

Labyrinth Deception Platform

# Customer Presentation

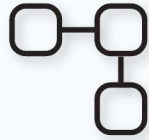
Choose innovation. Choose proactive defence.  
Choose Deception Technology



Labyrinth Security Solutions, 2024

# Cybersecurity challenge

Reactive approach to threat detection



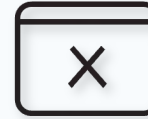
False positive alarms



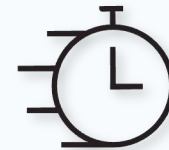
Difficult in usage



Information overload



More time to detect and react

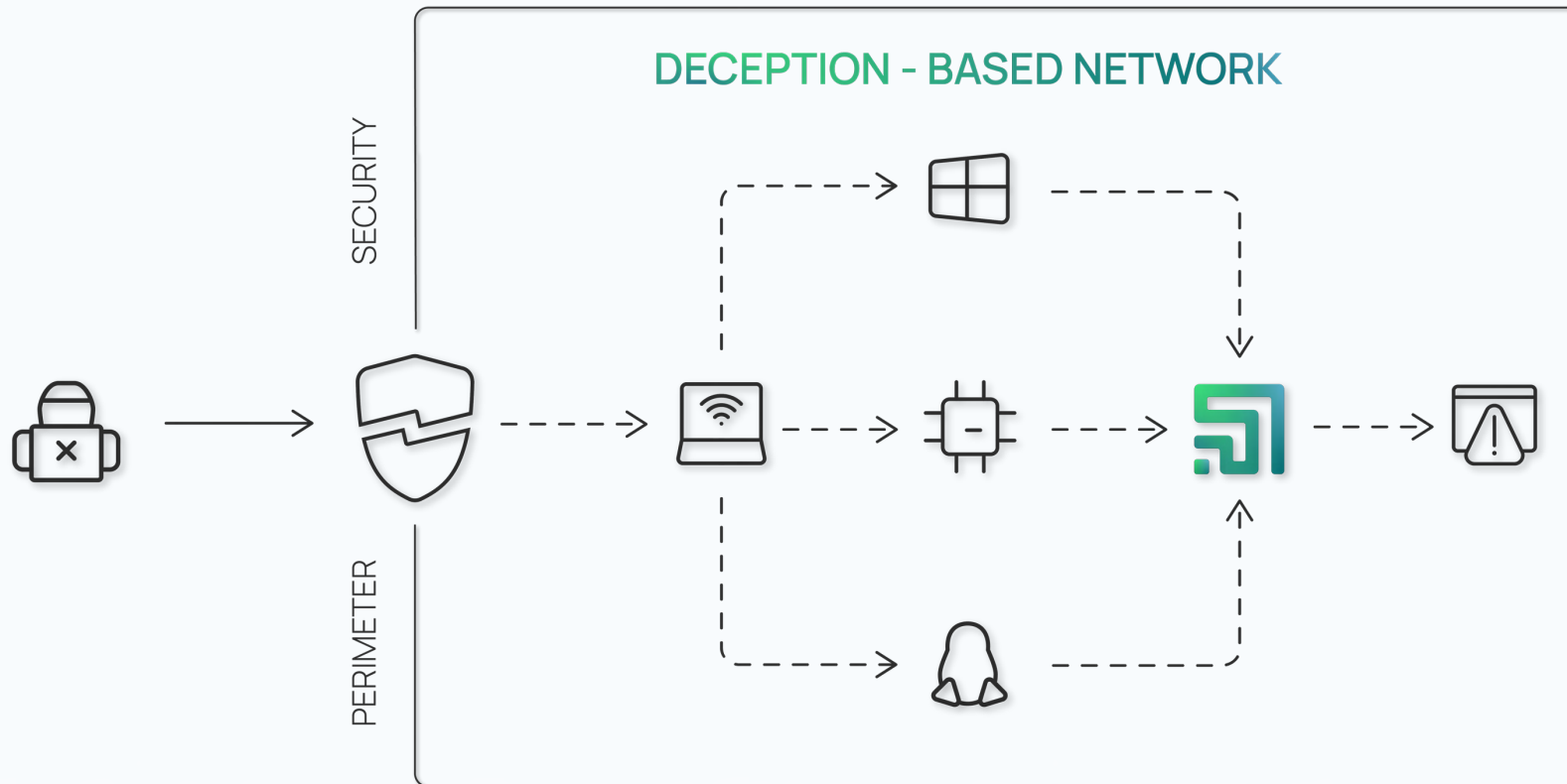


Breaches



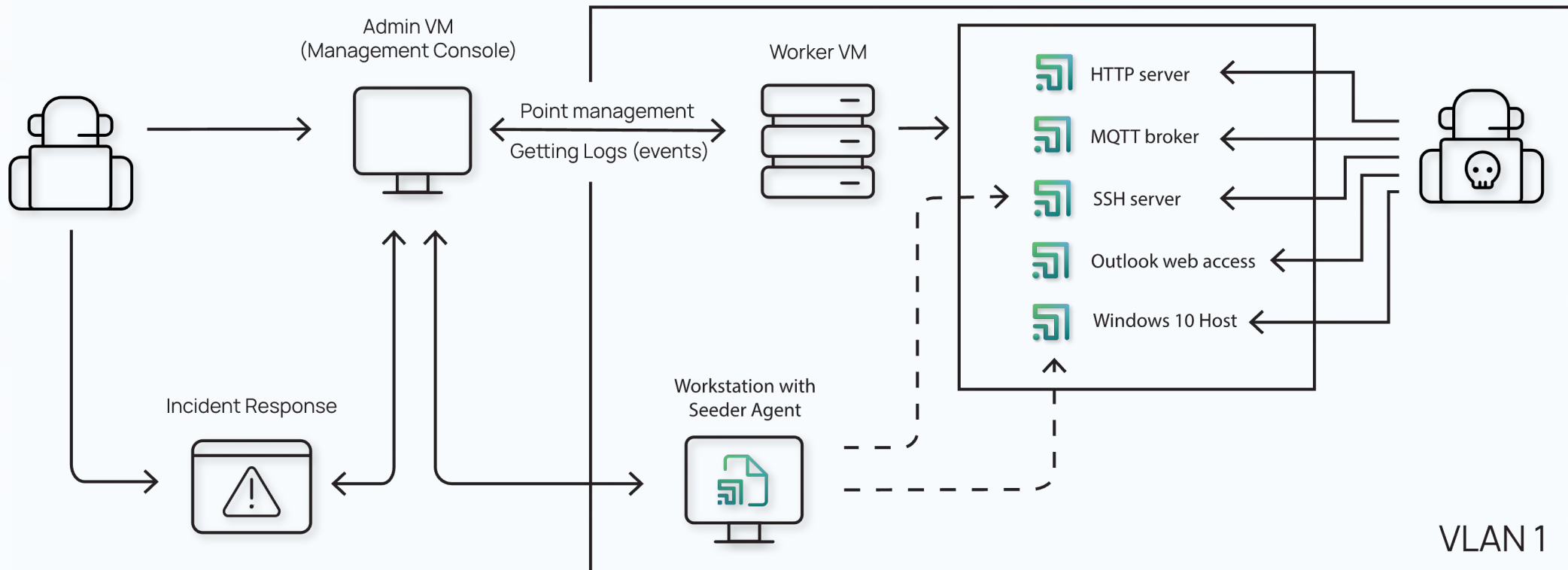
# Deception-based threat detection

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



# Labyrinth Deception Platform

The platform creates vulnerable IT services and applications, increasing the attack surface and disorienting attackers. The Labyrinth provokes attackers to act, detects and tracks all their activities, and isolates them from the actual IT network.



# Business values



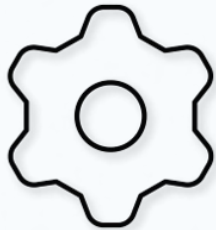
## Stops sophisticated threats

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.



## 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)

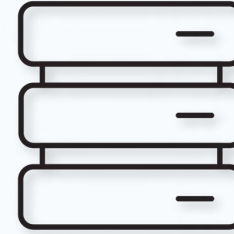
\*\* <https://www.bloomberg.com/press-releases/2020-09-14/cyber-deception-reduces-data-breach-costs-by-over-51-and-soc-inefficiencies-by-32>

# 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

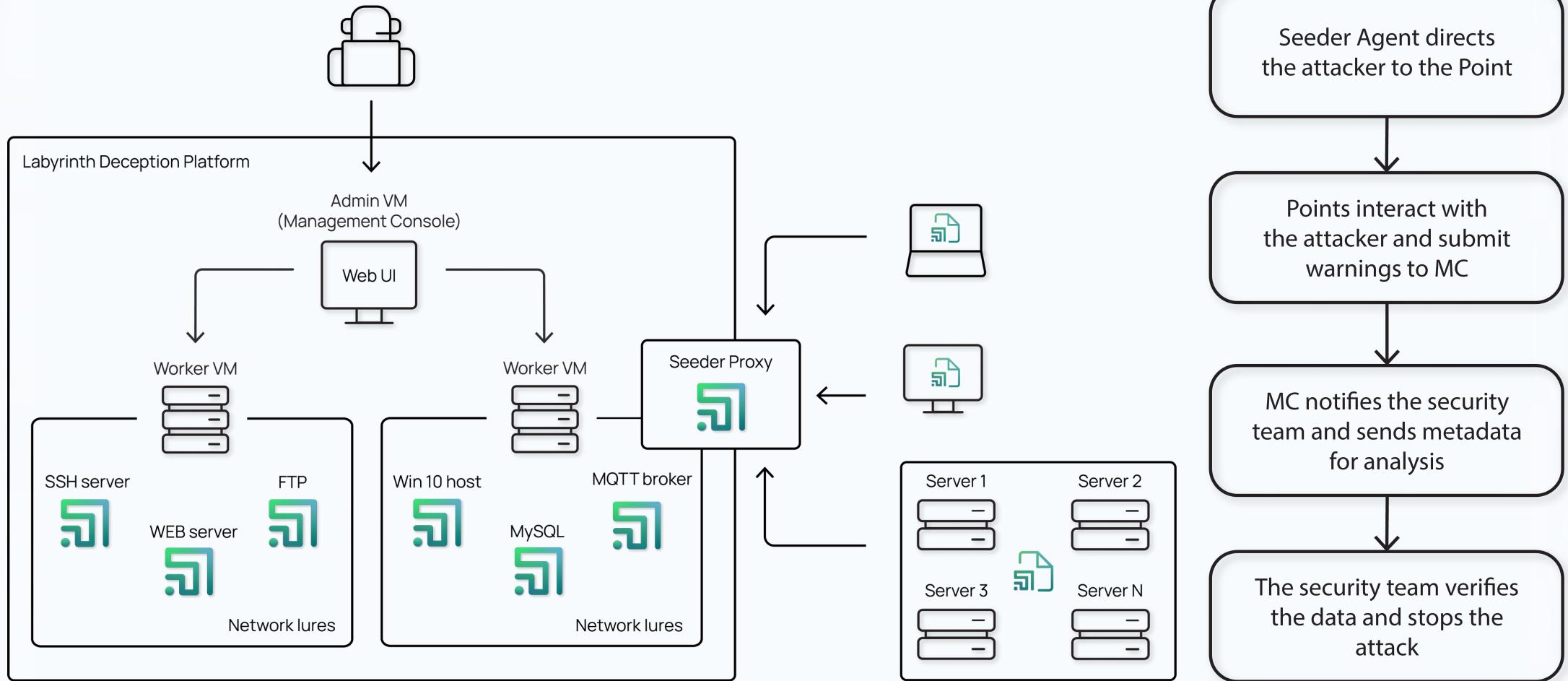
Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.



## 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.

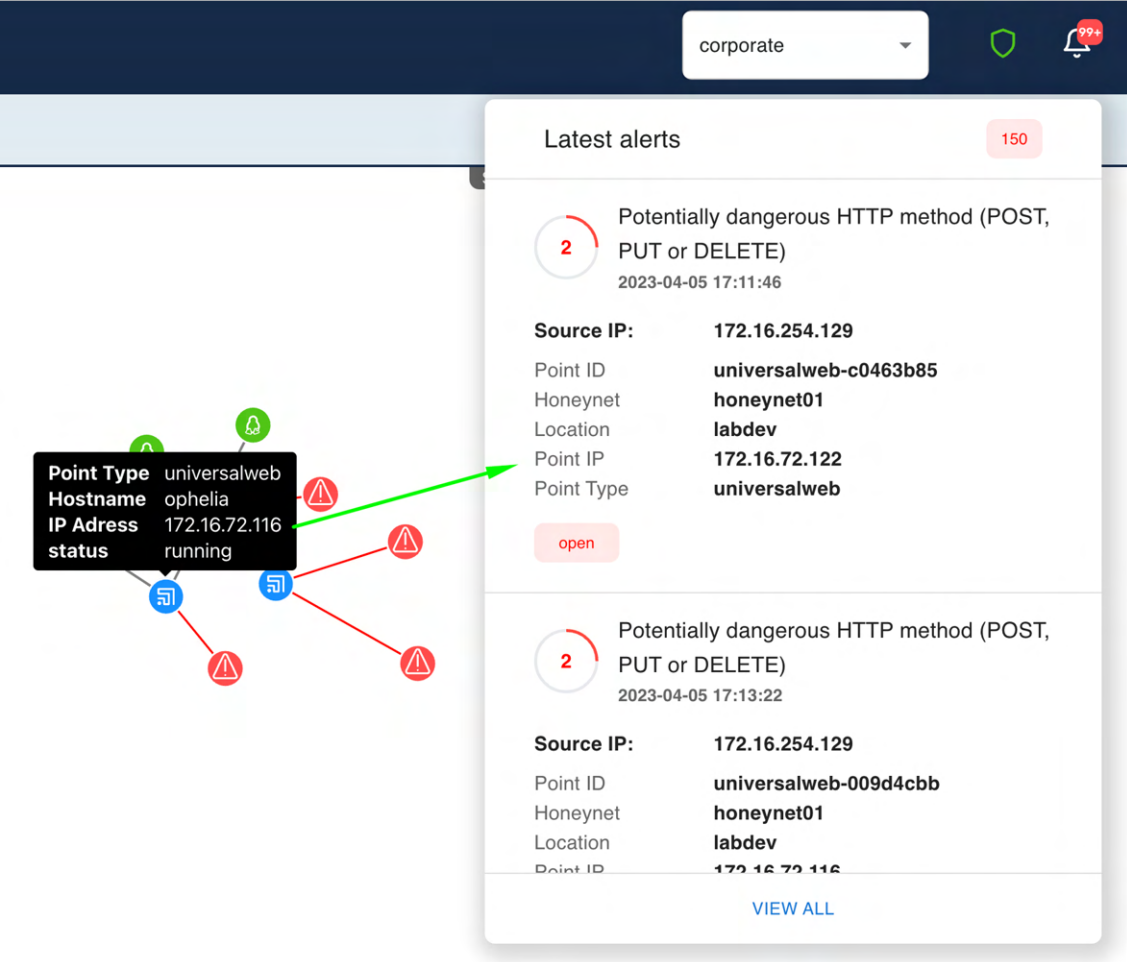
# Solution architecture



# 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 navigation bar with a dropdown menu set to 'corporate', a shield icon, and a notification bell with '99+'. Below the navigation bar, 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 of the network diagram, a 'Latest alerts' panel is visible, showing a list of alerts. The first 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.

The panel also includes a '150' alert count indicator, an 'open' button, and a 'VIEW ALL' link at the bottom.



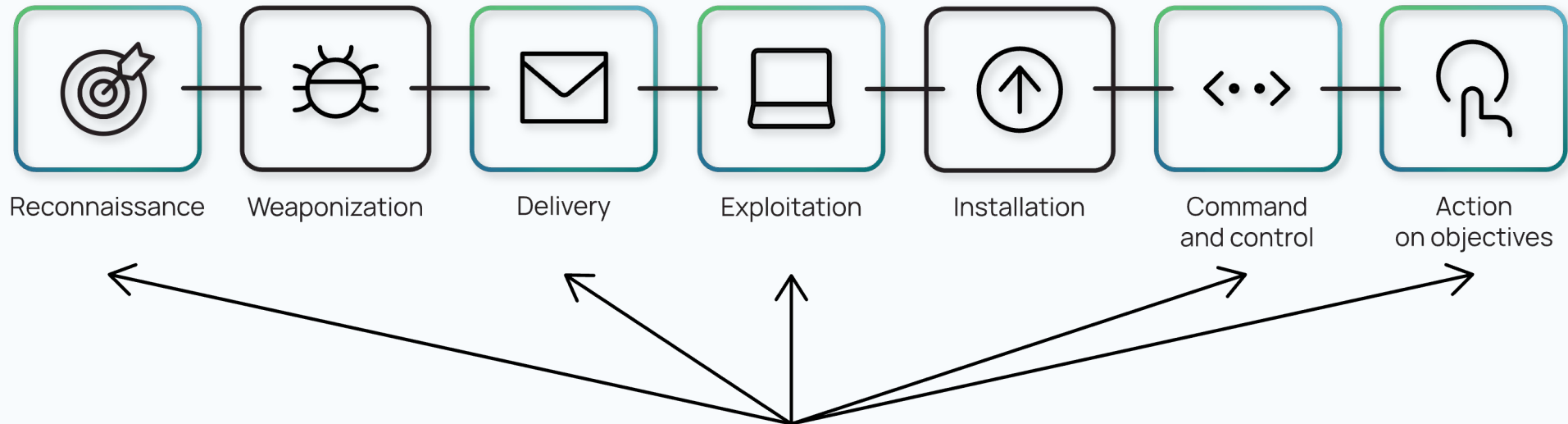
# Universal Web Point

The image displays two side-by-side screenshots of a Cisco Switch login page in Mozilla Firefox. The left screenshot shows the page with a red box highlighting the 'Domain' column in the Network tab, which contains the IP address 192.168.200.20. The right screenshot shows the same page with a red box highlighting the 'Domain' column in the Network tab, which contains the IP address 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).

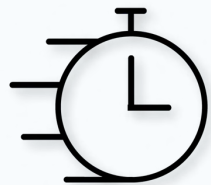
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.200.20	button.gif	img	gif	6.47 KB	6.26 KB
200	GET	192.168.200.20	favicon.gif	FaviconLoader.jsm:1...	gif	1.33 KB	1.12 KB
200	GET	192.168.200.20	logo_cis.gif	log_off_page.htm:5...	gif	891 B	678 B
200	GET	192.168.200.20	pageBackground.jpg	log_off_page.htm:5...	jpeg	14.85 KB	14.64 KB
200	GET	192.168.200.20	Status_information_icon.png	log_off_page.htm:5...	png	2.29 KB	2.08 KB
200	GET	192.168.200.20	ContextMessageArrow_DownT.gif	log_off_page.htm:5...	gif	1.03 KB	839 B
200	GET	192.168.200.20	login_progress.gif	log_off_page.htm:5...	gif	886 B	673 B
200	GET	192.168.200.20	topLeft.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.20	topRight.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.20	bottomLeft.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.20	bottomRight.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.20	bar.gif	log_off_page.htm:5...	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



LABYRINTH



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

```
~ % ssh test3.test2@172.16.132.28
The authenticity of host '172.16.132.28 (172.16.132.28)' can't be established.
ED25519 key fingerprint is SHA256:XEYAIhSySo8BfIu8k/5l+iXZ+Wr6Itfynjptz+KEbnc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.132.28' (ED25519) to the list of known hosts.
test3.test2@172.16.132.28's password:
test3.test2@tethys:~$ whoami
test3.test2
test3.test2@tethys:~$
```

<input type="checkbox"/>	Severity	Status	Timestamp	Point ID	Attacker IP	Alert Reason	
<input type="checkbox"/>	L	open	2024-06-02 20:52:30	sshd-26e9adf2	172.16.254.4	Connection to sshd port detected	^

DETAILS   **EVENTS**   ACTIVITY(0)

2024-06-02 20:53:22	Hostname: - Message: <b>CMD: whoami</b>
2024-06-02 20:52:37	Hostname: -
2024-06-02 20:52:37	Hostname: - Message: <b>Terminal Size: 176 50</b>
2024-06-02 20:52:37	Hostname: - Username: <b>test3.test2</b> Message: <b>login attempt [test3.test2/15061988] succeeded</b>
2024-06-02 20:52:37	Hostname: - Name: <b>LC_CTYPE</b> Message: <b>request_env: LC_CTYPE=UTF-8</b>
2024-06-02 20:52:30	Hostname: - Message: <b>SSH client hassh fingerprint: aae6b9604f6f3356543709a376d7f657</b>

# Use case scenario: network scanning

□ L open 2024-06-02 21:37:56 win\_generic-6cf15eea 172.16.254.4 Port scan detected (TCP SYN e.g. nmap -... ^

[DETAILS](#) [EVENTS](#) [ACTIVITY\(0\)](#)

**2024-06-02 21:37:56**

Alert ID	767944f8-1d05-49eb-ba17-6d2c254398b1
Alert Reason	Port scan detected
Destination IP	172.16.132.30
MITRE	
Technique	<a href="#">T1595</a>
Tactic	<a href="#">TA0043</a>

```
~ % nmap 172.16.132.30
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-02 21:38 EEST
Nmap scan report for 172.16.132.30
Host is up (0.031s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp filtered unknown
49153/tcp filtered unknown
49154/tcp filtered unknown
49156/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 5.93 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 network map is visible, showing various nodes and connections. A red arrow points from the search bar to a specific node on the map. A large, semi-transparent modal window is overlaid on the map, displaying the following information:

- CLOSE** (button)
- 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**
  - Status: open
  - IR Link: N/A (Case not created yet)
- 13.04.2021 18:37:05** (Timestamp)

At the bottom of the modal window, there are three green circular icons with white exclamation marks, indicating alerts or warnings. The interface also includes a 'Map' tab, 'Minimap', 'Actions', 'Legend', and 'Controls' sections.

# Use case scenario: detecting MITM

```
$ sudo python2 Responder.py -I eth2  
  
[+] [REDACTED]  
  
NBT-NS, LLMNR & MDNS Responder 2.3  
Author: Laurent Gaffie (laurent.gaffie@gmail.com)  
To kill this script hit CTRL-C  
  
[+] Poisoners:  
LLMNR [ON]  
NBT-NS [ON]  
DNS/MDNS [ON]  
  
[+] Servers:  
HTTP server [ON]  
HTTPS server [ON]  
WPAD proxy [OFF]
```

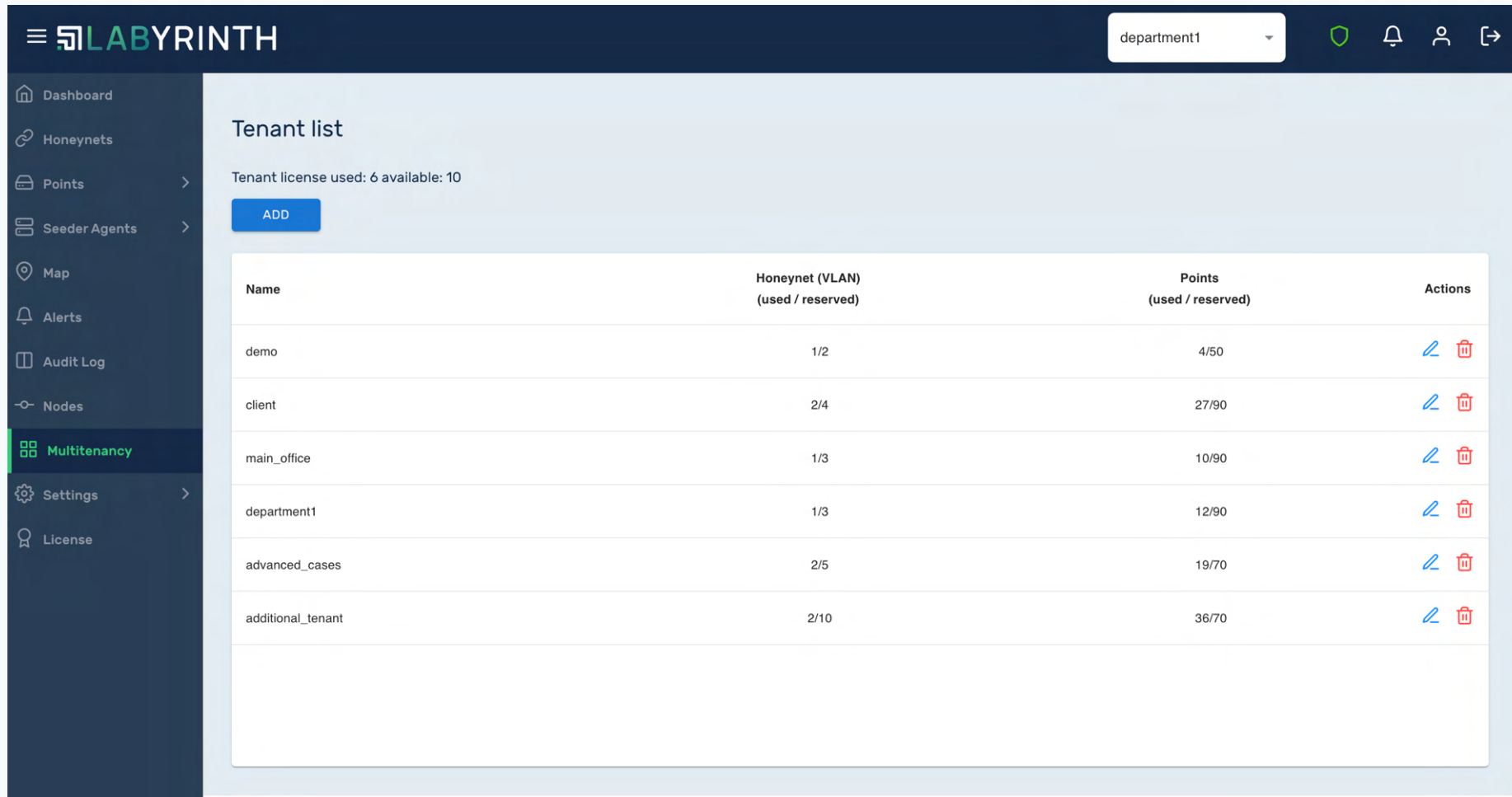
□ H open 2023-12-28 20:07:58 clientos-27a91f04 172.16.12.252 Responder-like tool responded for Ne... ^

[DETAILS](#) [EVENTS](#) [ACTIVITY\(0\)](#)

**2023-12-28 20:07:58**

Alert ID	7d3a5abc-27d4-4f35-9cbe-14bee90456b1
Alert Reason	Responder-like tool responded for NetBIOS request
Destination IP	172.16.12.11
<b>MITRE</b>	
Technique	<a href="#">T1557.001</a>
Tactic	<a href="#">TA0006</a>

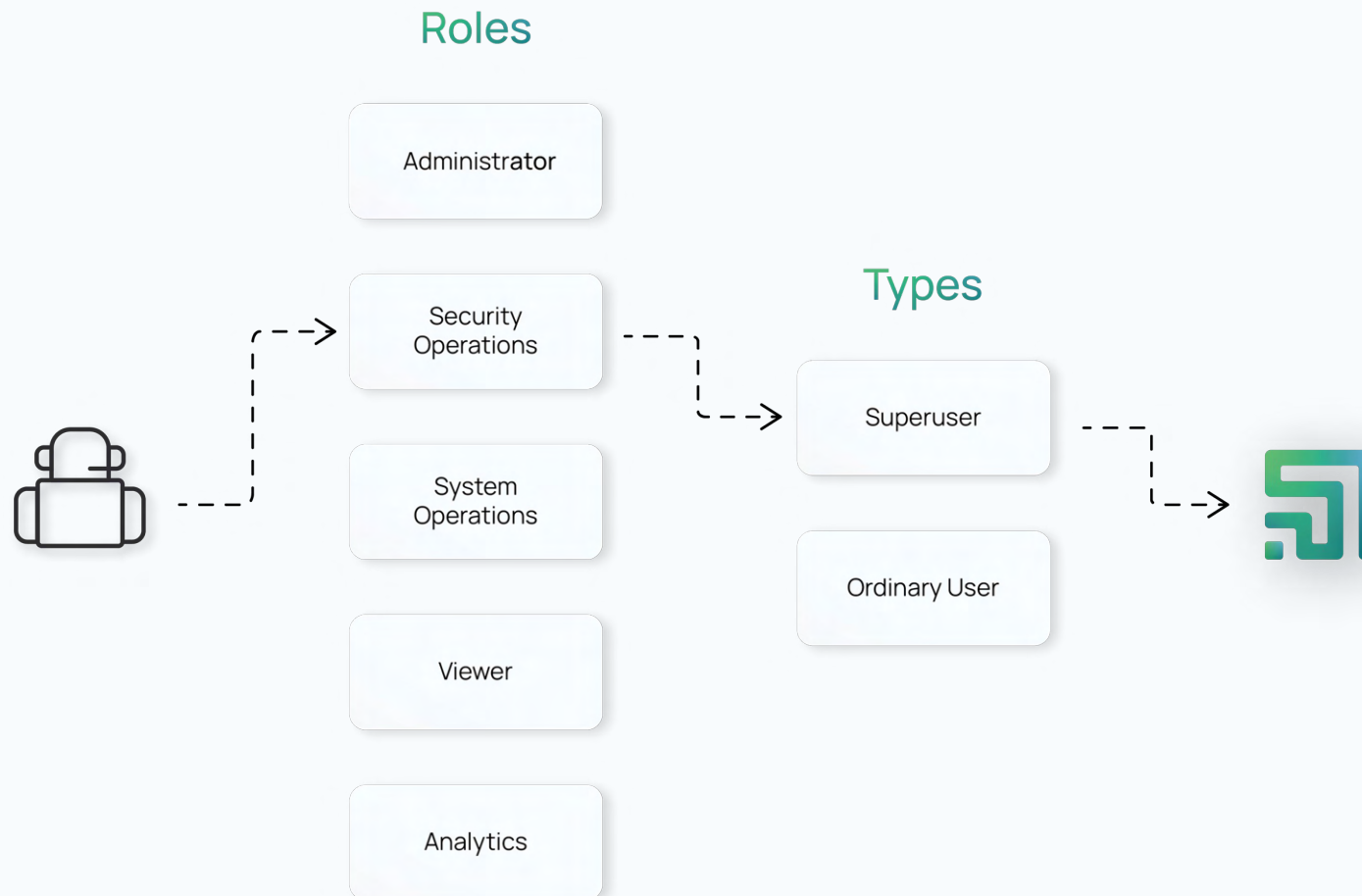
# Multitenancy



The screenshot displays the Labyrinth web interface for managing multitenancy. The top navigation bar includes the Labyrinth logo, a dropdown menu set to 'department1', and icons for security, notifications, user profile, and help. The left sidebar contains a menu with options: 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 listing tenants with their names, Honeynet (VLAN) usage, Points usage, and action icons.

Name	Honeynet (VLAN) (used / reserved)	Points (used / reserved)	Actions
demo	1/2	4/50	<a href="#">edit</a> <a href="#">delete</a>
client	2/4	27/90	<a href="#">edit</a> <a href="#">delete</a>
main_office	1/3	10/90	<a href="#">edit</a> <a href="#">delete</a>
department1	1/3	12/90	<a href="#">edit</a> <a href="#">delete</a>
advanced_cases	2/5	19/70	<a href="#">edit</a> <a href="#">delete</a>
additional_tenant	2/10	36/70	<a href="#">edit</a> <a href="#">delete</a>

# RBAC: system users





# Integrations



State	Name	Edit
<input type="radio"/>	CrowdStrike	<a href="#">/</a>
<input checked="" type="radio"/>	FortiGate	<a href="#">/</a>
<input type="radio"/>	Microsoft Teams Notifications	<a href="#">/</a>
<input type="radio"/>	IBM QRadar	<a href="#">/</a>
<input checked="" type="radio"/>	Slack Notification	<a href="#">/</a>
<input type="radio"/>	SMTP Notification	<a href="#">/</a>
<input checked="" type="radio"/>	Splunk	<a href="#">/</a>
<input checked="" type="radio"/>	SIEM Integration (Syslog forwarder)	<a href="#">/</a>
<input type="radio"/>	TheHive	<a href="#">/</a>
<input type="radio"/>	Webhook	<a href="#">/</a>

# API

Overview ▼

- Authentication
- Content-Type
- Timezone

Resource Group ▼

- Get status ↓
- Get License Info ↓
- List All Tenants ↓
- List All Nodes ↓
- Audit logs
- Autocomplete ↓
- List existing logs ↓
- List All Honeynets ↓
- Points
- List All Points ↓
- Get Point Details ↓
- Manage Point ✎
- Delete Point ✖
- Alerts
- List All Alerts ↓
- Get Alert Details ↓
- Manage Alert ✎
- Download traffic dump ↓
- List All Seeders ↓
- List Seeders Tasks ↓

<https://your-provider-host.com/api/v1>

## Labyrinth API v.1

The Labyrinth API provides a way to manage Labyrinth resources. The API is compliant to all REST standards: resource-oriented URLs, returns JSON-encoded responses, uses standard HTTP response codes and verbs, authenticates and communicates through secure HTTPS connections.

**AUTHENTICATION**

Each request must be authenticated with private token. The API v.1 uses Bearer authentication scheme. Building authorization header example: `Authorization: Bearer <token>`

**CONTENT-TYPE**

Needs to be "application/json" for POST and PUT, but "" for GET and DELETE.

**TIMEZONE**

The times returned are in UTC.

### Resource Group

**API STATUS**

GET Get status

**Example URI**

GET <https://your-provider-host.com/api/v1/status>

**Response** 200 Show

**Response** 401 Show

**Response** 429 Show

**LICENSE**

GET Get License Info

**Example URI**

GET <https://your-provider-host.com/api/v1/license>

**Response** 200 Show

**Response** 401 Show

**Response** 429 Show

**TENANTS**

Back to top

# 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)

