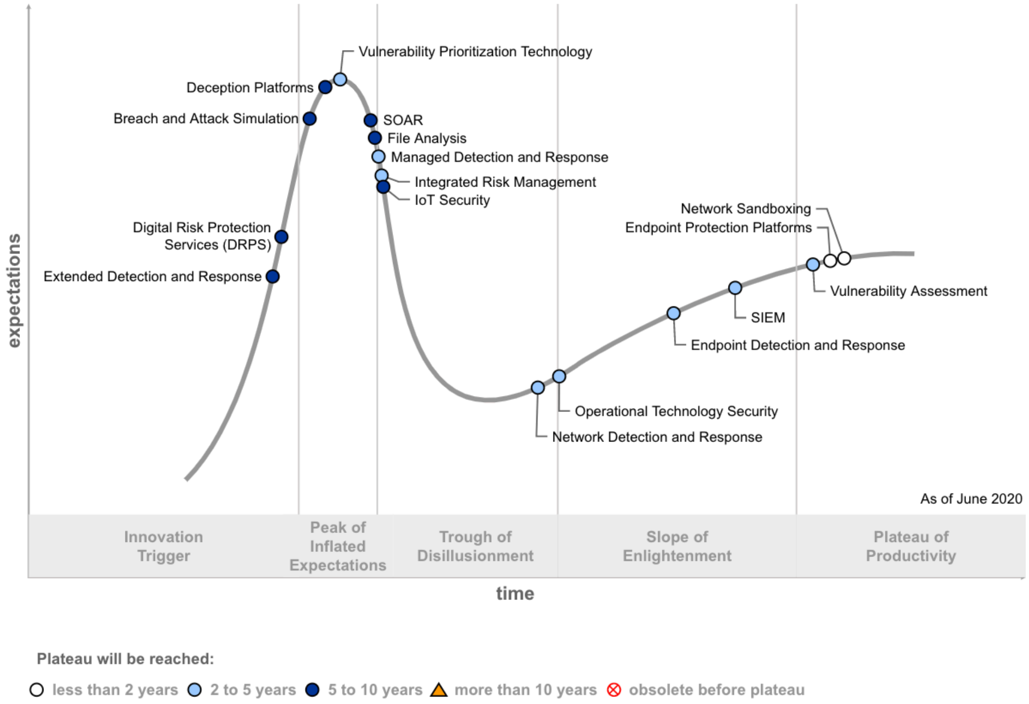
Are You Ready for Cyber Deception?

CounterCraft

Introduction

Most organizations' stance on cyber deception stem from the belief that only the ones that are mature enough can implement it into their current cybersecurity strategy. This is a common misconception that keeps them from making the most out of a strategic proactive approach against their adversaries.

What these organizations should know is that it's not about maturity, but about wanting to make intelligent business-driven decisions —defined by Gartner as thinking about being able to detect attack vectors well before they get anywhere near their networks. On their thought-provoking Hype Cycle for Security Operations 2020 report, Gartner show 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?'



© 2020 Gartner, Inc.

Security Leaders

It will prove to be an impossible task for any leadership team to be confident that their current security control set allows them to be prepared for every eventuality. More importantly, leadership teams need to try and deliver cyber resilience and keep systems operational. Therefore, being able to detect threats on their own may not be 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. To empower yourself to make the right decision means that you need the correct data points.

Data Points

For data points to empower your decision making, they need to possess a number of key characteristics. The data points must be contextualised, relevant and timely, and have a very low operational overhead to generate and process. Deception technology can produce these types of data sets in an automated manner, delivering the right ones at the right time, thus empowering decision making that is business-centric and intelligent. Most importantly, you do not have to wait to detect the attackers once they are inside your network and impacting your operational processes. Having the ability to deploy deception campaigns beyond your network perimeter (including cloud or a hybrid infrastructure) empowers you to get ahead of your adversaries. Understanding what tactics, techniques and procedures are being used against your organisation (TTPs) will enable a preventative posture to be adopted by leadership teams. Collect the correct data sets on attackers that enable you to detect them whilst they are trying to breach your network and not after the event. Data that empowers intelligent business-driven decisions.

Maturity

In the Hype Cycle Report it is made clear that organisations 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-Maturity Organisations

Low maturity organisations 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 organisations would benefit enormously from deception technology. 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 organisations. 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 organisations and fully correlated and contextualised. Pivot away from simple detection and into prevention and actionable intelligence.

Medium-Maturity Organisations

These are defined as organisations 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. So, in order to mitigate these pain points, deception technologies can provide a different means of detecting the attackers by forcing them to be right all of the time instead of those that are defending the network. Would you not rather turn the probability of detecting an attacker in your favour by forcing them into impossible choices? 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-Maturity Organizations

High-maturity organisations, according to the report, 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, the report states that deception technology has the ability to generate local threat intelligence. Mature security organisations use deception technology to actively collect data points on different types of threat vectors and actors that are looking to target them. 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 organisation 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 organisation to create intelligence-led deception campaigns and gather the intelligence they need to empower themselves and make *"intelligent business-driven decisions".*

If you want to make intelligent business-driven decisions, leverage the power of cyber deception to empower your organisation. 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.

About CounterCraft

CounterCraft is a pioneering provider of full-spectrum cyber deception technology offering attack detection, threat intelligence collection and proactive defence to clients. 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