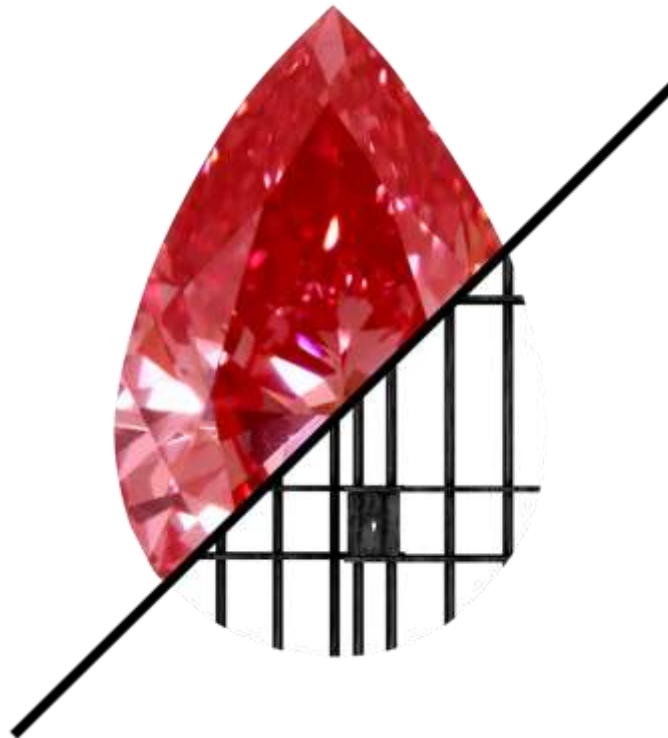
[Market Guide for Security Threat Intelligence Product and Services](#)



**INTERESTED? COME TO OUR BOOTH
AND LET'S TALK!**

Cyber Deception Platform

Counter Craft



craft@countercraft.eu
www.countercraft.eu

The content of this document is confidential and intended for the recipient and purpose of the related communication to which it's attached only. It is strictly forbidden to share any part of this document with any third party, without a written consent of CounterCraft.

Should you receive this document by mistake, we also ask that you delete it, and do not forward it or any part of it to anyone else. Thank you for your cooperation and understanding.