The Role of Deception in Securing Active Directory

Introduction

90% of businesses around the world use Active Directory as their primary Directory Service. It plays an essential role in the identity and access management of large enterprises. In the past few years, attacks on Active Directory have soared. This is because it is a central platform where all the identities and accesses of employees are hosted, making it the keys to your enterprise. According to research, 80% of all security exposures stem from Active Directory accounts, which shows what a lucrative target it is for cyber attackers.

Protecting your AD is important for maintaining the overall security posture of an organization, protecting its data, and ensuring smooth and secure operations. Attackers can use compromised AD access to deploy ransomware across the network, encrypting data and demanding ransom.

Attackers who already have a foot hold on the network take advantage of access to Active Directory (AD) and use it to enumerate vulnerable assets, gain privileges and move laterally to other higher-valued targets on the network. Working with AD allows attackers to learn about the network while communicating only with the Domain Controller (DC) server, instead, for example, of doing a noisy scan on the network.

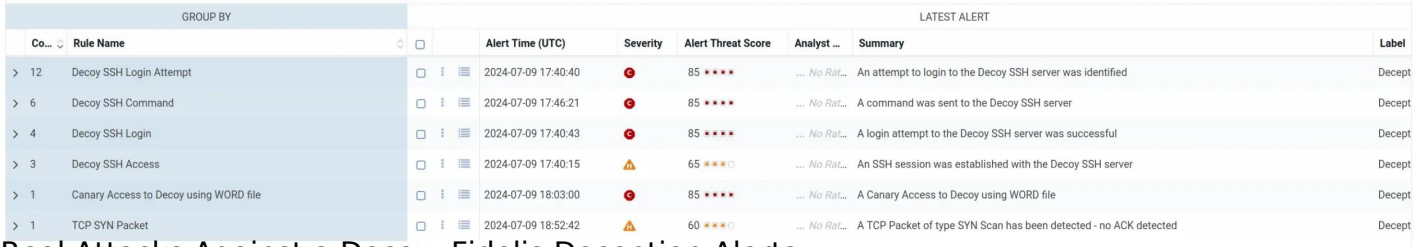
Modern Active Directory security solutions or Identity Threat Detection and Response (ITDR) solutions are equipped with features to secure it end to end. One such feature which is vital for Active Directory security is deception technology. Let’s understand this better.

Decoding Deception Technology

Fidelis Deception technology is designed to trick attackers by setting up convincing traps to lure hackers and discover their presence. Fidelis offers the most advanced enterprise Deception solution. is a more evolved version of honeypots in your network. We developed our system to sniff out malicious insiders quickly and efficiently.

An integrated deception technology works because there’s no real reason why someone from within the enterprise would know of or have any reason to interact with any deceptive mechanism including access decoys. Fidelis deploys breadcrumbs on real assets to widen the net and detect malicious activity faster. Which means that if someone does access it or engage with it, it’s most likely a malicious activity. This drastically reduces the probability of getting false positive. Deception technology also can collect data from the hacker like what tactics they are using, what they want to access and more. It may also give information about things that have already been exploited.

Once you detect activity within Fidelis Deception, we give you actionable data to quickly eradicate the threat actor.



GROUP BY			LATEST ALERT					
Co...	Rule Name		Alert Time (UTC)	Severity	Alert Threat Score	Analyst ...	Summary	Label
12	Decoy SSH Login Attempt		2024-07-09 17:40:40		85	... No Rat...	An attempt to login to the Decoy SSH server was identified	Decept
6	Decoy SSH Command		2024-07-09 17:46:21		85	... No Rat...	A command was sent to the Decoy SSH server	Decept
4	Decoy SSH Login		2024-07-09 17:40:43		85	... No Rat...	A login attempt to the Decoy SSH server was successful	Decept
3	Decoy SSH Access		2024-07-09 17:40:15		65	... No Rat...	An SSH session was established with the Decoy SSH server	Decept
1	Canary Access to Decoy using WORD file		2024-07-09 18:03:00		85	... No Rat...	A Canary Access to Decoy using WORD file	Decept
1	TCP SYN Packet		2024-07-09 18:52:42		60	... No Rat...	A TCP Packet of type SYN Scan has been detected - no ACK detected	Decept

Real Attacks Against a Decoy. Fidelis Deception Alerts.

Role of Deception in Securing Active Directory

The main role that deception comes in after the attackers have already passed 3 to 4 lines of defense and now are after your Active Directory which is their number one target. Its primary role is detecting attackers that have already made their way into your enterprise. So, it focuses on post-breach detection of attacks.

This is made possible because deception technology deploys decoys that mimic AD servers, user accounts, and other AD-related assets. These decoys attract attackers who attempt to compromise Active Directory.

Challenges

Fidelis Security makes it easy to implement deception. We incorporate the Active Directory feature using a simple configuration wizard.

As the team that installs this solution, we often find the biggest challenge is removing communication barriers between the AD (Sysadmin team) and the security team. Hence, this implementation requires these groups to understand each other’s roles and the importance of AD security and working together to secure organization.

Bringing the system or AD administrators and security team together is a necessary first step. By understanding what protections are in place, and the value of adding deception to your AD infrastructure everyone will be on the same page.

Why Should you Consider Deception Technology for securing your AD?

There are a lot of security technologies that may impede the organizations’ operations by affecting the performance or people’s ability to get things done. But deception does not do that. It is very easy to deploy which means that it doesn’t affect your existing security posture, but just sits on top as an additional layer of defense. It is also an extremely cost-efficient add on to have.

Attackers are sometimes on a network for a long time before they are detected. It’s hard to look for something “evil” on your network, especially with attackers getting more sophisticated and better at avoiding detection. It’s much easier to identify someone interacting with an asset that nobody should be interacting with. This means your security team isn’t wasting their time on false positives. Instead, you are causing your adversary to waste time.

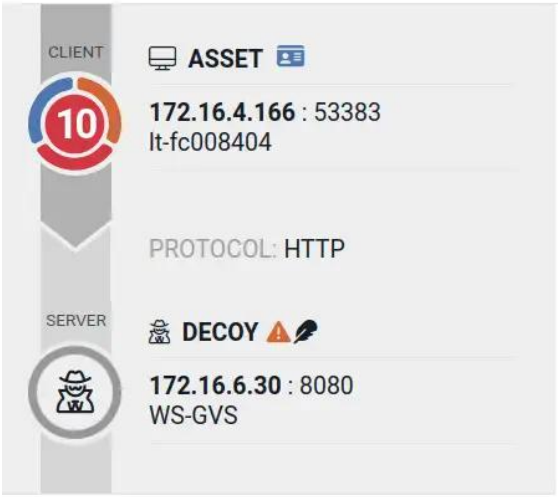
This means that there’s no downside to deploying deception technology, your organization doesn’t lose anything with integration of deception. Fidelis Deception technology requires little maintenance while still providing actionable high confidence alerts to your security team.

Fidelis Deception®

Fidelis offers the most fully featured enterprise deception solution on the market.

It comes with a tremendous number of options for deceptive practices from decoys (honeypots), fictitious users, services and files managed from a single interface.

Fidelis Active Directory Deception integrates with your Microsoft Active Directory service. You enable this functionality using an easy-to-use wizard. This wizard defines the users and decoys on the Active Directory server and binds them to Active Directory. Activity from a deceptive (fictious) user will alert your domain administrators to malicious activity on your domain. Fidelis Deception allows organizations to create canary files. These canary files will send a beacon if they are opened, alerting you to a data exfiltration event.



Severity	Critical
Threat Score	85
Alert Time	2024-07-09 18:03:00
Rule Name	Canary Access to Decoy using WORD file
Threats	Credential Access Tar...
Conclusion ID	1558 Go to Conclusion
Summary	A Canary Access to Decoy using WORD file
Labels	Deception Alerts
MITRE ATT&CK™	Lateral Movement /Remote Services Lateral Movement / Exploitation of Remote Services
Decoding Path	

Additional Information

Alert Type	Decoy - Emulation
Alert UUID	81c27a7a-4fe7-40eb-b9ab-59af05263d93
Alert ID	1613500
Insert Time	2024-07-09 18:05:08
Age of Alert	a month ago
Compression	0
Entropy	[Empty]
Session ID	1718020964408
Action	alert
CommandPost	Console
Component Name	decoy.packet.lab
Component IP	172.16.5.42

Canary File Access Alert

When combined with Fidelis Network, we can automate many parts of deception deployment to make it even easier to adopt this technology.

Our Deception Technology solution includes:

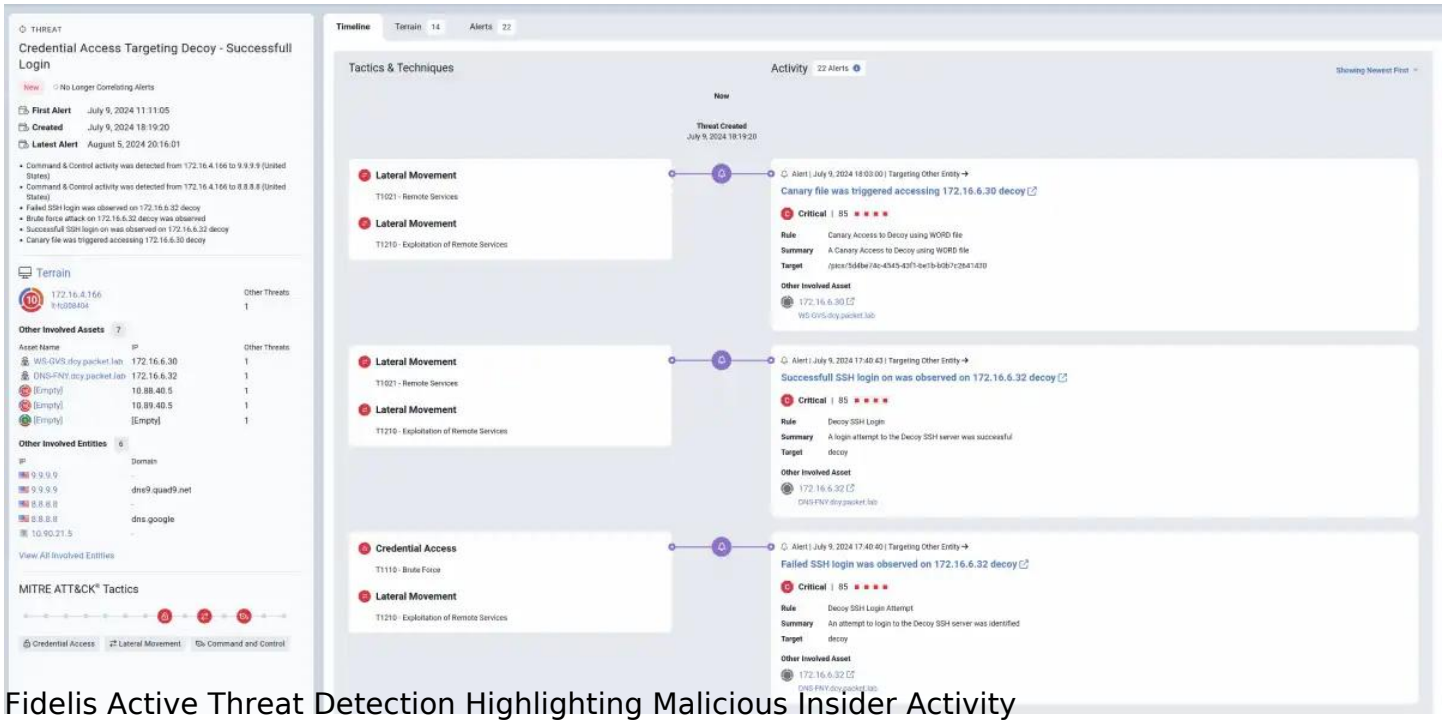
- Automatic or manual deployment of authentic deception layers
- High-fidelity alerts eliminating false alarms
- Active sandbox analysis
- Breadcrumbs
- Canary Files

Conclusion

We foresee a future where Deception is adopted more widely. Unlike firewalls and other traditional systems, it does not create noisy alerts. It will allow your security team to place decoys (traps), breadcrumbs (lures), and fictious users throughout the environment. Any interaction is an immediate red flag and notice that you have unwanted insider activity.

This helps your security team focus and solve real problems rather than fake alerts. Moreover, it is a super easy to implement layer of defense which means there's no downside for your business in adopting deception technology.

We have recently introduced more Active Directory focused security awareness through our Active Directory Intercept feature. This development was driven largely by our experience with our successful AD Deception feature set.



Fidelis Active Threat Detection Highlighting Malicious Insider Activity