# Labyrinth Deception Platform advantages

Labyrinth Security Solutions, 2024

Labyrinth Deception Platform changes an attack surface providing adversaries with an illusion of real infrastructure vulnerabilities. Each part of the imitated environment reproduces the services and content of a real network segment.

The solution is based on Points - smart imitation hosts that mimic special software services, content, routers, devices, etc. Points detect all malicious activities inside a corporate network providing comprehensive coverage of all the possible attack vectors.

Labyrinth provokes the attacker for actions and detects suspicious activities. While an attacker proceeds through the fake aim infrastructure, the Platform captures all the hostile's details. The security team receives information about threat sources, the tools that were used, and about exploited vulnerabilities and the attacker's behavior.

## Advantages of LDP

- Detects and stops targeted and advanced cyber-attacks without requiring any prior knowledge of the threat's form, type, or behavior
- Reduces cybersecurity operating costs by up to 30%: does not collect tons of data, does not generate false positives, and no special skills are required
- Accelerates incident response by reducing the average time to detect and respond to threats (MTTD, MTTR)
- No negative impact on the performance of network devices, hosts, servers, or applications
- Fast and easy deployment, no system conflicts, and no need for maintenance - no databases, signatures, or rules to constantly configure and update

# Advantages over other cyber threat detection approaches

### Advanced Threat Detection

- Allows you to detect intruders on your corporate network up to 12x faster
- Detects basic and advanced threats regardless of the methods used
- Collects data about the movements of attackers and the tools they use

### Process optimization for SOC

- Significantly simplifies the process of prioritizing incidents
- Reduces time spent on false positive notifications
- Provides full visibility of the attack in real-time

### No deep knowledge required

- Easy installation and setup
- No special skills are required to use the solution
- Automatic incidents detection and response when integrated with third party tools

# Technical advantages over other Deception solutions

- All simulations created by Labyrinth are highly engaging decoys: providing at the level of at least responding to scan interactivity, prompting for credentials, and displaying a graphical and/or text interface. Each hook is unique, with one IP address; no IP alias is used. This approach provides the industry's best believability for the created simulations
- Universal Web Point is a unique type of trap. By providing an IP address of your real asset, highly interactive decoy with an addition of vulnerabilities and the possibility of exploiting them (scan responses, requesting credentials, displaying a graphical

interface) can be created. Each decoy is powered by Web Application Firewall to ensure more precise detection

## Advanced system features

- Multitenancy - allows to isolate and serve users from different organizations in one installation (MSSP approach)
- All decoys in Labyrinth Deception Platform are highly customizable. By updating YAML configuration files, Points can be adjusted to the existing needs
- Active decoys for:
  - OT/SACADA and IoT emulation
  - MiTM (man-in-the-middle) attack detection
- Wide range of integrations that includes:
  - Integrations that provide network isolation
  - Two-way integration with SIEM solutions that allows not only send data to SIEMs, but also receive necessary information from them

## Commercial advantages over other Deception solutions

- Industry-leading Time to Value: the entire system deployment process from start-up to production takes only a few hours
- For the full functioning of the system, no additional purchase of third-party software licenses (for example, Windows) is required
- Does not require a lot of hardware resources to deploy the system
- Supports VMware, Hyper-V and Azure
- Flexible licensing based on infrastructure size and customer needs
- Not licensed by the number of Breadcrumbs, Endpoints, etc. – in practice only the number of network segments is licensed. Each segment can deploy up to 15 Points (decoys).

- Prices for the solution are much more affordable than those that are proposed by competitors.