Honeypot vs Deception Tech: Understanding the Difference

Luring cybercriminals away from real IT assets using a decoy has been a well-known strategy used by security experts. The goal of this strategy is to gain protection against all unauthorized access and minimize damage.

Over the years, honeypot, a prominent decoy system, has been used as bait to attract cyber attackers away from legitimate targets and gather data about their methods, intentions, and capabilities as well as any vulnerabilities of the network. Honeypots laid the foundation of today's sophisticated and advanced deception technologies used by modern organizations.

Honeypots and modern deception tech share the same principles and approach of luring threat actors to fabricated resources that appear to be genuine enterprise systems. While they share quite a few similarities, modern deception tech goes beyond traditional honeypots by creating a dynamic and adaptive environment that mimics real network assets. Thus, there are distinct differences between them that should be learnt before enterprises adopt them as part of their cyber security arsenal.

In this honeypot vs deception tech article, we will discuss key differences between traditional honeypot and modern deception technology.

Honeypot vs Deception Tech: Key differences

We have highlighted eight key differences between honeypot and deception tech solutions to help enterprises and security professionals understand the similarities and dissimilarities better. This differentiation can also help them understand which tool suits best for their security requirements.

Features Honeypot Deception Tech

Deployment

Deploying and maintaining a honeypot is a manually intensive process which can be a long and time-consuming process. It can be costly and complex to deploy. Deploying and maintaining deception tech solutions is quite an automated process and requires comparatively less human effort.

Scalability

Honeypots are not considered to be highly scalable due to manual configurations, deployment, and updates. Deception tech solutions can implement decoys at a significant scale due to the high level of automation involved.

Specialized use cases

Generally deployed in highly targeted areas of a network where they are most likely to attract cyber attackers like a database of a financial service. Modern

deception solutions

can mimic servers, applications, an endpoint device, and IoT devices. They can emulate just about anything.

Maintenance

Requires cybersecurity personnel to work between systems in order to maintain and update the decoy. Automation reduces maintenance efforts and operational overhead; the vendor also provides technical support and consultation.

Complexity

Honeypots are generally deployed as a single-purpose and static system attached to the network. They simulate specific vulnerabilities or assets to lure attackers. Encompass a broader and more advanced approach to seamlessly deploy a network of decoys and breadcrumbs to lure attackers.

Capabilities

Acts as a network-attached system to gather insights into strategies and attack methodologies. It is not viewed as a solution to network security but as an aid to it. Proactively engages with attackers, redirecting them to the decoy to mislead them dynamically and gain intelligence on their tactics, techniques, and procedures (TTPs).

Integration

Offers limited integration capabilities into enterprise security infrastructure as it is deployed as a stand-alone system. Seamlessly integrates with modern cybersecurity tools such as security information and event management (SIEM) and security information and event management (SOAR).

Usability for enterprises

Suitable for small and medium scale organizations and specialized use cases in larger organizations. Modern deception solutions are designed for enterprise-wide implementation with complex IT and OT environments.

Advantages and Disadvantages of Honeypots & Modern Deception Technology

After learning the key differences between honeypot and deception tech, it can be easily concluded that deception technology is an evolution of traditional honeypots. As we create a differentiating line between these two, both honeypot and deception tech serve as valuable cybersecurity tools for organizations today. It is essential to understand the limitations and benefits of both technologies for a deeper understanding.

Advantages of Honeypot

- Honeypots act as a rich source of information on attack methodologies and vulnerabilities. Once deployed, they gather data continuously in real-time, giving organizations an opportunity to improve their security posture.
- A honeypot can lure threat actors inside the organization who attempt to access sensitive data with a malicious intent.
- It wastes time and resources of the cyber attackers.

- It acts as a security layer and aids the overall security posture of the organization.
- It identifies malicious activity even if encryption is used.

Disadvantages of Honeypot

- One of the major disadvantages of a honeypot is that skilled attackers can detect them by distinguishing them from production systems. They can identify the real identity of the honeypots.
- A honeypot is required to be updated and maintained to match with real enterprise systems as closely as possible. This constant maintenance and upkeep present an operational burden and cost on the organization.
- A honeypot is only useful for catching threats and attackers that interact directly with the decoy system.
- A honeypot once attacked can be used to attack other systems.
- It is made to lure only a certain kind of attacker and threat.

Advantages of Deception Technology

- Deception tools provide early warnings by triggering alerts as soon as attackers interact with the decoy. This massively reduces the duration attackers remain undetected within the network.
- Deception tech helps in gaining deep insights into the attackers' tactics, techniques, and procedures (TTPs).
- It acts as an additional layer of defense by working together with existing security tools like EDR, NDR and XDR.
- It also integrates seamlessly with security information and event management (SIEM) and security information and event management (SOAR) to enhance their effectiveness.
- Deception tech offers advanced threat hunting capabilities such as identifying zero-day attacks and insider threats.

Disadvantages of Deception Technology

- Deception tech can be complicated to set up and manage as the enterprise networks today are growing vast and complex.
- Deception tech can be expensive to buy and deploy, however, its cost can be offset by the savings that are realized from early detection and prevention.

You May Also Be Interested In:

- **Deception vs. Traditional Threat Detection: A Detailed Comparison**
- **How Fidelis Deception Turns Your Attack Surface into a Defensive Advantage**
- **Cyber Deception as a Strategic Pillar in Active Defense**

Safeguarding your enterprise with Fidelis Deception®

Today, cyberattacks have become more sophisticated and dangerous. The level of damage they can inflict on bigger organizations is unimaginable. Deception tech proves to be an advanced tool to protect against a wide range of cyberattacks and enhance the overall security posture of an enterprise.

That is where Fidelis Deception® steps in as a comprehensive platform that uses decoys, breadcrumbs, and active deception to trap cyber attackers and examine their moves/attack patterns, enabling organizations to detect attacks earlier and mitigate them before damage occurs.

Fidelis Deception® automatically maps the cyber terrain, identifies vulnerabilities in assets, and strategically places decoys across networks, endpoints and cloud environments. These decoys lure cyber attackers to interact with them to understand their motive and methodologies as they move in the network. Fidelis Deception® offers various benefits:

- Detection of high-risk assets and vulnerable attacks points that attackers are most likely to target.
- Dynamically generates decoys that mimic real assets of the enterprises and captures detailed insights into attacker's tactics, techniques, and procedures (TTPs).
- Uses machine learning and automation tech to constantly update the decoy, making it extremely hard to detect by attackers.
- Triggers real-time alerts when attackers or insiders interact with decoys. It also limits false positives, so the security teams focus only on genuine cases.

Fidelis Deception® acts as a solid proactive defense mechanism for enterprises looking to keep their data protected and attackers at distance. While the tool works flawlessly on its own, it has the capability to be integrated with Fidelis Elevate®, a leading extended detection and response (XDR) platform for modern enterprises. With the integration, Fidelis Deception® can deliver high contextual visibility and rich cyber terrain mapping across the entire IT landscape.

Our Customers Detect Post-Breach Attacks Over 9x Faster

Our Secret – Fidelis Deception Technology

- See why security teams trust Fidelis
- Simplify security operations
- Provide unmatched visibility and control

Book a Demo Now!

Frequently Ask Questions

What is the difference between deception tech and honeypot?

The key difference between deception tech and honeypot is that honeypots are comparatively older solutions that are generally deployed as a single-purpose and static system. They simulate specific vulnerabilities or assets to lure attackers. On the other hand, deception tech is an

advanced solution that uses machine learning and automation to create dynamic decoys which are hard to detect.

Is deception tech better than honeypot?

When deployed effectively, modern deception tech can perform better than traditional honeypots. However, it is important to assess the security needs and objectives before choosing the right approach.

What are the advantages of deception tech?

Deception technology acts as a proactive security layer for enterprises. It integrates seamlessly with modern cybersecurity tools to significantly improve the overall security posture of the enterprises.