How Deception Technology Helps CISOs Meet the Challenges of Cyber Security

CounterCraft

Introduction

In this paper, Nahim Fazal, Cyber Threat Intelligence expert, declares that not all deception technology is equal. Here, Nahim demonstrates how CISOs and their security teams can use deception to significantly increase their capacity to identify and deflect attackers.

Current technology sets are simply not living up to the challenge of preventing breaches, and Nahim discusses the reasons why organizations should be compelled to consider alternative technology, from large scale cyber attacks, uncontainable financial losses, to serious reputational damage.

A powerful mix of regulatory guidelines and extremely high probability that your network will be breached means now is the time for CISOs to actively research deception technology. Nahim explains the characteristics CISOs should be looking for during the selection process that will reduce the workload for their SOC team, including event management and alerting, automated complex defense responses and a complex range of deception hosts. A deception platform will provide the CISO with data that quantifies and qualifies your risk exposure, as well as detailed intelligence that inform where limited security resources should be focused, and enable the CISO to demonstrate to the Board what is being done to improve the organization's overall security posture.

Executive summary

- Current trends to distribute network parameters around the globe combined with multiple alert-based security tools add unnecessary complexity for SOC teams and lead to sophisticated attacks going undetected.
- The 2017 Verizon Data Breach Investigations Report identified a 75:25 split between external and internal threat actors; insiders represent a significant threat that traditional security tools will not detect because privileged access to critical data and systems is not necessarily abnormal.
- The majority of today's threat intelligence solutions deliver low quality, generic intelligence that is not actionable.
- Leadership has increasingly high expectations for the CISO to present a cohesive strategy that manages the risk of regulatory fines and costs associated with data breaches.
- CISOs should be researching deception platforms with a view to empowering their SOC team to operate more efficiently; automated feature and asset-rich deception environments deliver targeted and sophisticated intelligence with the power to save time, money and resource.

How deception technology helps CISOs meet the challenges of cybersecurity

The concept of deception and how it can be used to strengthen defenses and identify internal and external threat actors is relatively new. In this article, we will demonstrate how CISOs and their security teams can use it to significantly increase their ability to identify and deflect potential attackers. This is not just about security; organisations spanning every sector are currently embarking on ambitious digital transformation programs. In the first instance, the foundations for successful transformation require consumers to trust organisations with their data, and in order to ensure this, robust frameworks have been introduced to enforce this. You don't need reminding of the introduction of the GDPR (General Data Protection Regulation). But let us take a step back and examine where we are today when it comes to network intrusion and detection.

Data Breaches

There is no escaping the fact that the frequency and impact of newsworthy data breaches is on the up. Reflecting on some of the big breaches reported so far in 2018, the list is littered with well-known brands such as Verizon, Uber, Deloitte, Equifax or Dun & Bradstreet. In each case, it was customer information that the threat actors sought, found and extracted, affecting millions of end users. What this demonstrates is that the current technology sets deployed to prevent data breaches are simply not able to do so. Unsurprising, when we factor in the ever-evolving threat landscape, the diversity of the threats, and the budgetary and resource constraints that most organisations face. The costs associated with data breaches are staggering. Aside from any liability that may have existed under GDPR had it been in force, this figure alone should be a compelling reason for organisations to examine alternative and more advanced technology to help minimise the risk of incurring the financial loss and reputational damage that come with a data breach.

Deception Technology

It must be said that not all deception technology is equal. There are many different approaches to the steps required to identify threat actors, and through the use of deception, prevent a breach by moving them out of the production environment and into the deception platform. CISOs should look for some, if not all of the following characteristics (please note this is a starting point rather than an exhaustive list).

Event Management & Alerting

The deception platform should produce zero false positives; therefore, the event alerting should be concise, clear and feature-rich. This means detailed intelligence on what triggered the alert, who triggered the alert, and the ability to track the source of the alert right through all of the deployed deception assets. Attack graphs are particularly useful to SOC analysts in this instance, that help to address missed alerts and the volume of false positives generated.

Challenges

So, the first key problem that CISOs face is how to effectively defend their network parameters, that in 2018, are probably a complex mix of multiple different technology stacks, and likely distributed across the globe. This scenario alone makes the job of a SOC team infinitely more complex. Factor in the number of existing security tools that are firing of alerts on a regular basis, and the task of identifying real APT or zero-day threats becomes almost impossible. These types of sophisticated attacks have the ability to silently slip under the radar of existing network security measures and go undetected. And external threats represent just one aspect of the challenge; we must consider the additional risk of insider threats too. There will be employees with detailed knowledge of the corporate network and where critical data assets are located within this network.

Their behaviour wouldn't trigger any legacy security tool sets because it would fall within the normal range of expected behavior. The 2017 Verizon Data Breach Investigations Report identified a 75:25 split between breaches carried out by external perpetrators and internal threat actors, for those included in the study.

Some organisations have resorted to using threat intelligence in an attempt to become better informed and better equipped to identify the vast array of threats out there. The problem with this, however, is the poor quality and generic nature of the threat intelligence collected, that together render it very difficult to act upon. This is where distributed cyber deception platforms offer value.

To summarise, the key pain points for CISOs are:

- The inability to detect corporate network breaches in a timely manner
- Effectively detecting the insider threat
- The inability to detect advanced attack techniques that leverage APT and zero-day threats
- Too many false positives associated with current technology
- Regulatory demands for effective breach detection and investigation
- Targeted, client-specific threat intelligence
- Equipping the SOC team with the tools they need to be more efficient
- Missed alerts

With each pain point identified above, there is an associated cost and the potential for a data breach running into hundreds of millions of dollars. These issues simply can't be ignored. At board level, leadership teams increasingly expect to see a cohesive strategy that details how the risk of regulatory fines and costs associated with data breaches will be managed effectively.

Automated Complex Defense Responses

To effectively reduce the workload for the SOC team, the deception technology should include automated functionality. Automation allows the deception environment to be manipulated in response to the attacker's actions. This targeted intelligence informs incident response processes with the level of sophistication needed to save time, money and resource. Consequently, the SOC team is empowered to operate more efficiently, their time freed up to focus on real threats targeting the wider network.

Complex Range of Deception Hosts

In order to effectively identify threat attackers within your network and keep them engaged in the deception environment, the deception platform must be capable of deploying a diverse and rich range of deception hosts. Fully functional operating systems covering both Windows and Linux should be a baseline requirement to support this. In addition, routers, Wi-Fi access points and even mobile devices should all be considered for use as deception assets. Remember that the richer and more complex the deception environment, the more likely you are to root out not only external threats, but those that lay inside your network too. But it should not stop there. One of the final key points identified earlier was the lack of client-specific intelligence. You need to know who is attacking, how are they attacking, and what data sets are they after - if that is in fact what they want. This means any deception technology should be able to deploy external deception campaigns in order to collect detailed information on what comprises the threat actors targeting your organisation. You cannot create a cohesive security strategy unless you can answer some basic questions; am I being targeted by low level threat actors relying on third party tools and automation, or am I in fact being attacked by APTs using bespoke toolkits and crafted malware?

Conclusions

Now is the time for CISOs to actively research deception technology. The rationale behind this a powerful mix of regulatory guidelines and the increasing probability of attackers breaching your network. There are significant business benefits to be leveraged through the use of such technology, including, but not limited to;

- **Faster detection of threats at a lower cost**
- **Enhanced detection of advanced threats**
- **Collecting specific threat intelligence on if and how you are being targeted**
- **Developing a cohesive security strategy based on objective data sets**
- **Reducing false positives and not missing alerts**
- **Reducing the overall the cost of detection**
- **Potential to reduce your overall security spend**
- **Delivering rigorous management information on how effectively the cyber risks are addressed**

Ultimately for a CISO, a deception platform will vastly reduce the probability of your organisation suffering a data breach, regardless of the source. It will provide you with informed data analytics that quantify and qualify your risk exposure to threat actors, and provide you with detailed intelligence on which attack surfaces and tools might be used to target your organisation. These data sets will not only inform where you should be focusing your limited security resources, but also demonstrate to the board how effectively managing cyber risk, and what you're doing to improve your organisation's overall security posture.