

Labyrinth Deception Platform

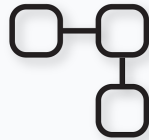
# Customer Presentation

Choose innovation. Choose proactive defence.  
Choose Deception Technology



# Cybersecurity challenge

Reactive approach to threat detection



False positive alarms



Difficult in usage



Information overload



More time to detect and react

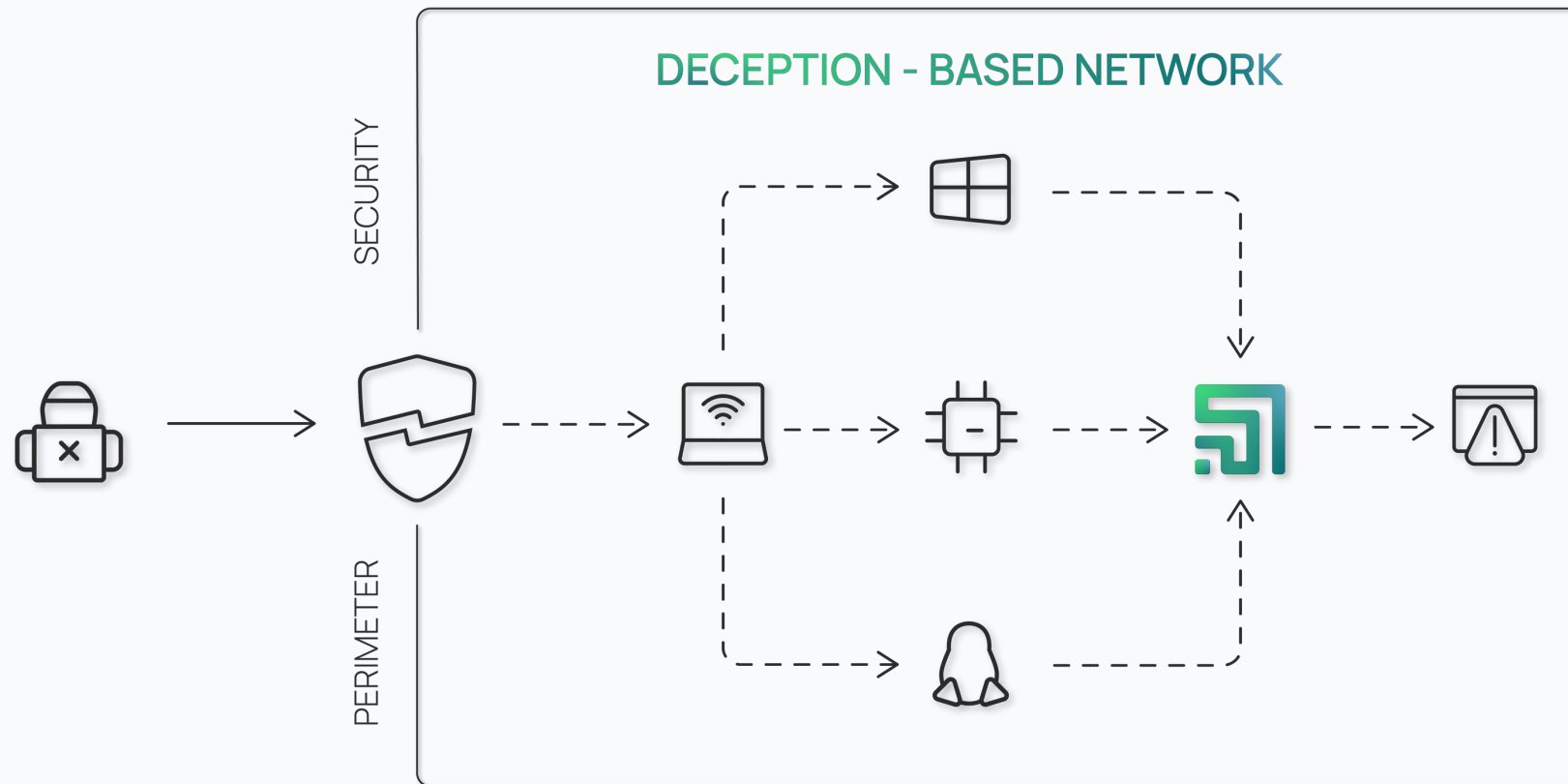


Breaches



# Deception-based threat detection

The Labyrinth Deception Platform is changing the cybersecurity paradigm by taking a proactive approach to threat detection.



# Business values



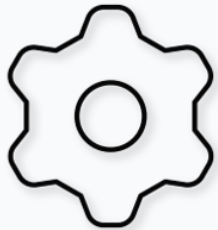
## Stops sophisticated threats

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.



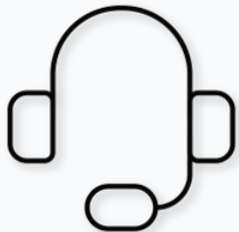
## Simple implementation

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.



## Technical support 12/7

Upgrades, software maintenance and technical support 12/7 (GMT+2) included in the subscription price.



## Incident response automation

Speeds up incident response by reducing the average time to detection and response (MTTD, MTTR) by up to 12\*\* times.

\* [https://www.enterprisemanagement.com/news/press\\_release.php?p\\_id=2659](https://www.enterprisemanagement.com/news/press_release.php?p_id=2659)

\*\* <https://www.bloomberg.com/press-releases/2020-09-14/cyber-deception-reduces-data-breach-costs-by-over-51-and-soc-inefficiencies-by-32>

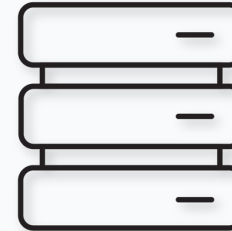


# Labyrinth's components



## 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

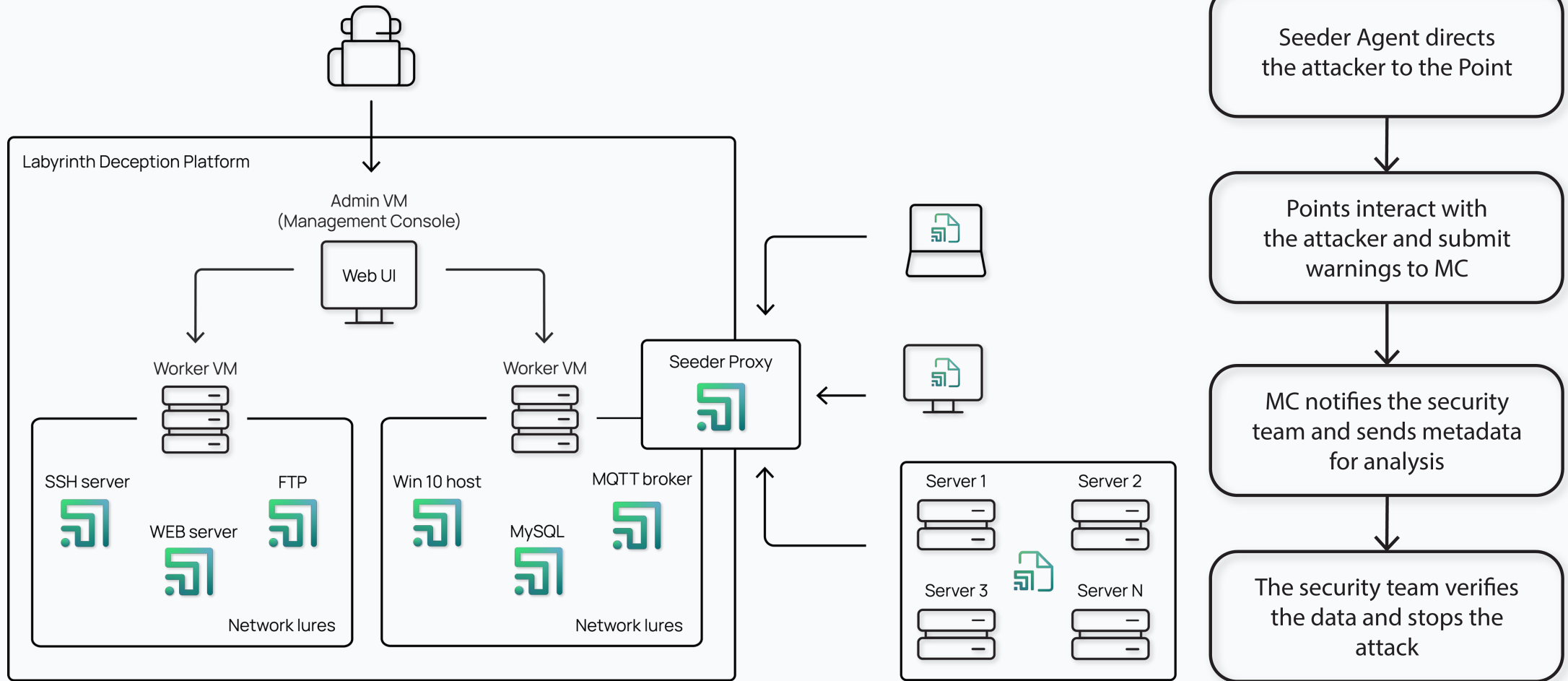
Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.



## 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.

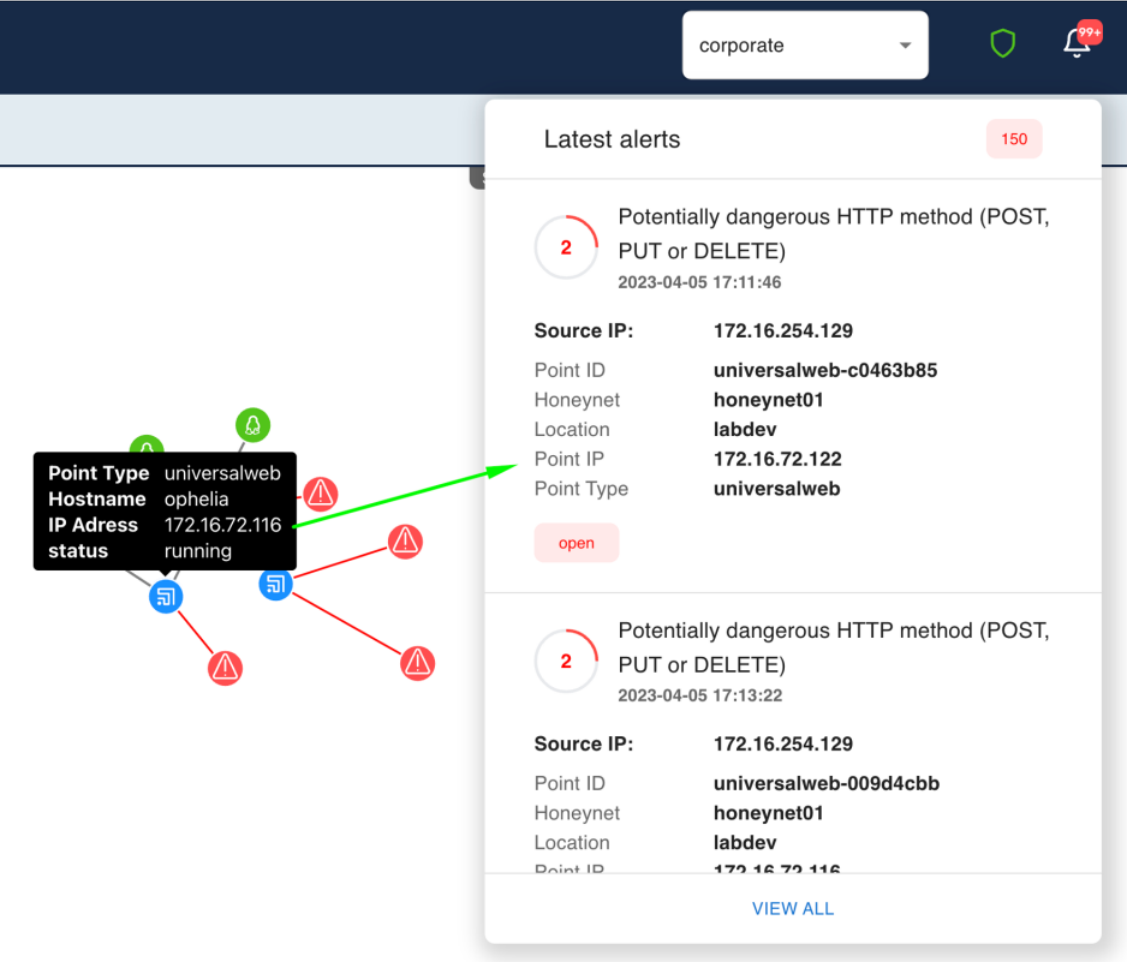
# Solution architecture



# Universal Web Point

Attackers most often use web application vulnerabilities to hack into corporate networks.

Labyrinth has implemented a unique technology that provides additional protection for the most used targets by hackers - web applications and services.



The screenshot displays the Labyrinth Deception Platform interface. At the top, there is a dark blue header with a dropdown menu set to 'corporate', a shield icon, and a notification bell with '99+'. Below the header, a network diagram shows several nodes connected by lines. A central node is highlighted with a black tooltip box containing the following information:

Point Type	universalweb
Hostname	ophelia
IP Address	172.16.72.116
status	running

Other nodes in the diagram are marked with red warning triangles. To the right, a 'Latest alerts' panel shows a list of alerts. The top alert is:

- Alert 1:** Potentially dangerous HTTP method (POST, PUT or DELETE) - 2023-04-05 17:11:46. Source IP: 172.16.254.129. Point ID: universalweb-c0463b85. Honeynet: honeynet01. Location: labdev. Point IP: 172.16.72.122. Point Type: universalweb.
- Alert 2:** Potentially dangerous HTTP method (POST, PUT or DELETE) - 2023-04-05 17:13:22. Source IP: 172.16.254.129. Point ID: universalweb-009d4cbb. Honeynet: honeynet01. Location: labdev. Point IP: 172.16.72.116.

Each alert has a red 'open' button. A 'VIEW ALL' link is at the bottom of the alerts panel.



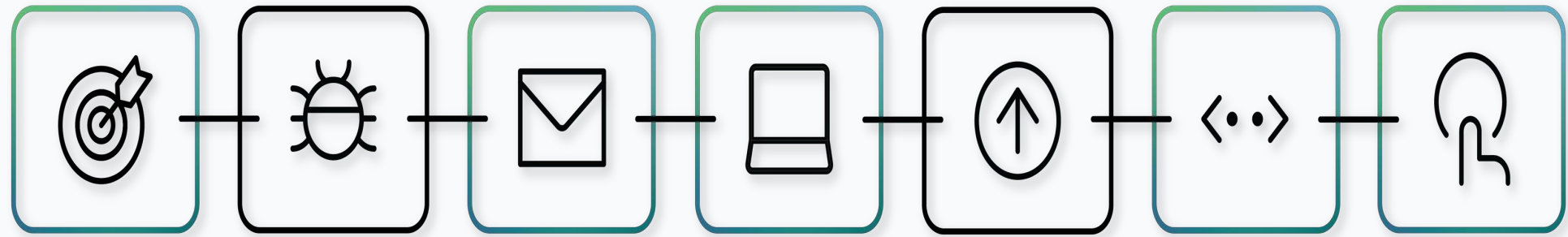
# Universal Web Point

The image displays two side-by-side screenshots of a Mozilla Firefox browser window. Both windows show the Cisco Switch login page at the URL `192.168.200.20/cse0cb8c1/config/log_off_page.htm`. The left window shows the page with a red box highlighting the 'Domain' column in the Network tab, which lists '192.168.200.20'. The right window shows the same page with a red box highlighting the 'Domain' column in the Network tab, which lists '192.168.200.32'. Both screenshots show the login form with fields for Username, Password, and Language, and buttons for 'Log In' and 'Secure Browsing (HTTPS)'. The Network tab in both windows shows a list of requests with columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.200.20	button.gif	img	gif	6.47 KB	6.26 KB
200	GET	192.168.200.20	favicon.gif	FaviconLoader.jsm:1...	gif	1.33 KB	1.12 KB
200	GET	192.168.200.20	logo_cis.gif	log_off_page.htm:S...	gif	891 B	678 B
200	GET	192.168.200.20	pageBackground.jpg	log_off_page.htm:S...	jpeg	14.85 KB	14.64 KB
200	GET	192.168.200.20	Status_information_icon.png	log_off_page.htm:S...	png	2.29 KB	2.08 KB
200	GET	192.168.200.20	ContextMessageArrow_DownT.gif	log_off_page.htm:S...	gif	1.03 KB	839 B
200	GET	192.168.200.20	login_progress.gif	log_off_page.htm:S...	gif	886 B	673 B
200	GET	192.168.200.20	topLeft.gif	log_off_page.htm:S...	gif	1 KB	816 B
200	GET	192.168.200.20	topRight.gif	log_off_page.htm:S...	gif	1 KB	816 B
200	GET	192.168.200.20	bottomLeft.gif	log_off_page.htm:S...	gif	1 KB	816 B
200	GET	192.168.200.20	bottomRight.gif	log_off_page.htm:S...	gif	1 KB	816 B
200	GET	192.168.200.20	bar.gif	log_off_page.htm:S...	gif	0.99 KB	801 B

Labyrinth automatically detects all web applications on the network and creates Universal Web Points that mimic the detected applications and embed additional vulnerabilities in them to make them more attractive to attackers.

# Use cases



Reconnaissance

Weaponization

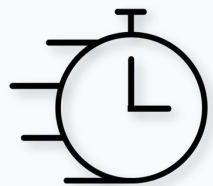
Delivery

Exploitation

Installation

Command and control

Action on objectives



Early detection of network threats  
Proactive protection  
Targeted attack detection  
Reduced Dwell Time



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

# Use case scenario: stolen credentials

```
(base) % ssh uat_test3@172.16.66.100
The authenticity of host '172.16.66.100 (172.16.66.100)' can't be established.
RSA key fingerprint is SHA256:P+IN8hlmCTYfVzdyuJrZIXxf6i+bIjH/uAJ0zTd5M8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.66.100' (RSA) to the list of known hosts.
uat_test3@172.16.66.100's password:
```

```
The programs included with the Debian GNU/Linux system
are free software; the exact distribution terms for each program
are described in the individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
uat_test3@thalassa:~$ whoami
uat_test3
uat_test3@thalassa:~$
```

02.01.2023 22:17:50	Status: <b>open</b> Alert Score: <b>1</b> Risk Score: <b>484</b> Attacker Ip: <b>172.16.254.8</b>	Point ID: <b>sshd-b2e17d78</b> Point IP: <b>172.16.66.100</b> Point Type: <b>sshd</b>	Alert reason: <b>Connection to sshd port detected</b> Alert source: <b>Logs</b> client_ip: <b>172.16.254.8</b>
02.01.2023 22:17:57	Status: <b>open</b> Alert Score: <b>4</b> Risk Score: <b>482</b> Attacker Ip: <b>172.16.254.8</b>	Point ID: <b>sshd-b2e17d78</b> Point IP: <b>172.16.66.100</b> Point Type: <b>sshd</b>	Alert reason: <b>sshd successful login detected</b> Alert source: <b>Logs</b> Password: <b>anders</b> Username: <b>uat_test3</b> client_ip: <b>172.16.254.8</b>
<b>Comments</b> No comments found			
<b>Events related to the Alert</b>			
Timestamp <b>2023-01-02 22:18:12</b> . Message <b>CMD: whoami.</b>			
Timestamp <b>2023-01-02 22:17:57</b> . Name <b>LC_CTYPE</b> . Message <b>request_env: LC_CTYPE=UTF-8.</b>			
Timestamp <b>2023-01-02 22:17:57</b> . Username <b>uat_test3</b> . Message <b>login attempt [uat_test3/anders] succeeded.</b>			
Timestamp <b>2023-01-02 22:17:57</b> .			
Timestamp <b>2023-01-02 22:17:57</b> . Message <b>Terminal Size: 158 45.</b>			

# Use case scenario: network scanning

10.08.2023 14:22:54	Status: <b>open</b> Alert Score: <b>2</b> Risk Score: <b>297</b> Attacker Ip: <b>172.16.254.8</b>	Point ID: <b>ftpd-04a39433</b> Point IP: <b>172.16.4.140</b> Point Type: <b>ftp_ed7</b>	Alert reason: <b>Port scan detected (TCP SYN, e.g. nmap -sS -T4)</b> Alert source: <b>Logs</b> DestinationPort: <b>25</b>
	<b>Comments</b>		
	No comments found		
	<b>Events related to the Alert</b>		
	Timestamp <b>2023-08-10 14:22:58</b> . Transport <b>tcp</b> . Source IP <b>172.16.254.8</b> . Source Port <b>297</b> . Destination Port <b>425</b> . TCP Flags <b>SYN</b> .		
Timestamp <b>2023-08-10 14:22:58</b> . Transport <b>tcp</b> . Source IP <b>172.16.254.8</b> . Source Port <b>297</b> . Destination Port <b>20221</b> . TCP Flags <b>SYN</b> .			
Timestamp <b>2023-08-10 14:22:58</b> . Transport <b>tcp</b> . Source IP <b>172.16.254.8</b> . Source Port <b>297</b> . Destination Port <b>687</b> . TCP Flags <b>SYN</b> .			
Timestamp <b>2023-08-10 14:22:58</b> . Transport <b>tcp</b> . Source IP <b>172.16.254.8</b> . Source Port <b>297</b> . Destination Port <b>1055</b> . TCP Flags <b>SYN</b> .			

```

~ % nmap 172.16.4.140
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-10 14:22 EEST
Nmap scan report for 172.16.4.140
Host is up (0.0064s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
21/tcp    open       ftp
22/tcp    filtered   ssh
88/tcp    filtered   kerberos-sec
443/tcp   filtered   https
1024/tcp   filtered   kdm
1056/tcp   filtered   vfo
1123/tcp   filtered   murray
1145/tcp   filtered   x9-icue
1935/tcp   filtered   rtmp
2605/tcp   filtered   bgpd
3551/tcp   filtered   apcupsd
5100/tcp   filtered   admd
50389/tcp  filtered   unknown

Nmap done: 1 IP address (1 host up) scanned in 16.53 seconds
    
```

# Use case scenario: web scanning

The screenshot displays the Labyrinth Deception Platform interface. At the top, a search bar contains the IP address "192.168.200.201". Below the search bar, a large network map is visible, featuring various nodes and connections. A red arrow points from the search bar to a specific node on the map. A modal window is open over the map, displaying the following information:

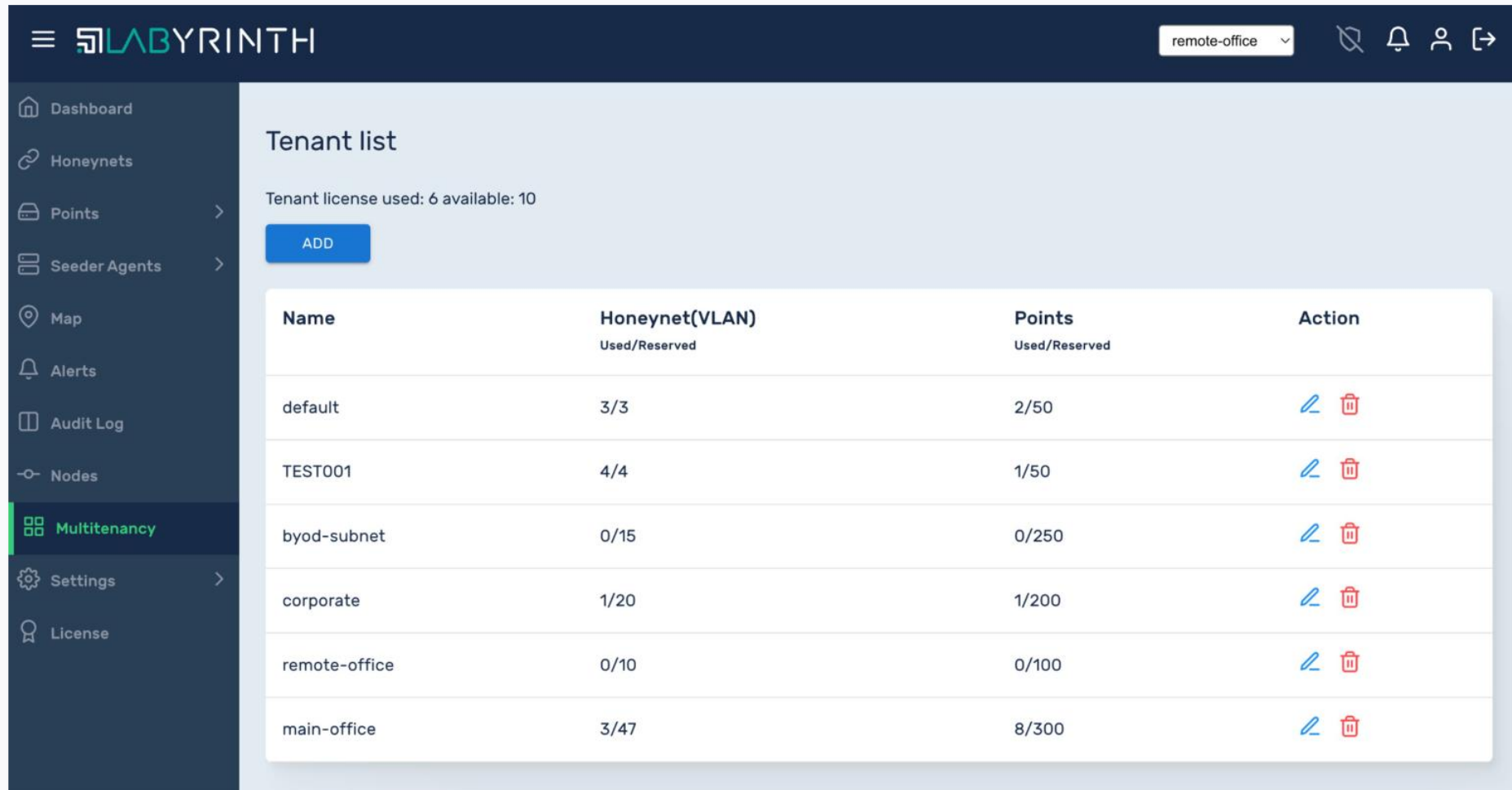
- Web scanner has been detected** (Alert Title)
- Point Info**
  - Point ID: vmware\_esx-b3aa40df
  - Point IP: 192.168.200.45
  - Point Type: vmware\_esx
- Attacker Info**
  - Source IP: 192.168.200.201
  - Reason: Web scanner has been detected
  - Alert Score: 1
  - Risk Score: 2010
- IR Info**
  - Status: open
  - IR Link: N/A (Case not created yet)
- Timestamp:** 13.04.2021 18:37:05

The interface also includes a "Map" tab, a "Search" button, and a "Controls" panel at the bottom. The network map shows various nodes, some of which are highlighted with red warning icons.





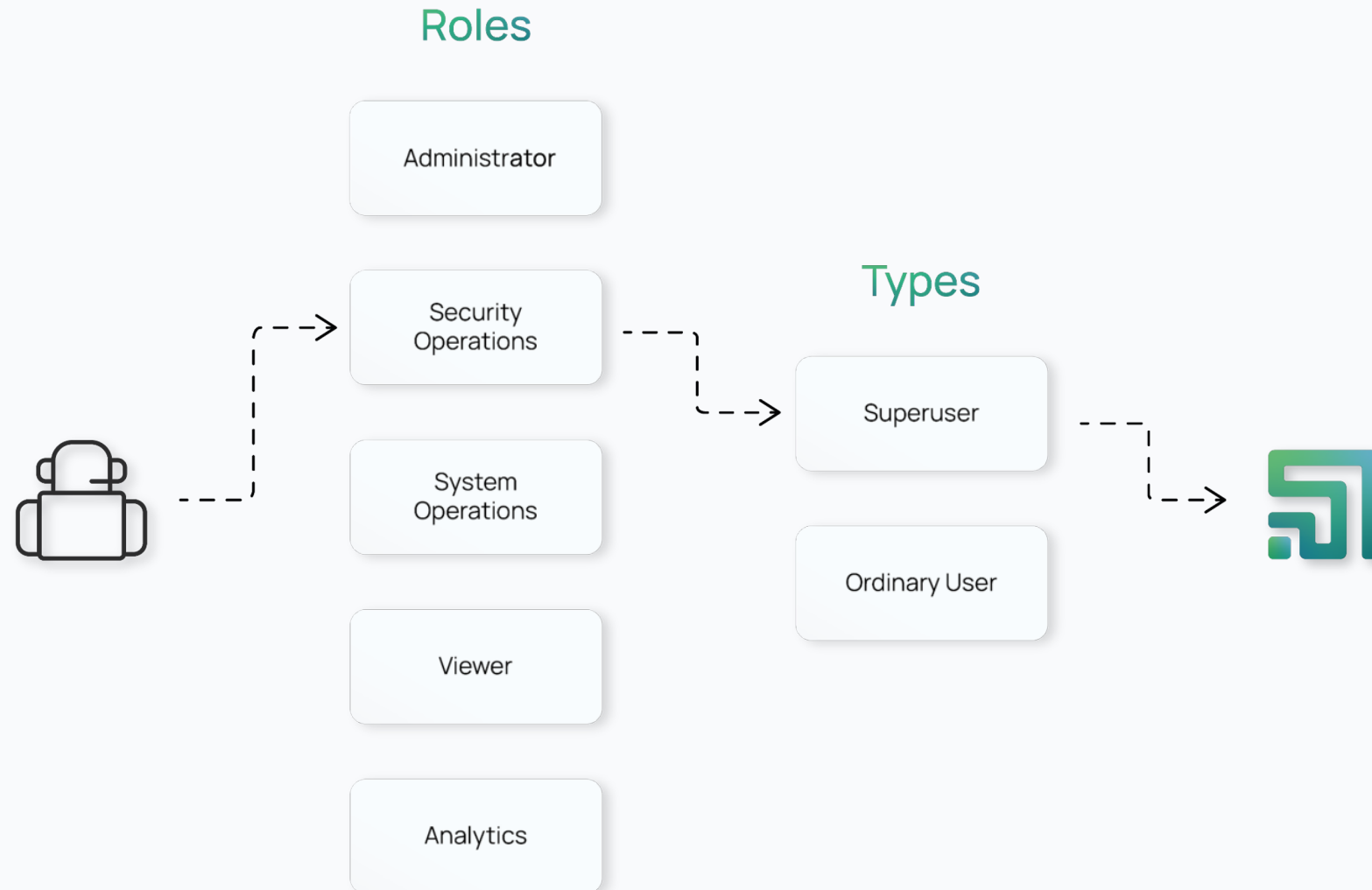
# Multitenancy



The screenshot displays the Labyrinth web interface. The top navigation bar includes the Labyrinth logo, a dropdown menu set to 'remote-office', and icons for search, notifications, user profile, and help. The left sidebar contains a menu with items: Dashboard, Honeynets, Points, Seeder Agents, Map, Alerts, Audit Log, Nodes, Multitenancy (highlighted), Settings, and License. The main content area is titled 'Tenant list' and shows 'Tenant license used: 6 available: 10' with an 'ADD' button. Below this is a table with columns for Name, Honeynet(VLAN) Used/Reserved, Points Used/Reserved, and Action.

Name	Honeynet(VLAN) Used/Reserved	Points Used/Reserved	Action
default	3/3	2/50	<a href="#">Edit</a> <a href="#">Delete</a>
TEST001	4/4	1/50	<a href="#">Edit</a> <a href="#">Delete</a>
byod-subnet	0/15	0/250	<a href="#">Edit</a> <a href="#">Delete</a>
corporate	1/20	1/200	<a href="#">Edit</a> <a href="#">Delete</a>
remote-office	0/10	0/100	<a href="#">Edit</a> <a href="#">Delete</a>
main-office	3/47	8/300	<a href="#">Edit</a> <a href="#">Delete</a>

# RBAC: system users





# Integrations



State	Name	Edit
<input type="radio"/>	CrowdStrike	<a href="#">Edit</a>
<input type="radio"/>	Cuckoo Sandbox	<a href="#">Edit</a>
<input type="radio"/>	Fortigate	<a href="#">Edit</a>
<input checked="" type="radio"/>	Microsoft Teams Notifications	<a href="#">Edit</a>
<input checked="" type="radio"/>	IBM-Qradar	<a href="#">Edit</a>
<input checked="" type="radio"/>	Slack Notification	<a href="#">Edit</a>
<input type="radio"/>	SMTP Notification	<a href="#">Edit</a>
<input checked="" type="radio"/>	Splunk	<a href="#">Edit</a>
<input checked="" type="radio"/>	SIEM Integration (Syslog forwarder)	<a href="#">Edit</a>
<input type="radio"/>	TheHive	<a href="#">Edit</a>

# 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)

