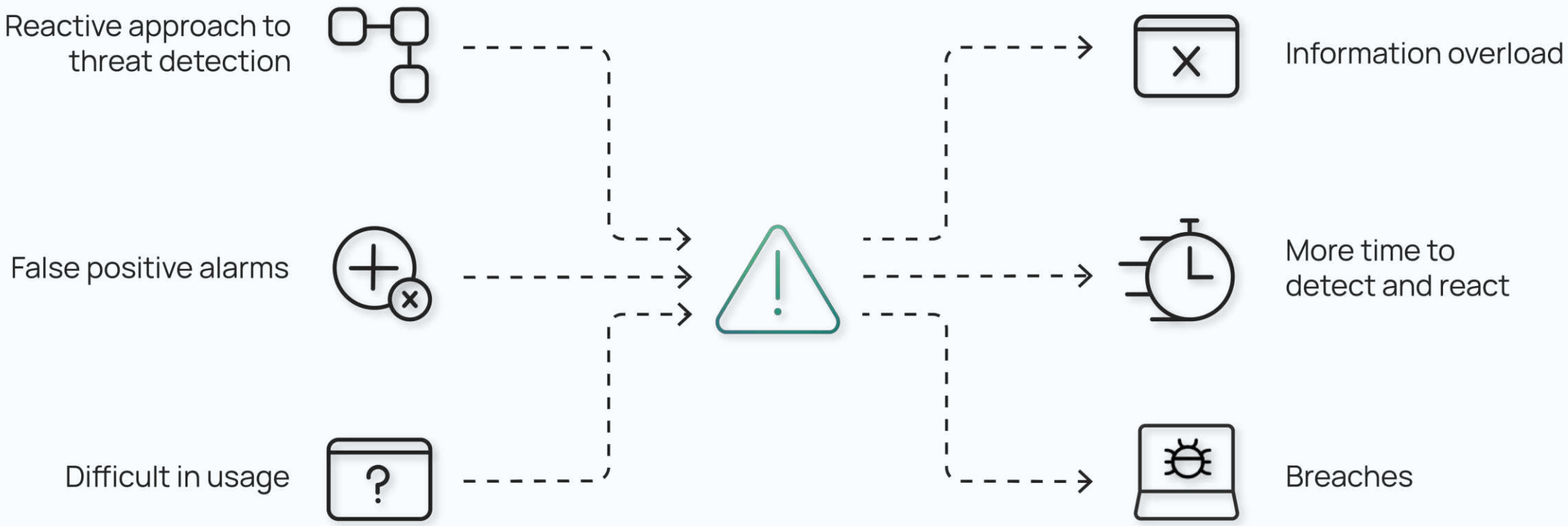
Labyrinth Deception Platform

Customer Presentation

Choose innovation. Choose proactive defence.
Choose Deception Technology

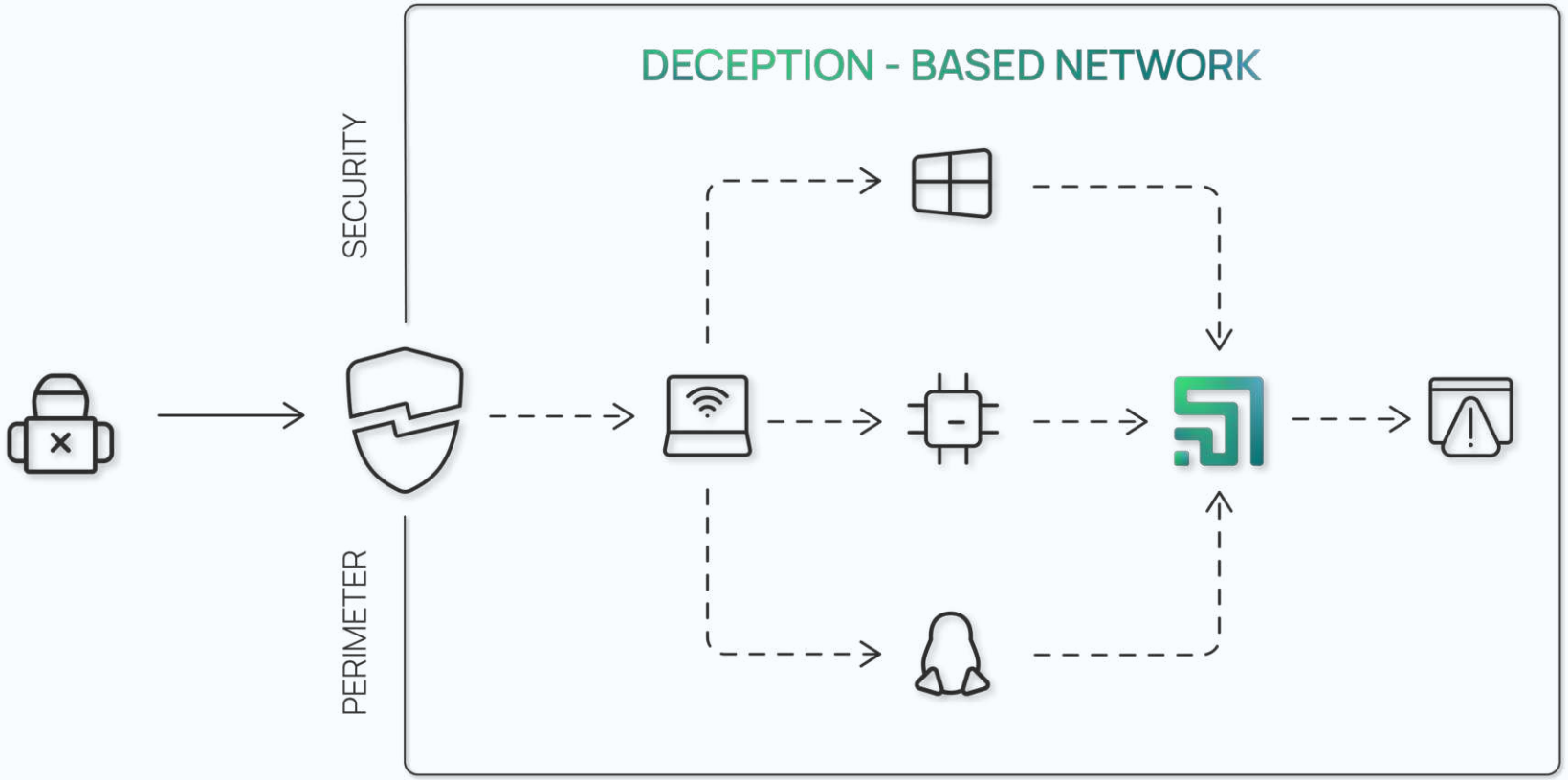
Labyrinth Security Solutions, 2025

Cybersecurity challenge



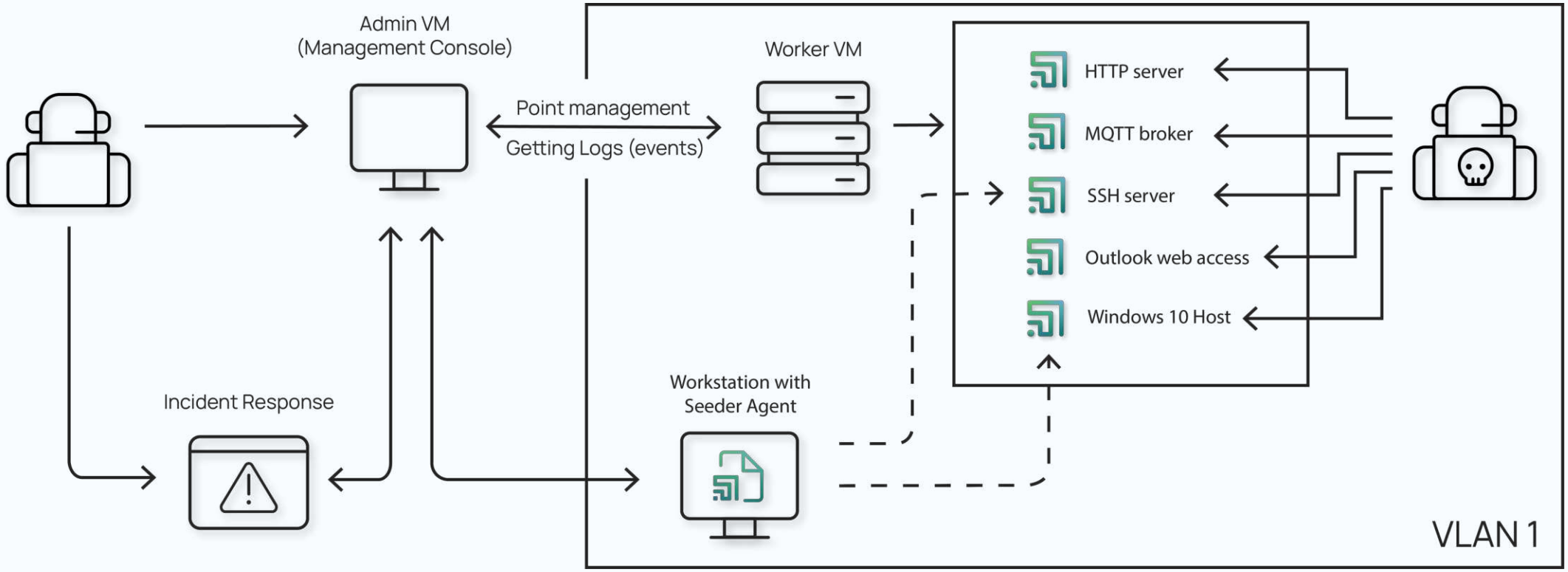
Deception-based threat detection

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.



LABYRINTH

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.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.

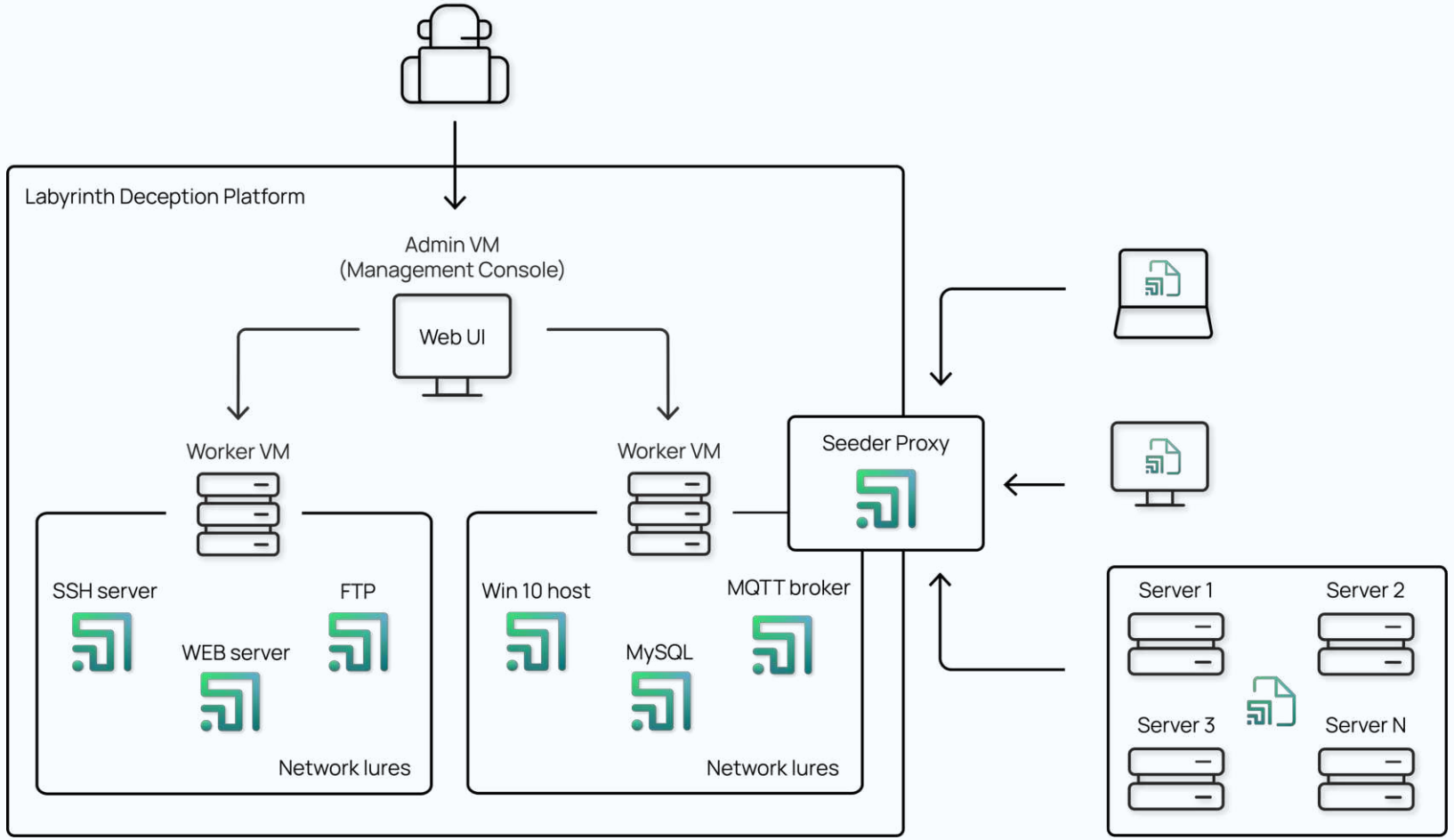
Point

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



Seeder Agent directs the attacker to the Point

Points interact with the attacker and submit warnings to MC

MC notifies the security team and sends metadata for analysis

The security team verifies the data and stops the attack

Points

POINT TYPES | POINT TYPE BASES

Id	Name	Default	Tags	Description
1c	1C8.1	✓	1c,web	1C: Предприятие Web login page
ab_ethp	Allen Bradley Ethernet Processor...	✓	web,scada,ot	Allen Bradley Ethernet Processor SLC-500 (1747-L552/C)
ab_plc	Allen Bradley PLC	✓	web,scada,ot	Allen Bradley PLC CompactLogix 5069-L320
askod	АСКОД WEB	✓	askod,web	АСКОД WEB Login page imitation (Ukraine)
clientos	Workstation	✓	workstation,client,desktop	Workstation network activity imitation and MI
dns_bind	DNS server with AXFR	✓	dns	DNS server with AXFR enabled (zone transf
dns_bind_wo_axfr	DNS server (AXFR disabled)	✓	dns	DNS server with AXFR disabled (zone transf

Points provide services tailored to various sectors, ranging from Basic IT to OT and IoT.

Point config

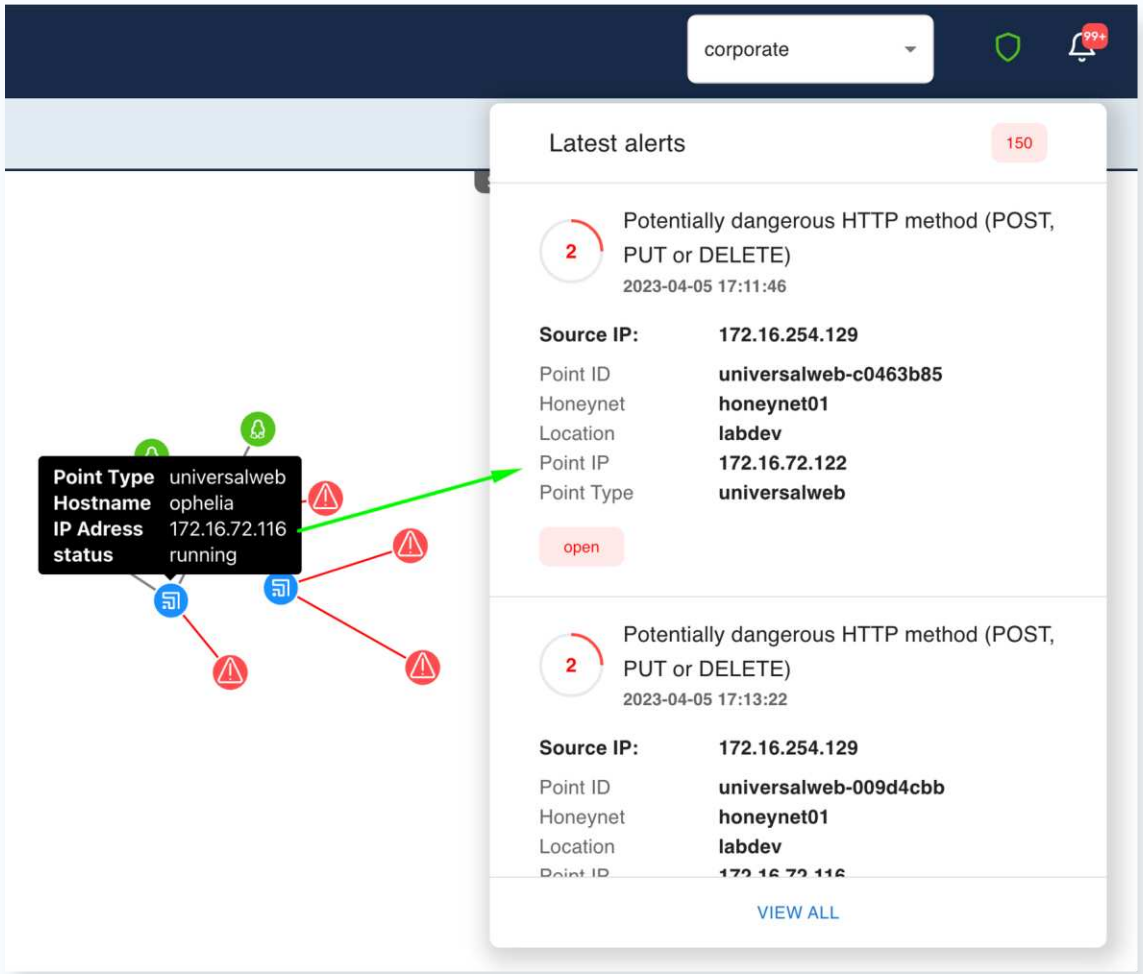
```
## Option: hostname
## Required: no
## Description: hostname value is short domain name or Fully Qualified Domain Name of the Point host.
##              This option may be omitted. In this case hostname value will be generate for each instance of a Point:
##                1. from hostnames wordlist which is specified in Point Type configuration
##                2. from hostnames wordlist which is specified in Honeynet configuration.
#
# hostname: my.host.name
#
## Option: fake_ports
## Required: no
## Description: fake_ports are TCP and UDP ports which will be visible to network scanners as filtered ports.
##              Main goal of fake ports is simulation of services which are binds to Point's ports but are filtered by firewall.
##              Actually there is no any service which is listening on fake ports.
##              fake_ports is a list of objects which have tcp and udp properties or just tcp or udp.
##              During generate process for each instance of Point which uses current configuration will be randomly chosen one of fake ports groups.
#
# fake_ports:
```

Each decoy can be easily customized through user-friendly YAML configuration, allowing to adjust solution to your specific needs.

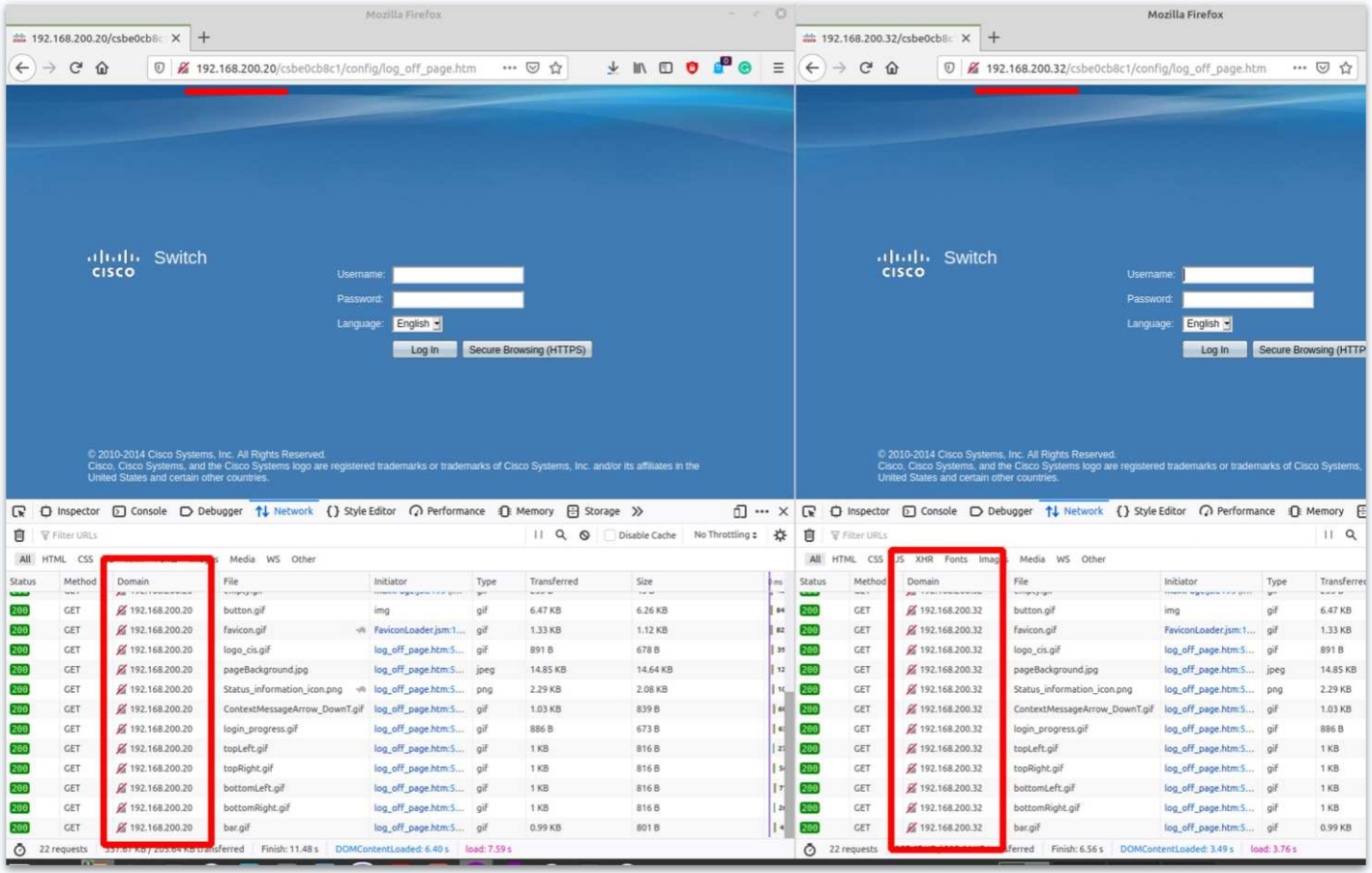
Universal Web Point

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**.

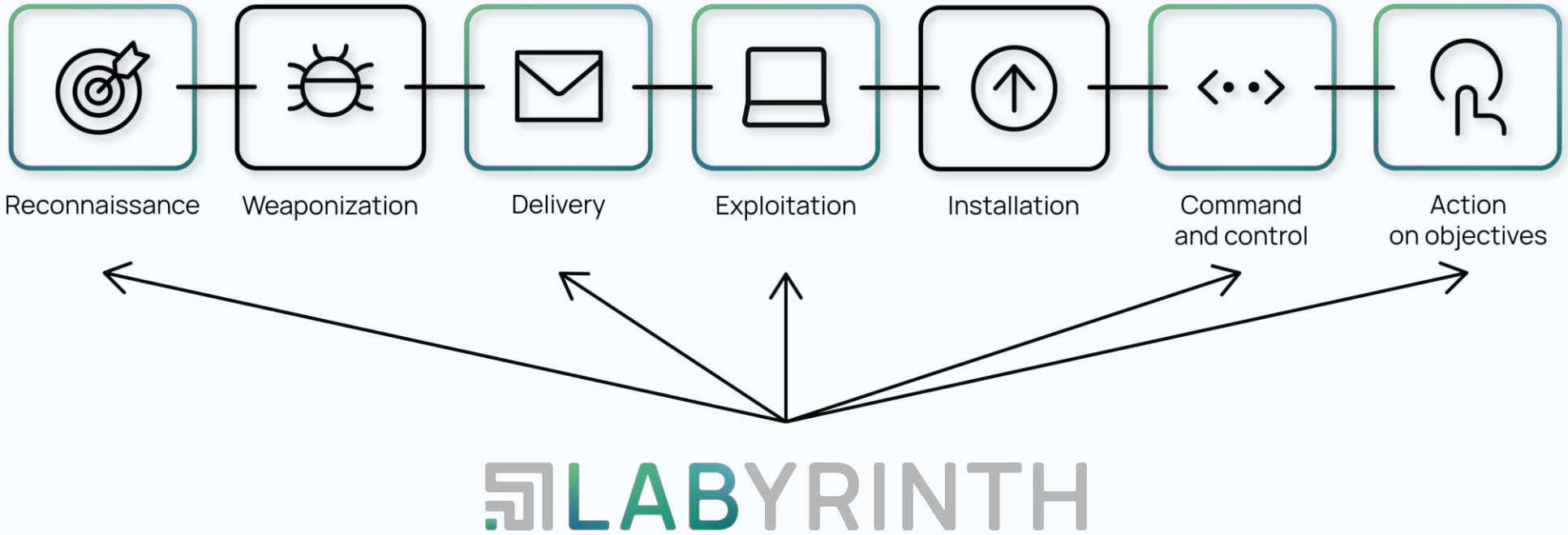


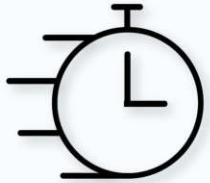
Universal Web Point



Labyrinth generates sophisticated emulations of existing web resources, known as **Universal Web Points** (UWP). These emulations are further enhanced by embedding additional vulnerabilities, making them more enticing targets for attackers.

Use cases





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+Wr6Itfynjpzt+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 '172.16.13
test3.test2@172.16.132.28's password:
test3.test2@tethys:~$ whoami
test3.test2
test3.test2@tethys:~$
```

Severity	Status	Timestamp	Point ID	Attacker IP	Alert Reason
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: **CMD: whoami**
2024-06-02 20:52:37	Hostname: -
2024-06-02 20:52:37	Hostname: - Message: **Terminal Size: 176 50**
2024-06-02 20:52:37	Hostname: - Username: **test3.test2** Message: **login attempt [test3.test2/15061988] succeeded**
2024-06-02 20:52:37	Hostname: - Name: **LC_CTYPE** Message: **request_env: LC_CTYPE=UTF-8**
2024-06-02 20:52:30	Hostname: - Message: **SSH client hassh fingerprint: aae6b9604f6f3356543709a376d7f657**

Use case scenario: network scanning

		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**

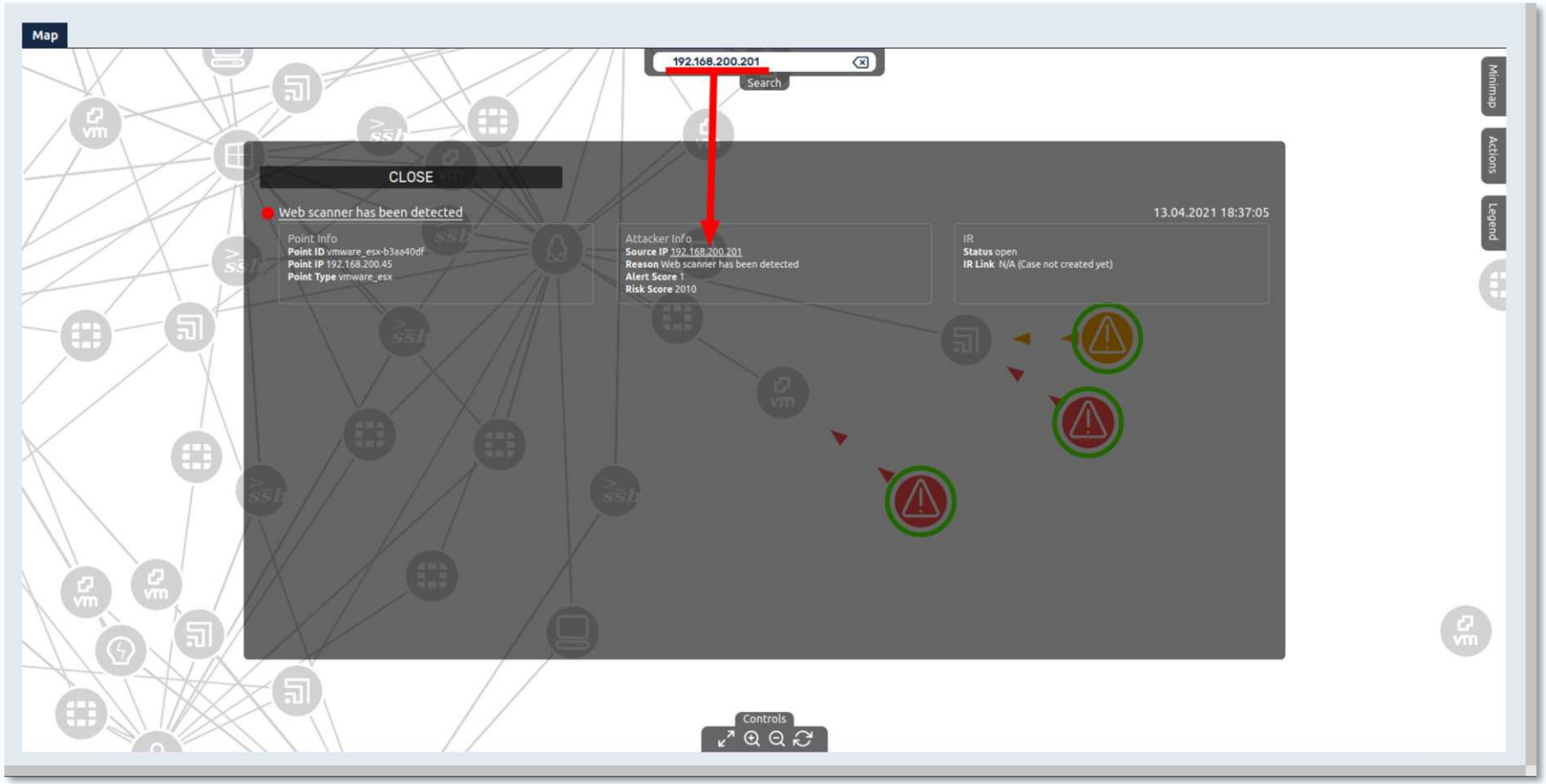
MITRE

Technique	T1595
Tactic	TA0043

```
~ % 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



Use case scenario: detecting MITM

```
└─$ sudo python2 Responder.py -I eth2
                                                    __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-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)

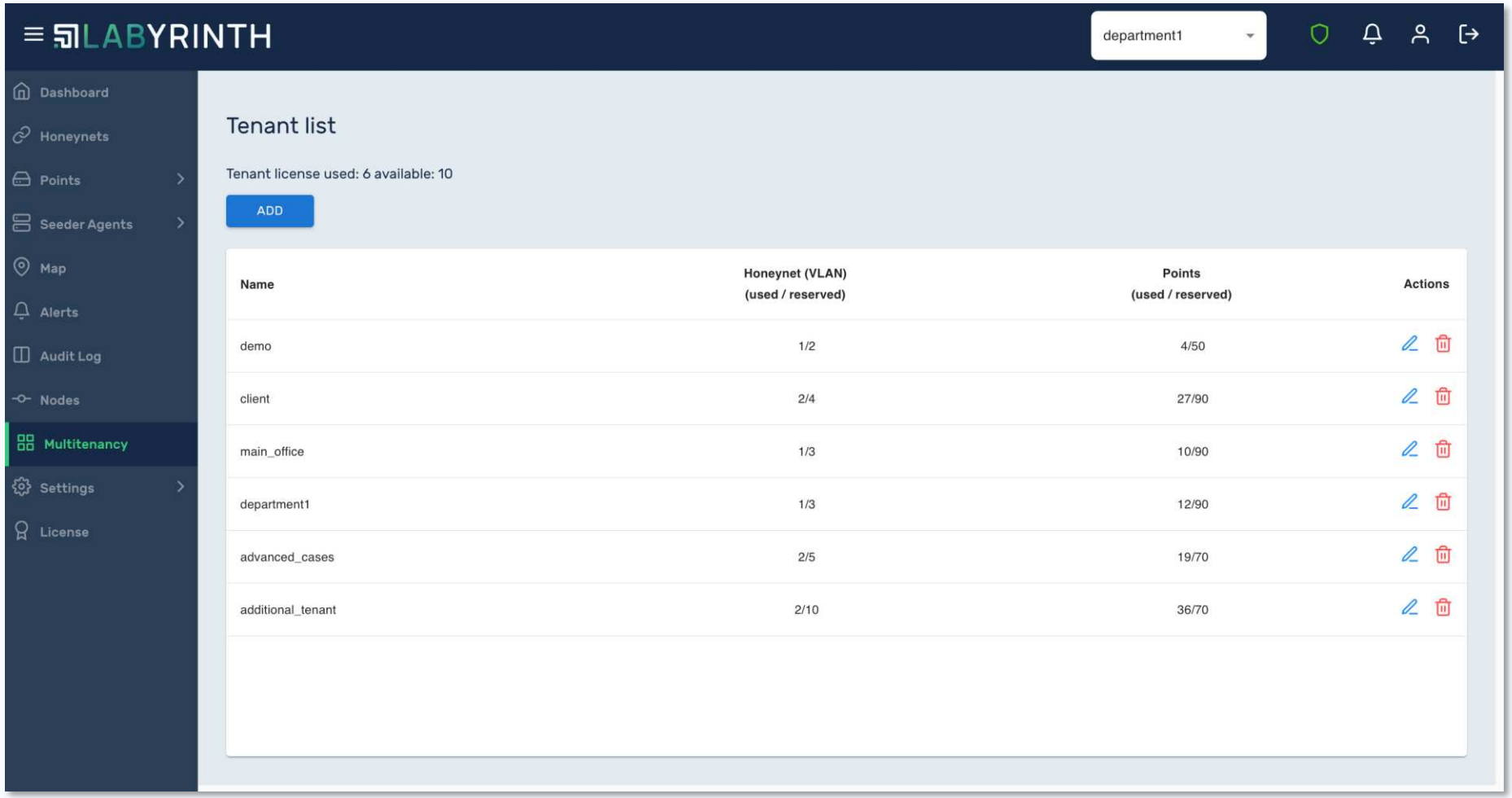
2023-12-28 20:07:58

Alert ID	**7d3a5abc-27d4-4f35-9cbe-14bee90456b1**
Alert Reason	**Responder-like tool responded for NetBIOS request**
Destination IP	**172.16.12.11**

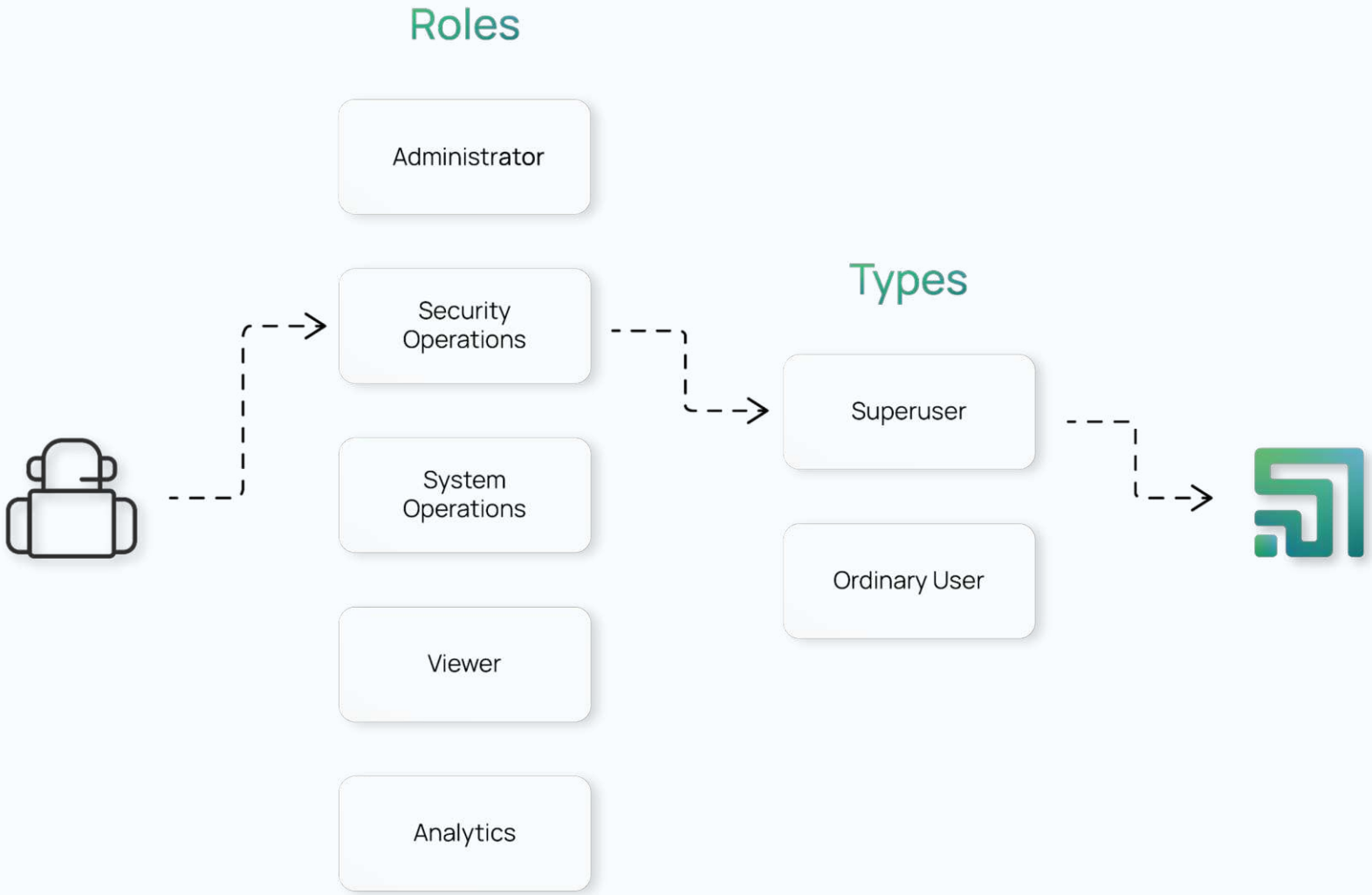
MITRE

Technique	T1557.001
Tactic	TA0006

Multitenancy



RBAC: system users



Integrations

TheHive

CROWDSTRIKE

splunk>

QRadar®

FORTINET®

State	Name	Edit
	CrowdStrike	
	FortiGate	
	Microsoft Teams Notifications	
	IBM QRadar	
	Slack Notification	
	SMTP Notification	
	Splunk	
	SIEM Integration (Syslog forwarder)	
	TheHive	
	Trellix	
	Webhook	

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 `/status` — Get status

Example URI

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

Response `200` Show

Response `401` Show

Response `429` Show

LICENSE

GET `/license` — Get License Info

Example URI

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

Response `200` Show

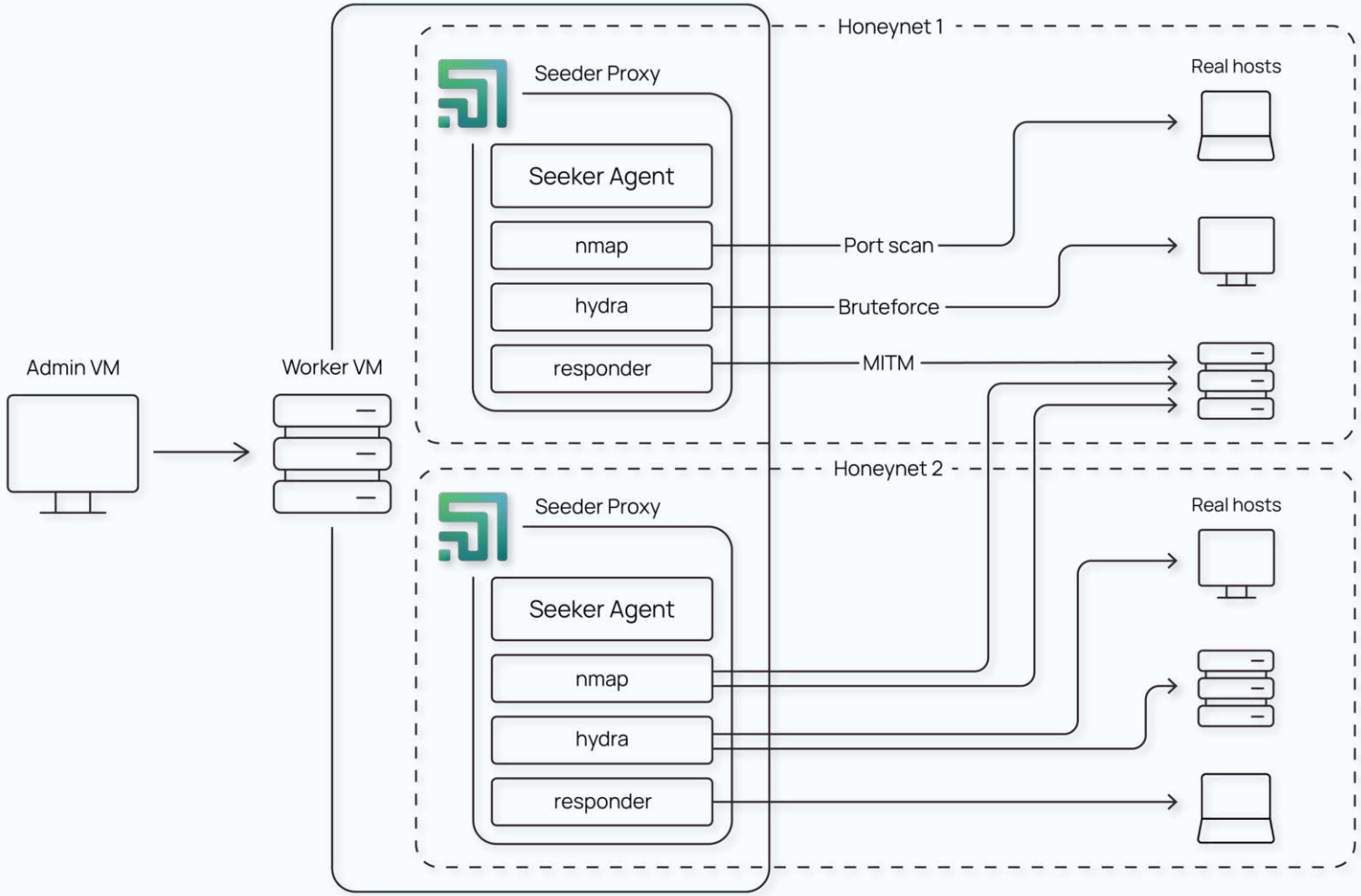
Response `401` Show

Response `429` Show

TENANTS

Back to top

Seeker


Honeynet 1
Seeder Proxy
Seeker Agent
nmap
hydra
responder
Real hosts
Port scan
Bruteforce
MITM
Admin VM
Worker VM
Honeynet 2
Seeder Proxy
Seeker Agent
nmap
hydra
responder
Real hosts

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