



CYBERSECURITY  
MADE IN EUROPE



CISO CHOICE AWARD 2025  
FINALIST

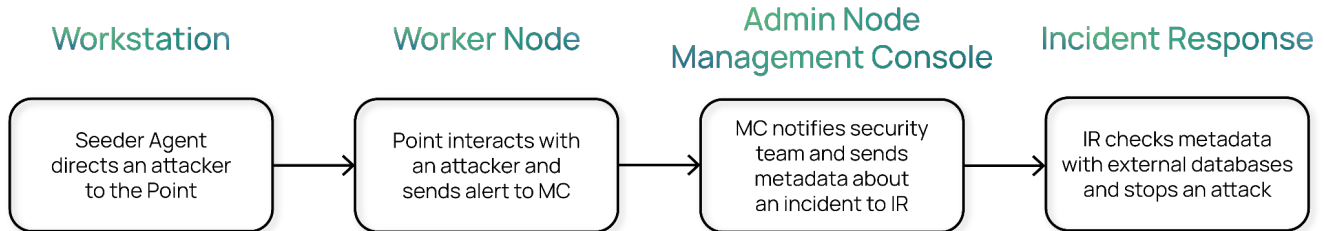
**Labyrinth Deception Platform** changes an attack surface providing adversaries with an illusion of real infrastructure vulnerabilities. Each part of the imitated environment reproduces the services and content of a real network segment. The solution is based on Points - smart imitation hosts that mimic 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.



LDP 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 OT/SCADA infrastructure, 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

secureVISIO

IBM Radar

ENERGY LOGSERVER

splunk

FORTINET

CROWDSTRIKE

wazuh.

Trellix

PROXMOX

Microsoft Hyper-V

vmware

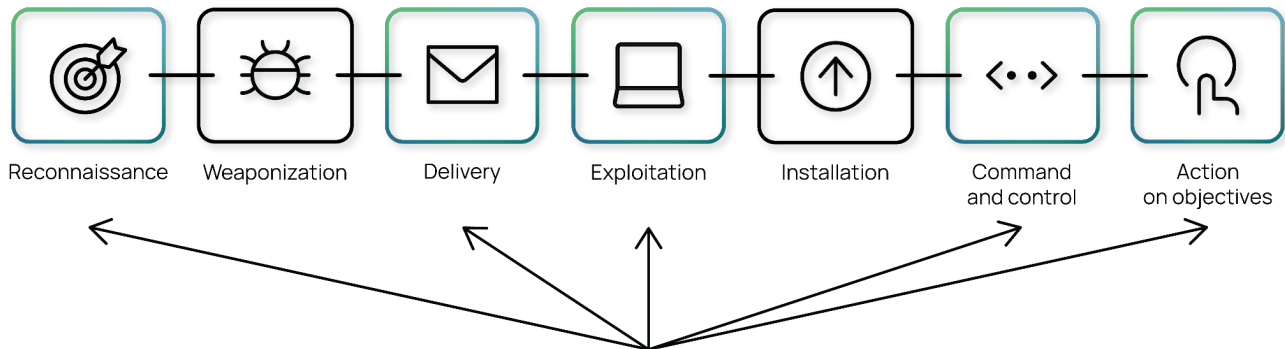
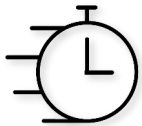
Microsoft Azure

Google

Microsoft

yubico

## 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

Installation in VMware vSphere 6.5 or above, Microsoft Hyper-V 2016 or above, Microsoft Azure Cloud and Proxmox 8.2 is officially supported.

<b>AdminVM (Management Console)</b>	4 vCPU (cores), 16 GB RAM, 500 GB HDD
<b>Worker Node</b>	8 vCPU (cores), 16 GB RAM, 200 GB HDD

Details of the installation process are described in the Labyrinth Knowledge Base.