Deception Technology: A Deceivingly Simple Solution to Complex Threats

July 6, 2018
by Marc Feghali

You have almost certainly heard about Deception Technology for cybersecurity, but may be wondering what it will take to implement it in your environment. It seems complex. How can you possibly deploy it in your own diverse, distributed, and complicated network? No doubt you have the battle scars attesting to the challenge of deploying new security controls on your network. So how do you proceed?

Deception Case Study

To illustrate our point on simplicity, this enterprise case study will show, even with a larger installation, that deception is exceptionally easy to prepare, deploy, and operate. Here is an example of a deployment that a current customer of ours implemented.

Goal: Deploy deception inside the network to cover network-based attacks, credential-based attacks, attacks against Active Directory, detect Man-the-Middle attacks while providing network visibility across all locations.

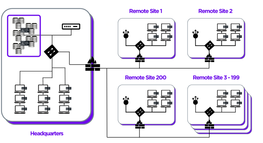
Integrate seamlessly with existing EDR, NAC, and SIEM solutions to automatically quarantine infected systems

The Network: 100 local VLANs/subnets distributed between access networks and a hybrid datacenter. 200 remote locations with up to 8 VLANs each and a data center. 10,000 employees spread across multiple locations.

The Solution: Hologram Deception

Example Architecture

1 HQ site with 100 VLANs, users and a datacenter.
200 Remote sites with up to 8 VLANs each, users and datacenter
10000 users total



Using this configuration, the customer blanketed their entire local and remote network environment with full visibility and deception on all of their VLANs and subnets. It took less than a day to fully deploy the system at HQ with a rolling thunder deployment covering the endpoints and remote locations, enabling the customer to stick to scheduled maintenance windows.

The Deployment Process

The customer started by mounting their Hologram appliance (it can deploy as a physical appliance, virtual appliance, or a cloud instance) and connecting it to a trunk port on their network. Once on the network, the Hologram server automatically identified connected VLANs and subnets and requested IP addresses in each. Alternatively, the customer could have chosen to assign IP addresses manually across the desired VLANs.

Using the SingularityTM Identity solution on the endpoints, a Hologram server generates, manages, and updates decoy applications and cloud credentials to help guard against targeted attacks. In this case, the customer deployed Singularity Identity to their endpoints, servers, and in Active Directory. The decoy credentials are hidden from normal users. Any use of these credentials generates a high-fidelity alert identifying the compromised system, stolen credentials used, and all of the attack details.

To support their remote locations and data center, the customer deployed Hologram at each location. This gave them coverage of the remote VLANs and subnets, extending the Hologram server capabilities to those sites without losing functionality. Through Hologram, the customer gained visibility into their remote locations, meaning any attacker would have to traverse a deception minefield in the remote sites, not just on the headquarters network.

The Hologram solution was also configured to automatically quarantine an attacker by leveraging their existing security infrastructure. In practice, once an attacker engages with the deception environment, the Hologram solution contains the attack, collects TTPs and IOCs, and shares this intelligence with other security solutions to expedite remediation. The Hologram solution has extensive integrations with NAC, EDR, endpoint solutions, SIEM, firewalls , and gateways to make this automatic and simple.

Conclusion

Implementing deception is a straightforward proposition that dramatically reduces dwell time and mean-time-to-remediation. It's versatile enough to fit into any environment, it is highly scalable, and is extremely easy to deploy, manage, and operate. In today's threat landscape, it really can't get much easier than this to gain the upper hand against attackers. To learn more about the Hologram solution, visit our product page.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Why Credential-based Deception Used Alone is Not Enough -2/5
- Detecting Unconstrained Delegation Exposures in AD Environment
- Top 10 Ways to Protect Your Active Directory
- Protecting Your Active Directory from Admin$DHolder Attacks
- Detecting a Rogue Domain Controller – DCShadow Attack
- Rise in Identity-Based Attacks Drives Demand for a New Security Approach