LABYRINTH

LABYRINTH DECEPTION IN A MSSP MODEL

Labyrinth Deception Platform, 2023

https://labyrinth.tech

info@labyrinth.tech

Labyrinth Development

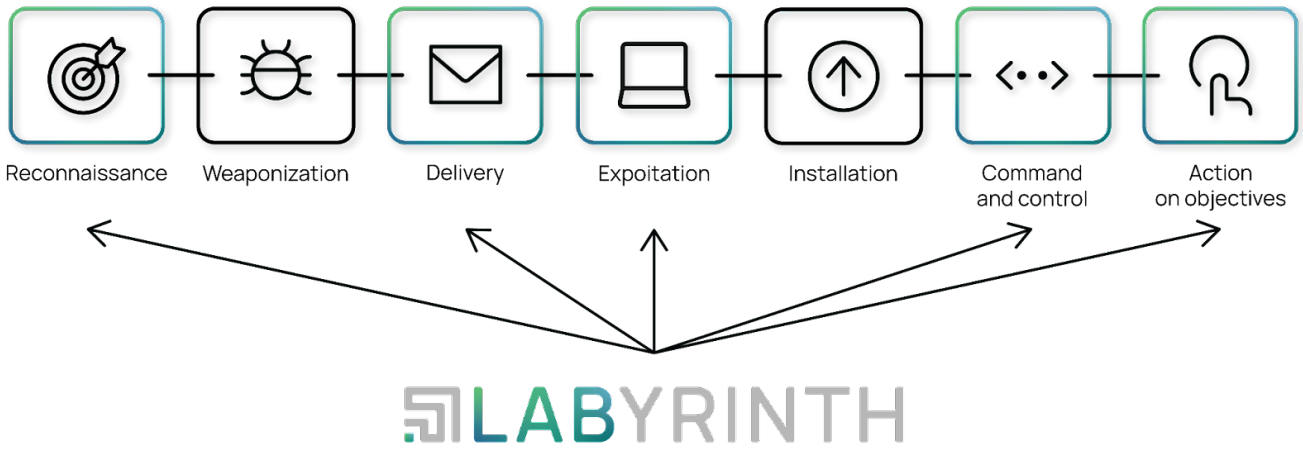
1. GENERAL SYSTEM DESCRIPTION

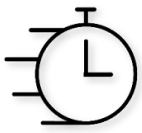
Labyrinth Deception Platform is a cyber threat detection platform that intentionally protects the network from targeted attacks, unknown threats, botnets, 0-day and malicious insiders by detecting and blocking cyber attacks within the corporate network.

The solution does not require additional software installation and has an intuitive interface. The platform provides a simple and effective tool for detecting intruders as soon as possible and complete visibility into the development of attacks with event correlation to make correct and quick decisions.

1.1. System functionality

Labyrinth Deception Platform covers 5 of the seven steps in the Cyber kill chain.





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

1.1.1. Early detection of threats in the network

The system detects any targeted suspicious activity early in an attack. The traps are designed to detect an attacker's actions as he tries to explore the network and find his target. As soon as the attacker starts interacting with the Points, the system collects all the details about him: threat sources, tools used, and weaknesses. At the same time, all real assets and services operate without any negative impact.

1.1.2. Rapid response to an incident

The system provides an analytics tool for incident investigation and threat detection. All collected events are enriched with the necessary security data from the Incident Response Platform. Indicators of Compromise (IoC) created by Labyrinth are automatically synchronized with Threat Prevention Solutions.

This allows you to take action on an attack immediately: investigate, investigate, respond with confidence, and develop better defenses for the future.

1.1.3. Disclosure of targeted attacks

To effectively oppose targeted attacks, it is essential to understand the attackers' methods, means, and goals. The Labyrinth solution gives hackers or insiders a false sense of security and allows you to investigate their skills and motives. Knowing what the attackers know about the company's IT infrastructure, services, and employees help to create the most accurate profile of the attackers and apply the best possible defense against them. The platform also identifies gaps in corporate security systems that attackers can exploit in the future.

1.1.4. Post-Intrusion Detection

The system implemented in the company's networks can serve as a reliable notification system for attacks that have bypassed perimeter security controls. Agents are deployed on servers and workstations and mimic the most attractive artifacts for attackers. What looks like a high-privilege, low-security administrator account is a trap that lures an attacker into the Labyrinth, where you can follow the attacker's actions, gathering valuable insights into the threats that have infiltrated your network.

1.1.5. Reduced dwell time

A long dwell time is an essential condition for a successful attack. Labyrinth's detection mechanism effectively reduces dwell time when an attacker remains undetected inside a corporate network. The system reduces the time and opportunity for attackers to move within the company's networks and stops them before they reach critical assets and services.

1.2. Benefits of use

1.2.1. Reduced operating costs

The system reduces cybersecurity operating costs by up to 30% - it does not collect tons of data, does not generate false positives, and does not require special skills to use.

1.2.2. Automation of incident response

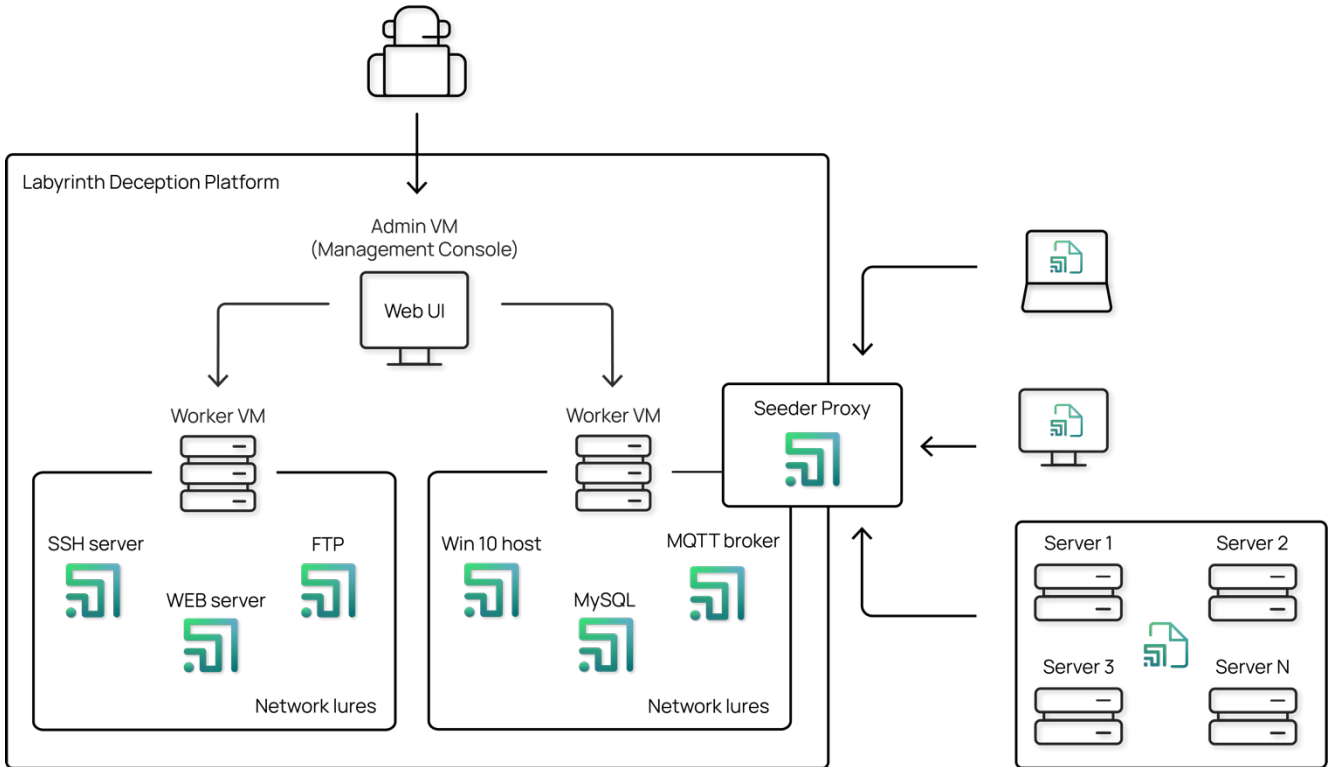
Speeds up incident response by reducing the average time to detect and respond to threats (MTTD, MTTR) by 12 times.

1.2.3. Easy to deploy

Fast and easy deployment, no system conflicts, and no maintenance. No databases, signatures, or rules to constantly configure and update.
Labyrinth detects and stops targeted and advanced cyberattacks without requiring prior knowledge of the threat's shape, type, or behavior and without impacting the performance of network devices, hosts, servers, or applications.

1.3. Logic architecture

The general architecture of the platform is shown in Figure:



System components:

1. **Admin VM (Management Console)** is the main module that performs system management functions, provides a web interface, collects and stores information about security incidents, generates alerts, etc. In other words, it also includes multi-tenancy or environment isolation.

   Admin VM communicates with Workers through encrypted channels.

2. **Worker Node** is a Linux-based virtual machine designed to create, store, and run network decoys (Points). The system can include one or more Worker VMs depending on the scalability requirements or features of the Customer's network infrastructure.

   On the Worker Node, you need to connect a TRUNK with a list of VLANs in which you plan to deploy network decoys so that each virtual machine can simultaneously serve one and several VLANs.

3. **Point** is a network decoy that imitates a specific service/s. System objects of this type can include imitations of various vulnerabilities, which will generate an attack notification (Alert) when an attacker tries to exploit them.

   Points keep the attacker inside the Labyrinth Deception Platform until all the necessary information is collected.

4. **Seeder Agent** is a binary file for Windows and Linux systems that provides logical connections between real and generated infrastructure. When launched on a real host, the Seeder Agent communicates with the Admin VM and receives tasks to create breadcrumbs.

   It can function in two modes:
   a. as a one-time start and stop of its process after all breadcrumbs are created;
   b. run as a permanent process with a connection to the Admin VM.

   Seeder Agents are located on servers and workstations and imitate the most attractive artifacts for hackers. When launched by attackers, the agent directs them to Points.

5. **Seeder Proxy Point** - all interaction between the Seeder-Agent and the Admin VM (Management Console) goes through the Seeder-Proxy service, which is implemented as a separate Point type. In this case, the Seeder-Agent connects to port 443/tcp on the Seeder-Proxy.

   Thus, this type of network bait simultaneously performs two functions:
   a. imitates a vulnerable Web application
   b. mediates between Seeder-Agents on actual hosts in a particular VLAN and the Admin VM.

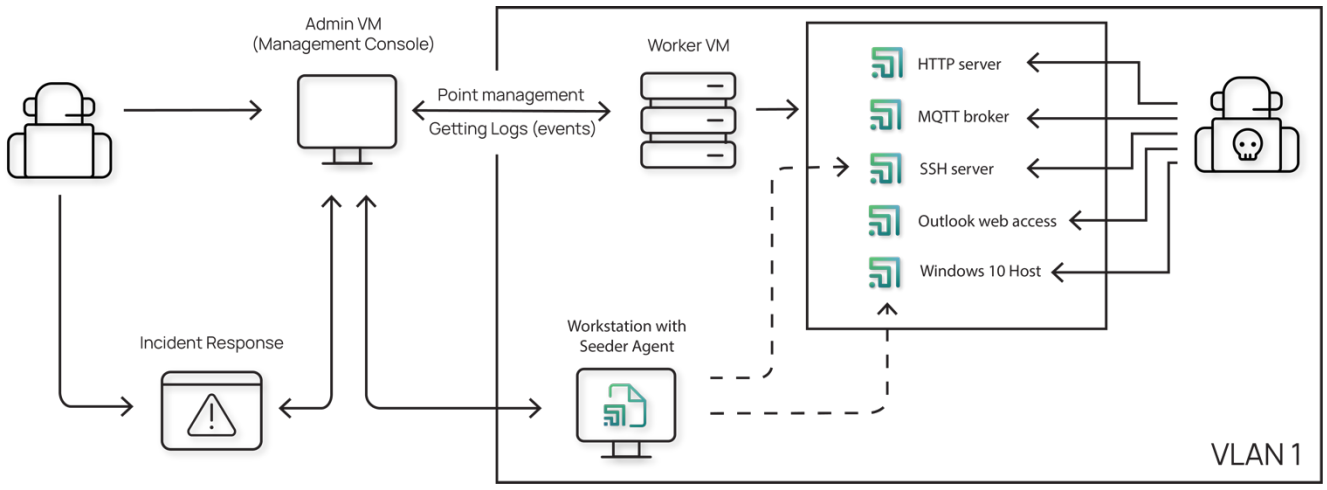
1.3. Description of the multitenancy and authentication subsystem (RBAC)

For MSSPs, it is critical to have tools that will allow them to provide services to customers with low hardware costs and minimal time to deploy the necessary components/modules. This is facilitated by multitenancy functionality and a flexible role model for system users.

Simply put, **multitenancy** is the ability of different users or even companies to use resources in isolation within a single installation.

Today, multitenant architecture is one of the most efficient models for delivering IT services and is one of the ways to save vast amounts of computing resources and disk storage. A single instance of an application running on a single server infrastructure but available to multiple users and businesses simultaneously helps minimize the cost of providing IT services and maximize their quality.

Labyrinth Deception Platform supports multi-tenancy, which allows you to provide isolated environments for different departments or divisions of a company or customers of an MSSP company within the same installation. This means tenants are entirely isolated from each other, i.e., users, alerts, honeynets, etc., are available within a tenant and not in other tenants.

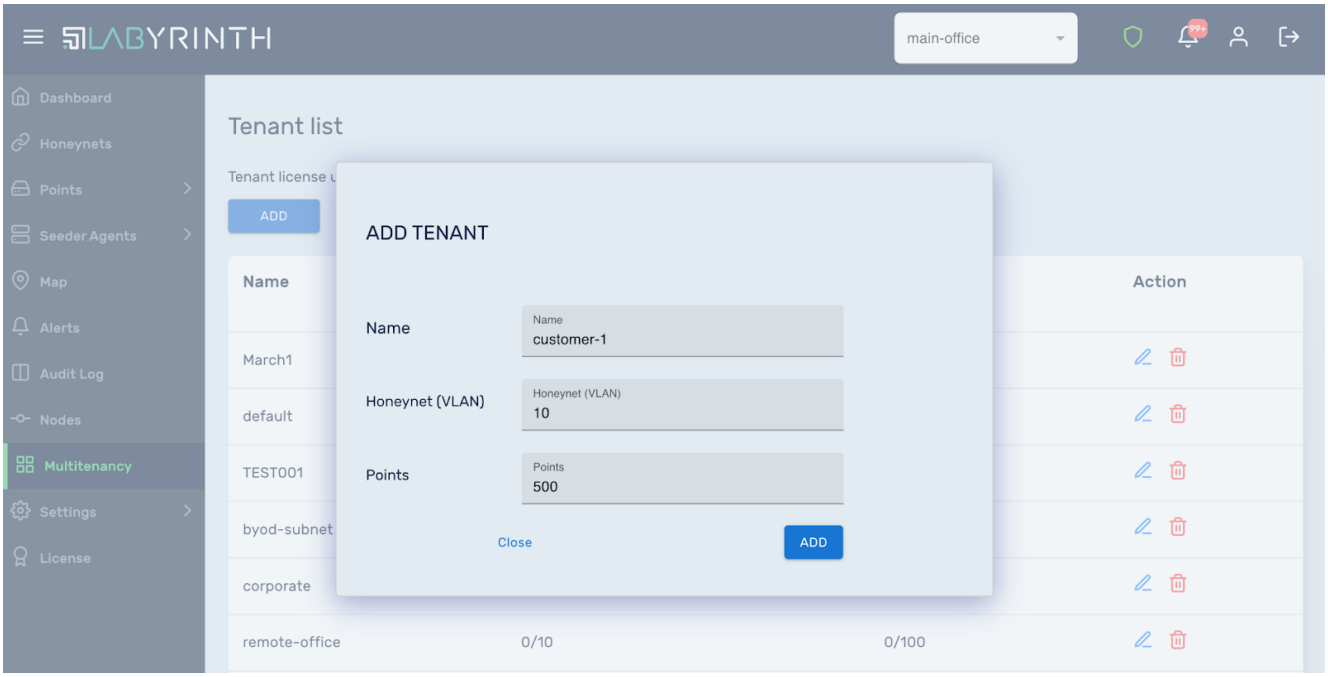


The **Admin VM** is located at the central office of the MSSP company or in the primary data center. Access to its Web interface on the **443/tcp(https)** port is limited to the management segment of the network.

Worker VMs are placed in the networks of the MSSP company's customers who use the Labyrinth deception system to detect attacks. Worker VMs are synchronized with the Admin VM on network port **20202 (tcp/udp)**. The channel between the virtual systems is encrypted.

The ChaCha20 crypto algorithm is used for data transmission.

When creating or editing a Tenant, you must specify the number of Honeynet (VLAN) and Points assigned to this Tenant from the general license:



This ensures the expected distribution of the license among tenants and eliminates the undesirable possibility that one Tenant has the potential to utilize the full license.

Configuration settings and other actions related to tenant management are performed using **credentials with superuser rights**. After creating one or more tenants, the superuser can switch between tenants.

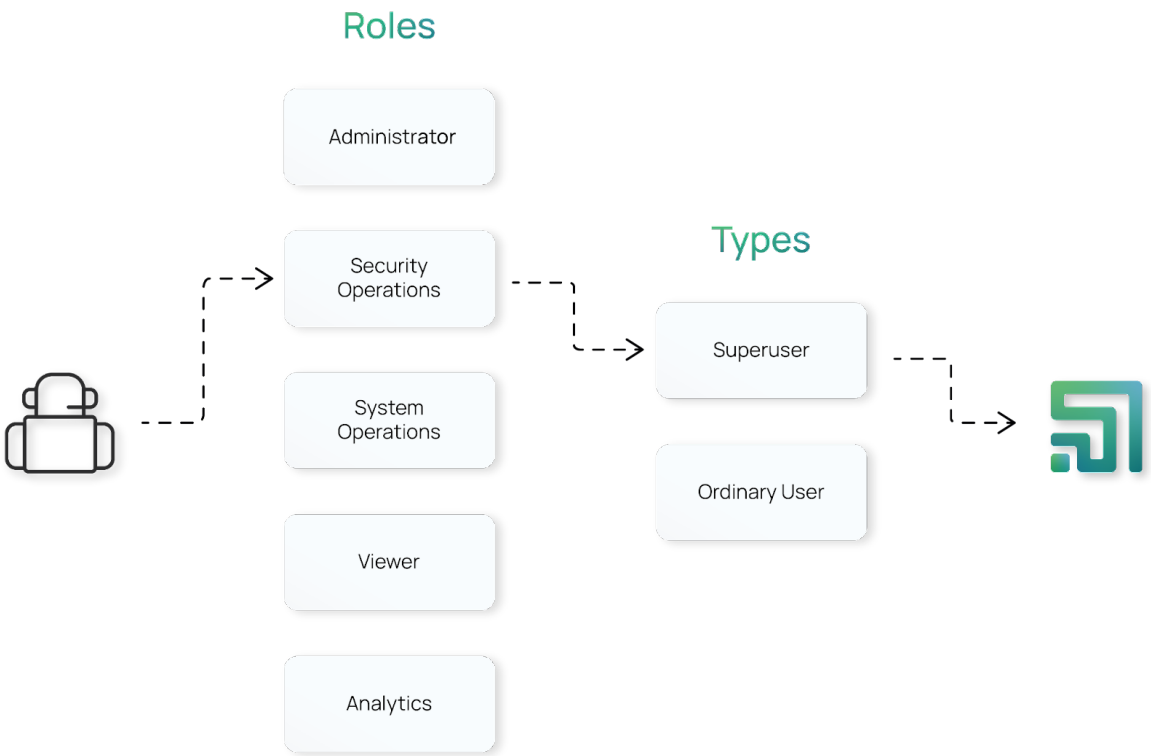
Users created within a tenant, including users with Administrator status, can create both a superuser and a user with administrator rights in the current tenant. User roles are regulated through RBAC.

The essence of the RBAC (Role-based access control) approach is to create roles that mirror business roles in the company and assign them to users. The user's ability to perform a particular action is checked based on these roles.

A **role** is a template of privileges and accesses in the system defined when a user is created. Later, it can be changed by the Superuser or a user of this tenant with the Administrator role.

For users within a tenant, there are five roles for the created user:

1. **Administrator** is a role with full rights within a tenant. A user with this role can create other users within the tenant, including those with the Administrator role.
2. **System Operations** is a role that has access to system components for configuration. Data on security incidents is not available.
3. **Security Operations** is a role that is assigned to handle security incidents. This role has access to data on detected attacks (Alerts) and management of Honeynet, Point, and Seeder but does not have access to system settings within the tenant.
4. **Analytics** is a role that only has access to data about security incidents.
5. **Viewer** is similar to the Administrator role but in read-only mode.



IT/IS engineers of the Client Company are appointed as users in the tenant. This allows you to transfer some of the functions of configuring and monitoring events in the tenant to local users.

1.4. Licensing

The system is licensed by the number of network segments (VLANs) and bait points. Breadcrumbs and the number of users/IP addresses on the network are not licensed separately.

To obtain a license, you need to ensure that the licensing server is available - https://update.labyrinth.tech/

The full license issued can be divided between tenants at the discretion of the MSSP Company.

2. SUPPORT PROGRAMS

All evaluating / existing customers have full access to our team of support engineers. Although a support request can be raised 24/7, it is important to keep in mind the support availability hours for your specific program.

Program	Support Availability	Contact channels
Full support	Mon-Sun 8 am - 8 pm (GMT+2)	Phone / Web / Email
Evaluation support	Mon-Fri 9 am - 6 pm (GMT+2)	Web / Email

Each program can be adjusted to the customer's needs upon agreement.

For a great overall experience for all of our existing customers and evaluating customers, we have set some severity guidelines to ensure the higher the severity of the issue the quicker the initial target response time will be.

Requests severity levels

Severity	Description	First Response Time (FRT)	
		Evaluation Support	Full Support
High	Critical issue where the solution is inoperable or there is an impact on the IT environment it is deployed into.	24 hours	12 hours

	E.g.: IP addresses collision or performance of infrastructure being adversely affected.		
Medium	Not impacting production infrastructure, solution working correctly but maybe not desirably.	48 hours	24 hours
	E.g.: configuration adjustments and report tuning		
Low	Minor issue that does not impact the functionality of the solution or the IT environment it has been deployed into.	72 hours	48 hours
	E.g.: general configuration question, feedback, suggestion, or feature request.		

For more details, please refer to the Customer Support reference guide.

3. TECHNICAL REQUIREMENTS

3.1. Requirements to the Customer (MSSP company)

The necessary conditions include the following:

1. Approval of server capacity allocation. The parameters are given in section "2.2 Computing resources";
2. Approval of the configuration of the required accesses:
    1. You need network access to the Web interface of the hypervisor on which the system will be deployed and access via HTTPS & SSH to the Labyrinth virtual machines.
    2. Network port/port configuration requirements.
    3. Availability of virtual uplinks for user operators.
    4. Provide IP addresses and Host-name for Worker Node to manage VLANs.
    5. It is necessary to ensure network connectivity between AdminVM (in the MSSP company's network) and Worker Nodes in the networks of Client companies.
    6. You need to get a list of IP addresses for each VLAN that needs to be protected. These IP addresses will be used to generate network decoys (Points) if static addressing is used to create network decoys.
3. Settle the configuration and ensure the configuration of the necessary open ports and protocols following paragraph 3.3 Network access policies;

3.2. Computing resources

Labyrinth Deception Platform components are distributed as a virtual machine image in OVA (for VMware) or a Zip archive (for Hyper-V) format. They are currently officially supported by the following virtualization/cloud platforms:

- VMWare vSphere 6.0/6.5/7.0;
- Microsoft Hyper-V with a minimum version of Hyper-V 2008 R2;
- Microsoft Azure Cloud;
- KVM-based solutions (Proxmox, OpenStack, etc.) for Admin VM.

The Client Companies served by the MSSP company install a component - Worker Node (one or more, depending on the needs).

Components	Up to 150 Points Up to 15 VLANs	Up to 300 Points Up to 50 VLANs	Up to 500 Points Up to 100 VLANs	More than 500 Points More than 100 VLANs
	vCPU(cores), RAM(GB),HDD(GB)	vCPU(cores), RAM(GB),HDD(GB)	vCPU(cores), RAM(GB),HDD(GB)	vCPU(cores), RAM(GB),HDD(GB)
Admin VM (Management Console)	4 vCPU(cores) 28 GB RAM 500 GB HDD	4 vCPU(cores) 28 GB RAM 500 GB HDD	4 vCPU(cores) 32 GB RAM 800 GB HDD	Contact your manufacturer representative
Worker Node	8 vCPU(cores) 16 GB RAM 200GB HDD	12 vCPU(cores) 24 GB RAM 250GB HDD	16 vCPU(cores) 40 GB RAM 500GB HDD	
Total	12 vCPU(cores) 44 GB RAM 700 GB HDD	16 vCPU(cores) 52 GB RAM 750 GB HDD	20 vCPU(cores) 72 GB RAM 1300 GB HDD	

For a Proof of Concept (non-production/test deployment), you can slightly reduce the allocated resources:

Admin VM (ManagementConsole)	4 vCPU (cores), 24 GB RAM, 200 GB HDD or more
Worker Node	4 vCPU (cores), 8 GB RAM, 200 GB HDD

3.3 Network access policy

For the platform to function correctly, it is necessary to ensure accessibility between different components of the system on specific network ports (TCP, UDP):

From ↓ / to →	Admin VM	Worker Node	update.labyrinth.tech	ntp.labyrinth.tech	Seeder Proxy	SIEM
Admin VM (Management Console)		20202 UDP	443 TCP	123 TCP 123 UDP		514 TCP 514 UDP

Worker Node	20202 UDP 20202 TCP					
PC Operator	22 TCP 443 TCP	22 TCP				
Real hosts with Seeder agents					443 TCP	

4. IMPLEMENTATION AND LAUNCHING OF THE SYSTEM

The system implementation plan can be characterized as the following:

№	Title of the activity	Number of business days
1	**Preparatory work for the start of the pilot project**	**4**
1.1	Allocation of server capacities	1
1.2	Adjusting network settings	1
1.3	Configuring the required accesses for Labyrinth components	1
1.4	Approval of a pilot project plan	1
2	**System deployment**	**1-3**
2.1	Setting up virtual machines	
2.2	Performing the license obtainment procedure	
2.3	Checking for updates and updating the system (if necessary)	
2.4	Uploading "custom" files by the system operator that will be used by the system as additional file decoys (wordlists)	
2.5	Seeder agent deployment on real hosts	
2.6	Configuring custom Point types (optional)	
2.7	Setting up Honeynets	
2.8	Generating Points, including: Universal Web Points for emulating existing in the network web services, SCADA/OT decoys, etc	
2.9	Verification of created network decoys (Points), file decoys (Seeder-Tasks/Breadcrumbs) distributed on real hosts	
3	**Implementing integrations depending on the available in the infrastructure solutions**	**1**

4	**Testing the system with the help of Instructions for the Implementation of pilot projects guide by the Labyrinth Development Team**	**3-5**
4.1	Simulating the use of information from standard file decoys (Seeder-Tasks / Breadcrumbs) by an attacker on real hosts in the MSSP Client network	
4.2	Performing attack on the generated Points, e.g. creating a Point that simulates RDP and WMI services and attempting to scan them and connect directly using the appropriate client software	
4.3	Testing the configured integrations	
5	**Generating a report on the results of the pilot project**	**1**
6	**Results presentation**	**1**
Total		11-15

The number of business days to implement and launch the system is approximate and heavily depends on the applied policies in your company.

Feel free to adjust it according to your own specific needs.