



**Ljubljana, 16.05.2024**

## Meeting agenda:

- Say hello
- Cyber security, my perspective
- Tools
- Deception
- Who we are?
- TECHNICAL DEMO (pass the mic to Marko!)
- What value the LABYRINTH can bring to You?
- Say something with AI and say it in Slovenian!
- Q&A

**Dobro jutro! 😊**

**CYBER SECURITY**

**firewall**

**antivirus**

**Intrusion prevention system**

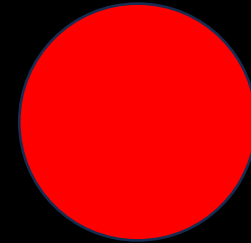
**Identity and access management**

**security information and event management**

**XXX**

**backup**

**vulnerability management**



**What is the goal of attacker?**

**THE POWER OF ANNALOGY  
PART ONE - VISUALISATION**



**STORMSHIELD**

**NETASQ**  
*we secure IT*





border 6

NON STOP INTERNET



waliliX



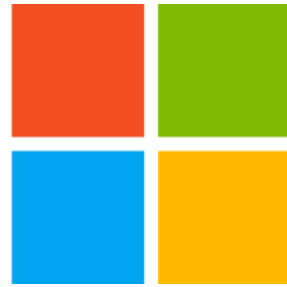
**THE POWER OF ANNALOGY**  
**PART TWO - STRATEGY**

# CYBER SECURITY TOOLS

*Coca-Cola*



**FORTINET**<sup>®</sup>



Microsoft



**BANK OF AMERICA**

**PASIVE | ACTIVE**  
**Attack Surface**  
**Detection & Response**

**PREVENT**

**DETECT**

**RECOVER**

**THE POWER OF ANNALOGY  
PART THREE - DECEPTION**



VOLVO  
ALARM

VOLVO





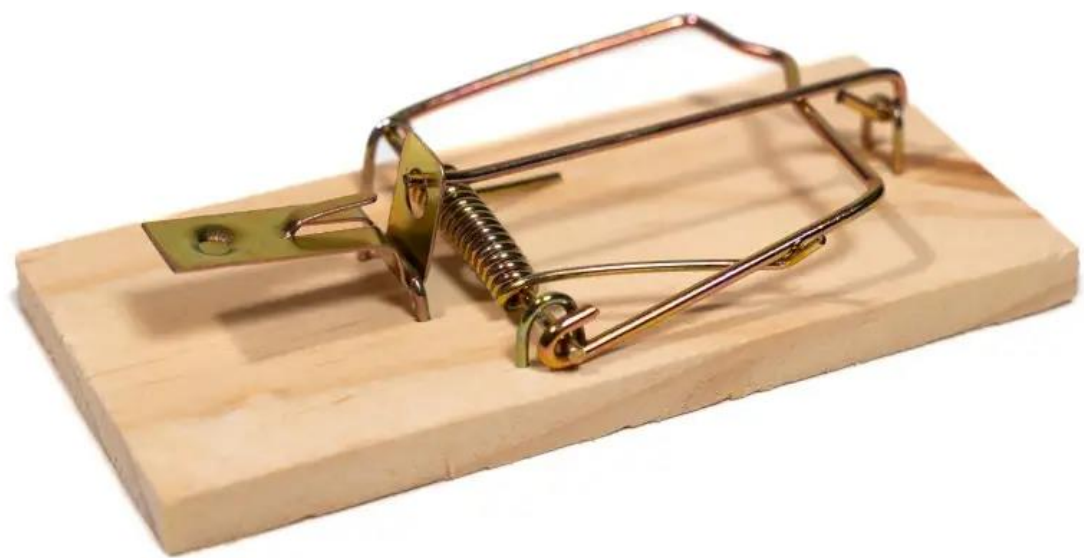
PEC134A/B0001  
VEHICLE IDENTIFICATION  
4402306

WARRANTY  
INFORMATION



# THE INTRUDER





# 1862 Cannon Mousetrap





7000V



**OWN EXPERIENCE**



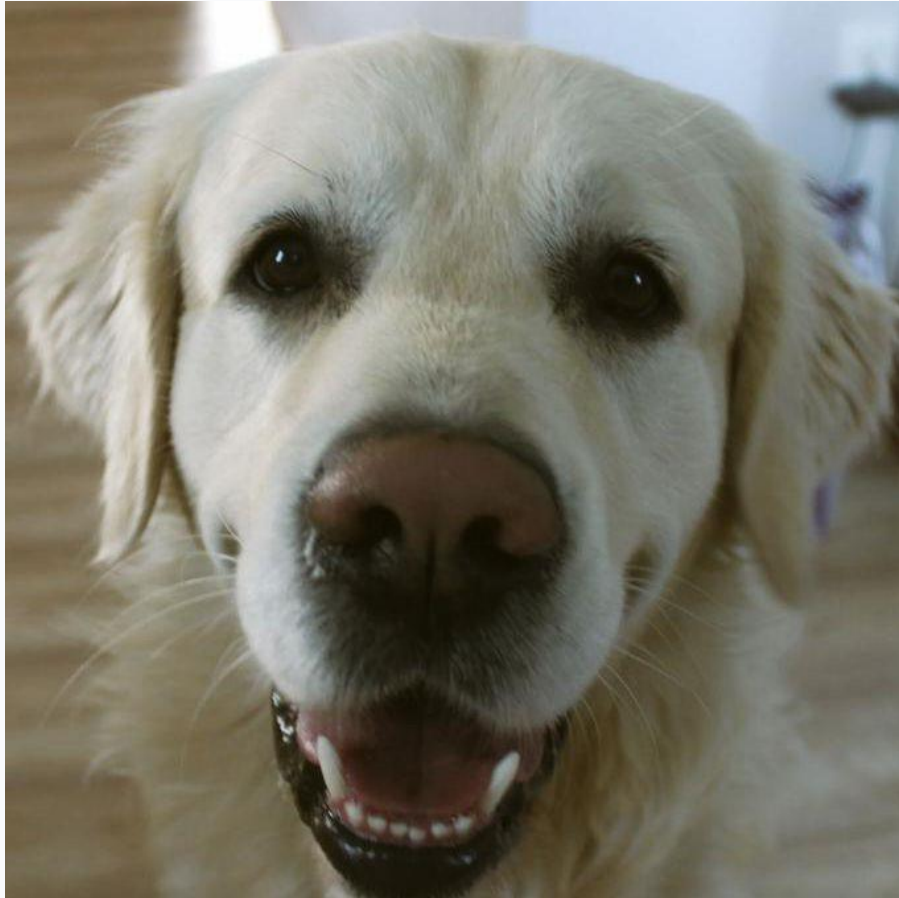
Q 41199  
A  
ST 4378

4378

VOLVO

Warnung  
4 Warning! 4

MADE IN SWEDEN



**THE NG-DOG**



**THE ATTACKER**



VACO  
PROFESSIONAL

ZIARNO  
NA GRYZONIE



TRUTKA

na myszy  
i szczury

SKUTECZNOŚĆ W 1 DAWCE

3  
kg

**THE POWER OF ANNALOGY**  
**PART FOUR – DETECTION METHODS**

**SIEM – Security Information and Event Management**

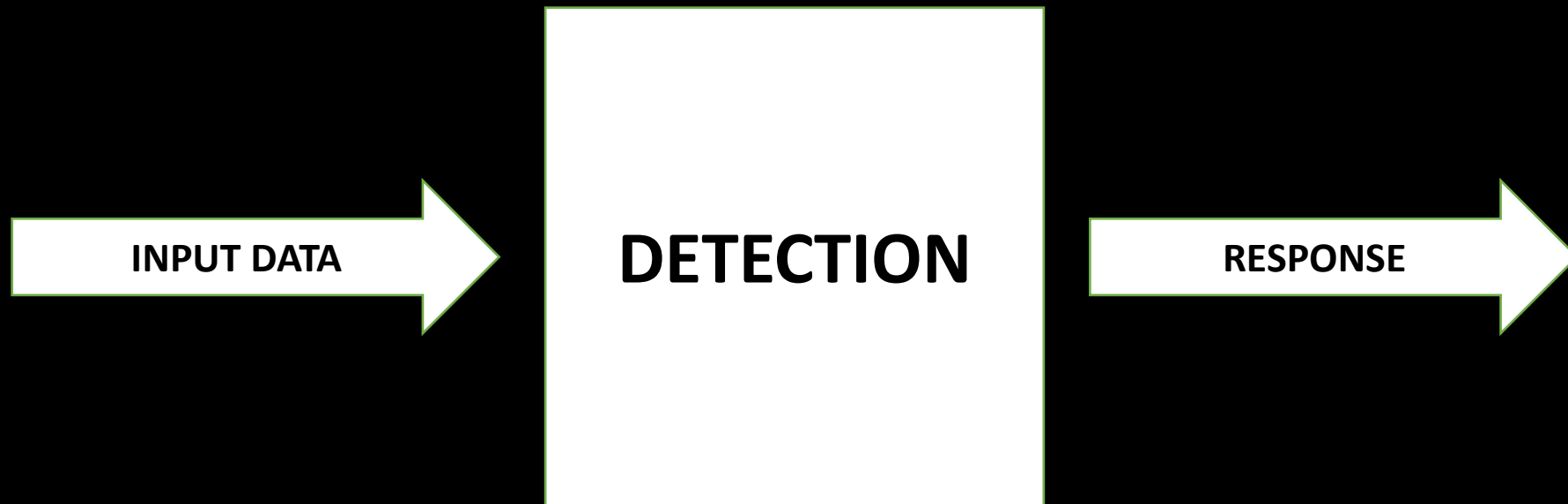
**EDR – Endpoint Detection and Response**

**NDR – Network Detection and Response**

**MDR – Managed Detection and Response**

**XDR – Extended Detection and Response**

**So great!**





# CYBER DECEPTION PLATFORM

Choose innovation. Choose proactive defence.  
Choose Deception Technology



# Who we are?



**Yuri GATUPOV**



**Pawel RYBCZYK**

# Who we are?

- Founded in 2019
- HQ in Zabrze, Poland
- 30 customers – from SMB to LARGE enterprise (global accounts)
- 15 team members, based in Poland, Ukraine, Germany,
- Official website: [www.labyrinth.tech](http://www.labyrinth.tech)
- LinkedIn profile: [link](#)
- YouTube channel: [link](#)



All Categories > Network Detection and Response > Labyrinth > Labyrinth Deception Platform



# Labyrinth Deception Platform

by Labyrinth in Network Detection and Response

4.9 ★★★★★ 4 Ratings

Overview Reviews Alternatives [Show More](#)

Home > System Security Software > Deception Technology Software

## Best Deception Technology Software

Deception technology software is designed to help detect, analyze, and protect against unknown threats by tricking threat actors into thinking they have discovered zero-day or other vulnerabilities. These tools use decoys, traps, lures, honeypots, and other deceptively attractive data sources the attacker may consider valuable. This bait is visible to the attacker and alerts security teams when they have taken the bait. Security teams can then cut off access and investigate the attacker's behavior. Companies use these tools to allow hackers into their systems to monitor their behavior with the goal to better understand their navigation paths, operational mechanisms, and targets. In effect, this software helps provide the company with

4 Verified Reviews

### Compare Deception Technology Software

G2 takes pride in showing unbiased reviews on user satisfaction in our ratings and reports. We do not allow paid placements in any of our ratings, rankings, or reports. Learn about our [scoring methodologies](#).

#### Filter User Reviews By:

#### Displayed Reviews

Reviewed in Last 12 Months

#### Overall Rating

- ★★★★★ (3)
- ★★★★☆ (1)
- ★★★☆☆ (0)
- ★★☆☆☆ (0)

5.0 ★★★★★ Au

#### Implementing 1 of intranet eve

Reviewer Function: IT Risk Management

We have a very posi

[Read Full Review](#)

Segment Rating Language

No filters applied

23 Listings in Deception Technology Available

Sort By: Satisfaction



#### Labyrinth Cyber Deception Platform

★★★★★ (11) 4.9 out of 5  
[Save to My Lists](#)

#### Product Description

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... [Show More](#)

[How are these determined?](#)

**Users**  
No information available

**Industries**  
No information available

**Market Segment**  
• 45% Small-Business  
• 36% Mid-Market

**iiTD** INTELLIGENT  
IT DISTRIBUTION

**COMGUARD**

**A1**



**CYBERSHURE**

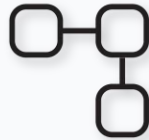
ENSURING CYBER RESILIENCE

**OUR VISION** is to shift the balance of power in favour of defenders.

**OUR MISSION** is to provide all kinds of organizations with a simple and efficient tool for the earliest possible detection of attackers inside the corporate network

# Cybersecurity challenge

Reactive approach to threat detection



False positive alarms



Difficult in usage



Information overload



More time to detect and react



Breaches

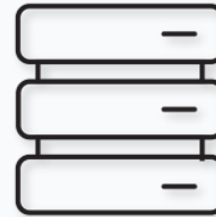


# Business values



## Stops sophisticated threats

Detects targeted and advanced attacks without requiring prior knowledge of the threat's form, type, or behavior.



## Zero impact on performance

No negative impact on the performance of network devices, hosts, servers, or applications behavior.



## Simple implementation

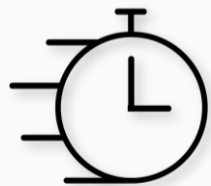
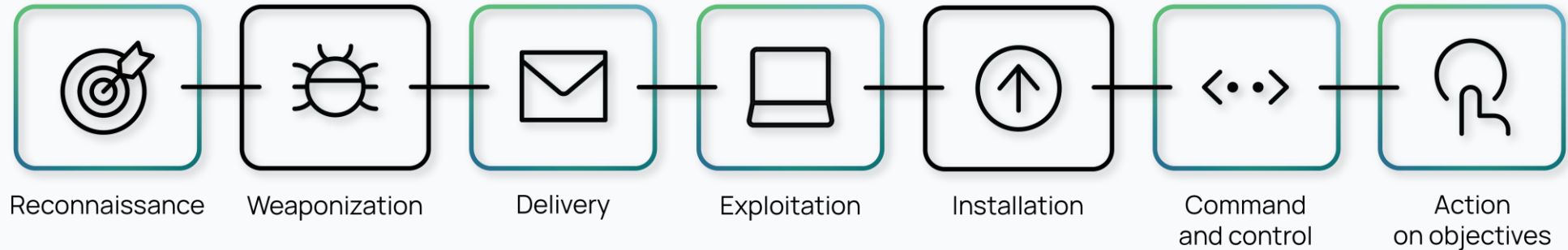
Quick and easy deployment with no system conflicts and minimal maintenance: no databases, signatures, or rules to configure and update.



## Operation costs reduction of by 30%\*

Doesn't collect tons of data, doesn't generate false positive alerts, doesn't require special skills to operate.

# Use cases



- Early detection of network threats
- Easy to deploy and maintain
- Targeted attack detection
- Reduced Dwell Time



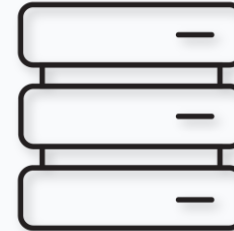
- Man-in-the-Middle detection
- Lateral Movement identification
- Rapid response to incidents
- Incident investigation

# Labyrinth's components



## Admin VM (Management Console)

All information collected at the Points is forwarded to the Management Console for incident analysis and response.



## Worker VM

The Worker VM is the host that hosts all the Points in Labyrinth. It can operate in multiple VLANs simultaneously.



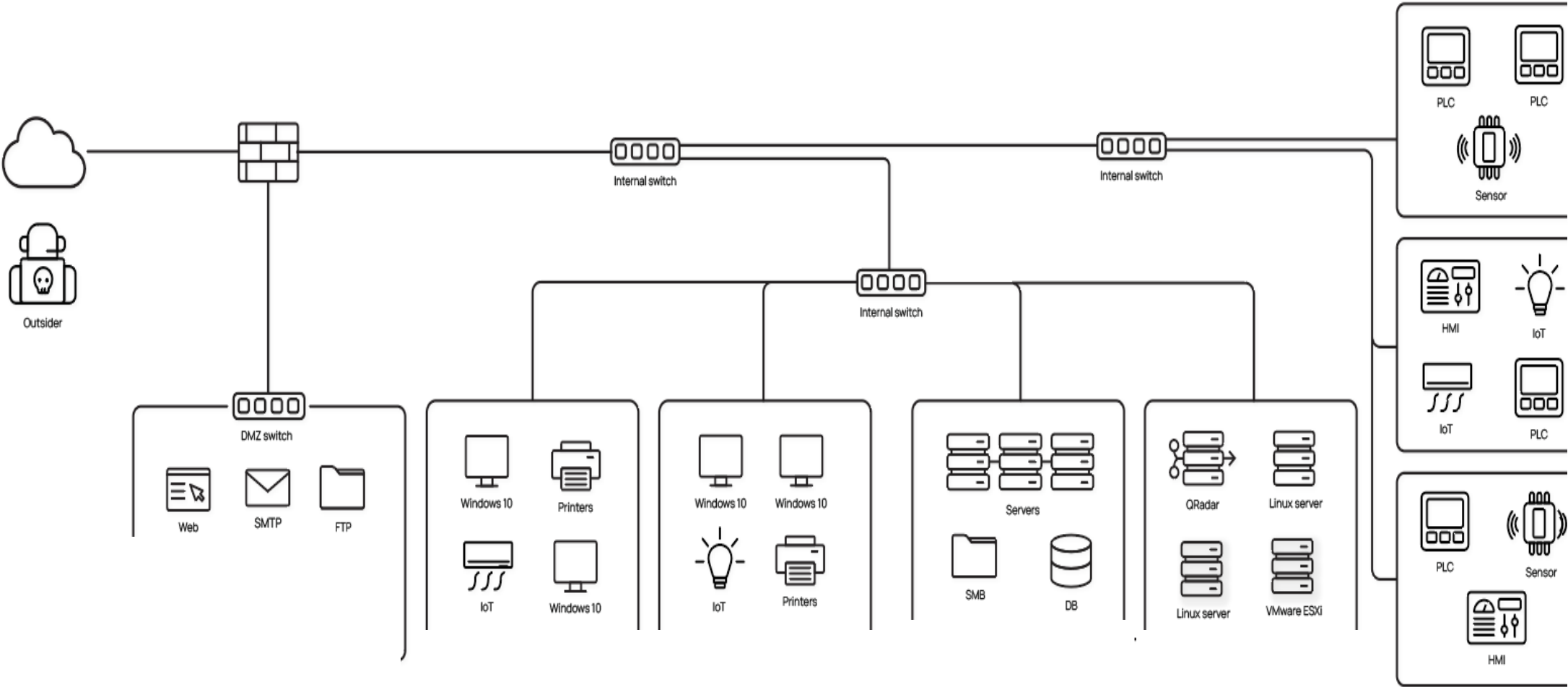
## Point

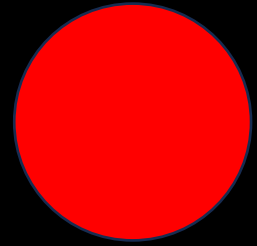
Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.

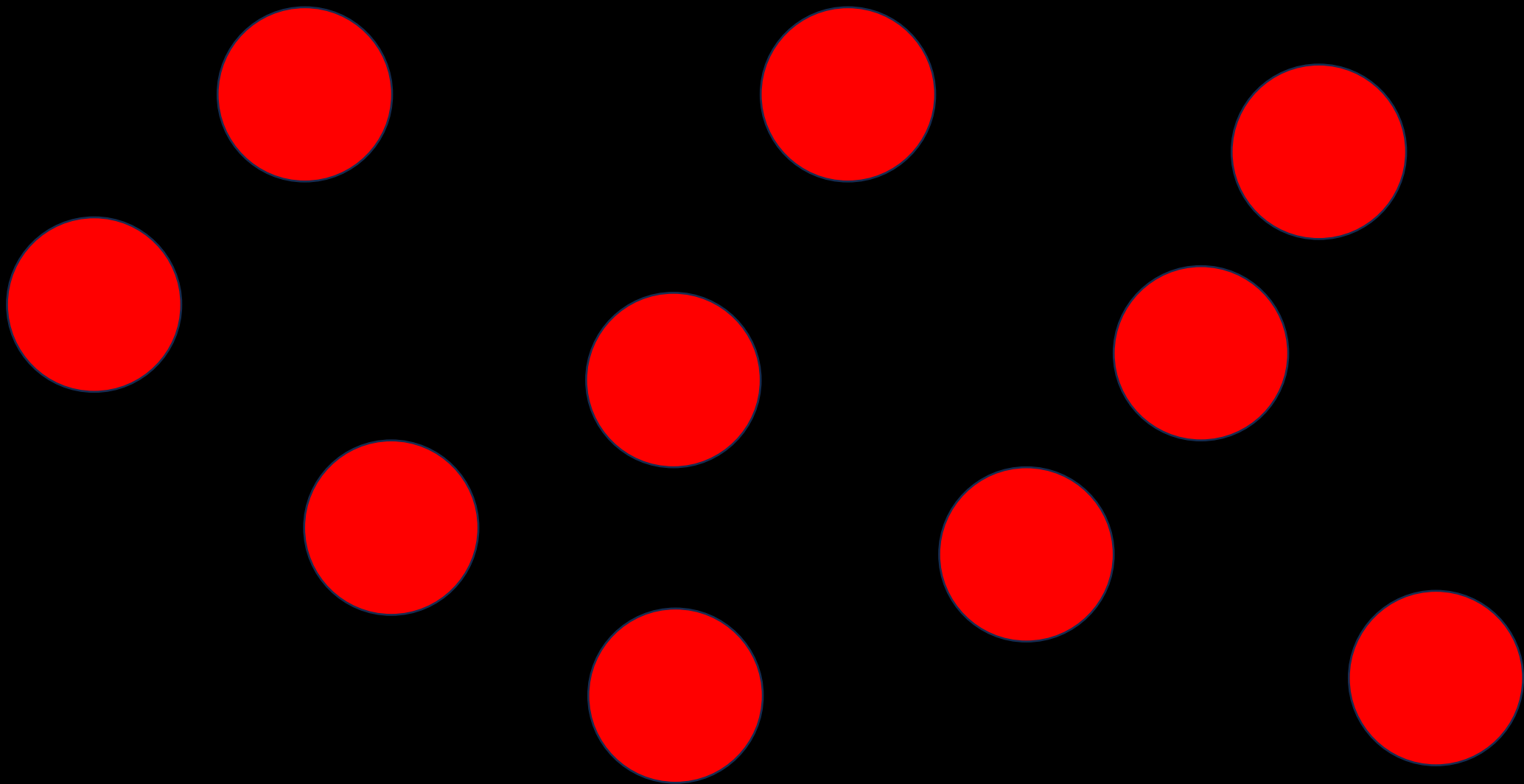


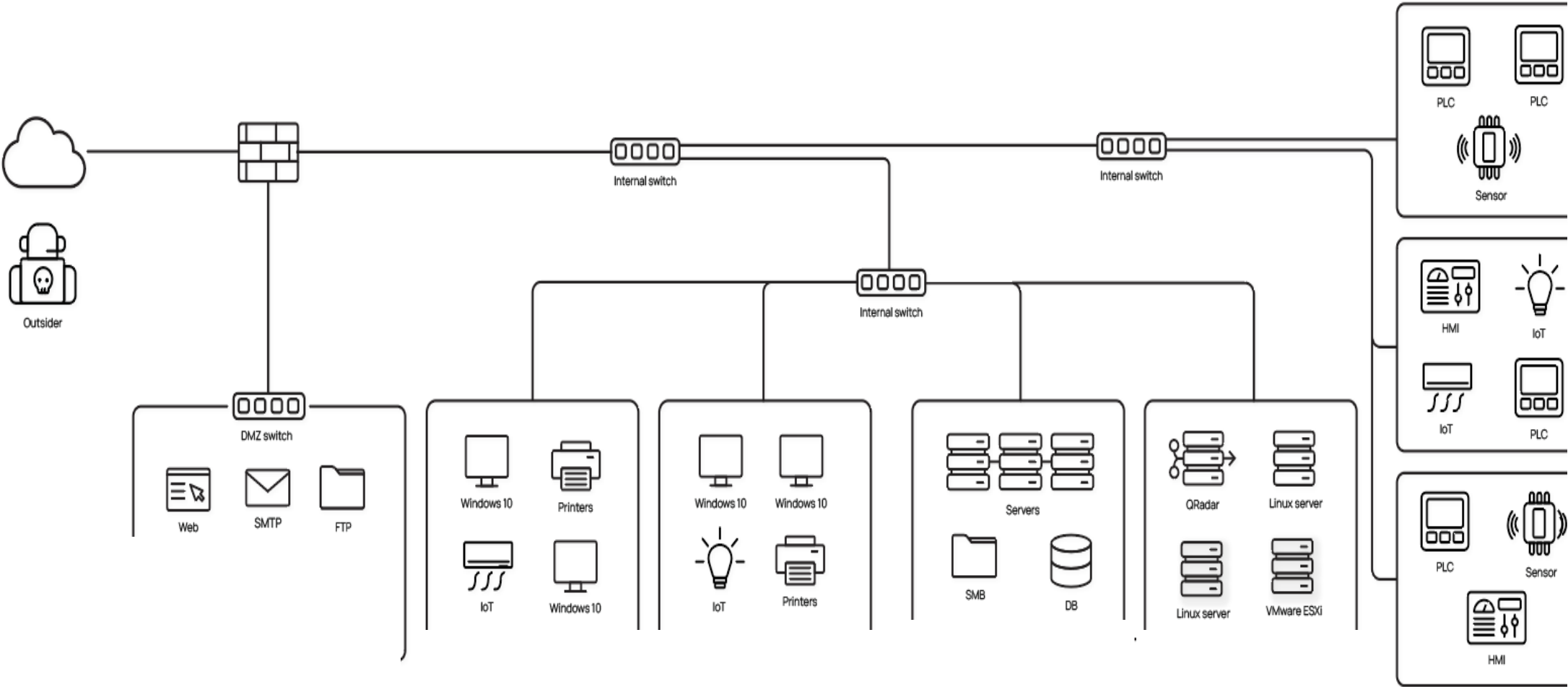
## Host with Seeder Agent

Agents are deployed on real hosts and distribute attractive artifacts to them. The artifacts used by attackers direct them to Points.









# TECHNICAL DEMO

# LABYRINTH

Labyrinth is a team of experienced cybersecurity engineers and penetration testers, which specializes in the development of solutions for early cyber threat detection and prevention.

Follow us on:



Labyrinth Development



Labyrinth Deception Platform



<https://labyrinth.tech>



[info@labyrinth.tech](mailto:info@labyrinth.tech)



# Allianz Risk Barometer 2024

- Cyber incidents such as ransomware attacks, data breaches, and IT disruptions, **rank as the top** global risk in the Allianz Risk Barometer
- The power of AI (to accelerate cyber-attacks)
- Security skills shortage a factor in incidents
- Early detection is **key**

Reference: <https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2024-cyber-incidents.html>

# The value

- I already have END-POINT security and EDGE SECURITY (FW/NGFW/UTM) – but I need something EXTRA but without EXTRA work on daily basis.
- NETWORK MONITORING as the “door opener” – DECEPTION as a EFFICIENT approach to do it.
- Easy to deploy and maintain
- Detection of attacks
- Slowing down the attack
- Enterprise: getting knowledge about attacker behavior

## Try it

- Proof of Concept / Proof of Value – free of charge
- Quick installation with local support
- TIP: evaluation during red-teaming?
- Give it a chance: start with 10 traps!

# Licensing

- Subscription (1y, 2y, 3y, 4y, 5y)
- License metric:
  - per “**NETWORK SEGMENT**” (VLAN) with max 15 points (decoys, traps), unlimited seeder agent.
  - Per “**PACKAGE of 10 points**”, unlimited seeder agent

# LABYRINTH

Labyrinth is a team of experienced cybersecurity engineers and penetration testers, which specializes in the development of solutions for early cyber threat detection and prevention.

Follow us on:



Labyrinth Development



Labyrinth Deception Platform



<https://labyrinth.tech>



[info@labyrinth.tech](mailto:info@labyrinth.tech)

