

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.

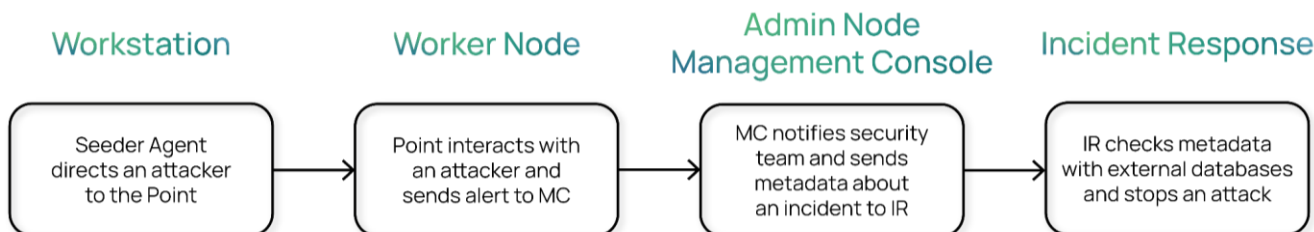


Labyrinth provokes the attacker for actions and detects suspicious activities. While an attacker proceeds through the fake aim infrastructure, the Platform captures all the hostile's details. The security team receives information about threat sources, the tools that were used, and about exploited vulnerabilities and the attacker's behavior. In the meantime, the whole real infrastructure continues to work without any impact.

Labyrinth simulates a broad range of real services (mail, web applications, etc.). Additionally, the system mimics the user's network connectivity and all kinds of decoys (files, links, ssh keys, etc.), to increase the probability of an attacker getting into simulated services.

To protect SCADA/OT infrastructure, new Point types have been developed that can emulate Web PLC interfaces and Siemens S7COMM, SNMP, Modbus protocols. For IoT protection a MQTT server imitation has also been added.

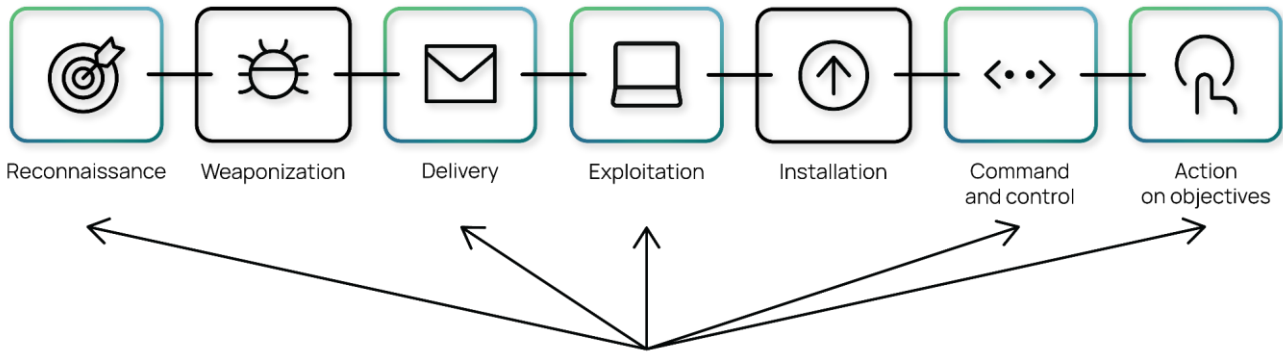
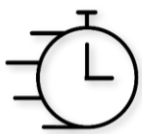
LABYRINTH ALERTS WORKFLOW



THIRD PARTY INTEGRATIONS

Detection			
Remediation			
Response			

USE CASES

Early Threat Detection
Proactive Defense
Targeted Attacks Uncovering
Dwell Time Reduction



Man-In-the Middle Revealing
Lateral Movement Recognition
Rapid Incident Response
Cyber Incident forensics

ADVANCED FEATURES

Deep integration with SIEMs



Two-way integration with SIEM solutions that allows not only send data to SIEMs, but also receive necessary information from them.

Advanced WEB application protection



Labyrinth embedded a unique technology which allows providing additional layer of security for the most desired by hackers target - WEB based applications and services.

Multitenancy



Integrated multitenancy and RBAC model allows to isolate and serve customers from different organizations in one installation (MSSP design).

SYSTEM REQUIREMENTS

VMware vSphere 6.0/6.5/7.0, Microsoft Hyper-V 2008 R2 or above, Microsoft Azure Cloud.
Installation of an AdminVM on KVM-based platforms (Proxmox, OpenStack, etc.) is officially supported.

AdminVM (Management Console)	4 vCPU (cores), 32 GB RAM, 800 GB HDD
Worker Node	8 vCPU (cores), 24 GB RAM, 500 GB HDD

Details of the installation process are described in the Deployment and Configuration Guide.