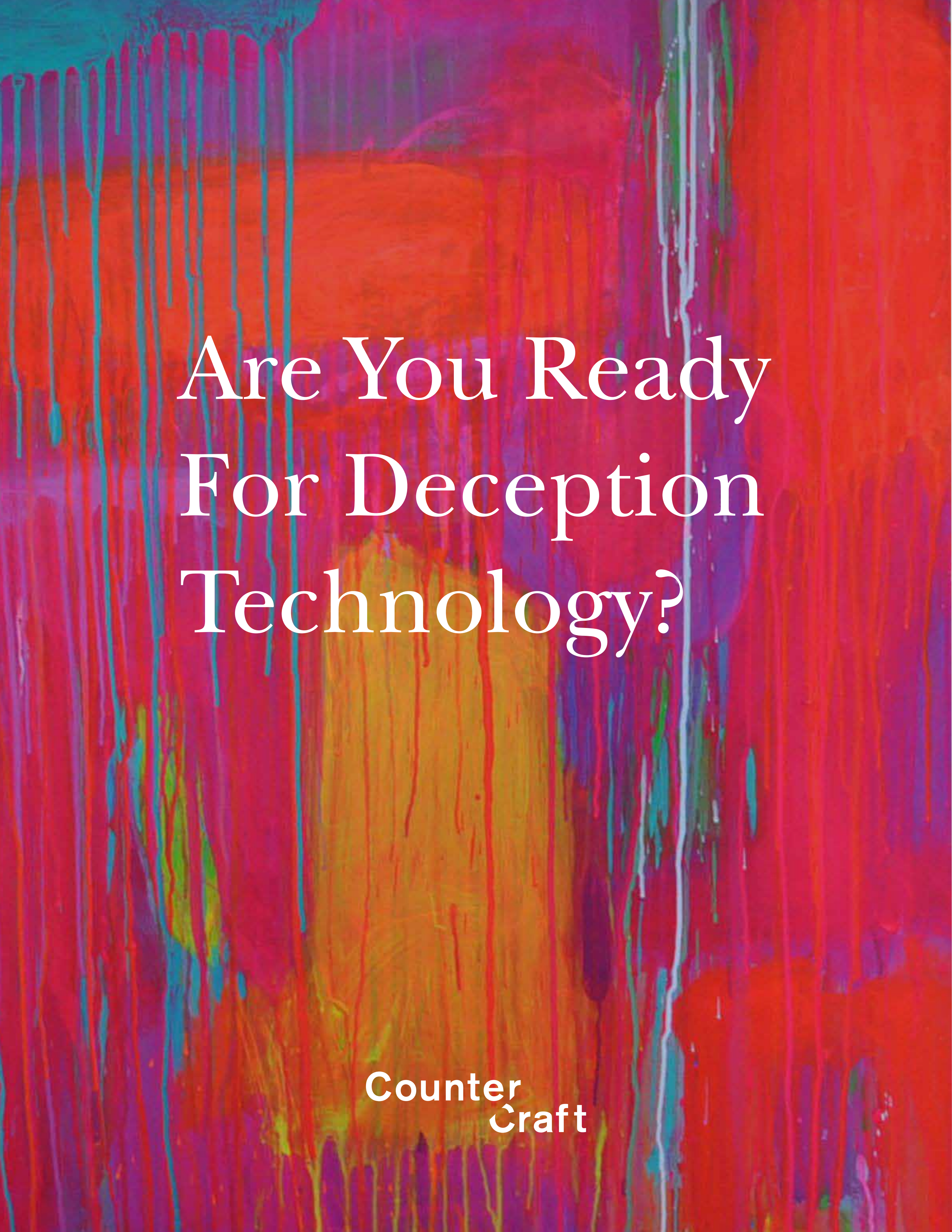


Are You Ready For Deception Technology?

Counter
Craft

01

Who can use cyber deception?

You've probably got some misconceptions about who can use deception technology. Read on.

Most organizations' stance on cyber deception stems from the belief that only mature businesses can incorporate deception into their current cybersecurity strategy. This is a common misconception that keeps many organizations from making the most out of a strategic proactive approach against their adversaries.

Incorporating cyber deception into your strategy is not about maturity—it's about wanting to make intelligent business-driven decisions.

Gartner defines these as decisions that allow organizations to detect attack vectors well before they get anywhere near their networks. In their thought-provoking Hype Cycle for Security Operations 2020 report, Gartner shows not only where cyber deception stands in the hype cycle, but also how the level of maturity in any organization's security operations may not be relevant to the central question: 'Am I ready for cyber deception?'

02

Deception technology seems to be oriented towards high-maturity organizations, but the truth is it can offer security benefits to almost any size of company. Nowadays, even small or local businesses are targeted by threat actors. Even worse, these businesses are often less prepared and have fewer recourses when it comes to network security.

The truth is, anyone looking for early detection, faster MTTR, and fewer false positives can benefit from deception. Even smaller companies can use deception to keep networks up during an attack, improve security posture, and quickly detect attacks.

In fact, deception can often be ideal for smaller companies. Many campaigns and tools don't require any additional investment and some, like CounterCraft Cloud™, are even run by a third party. This allows a tiny to nonexistent security team to put up a defense that gives them a chance against motivated attackers.

Deception, in summary, can be applied in different, creative ways according to an organization's size, goals, and resources. That makes it a great option for larger organizations as well as small businesses that need to have an agile response to any potential attacks.

So what, exactly, can deception do for businesses at different levels of maturity?

Quite a bit, it turns out.

find out more about low, medium & high maturity >>>

03

How mature should a business be?

Deception serves different functions depending on a business's maturity level.

In the Gartner Hype Cycle Report it is made clear that organizations of all security maturity should be examining the value that deception can bring them — allowing them to fuse prevention and detection into a fully strategic security operations model. What are the key strategic benefits of deception technology for each maturity level?

LOW

Low maturity organizations in the report are those defined as not being capable of managing solutions such as SIEMS due to a lack of resources. These types of organizations would benefit enormously from deception technology.

MEDIUM

These are defined as organizations that may already have SIEM and EDR-type technologies. The cost in terms of time and resources can make leveraging such technology to deliver preventive security very difficult. EDR is also up against a number of different techniques that can circumvent it, such as process hollowing.

HIGH

High-maturity organizations may want to use deception technology in a number of different situations, such as in operational environments (SCADA, OT), where traditional security toolsets are not a viable option. In addition to this, deception technology has the ability to generate local threat intelligence. Mature security organizations use deception technology to actively collect data points on different types of threat vectors and actors that are looking to target them.

LOW

The CounterCraft Cyber Deception Platform not only scales seamlessly but the scarcity of false positives and high fidelity of alerts powerfully remediates the pain points commonly suffered by such organizations. But it does much more than remediate paint points: it enables powerful new functionalities, such as the ability to generate threat intelligence that is specific to such organizations and fully correlated and contextualized. Pivot away from simple detection and into prevention and actionable intelligence.

MEDIUM

Deception technologies can provide a different means of detecting the attackers by forcing them to be right all of the time. The CounterCraft Cyber Deception Platform will allow you to pivot away from detection into prevention by allowing you to deploy campaigns that enable you to map and correlate attackers well before they get anywhere near your network. Fusing together detection and prevention into a single platform allows you to develop an in-depth strategy that is coherent and forward thinking.

HIGH

Rather than wait for attackers to get inside your network, map adversary behaviour to draw out not only TTPs but also the strategic objectives of the threat actors. Understanding both data sets allows an organization to understand if currently deployed security controls would be effective against attackers with these particular strategic objectives in mind. With the CounterCraft Cyber Deception Platform, multiple campaigns can be created and automated, allowing an organization to create intelligence-led deception campaigns and gather the intelligence they need to empower themselves and make decisions. Leverage the power of cyber deception to empower your organization. Intelligence-led decisions will not only create a more cohesive security strategy: they will also drive down risk and the costs associated with those risks if they were ever to materialize.

Deception looks different (and works) for every maturity level.

05

Deception is a foundational tool in any security strategy.

Deception serves different functions depending on a business's maturity level.

Even the best-prepared, most mature team will not be ready for every eventuality. The goal for security leadership at organizations of any size should be improving cyber resilience and keeping systems operational.

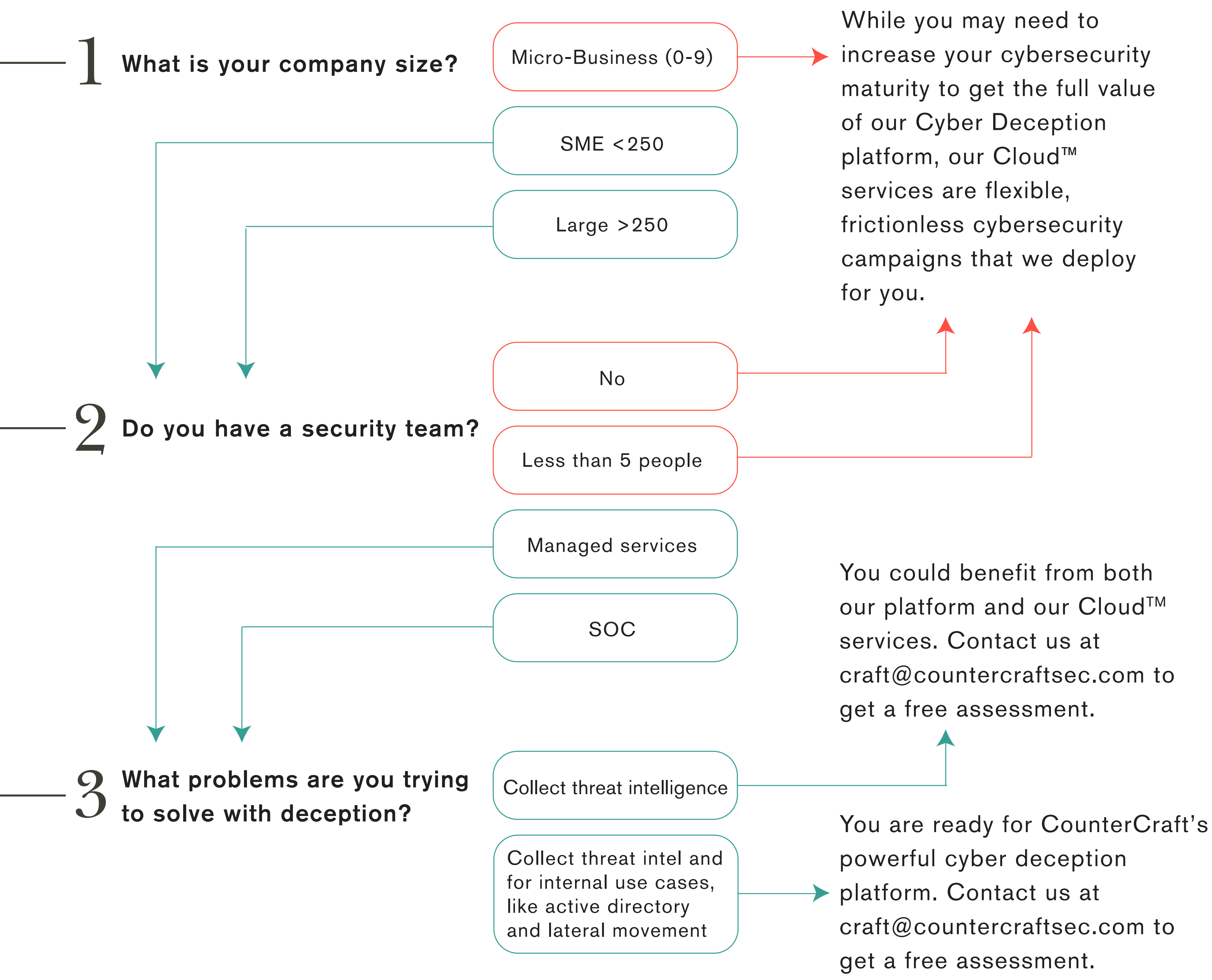
Detecting threats is vital, but on its own it is not enough. Detection and prevention need to be fused together in order to deliver operational resilience. The key is not to spend the security budget entirely on detection but to be able to make “intelligent business- driven decisions”. The challenge for security leaders is how to get to the point whereby they are empowered to make those types of decisions.

Deception can bring businesses of varying levels of maturity to a place where they have real, timely information to help them make informed decisions. Deception technology offers early insight into attacks by alerting security teams of threat actors, sometimes before they even penetrate the network.

Deception also helps to weed out false positives, meaning it can actually save a smaller SOC team critical resources. They now are able to devote their time to alerts that actually need attention.

Is my business ready for deception?

Take this short quiz to see if deception is right for you.



1 **What is your company size?**

- Micro-Business (0-9)
- SME <250
- Large >250

While you may need to increase your cybersecurity maturity to get the full value of our Cyber Deception platform, our Cloud™ services are flexible, frictionless cybersecurity campaigns that we deploy for you.

2 **Do you have a security team?**

- No
- Less than 5 people
- Managed services
- SOC

You could benefit from both our platform and our Cloud™ services. Contact us at craft@countercraftsec.com to get a free assessment.

3 **What problems are you trying to solve with deception?**

- Collect threat intelligence
- Collect threat intel and for internal use cases, like active directory and lateral movement

You are ready for CounterCraft's powerful cyber deception platform. Contact us at craft@countercraftsec.com to get a free assessment.

Gartner®

CounterCraft is the ONLY deception vendor to appear across multiple Gartner market guides :

- ✓ **Deception technologies**
- ✓ **Threat Intelligence**
- ✓ **Insider threat**
- ✓ **Operational Technologies**
- ✓ **Remote working**

These are the Gartner reports that mention CounterCraft:

1. Hype Cycle For Security Operations
2. Market Guide For Security Threat Intelligence Products and Services
3. Market Guide For Insider Risk Management Solutions
4. Market Guide For Operational Technology Security
5. Tips To Protect Data For Midsize Enterprise Remote Workers

About CounterCraft

CounterCraft is the next generation of threat intelligence. The CounterCraft Cyber Deception Platform offers active defense powered by high-interaction deception technology. Countercraft detects threats early, collects personalized, actionable intelligence, and enables organizations to defend their valuable data in real time. Their award-winning solution, fully integrated with MITRE ATT&CK®, fits seamlessly into existing security strategies and uses powerful automation features to reduce operator workload. Founded in 2015, CounterCraft is present in London, New York, New York and Madrid, with R&D in San Sebastian, Spain. Learn more at www.countercraftsec.com.

See all our resources,
documents and videos at

countercraftsec.com

or if you prefer contact us at

craft@countercraftsec.com