# LABYRINTH

## HIGHLY SCALABLE CYBERDECEPTION PLATFORM

# MAKE HACKERS CRY

## KEY BENEFITS

- EARLY THREAT DETECTION
- SLOWDOWN CYBER ATTACKS
- EASY TO DEPLOY AND MAINTAIN
- FLEXIBLE LICENSING OPTIONS

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

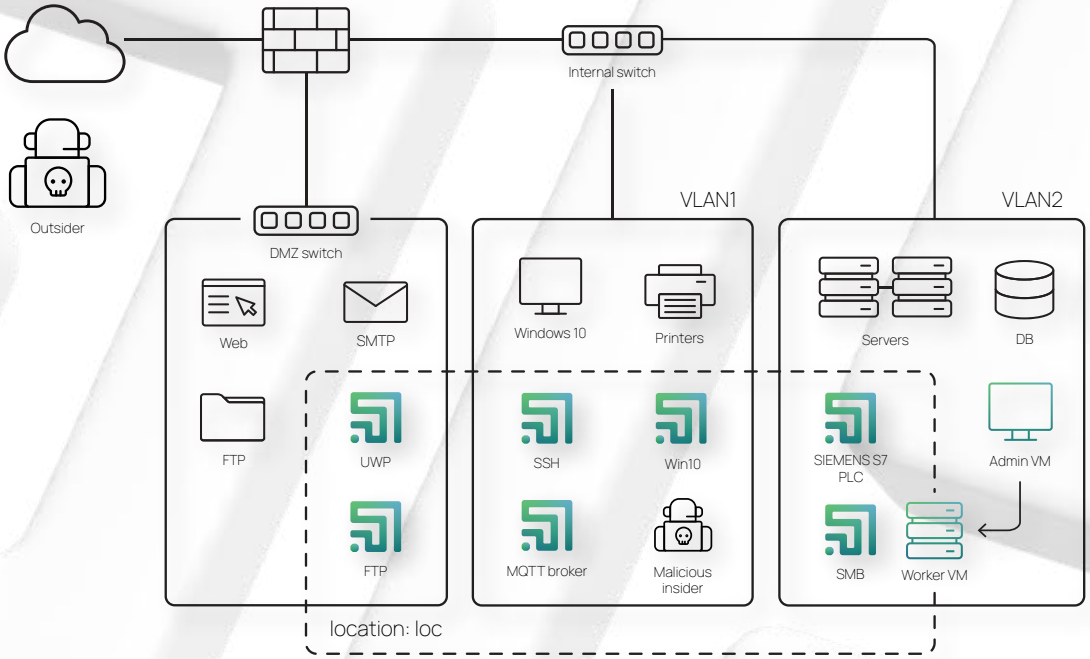
CISO CHOICE AWARD
2025
FINALIST

## KEY FEATURES

- ON-PREMISE DEPLOYMENT
- CENTRALLY MANAGED IT/OT DECOYS
- 3rd PARTY INTEGRATIONS
- MULTIPLATFORM SUPPORT
- MULTI-TENANCY ARCHITECTURE FOR LARGE DEPLOYMENTS OR MSSPS

www.labyrinth.tech
info@labyrinth.tech

**Labyrinth Deception Platform** emulates an attack surface, providing adversaries with an illusion of real vulnerable infrastructure. Based on Points - intelligent imitations that mimic services, content, routers, devices and more, the solution provides you comprehensive cover of all possible attack vectors. Labyrinth lures attackers into engaging with this fake infrastructure, capturing every detail of their actions. Your security team gains vital insights into threat sources, used tools, exploited vulnerabilities, and attacker behavior.




In the meantime, the 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, and Modbus protocols. For IoT protection, an MQTT server decoy has also been added.

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

Early Threat Detection
Proactive Defense
Targeted Attacks Uncovering
Dwell Time Reduction

secureVISIO
IBM QRadar
ENERGY LOGSERVER
splunk>
FORTINET
CROWDSTRIKE
wazuh.
NACVIEW
openstack.
Microsoft Hyper-v
vmware
Microsoft Azure
Google
Microsoft
yubico

www.labyrinth.tech
info@labyrinth.tech