Deception Technology

An integral part of the next generation SOC

Table of Contents

Executive Summary	2
Key Themes	2
1. Assuming Breach	3
2. Proactive Defence	3
3. Low False Positives	3
4. Data Analytics and Threat Intelligence	3
5. Orchestrated Response	4
6. Insider Threats	4

zscaler™

Executive Summary

With adversarial capabilities improving, greater than ever stakes around information security, and a fast evolving threat landscape, everyone wants a 'next-gen SOC'. But what does that really mean?

At its most basic, it involves evolving from simple log aggregation and static detection use-cases to a proactive, low false-positive detection model, with deep analytics to convert data to information, and finally, heavily automated response mechanisms.

Deception technology comes from a consideration of the attacker's point-of-view, and correspondingly, arms security operations teams with many of the most desired capabilities of a next-gen SOC.

This white-paper illustrates some of the key ways you can upgrade your monitoring capabilities with deception in order to thwart threats faster, more accurately, and with greater confidence.

Deception technology comes from a consideration of the attacker's point-of-view, and correspondingly, gives security operations teams many of the most desired capabilities of a next-gen SOC.

Key Theme

- Security operations centres must 'assume breach', and work as if the environment is already compromised, in order to find advanced threats.
- Proactive defences like deception and threat-hunting turn the tables on the attacker and shift economic, time, resource and cognitive costs to them. They must work hard to evade detection, rather than the security team working hard to detect them.
- False positives and bad data are the bane of most current-day SOCs. Deception has the lowest false positives of any class of solution, as any engagement with a deceptive asset is suspicious.
- With low false-positives, security teams can orchestrate their response to incidents, without needing human intervention.
- Deceptive assets only attract bad or anomalous engagement, so data analytics can be used to gain better insight, create threat intelligence and respond faster.
- Deception is a capability, not a product or technology, it involves training, processes and deception strategy that are risk-driven and linked to business imperatives.

Here's a break-down of the the **TOP 6 REASONS** why a deception platform is a crucial component of the next-generation SOC.

1 Assuming Breach

Gone are the days (if they ever really existed) where defenders could neatly divide their network into trusted and untrusted. With networks scaling and adversarial capabilities staying far ahead of the average security team's capabilities, the industry is moving to assuming that the environment is hostile, and is likely in various stages of compromise already.

This approach liberates defenders from having to try and plug every weakness (an impossible task!) to baselining and monitoring for compromise in progress. If security teams have a good baseline and reliable telemetry, they can find even the most sophisticated attackers dwelling within the network.

Deception technology already 'assumes breach'. Decoys are placed on endpoints, in Active Directory, and on the network, in such a way that an attacker in progress will engage with these deceptive assets and reveal their presence.

2 Proactive Defence

Deception technology is an 'active defence', designed to make the network hostile for attackers, and to shift the costs of remaining undetected onto them. In contrast, static security monitoring use-cases fall out of date quickly, and cannot keep up with changing attacker tactics, thus making it easier for attackers to evade detection and dwell within the network for months or even years.

However, deception does not rely on static use-cases. By targeting the human intent behind an attack, as opposed to the tools, exploits, or www.smokescreen.iotechniques being used, deception based defences can remain effective no matter what the bad guys try in the future. This means that the modern SOC can stay agile and adaptive to new threats without having to wait to see them first. Deception can also be used by threat-hunters and incident responders to lay down traps both to find evil, or dimension the spread of an on-going incident.

3 Low False Positives

Traditional SOCs have 'cried wolf' far too often. Even with significant tuning, finding the balance between too many alerts, and missing real incidents is extremely challenging and a constant process. A reduction in the number of false positives automatically makes the security team more productive as they can focus on real threats instead of chasing down ghosts.

Deception technology has extremely low false positives because nobody should even interact with a decoy system, credential, or file. Any interaction is worthy of investigation, and can even trigger an orchestrated response. This means that the SOC can reduce the number of alerts to only the ones that matter.

4 Data Analytics and Threat Intelligence

Most data analytics focuses on 'collecting everything' and then trying to make sense of the data. Security is not necessarily a big-data problem, it's more of a 'good-data' problem. Since deception systems only see anomalous or malicious traffic, data-analytics can be applied to better understand the threats within the network instead of hunting for a needle in a haystack (or ElasticSearch DB!).

This also means that the SOC can move from consuming static, external threat intelligence (which is not specific, and often stale) to creating its own threat intelligence and IOCs that are more relevant to the business, and can better inform future defences.

5 Orchestrated Response

In order to deal with threats at wire-speed, you need orchestrated response mechanisms. However, the challenge is to find orchestration triggers that are so reliable that a human being does not have to validate them before the response is actually fired. Failing to do so can mean that response actions trigger on false positives, which can lead to disruption of legitimate business activity.

With low false positives and built-in orchestration and integration capabilities, a deception platform can enable 'continuous response', reliably detecting compromised assets and users within the network, and investigating, containing or eradicating the threat automatically, without the need for human intervention.

6 Insider Threats

While security teams have typically focused more on external adversaries, the insider with legitimate access is far harder to tackle. They often have detailed knowledge of the security mechanisms in place, and can tailor their malicious intent to look completely benign.

Deception can detect insiders seeking out data on high-value target personnel, searching for systems they should not access, or copying and opening data that they are not authorised to. It also injects an element of unpredictability; deception deployments are invisible to normal users, and the placement of decoys is known only to a limited trusted circle, so the insider will either not know of the existence or the placement of the deception. This also serves as a deterrent against casual fraud or misplaced inquisitiveness by internal employees.

Deception is a crucial component of the modern SOC. The use of adversarial thinking against the attacker changes the game for defenders, letting them 'punch above their weight' against sophisticated adversaries.

Zscaler Deception's deception technology has helped some of the world's most mature security monitoring teams take their detection and response capabilities to the next level, as well as enabled new security teams to begin defending their networks against targeted threats with greater fidelity, productivity, automation and reliability.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com