How deception can change cyber security defences


Andrew Bushby

Andrew Bushby, Fidelis Cybersecurity

The use of deception technology in modern cyber security as a viable means of active, intelligent post-breach defence is a rapidly emerging phenomenon. But like any disruptive technology it comes with misconceptions. As cyber criminals continue to phish, bait, deceive and lure users, cyber defences need to move beyond being based on primarily detecting bad things within an ocean of good activity. Given how attackers are progressing, there is a clear case for invoking an active defence to lure, detect and defend against malware and intruders moving laterally within the network.

Whether it is camouflage in nature, or the spread of misinformation during human warfare, deception tactics often prove to be effective as a means of both defence and attack. In the realm of cyber security, phishing attacks and social engineering leverage the value of deception to deceive users to open, click and enable successful multi-stage attacks. However, cyber deception is just now making its way to the main stage for cyber security as a viable option for an active defence.

"Deception technology has evolved and improved far beyond the honeypot concept. Today, deception is about being active in terms of luring and baiting attackers to a deception environment"

When people hear the word 'deception' in cyber, they often immediately think of honeypots, which are static decoys that imitate simple computer systems and do nothing unless attackers stumble across them. However, deception technology has evolved and improved far beyond the honeypot concept. Today, deception is about being active in terms of luring and baiting attackers to a deception environment, as well as to the decoys.

Reducing noise

When attackers first penetrate a network, they need to carry out reconnaissance to learn about the environment and reduce their noise levels and evade detection, so it is clearly optimal to detect attackers during this stage, before they have the ability to identify the most valuable assets. Organisations often know to varying degrees what the attackers are looking for, what they expect to find and how they might attack and use the information they find – and with deception technology, you can use this knowledge against the attacker.

Ultimately, the goal of deception technology is to lure attackers to decoy assets that look and feel real but are not. This can be done through different methods, including traps in the network, on the endpoints and servers, data traps and more. By engaging with the decoy or deception environment, attackers or malicious insiders essentially reveal themselves to the organisation – but they do not know it.

Deception technology is quickly gaining the attention of organisations seeking an efficient post-breach detection strategy. Recent research conducted by Fidelis Cybersecurity found that 55% of global respondents would consider implementing detection defence methods with lures and bait desired by attackers with no risk to real systems, processes or data. And with the current threat landscape, it is not difficult to see why.

Critical deception

Most enterprises and their security operation centres (SOCs) are under siege. Indeed, security alerts are being triggered from all corners of the security stack – from the firewall, endpoints and servers, from intrusion detection systems and other security solutions. What's more, security teams do not have enough people or hours in a day to analyse the alerts that are coming in.

"After infecting an asset inside an organisation, hackers keep a low profile, moving laterally in the hunt for valuable, sensitive data. The longer they stay in the network, the harder it becomes to detect their trail"

According to the research, 27% of global respondents get 40+ alerts on average every day, which is more than most teams can handle. In addition,

many 'security events' do not even imply an attack is in progress or that data has been exfiltrated. They are often simply sharing information – such as failed connections – or are what is more commonly known as 'false positives', when a solution thinks it has found a specific vulnerability but, in fact, it hasn't.

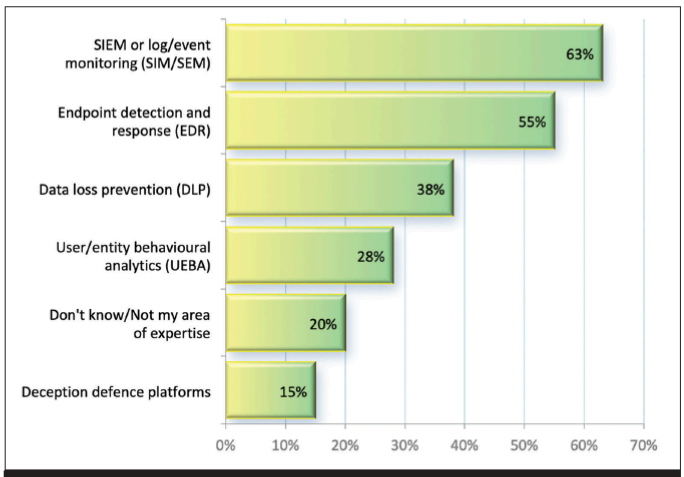
This is critical, not least because attackers use stealthy tactics that leverage these security challenges. After infecting an asset inside an organisation, hackers keep a low profile, moving laterally in the hunt for valuable, sensitive data. The longer they stay in the network, the harder it becomes to detect their trail. The average 'dwell time' – how long an attacker or malicious insider is inside an organisation's network – is measured in months, with some estimates as high as 200 days or more.

That is why it is critical for organisations – both large and small – to focus their cyber security strategies on earlier detection and faster response. One of the technology trends that is promising to do this is deception, and there are five ways that deception technology is changing the cyber security landscape.

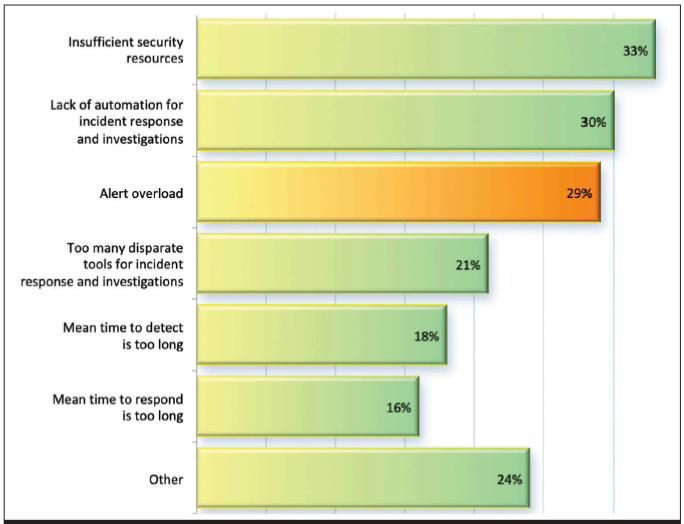
1. New visibility of threats

For many companies, prevention has been the primary cyber defence for decades with firewalls, anti-virus and patching. As perimeters fade and more than half of attacks do not use malware, the ability to improve detection of external intruders, malware and insiders becomes a new focus.

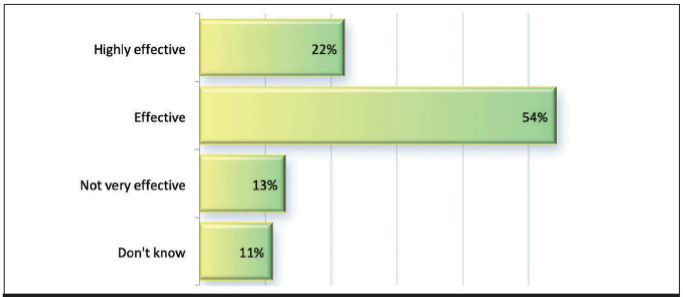
Often measured in dwell time or mean time to detect (MTTR), the numbers show months and days of hidden intruders in corporate networks. Organisations know the general information that attackers desire and this creates an opportunity to use deception technology to lure, detect and defend against attacks that evade preventive defences.



How organisations are currently detecting attacks. Source: Fidelis Cybersecurity.[1]



Key pain points for organisations include alert overload. Source: Fidelis Cybersecurity.



Answers to the question, 'How effective do you believe your preventative defences to be against targeted attacks?'. Source: Fidelis Cybersecurity.

2. Enabling early post-breach detection

With exercises such as 'capture the flag' and 'red versus blue team', businesses are quickly taught that months and days are really hours and minutes for the pace of how fast attackers can learn a new environment and quickly lower their noise level.

"False positives and dead ends waste critical time and resources within security operations if they are even being analysed at all. The noise factor is too high"

The Fidelis Cybersecurity research revealed that 63% of companies worldwide think it is 'very important' to detect post-breach attacks in the first few minutes and hours. Indeed, attacks are most vulnerable when they first enter a network and compromise a foothold system, making the focus on early post-breach detection very critical for detection. Deception defences provide an advantage with breadcrumbs on real assets to then lure attacks to decoys to detect and defend.

3. Fewer false positives and lower risk

Alert fatigue, false positives and dead ends waste critical time and resources within security operations if they are even being analysed at all. The noise factor is too high, and deception is a breath of fresh air, with high fidelity alerts and few false positives.

Deception is also low risk as an invisible defence for users with no impact on operations or risk to data and resources. When an attacker accesses or uses part of a deception layer, the alert is real and needs immediate attention where deception telemetry provides the required details.

4. Scaling automation

When it comes to enterprise security teams, they often do not get annual budget increases and new headcount positions. As such, they must protect and serve more effectively and efficiently year over year with the status quo. Deception with automation can scale to discover networks and profile assets to then auto-generate and deploy decoys, plus adapt deception layers to changing environments.

"Deception changes cyber security by providing unique breadcrumbs and decoys for legacy systems, industry-specific environments and devices, plus the Internet of Things (IoT) where low cost often prohibits security features"

Automation takes the manual effort away, enabling a tier-one security analyst to leverage deception defences in less than one hour per day. Companies are increasingly seeing the importance of automation when considering new cyber defences. According to the research mentioned earlier, 50% of global respondents cited automation as very important due to restricted security resources, illustrating the cost-effectiveness of this new technology.

5. Detecting shadow IT and legacy systems

When possible, having a security agent on devices provides optimal on and off the grid security to prevent and detect. However, not all devices are open to install security agents due to a lack of memory, firmware, manufacturer support or a host of other reasons.

Deception changes cyber security by providing unique breadcrumbs and decoys for legacy systems, industry-specific environments and devices, plus the Internet of Things (IoT) where low cost often prohibits security features.

Deploy the decoys

Prevention defences are certainly still needed within the enterprise: however, it is clear that advanced threats still have too much success. Put simply, early detection is now more critical than ever. Indeed, every business needs to be strategising about how to fill the detection-to-infection gap. With decoys that automatically adapt with their networks, businesses can immediately change their cyber security defences for the better.

With the threat landscape today, organisations must continually ask themselves, once inside, what does an attacker access or use to alert the security team? Deception technology helps answer that question. It enables security teams to detect threats faster and more effectively with automated investigation and response, ultimately giving you the ability to ensure an active post-breach defence. On top of this, it is easy to install, does not require a lot of resources to manage and it increases the effectiveness and efficiency of security teams.

About the author

Andrew Bushby leads Fidelis Cybersecurity's UK business with a focus on the company's network and endpoint cyber security technologies. He has over 25 years' experience working for IT companies and has held various senior leadership positions with companies that include Arbor Networks, Sun Microsystems, Novell and Oracle.

Reference

1. 'The State of Threat Detection'. Fidelis Cybersecurity, 3 Dec 2018. Accessed Dec 2018. www.slideshare.net/Fideliscybersecurity/the-state-of-threat-detection-2019.