LABYRINTH

DECEPTION TECHNOLOGY OVERVIEW

Labyrinth Deception Platform, 2023

https://labyrinth.tech

info@labyrinth.tech

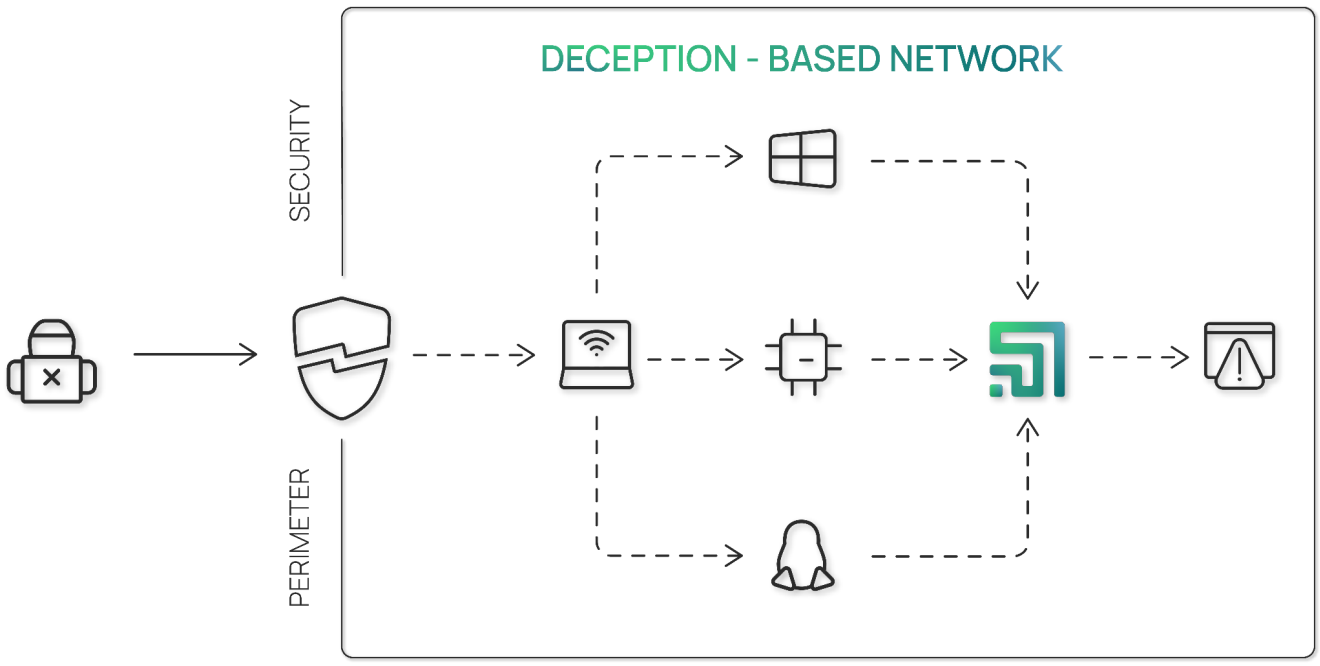
Labyrinth Development

1. DECEPTION TECHNOLOGY

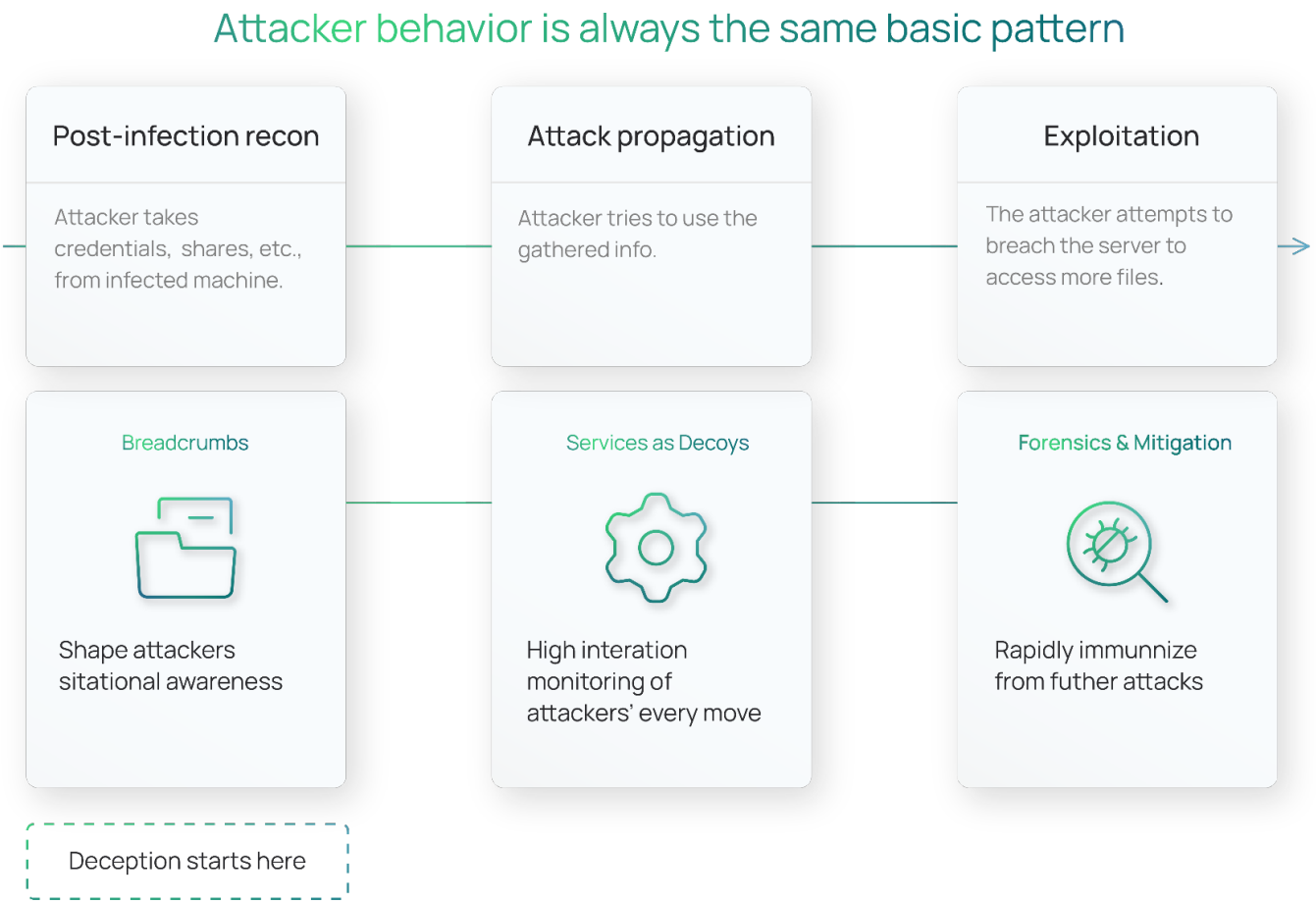
Cyberattacks are occurring at an unrelenting pace as sophisticated attackers continue to find ways to penetrate perimeter defenses. With each breach, security professionals are faced with mounting pressure to quickly detect and stop threats, before the damage is done. In addition to compliance expectations, new breach notification laws are being proposed with the promise of significant fines and potential jail time if notification expectations are not met.

Organizations of all sizes and across all industries are seeking innovation to mature their security models, close detection gaps, better understand their adversaries, and be prepared to adhere to breach tracking and disclosure requirements. Organizations are now shifting their security strategies from a reactive security model to an Active Defense approach, which is not solely based on reacting to attacks but instead applies the early detection and rapid response to threats.

Deception technology provides the innovation required to non-disruptively evolve to an Active Defense security posture. By deploying a fabric of deception-based detection throughout the network stack, companies are able to achieve efficient detection for every threat vector and the lifecycle of an attack. Utilizing high-interaction decoys and lures, deception deceives attackers into revealing themselves, thereby alerting on and identifying detection gaps on threats that have evaded other security controls.



With early-in -network visibility into threats and actionable alerts for incident handling, deception solutions are rapidly becoming the solution of choice for proactively uncovering and responding to external, internal, and supplier threat actors. Organizations of all security maturity levels are aggressively adopting deception technologies in order to mitigate risks related to employee credential theft, data exfiltration, ransomware, crypto-mining, and attacks with the intent to disrupt services or impact public safety. The accuracy and ease of use of threat deception has been a major driver in its adoption and wide-spread deployment.

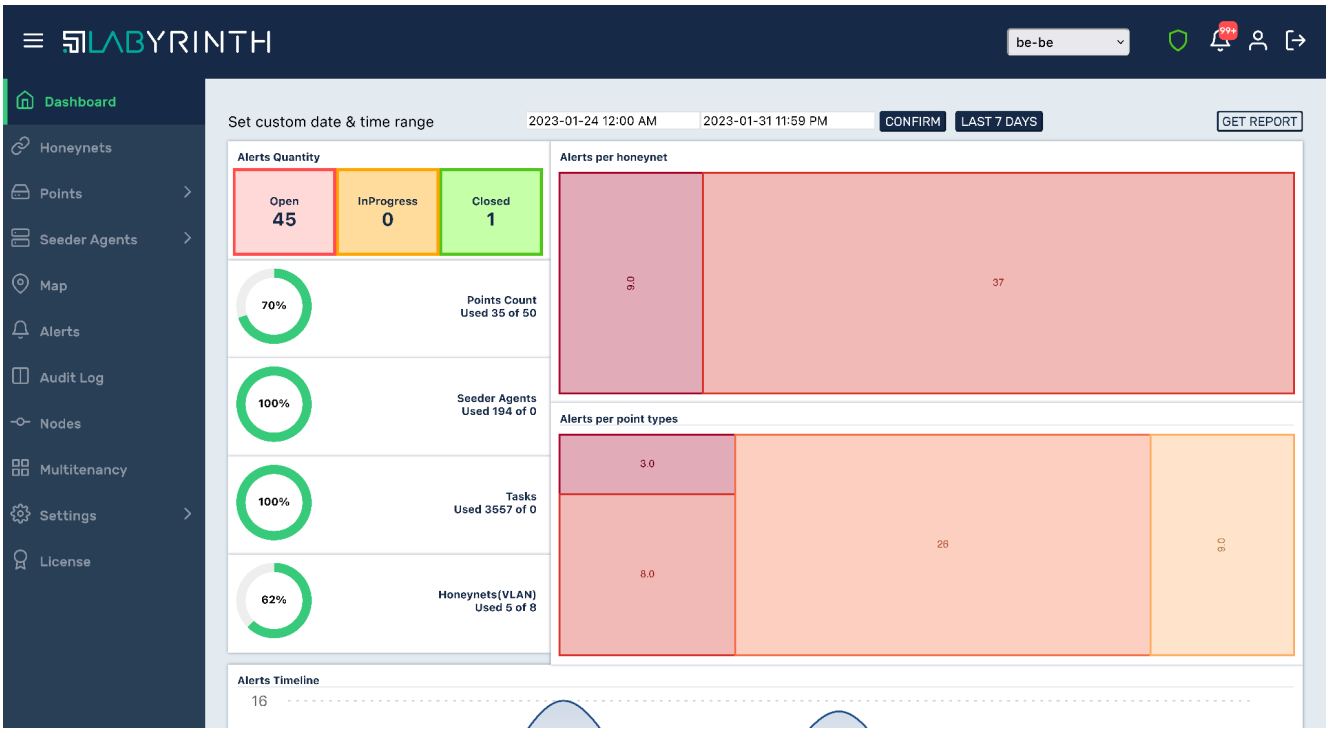


2. THE LABYRINTH SOLUTION

Labyrinth provides an illusion of real infrastructure vulnerabilities to an attacker. It's based on Points - the smart imitation hosts. Each part of the mimic environment reproduces the services and content of a real network segment.

Labyrinth provokes the attacker for actions and learns suspicious activity at the same time. Our experienced professionals are helping to construct the best Labyrinth for complex environments. Its features give powerful capabilities in order to detect Targeted Attacks, BOTNETS, 0-day Attacks and Malicious Insiders.

Points mimics special software services, content, routers, devices etc. Each Point detects all targeted suspicious activities. While the attacker proceeds through the fake aim infrastructure, Labyrinth captures all the hostile's details. The company receives information about threat sources, the tools that were used, and about exploited vulnerabilities and the attacker's behavior. In the meantime, the whole real infrastructure continues to work without any impact.



3. CUSTOMER BENEFITS AND USE CASES

BENEFITS:

- Accurate and early in-network threat detection for any threat vector
- Comprehensive solution with scalability for evolving attack surfaces
- Easy deployment, operation and scalability
- Ability to win additional time on incident response while attacker is in Labyrinth
- Detailed attack information, including attack tactics and tools.
- Less data for analysis and less digital "noise" production
- Highly reliable alerts with less than 1% false positives

USE CASES:

- Detect lateral movement and internal reconnaissance
- Credential theft detection
- Accurate external adversary, insider and supplier threat visibility
- Improve threat response and verify the reliability of existing security controls
- Detailed attack and root cause analysis with substantiated alerts and forensic reporting
- Accelerated incident response through 3rd party integrations that automate isolation, blocking, and threat hunting
- Detect malware infection and slow its spread

4.HARDWARE REQUIREMENTS

Deployment - Can be deployed on-premise

Benefits	Requirements
Admin VM (ManagementConsole)	32 GB RAM, 4 vCPU, 1 TB HDD
Worker VM	24 GB RAM, 8 vCPU, 500 GB HDD

FOR MORE INFORMATION ABOUT LABYRINTH OR FOR THE PRODUCT DEMONSTRATION, PLEASE CONTACT LABYRINTH.TECH AT INFO@LABYRINTH.TECH