CYBERSECURITY™ MADE IN EUROPE

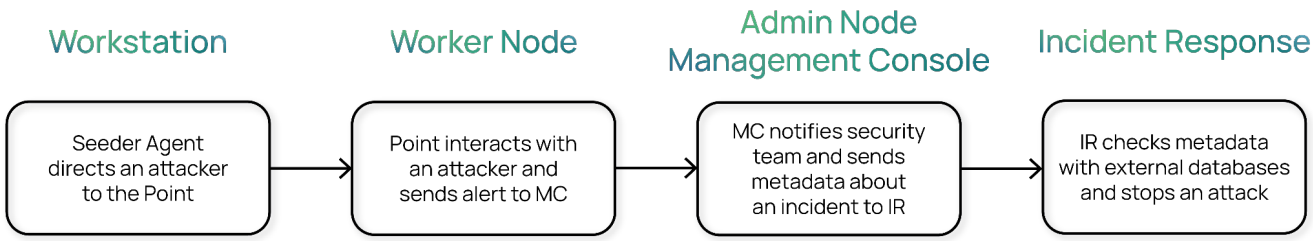
ECSO EUROPEAN CYBER SECURITY ORGANISATION CISO CHOICE AWARD 2025 FINALIST

Die Labyrinth Deception Platform verändert eine Angriffsfläche, die Angreifern die Illusion echter Infrastrukturschwachstellen vermittelt. Jeder Teil der nachgeahmten Umgebung reproduziert die Dienste und Inhalte eines echten Netzwerksegments. Die Lösung basiert auf Points - intelligenten Imitationshosts, die spezielle Softwaredienste, Inhalte, Router, Geräte usw. nachahmen. Points erkennen alle bösartigen Aktivitäten innerhalb eines Unternehmensnetzes und decken alle möglichen Angriffsvektoren ab.

Labyrinth simuliert eine breite Palette echter Dienste (E-Mail, Webanwendungen usw.). Darüber hinaus imitiert das System die Netzwerkkonnektivität des Benutzers und alle Arten von Täuschungsmanövern (Dateien, Links, SSH-Schlüssel usw.), um die Wahrscheinlichkeit zu erhöhen, dass ein Angreifer in simulierte Dienste eindringt.

Zum Schutz der SCADA/OT-Infrastruktur wurden neue Point typen entwickelt, die Web-SPS-Schnittstellen und Siemens S7COMM-, SNMP- und Modbus-Protokolle emulieren können. Für den IoT-Schutz wurde auch eine MQTT-Server-Imitation hinzugefügt.

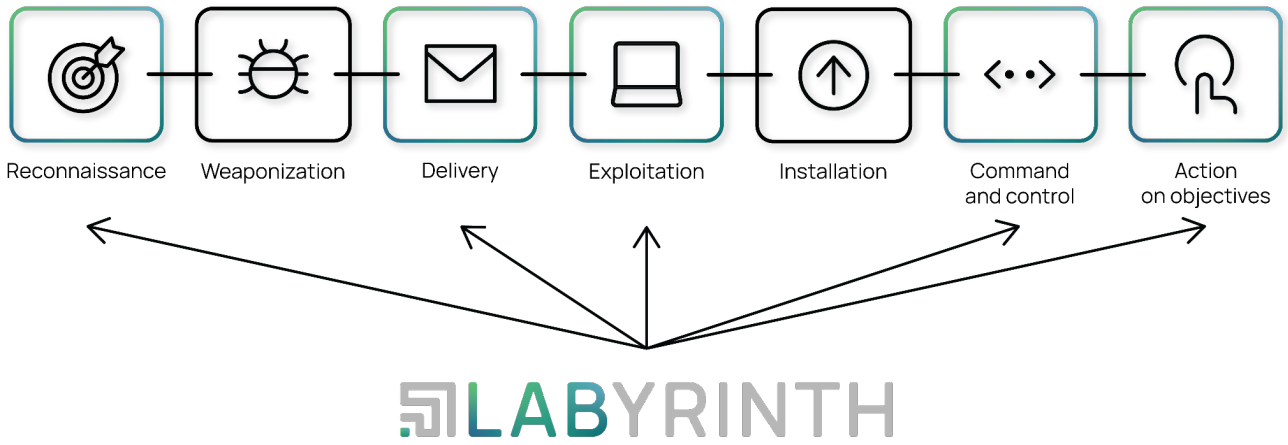
LABYRINTH ALERTS WORKFLOW



THIRD-PARTY INTEGRATIONS

secureVISIO · IBM QRadar · ENERGY LOGSERVER · splunk> · FORTINET · CROWDSTRIKE · wazuh. · NACVIEW · openstack. · 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 leer 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 6.0/6.5/7.0/8.0, Microsoft Hyper-V 2008 R2 oder höher, Microsoft Azure Cloud.
Die Installation einer AdminVM auf KVM-basierten Plattformen (Proxmox, OpenStack, etc.) wird offiziell unterstützt.

AdminVM (Verwaltungskonsole)	4 vCPU (Kerne), 32 GB RAM, 800 GB HDD
Arbeiter-Knoten	8 vCPU (Kerne), 24 GB RAM, 500 GB HDD

Einzelheiten zum Installationsprozess sind in der Anleitung zur Bereitstellung und Konfiguration beschrieben.