

Labyrinth Deception Platform

Labyrinth training program



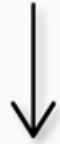
Labyrinth Deception Platform

01: Architecture and Seeders

Labyrinth training program



Deception approaches



Full OS

is based on **deployment within a hypervisor of one or several virtual machines;**



OS/Service emulation

is based on **creation of imitations which recreate certain services or service combinations as separate instances within a single VM;**

What is Labyrinth Deception Platform?

**Saves your time**

Labyrinth provides minimum manual configuration and allows to create 1 decoy as fast as a 100.

High scalability

Labyrinth does not need vast amounts of resources to work effectively.

Cuts operational costs

Does not collect tons of data, not generate false positive alerts, no need for special skills to operate.

Automated IR

Accelerates IR through 3rd party integrations that automate isolation, blocking, and threat hunting.

Stops advanced threats

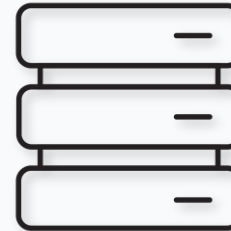
Detects targeted and advanced attacks without requiring any prior knowledge of the threat form, type, or behavior.

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

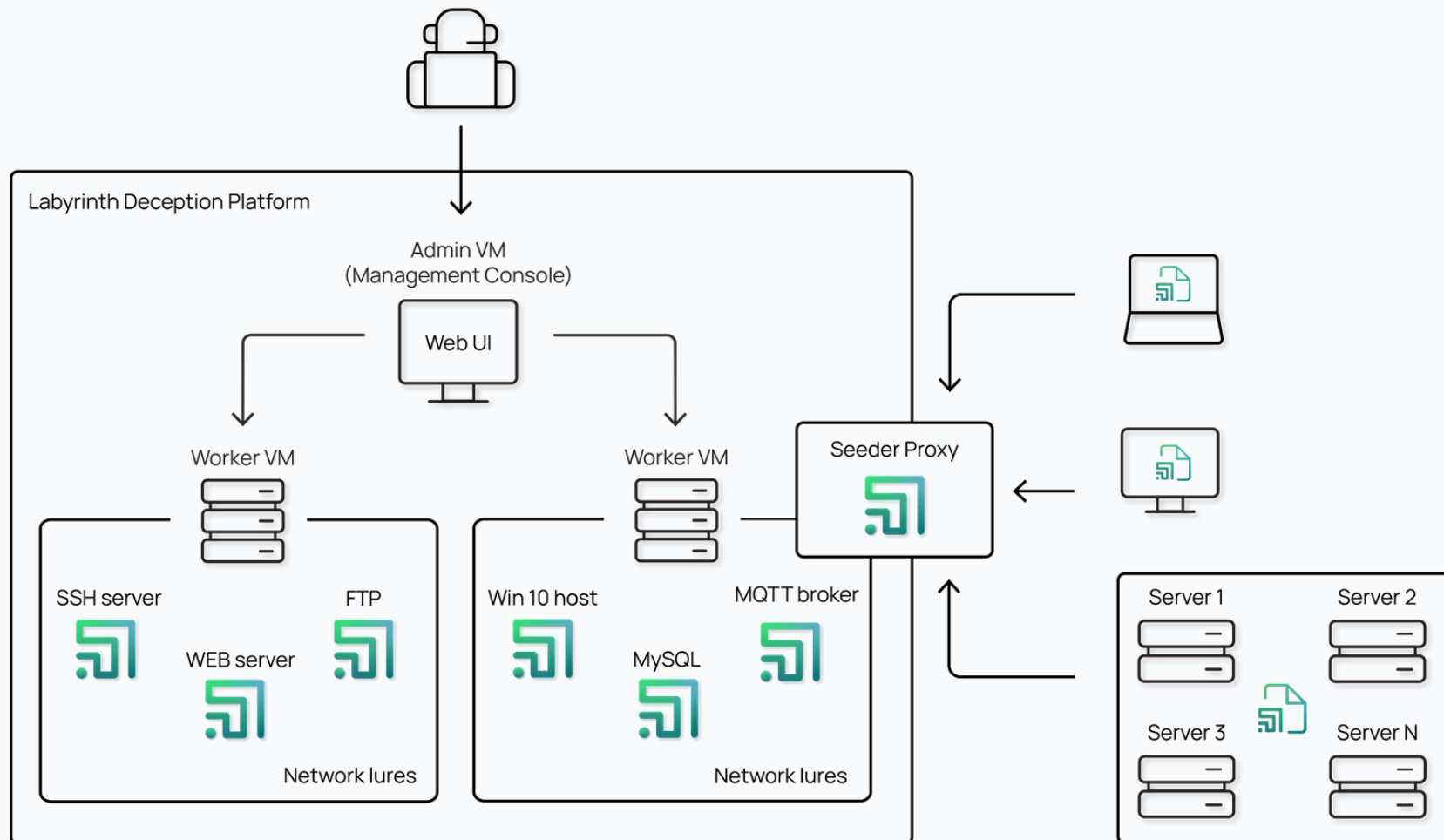
Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.



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.

Architecture



Worker location

Edit

Type: **static**
Id: **honeynet01**
Location: **labtest**
Description: **Test**
Gateway: **172.16.1.254**
Subnet: **172.16.1.0/24**
VLAN ID: **101**

Seeder Proxy:

Seeder Proxy Id:

Seeder Proxy Status:

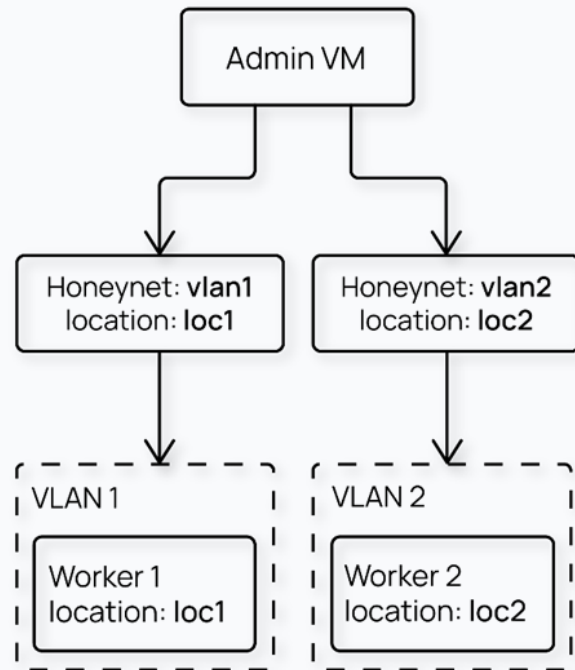
Allowed IP Addresses (CSV):

Nodes

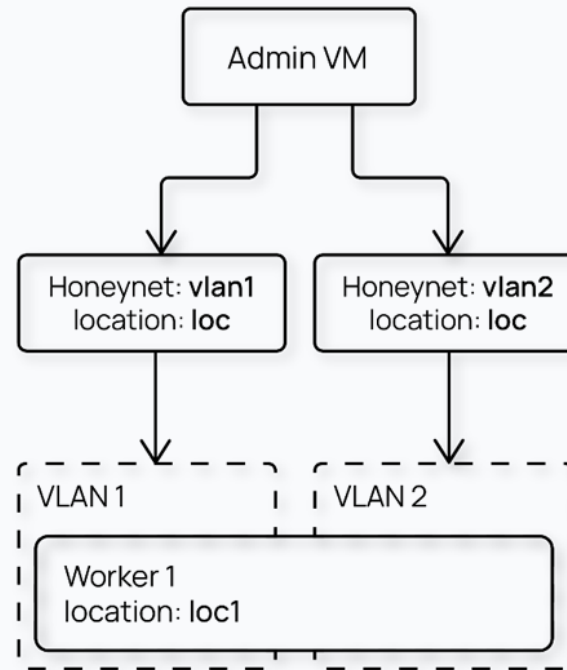
| Hostname | Type | Location | IP Address | Status | |
|-------------|--------|----------|---------------|--------|-------------------|
| worker-demo | worker | labtest | 192.168.200.6 | ready | i |
| admin-demo | admin | | 192.168.200.5 | ready | i |

Deployments: p1

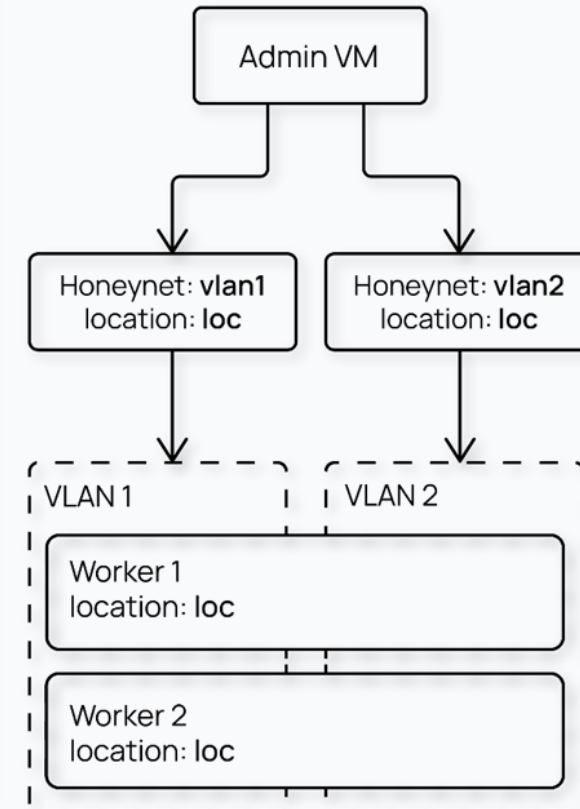
Worker per VLAN



Worker per multiple VLANs

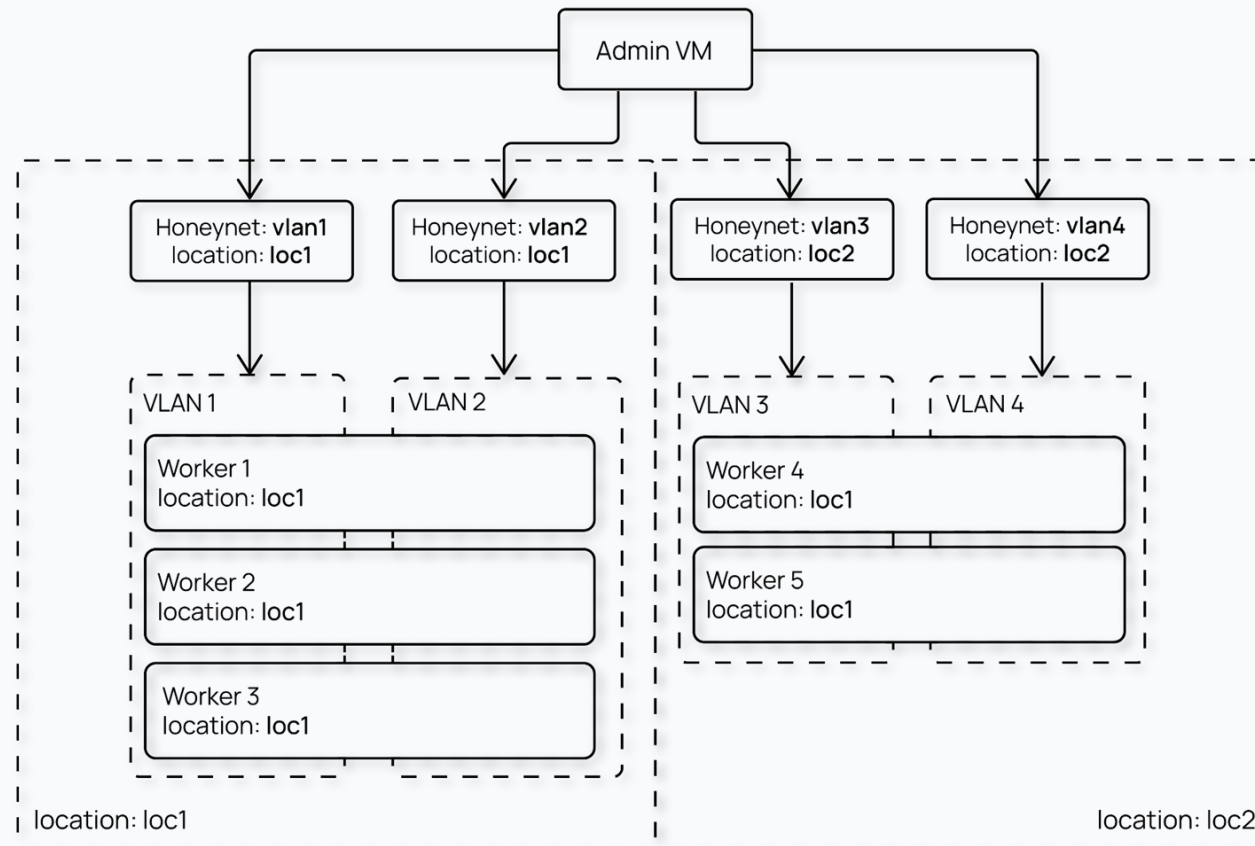


Multiple Worker Nodes per location



Deployments: p2

Multiple honeynet locations










Press to prepare

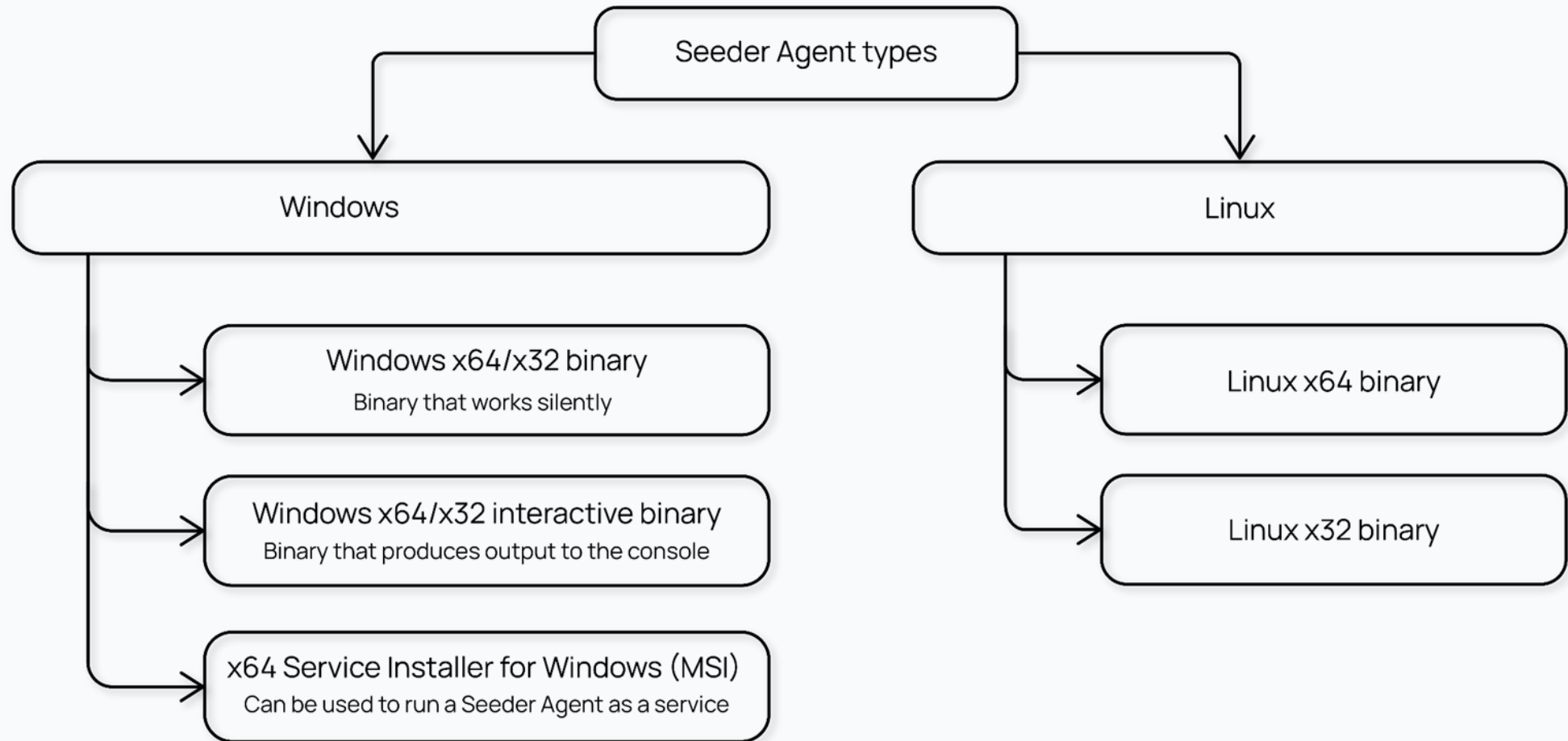
Press to prepare button builds new version of Seeder Agents, adding to the certificates, signed by freshly created CA.

Seeder Agents Download

PRESS TO PREPARE

| OS | Arch | Description | Download |
|---------|-------|--|---|
| windows | amd64 | Windows x64 binary |  |
| windows | 386 | Windows x32 binary |  |
| windows | amd64 | Windows x64 interactive binary |  |
| windows | 386 | Windows x32 interactive binary |  |
| linux | amd64 | Linux x64 binary |  |
| linux | 386 | Linux x32 binary |  |
| windows | amd64 | Seeder Agent x64 Service Installer for Windows (MSI) |  |

Seeder Agents



Seeder Agent usage

Windows:

- MSI:

```
msiexec /i seeder_service_x64.msi SVCPROXY=<Seeder proxy IP>
```

- x32/x64 basic binary:

```
seeder_x64.exe --host <Seeder Proxy IP>
```

- x32/x64 interactive binary:

```
seeder_x64.exe --host <Seeder Proxy IP>
```

Linux:

- x32/x64 binary:

```
./seeder_x64.exe --host <Seeder Proxy IP>
```

```
└─$ ./seeder_x64.bin --help
SYNOPSIS:
  seeder_x64.bin [--help|-h|-?] [--host <string>] [--location <string>]
                [--nolog|-s] [--version|-v] [<args>]

OPTIONS:
  --help|-h|-?           (default: false)

  --host <string>        IP address or Domain name of seeder-proxy (default: "")

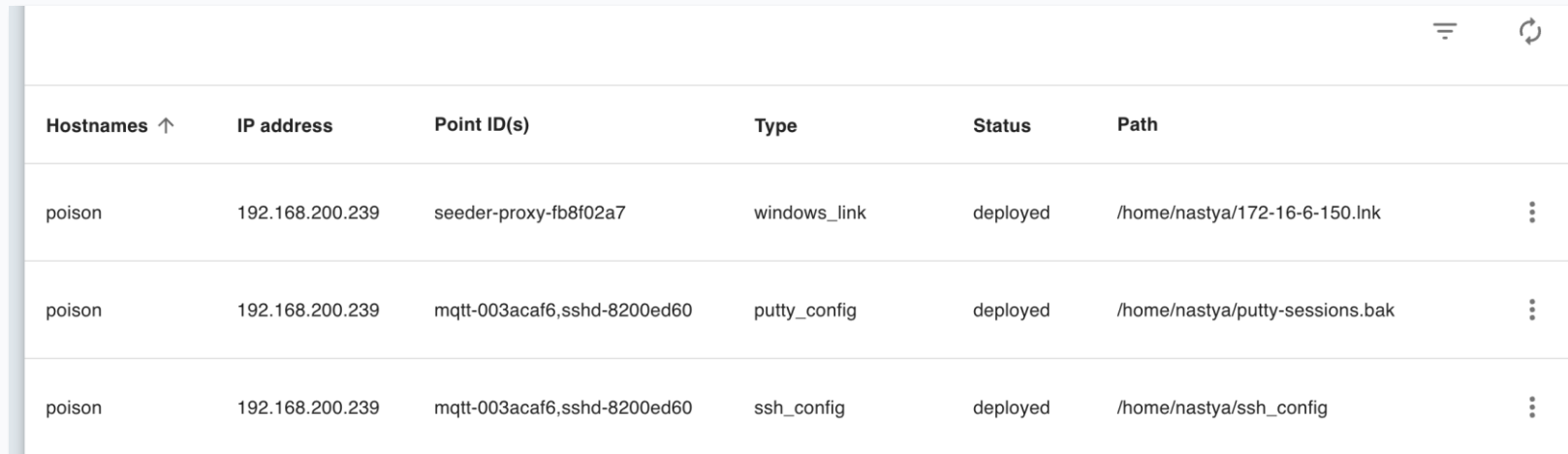
  --location <string>    Agent's location (default: "")

  --nolog|-s            Do not log to Event logging (default: false)

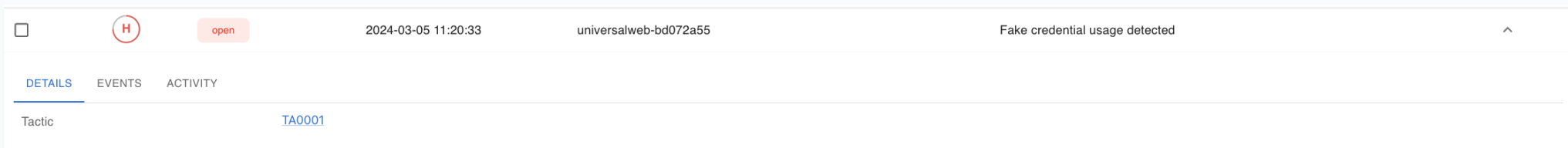
  --version|-v          Show Agent's version and exit (default: false)
```

Seeder Tasks

Seeder Tasks are extremely useful in combination with two-way integration with Splunk or IBM Qradar.



| Hostnames ↑ | IP address | Point ID(s) | Type | Status | Path | |
|-------------|-----------------|-----------------------------|--------------|----------|---------------------------------|---|
| poison | 192.168.200.239 | seeder-proxy-fb8f02a7 | windows_link | deployed | /home/nastya/172-16-6-150.lnk | ⋮ |
| poison | 192.168.200.239 | mqtt-003acaf6,sshd-8200ed60 | putty_config | deployed | /home/nastya/putty-sessions.bak | ⋮ |
| poison | 192.168.200.239 | mqtt-003acaf6,sshd-8200ed60 | ssh_config | deployed | /home/nastya/ssh_config | ⋮ |



□ (H) open 2024-03-05 11:20:33 universalweb-bd072a55 Fake credential usage detected ^

DETAILS EVENTS ACTIVITY

Tactic [TA0001](#)

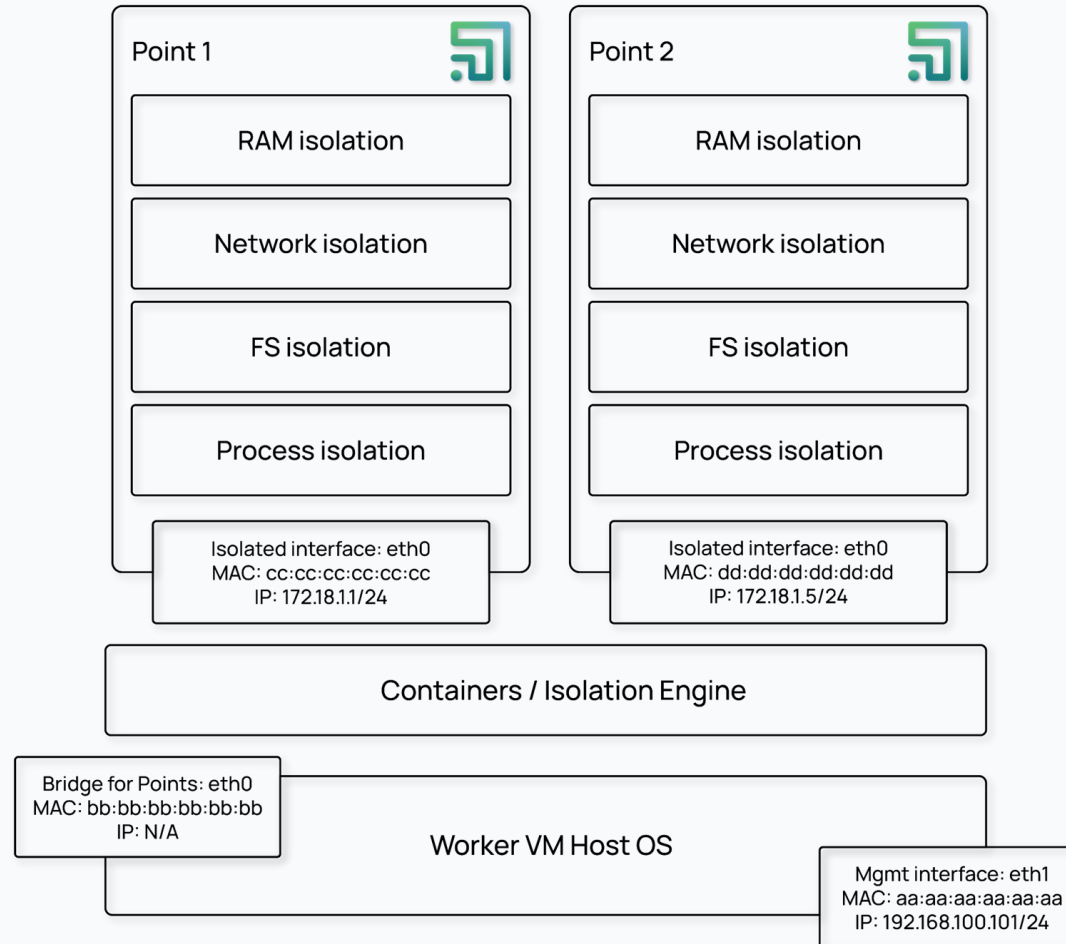
Labyrinth Deception Platform

02 - Points

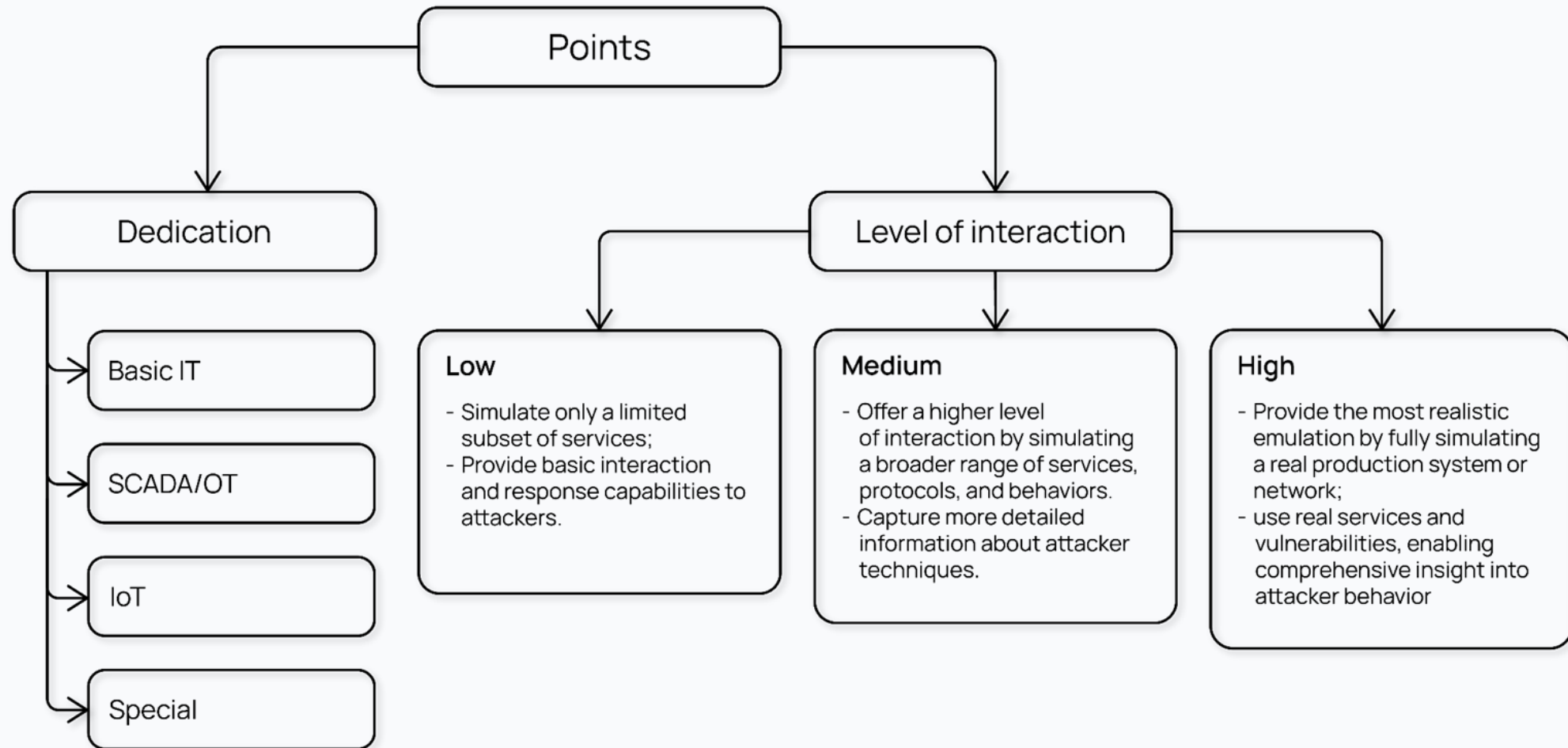
Labyrinth Training Program



What is a Point?

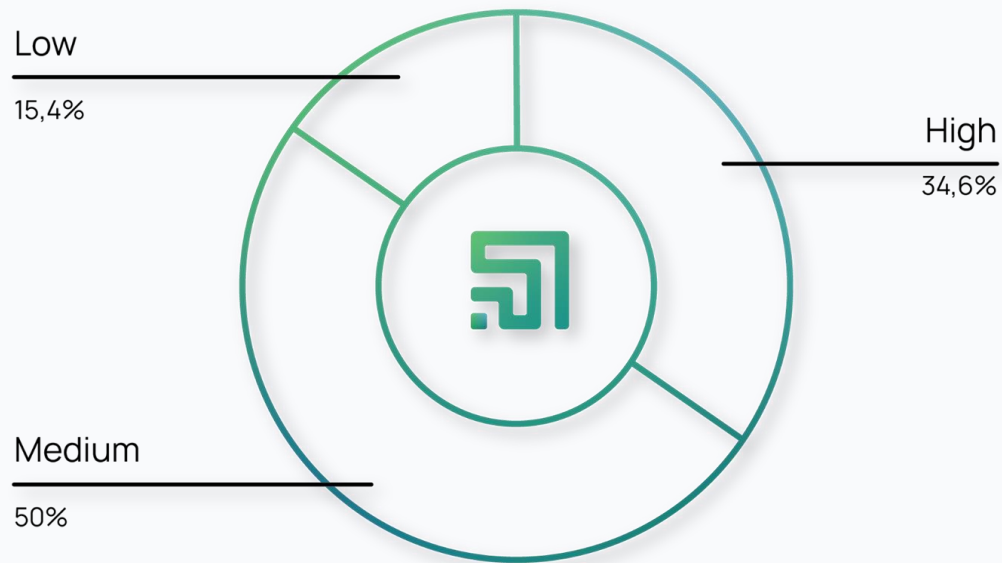


Classification



Some statistics

Distribution of interactivity levels



Distribution of Point dedication sectors



Low interaction Points

- ASKOD WEB
- Allen Bradley Ethernet Processor SLC-500
- Allen Bradley PLC
- Siemens SIMATIC HMI

Latest alerts

611



Port scan detected (TCP SYN, e.g. nmap -sS -T4)
2023-06-29 14:25:20

Source IP: 172.16.254.8
Point ID ab_plc-5ea777b6
HoneyNet ssh_test_4
Location labdev
Point IP 172.16.5.5
Point Type ab_plc

open

The screenshot displays the Allen Bradley Automation web interface for a device. The top navigation bar includes 'Home' and 'Faults (0/0)'. The main content area is divided into several sections:

- General Information:**
 - Device Name: 5069-L320ER/A
 - Project Name: Factory 1
 - Device Description:
 - Device Location:
 - Product Revision: 32.012
 - Firmware Version Date: May 13 2019, 22:48:39
 - Serial Number:
 - Uptime: 218 days, 16h:45m:33s
 - Port A1/A2 Ethernet Address (MAC): 02:42:ac:10:05:05
 - Port A1/A2 IP Address: 172.16.5.5
- Controller Diagnostics:**
 - Keyswitch Position: Remote
 - Controller Mode: Run
 - Change Detection Audit Value: 16#84D2_46A7_F3A7_CFB4
 - I/O Forces: Disabled - None Installed
 - SFC Forces: Disabled - None Installed
- Status Indicators:**
 - Controller Status: Run (green), Force (grey), SD (grey), OK (green)
 - EtherNet/IP Status: Net A1 (green), Link A1 (grey), Net A2 (black), Link A2 (grey)
 - Factory 1: Link A1 - 1Gb/FULL, Link A2 - 100/FULL
 - Port A1/A2 - 172.16.5.5
 - I/O Fault MCC2 #0204 Unconnected Message Timeout

At the bottom, there is a '4-Character Display Messages' section and a 'Seconds Between Refresh' dropdown set to 3, with a 'Disable Refresh with 0' option.

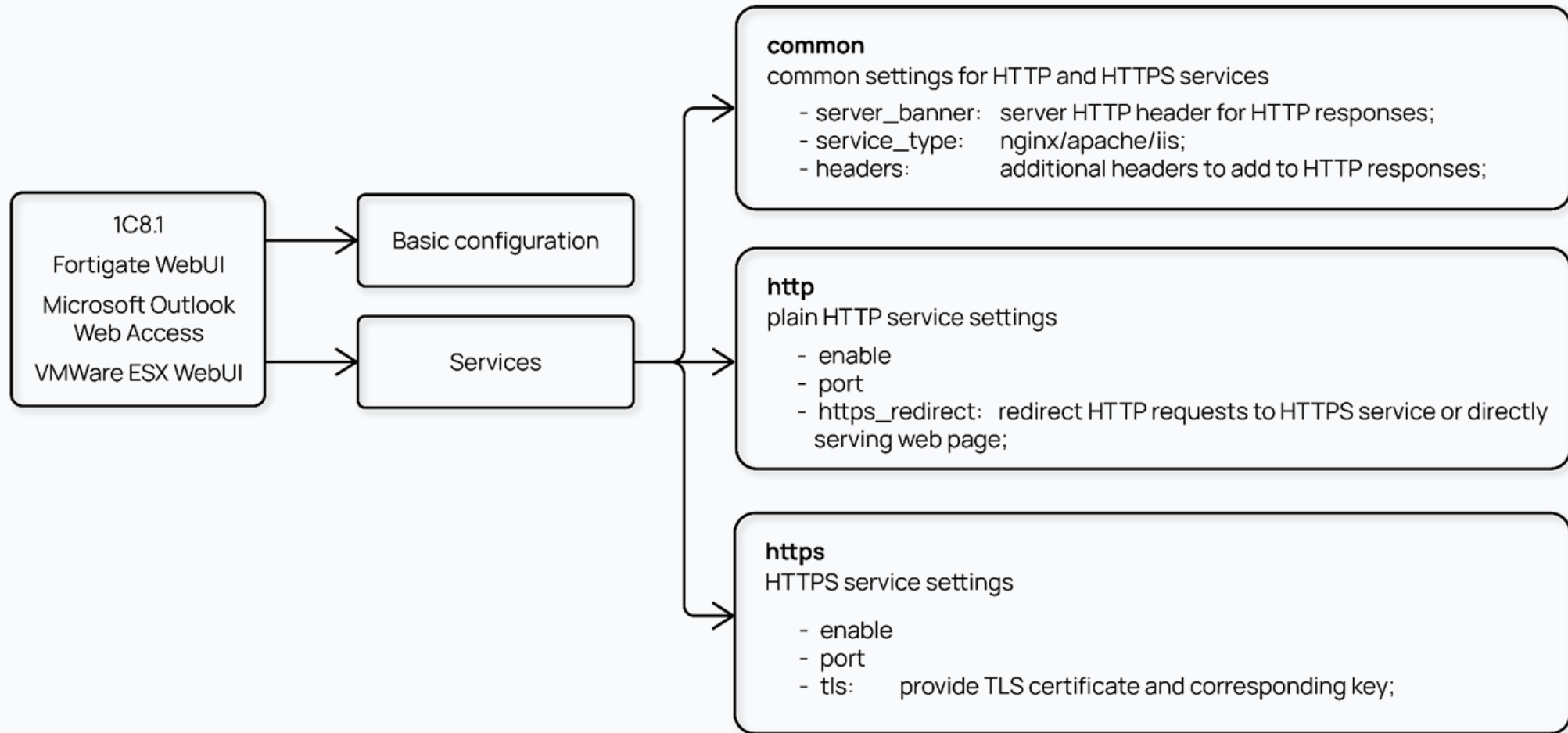
Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved.

Mid interaction

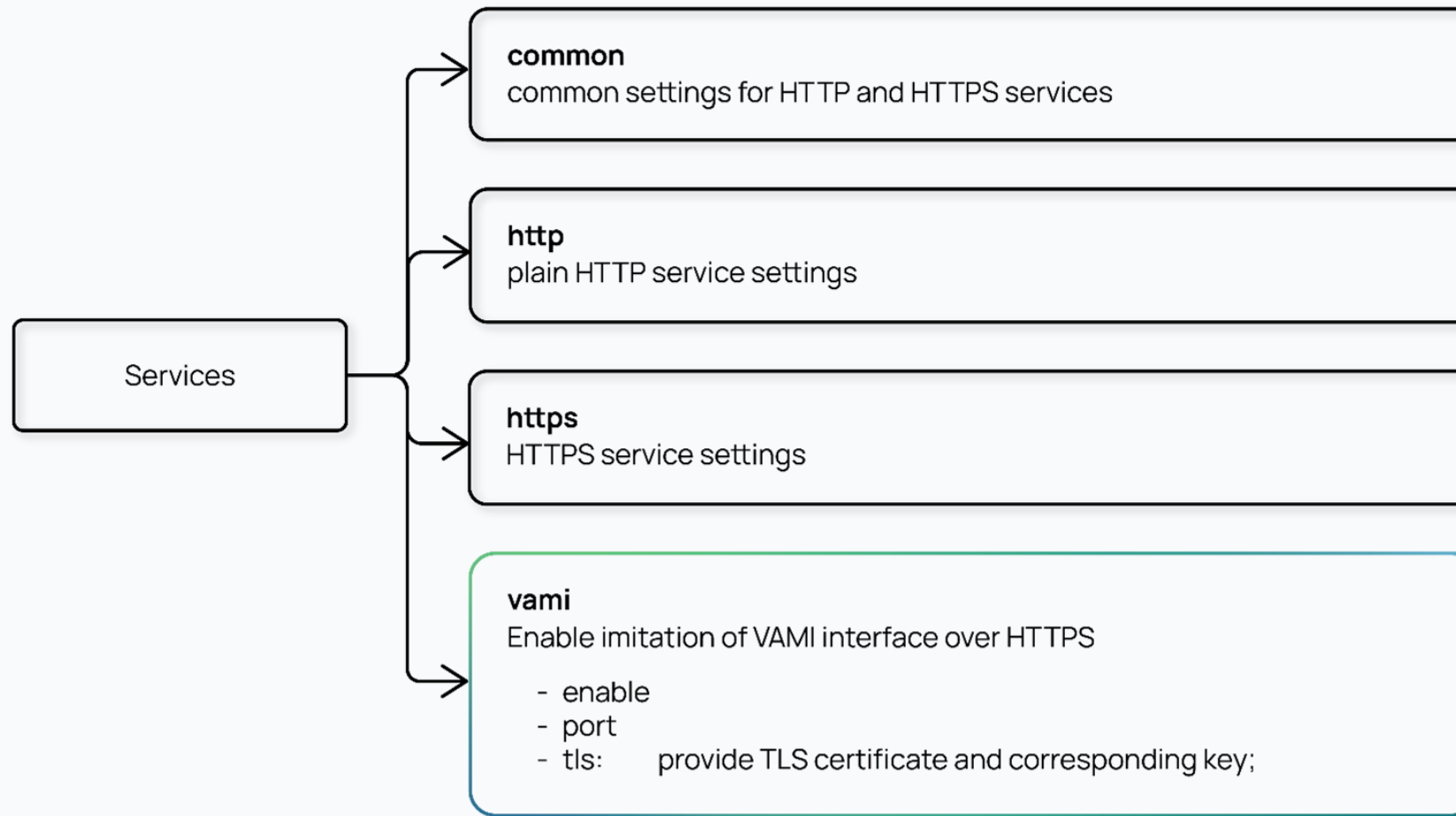
| Basic IT |
|--|
| 1C8.1 |
| Fortigate WebUI |
| Microsoft Outlook Web Access |
| VMWare vCenter Virtual Appliance (log4shell) |
| VMWare ESX WebUI |
| QRadar Server imitation |
| SSH daemon |
| Windows 10 Host |
| Client OS |

| SCADA/OT |
|-----------------------------|
| Modbus server |
| Siemens Simatic PLC S7-1200 |
| Siemens Simatic PLC S7-1500 |
| Siemens Simatic PLC S7-300 |

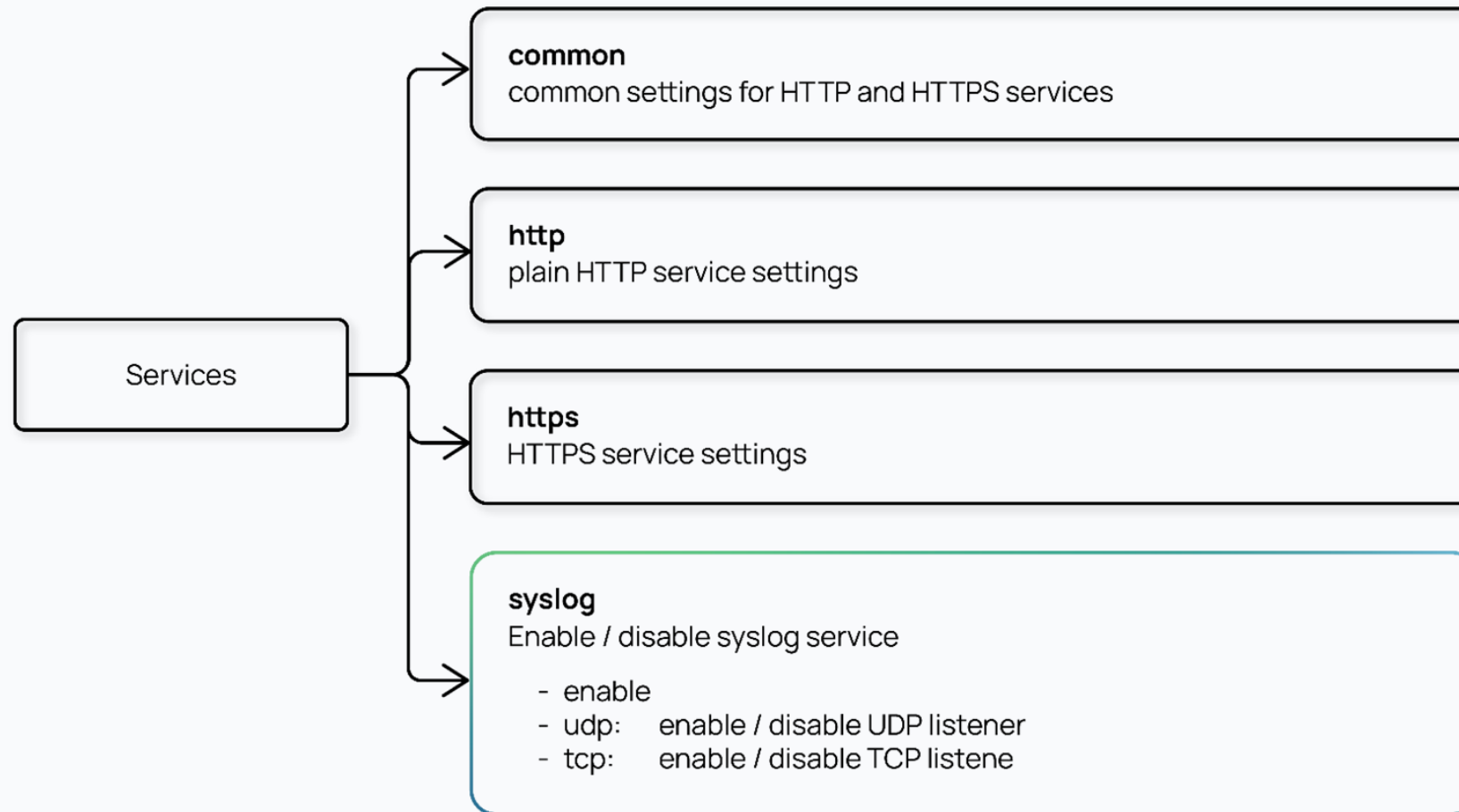
WEB services



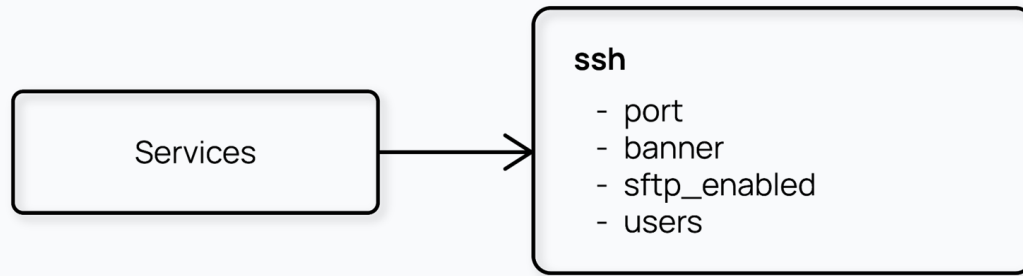
VMware vCenter virtual appliance



QRadar server imitation



SSH daemon



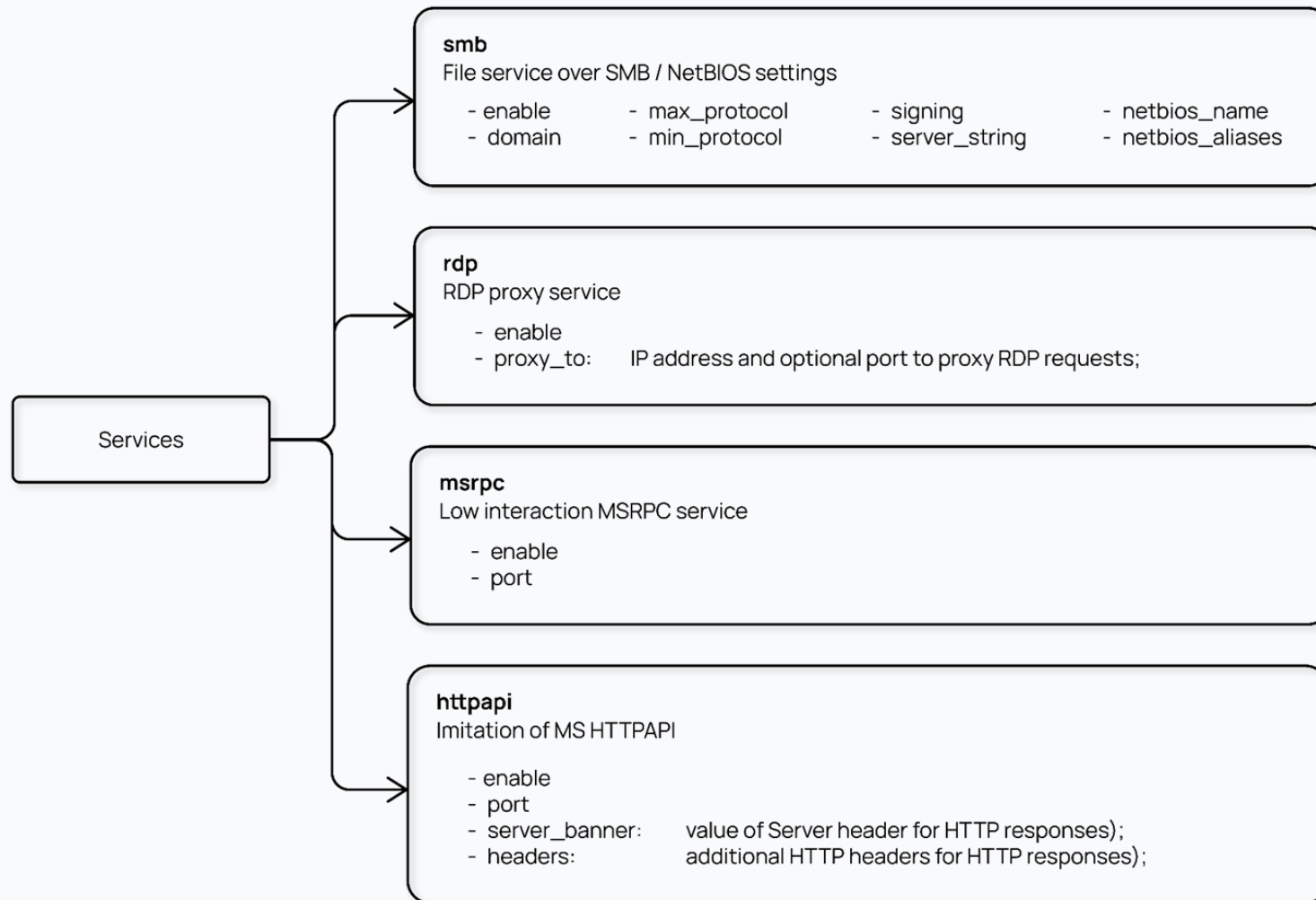
Users field may be one of:

- list of users (identified by `username` and `password` properties);
- or as a number of users to be selected from usernames and passwords wordlists;

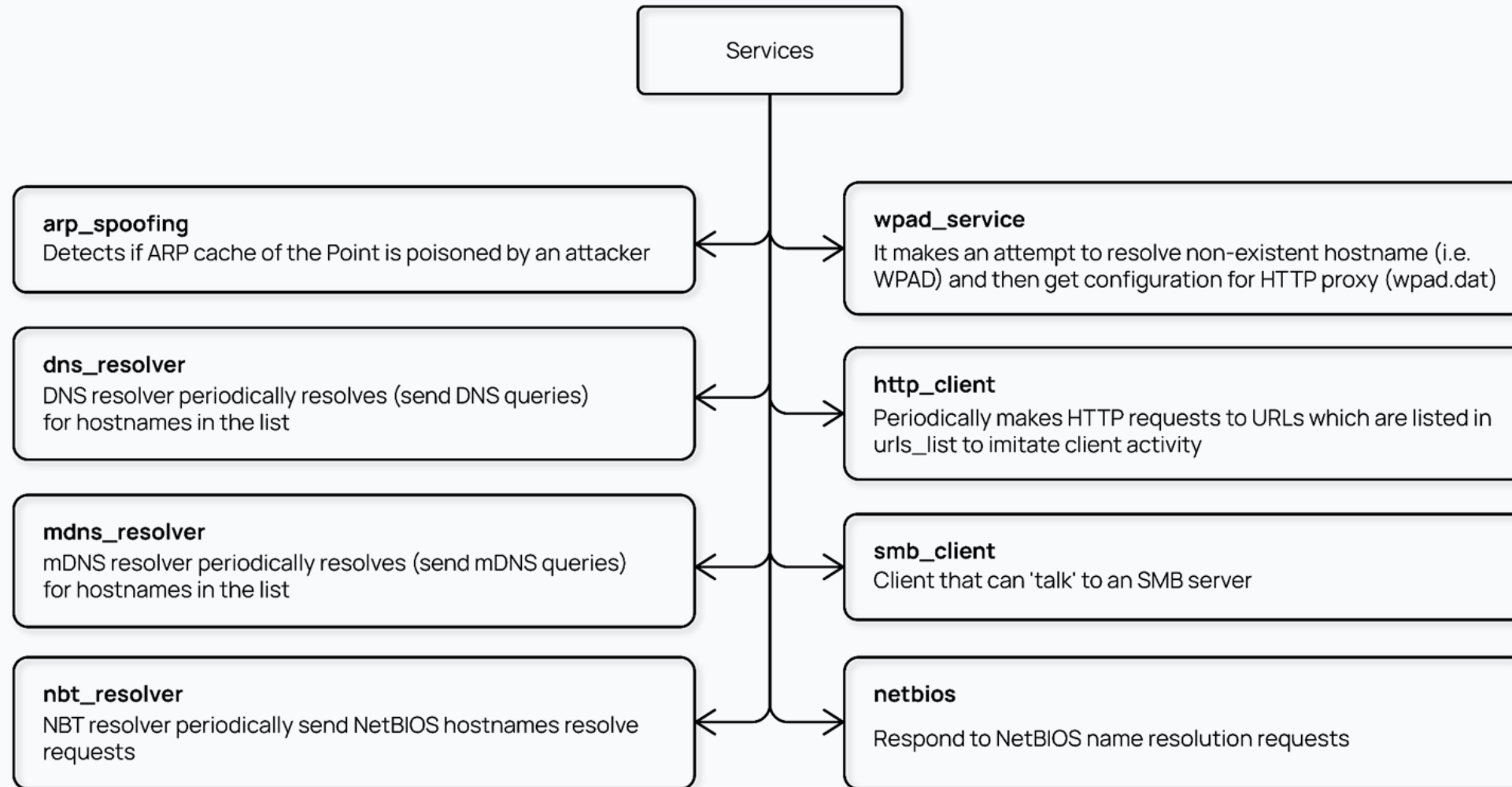
Point config

```
exist. I.e. main Point's service.
48 services:
49     ## Option: ssh
50     ## Required: yes
51     ## Description: configuration for ssh service.
52     ssh:
53         ## Option: port
54         ## Required: yes
55         ## Description: SSH service will bind to provided TCP port.
56         port: 22
57         ## Option: banner
58         ## Required: no
59         ## Description: banner of SSH service which will be provided
60         ## Examples:
61         ## * OpenSSH_8.4p1 Debian-5+deb11u1, OpenSSL 1.1.1n 15 Mar
62         ## * OpenSSH_8.4p1 Debian-5+deb11u1, OpenSSL 1.1.1n
63         banner: SSH-2.0-SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2
64         ##
```

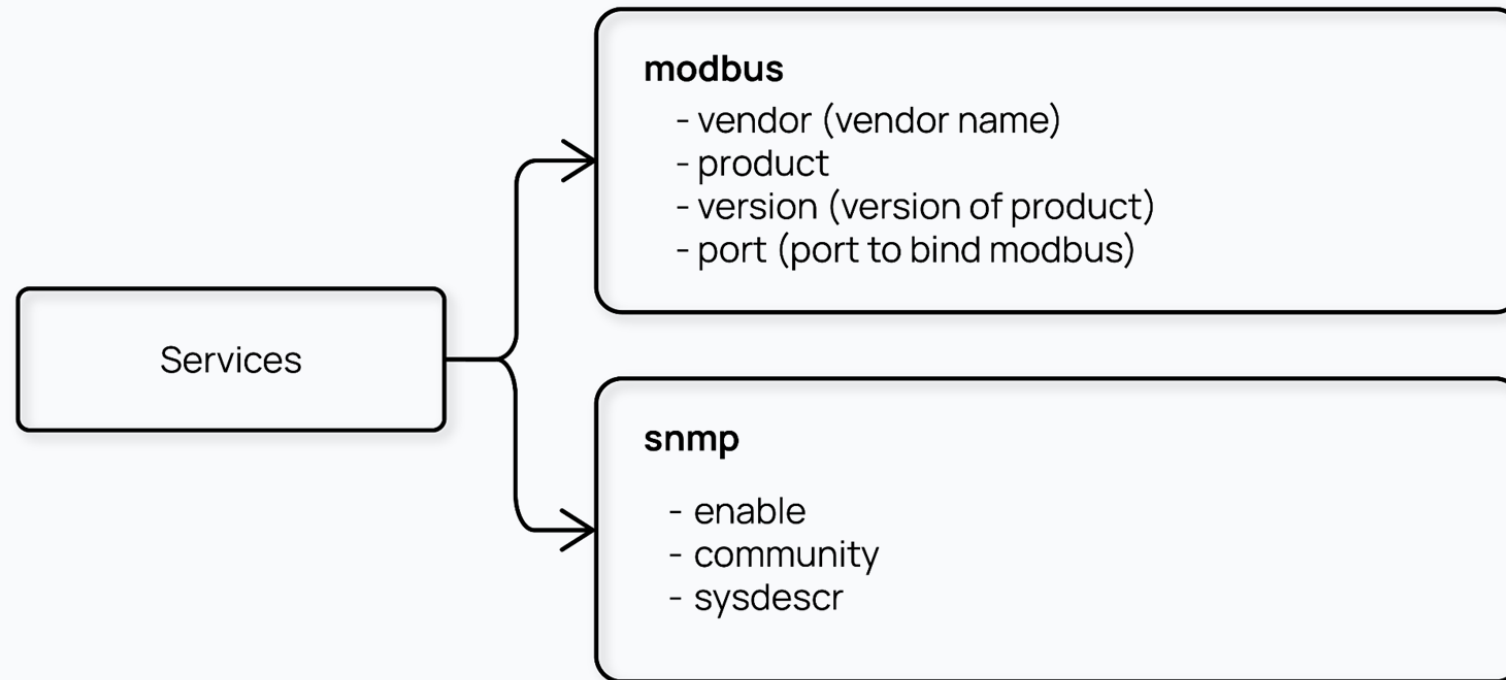
Win10 host



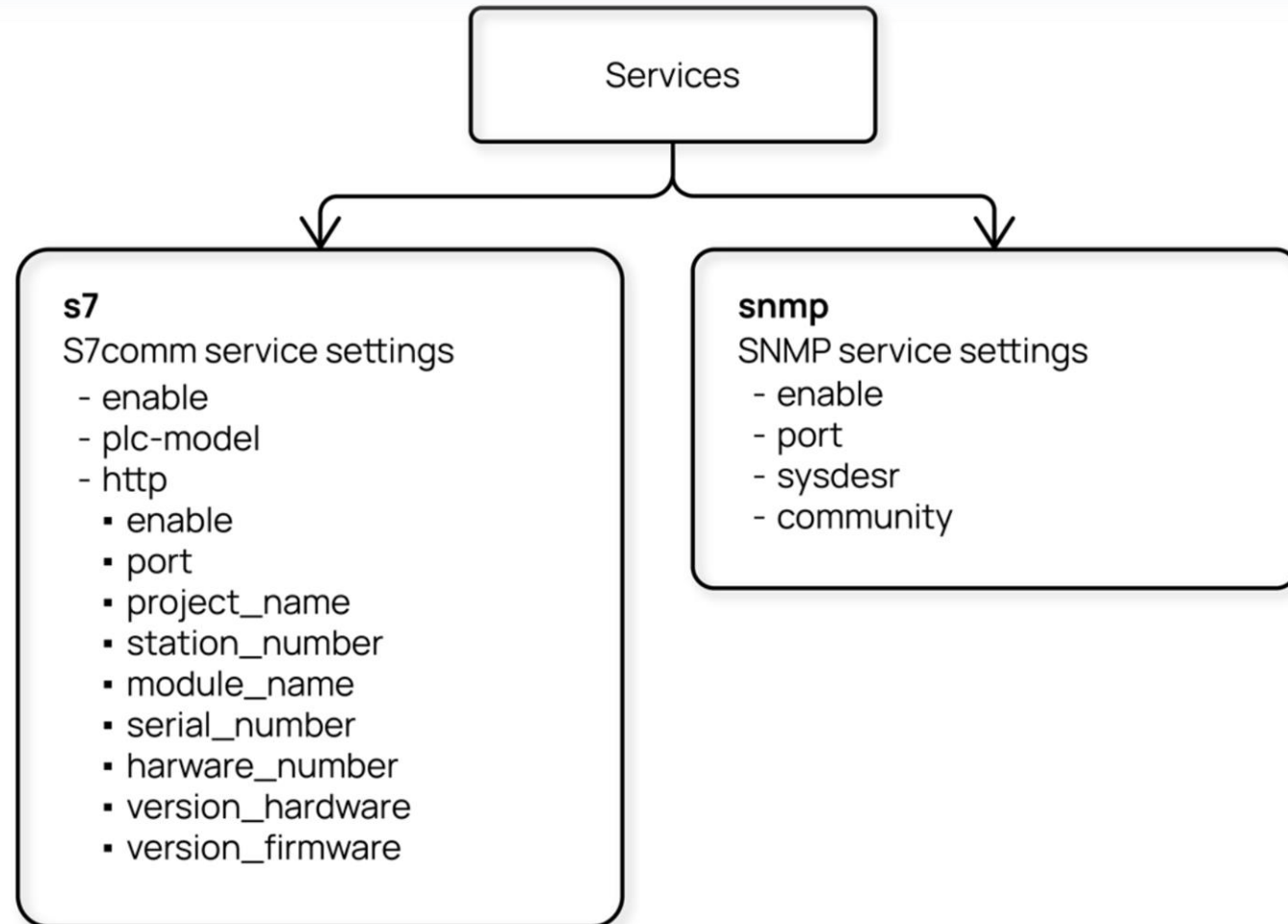
ClientOS



MODBUS server



SIEMENS PLCs



High interaction

- DNS server
- FTP server
- MQTT broker
- MySQL server
- PostgreSQL server
- Samba file server
- Universal Web Point

| Id ↑ | Location | Hostname | Honeynet | IP address |
|-----------------------|----------|----------|----------|--------------|
| dns-fe650cfa | labtest | enid | demo_hn | 172.16.12.13 |
| mqtt-16c3c50e | labtest | patoka | demo_hn | 172.16.12.20 |
| mqtt-4254c339 | labtest | dione | demo_hn | 172.16.12.21 |
| mysqld-6f20c51b | labtest | stump | demo_hn | 172.16.12.16 |
| postgresql-fde41334 | labtest | burke | demo_hn | 172.16.12.35 |
| samba-c9795fde | labtest | sinclair | demo_hn | 172.16.12.14 |
| universalweb-8aeee01c | labtest | galileo | demo_hn | 172.16.12.38 |

DNS server

| | | | | | |
|------------------|-----------------------|---|-----|---|---|
| dns_bind | DNS server with AX... | ✓ | dns | DNS server with AXFR enabled (zone transfer) | ⋮ |
| dns_bind_wo_axfr | DNS server (AXFR ... | ✓ | dns | DNS server with AXFR disabled (zone transfer) | ⋮ |

Services

dns

DNS service configuration

- banner
- port
- axfr_enabled: allow zone transfer requests for all available zones
- zones: list of domain name zones to be served by the Point

MQTT broker

| | | | | | |
|-----------|-----------------------|---|----------------|--|---|
| mqtt | MQTT Broker | ✓ | mqtt,linux,iot | MQTT Broker with anonymous access enabled | ⋮ |
| mqtt-auth | MQTT Broker with a... | ✓ | mqtt,linux,iot | MQTT Broker with anonymous access disabled | ⋮ |

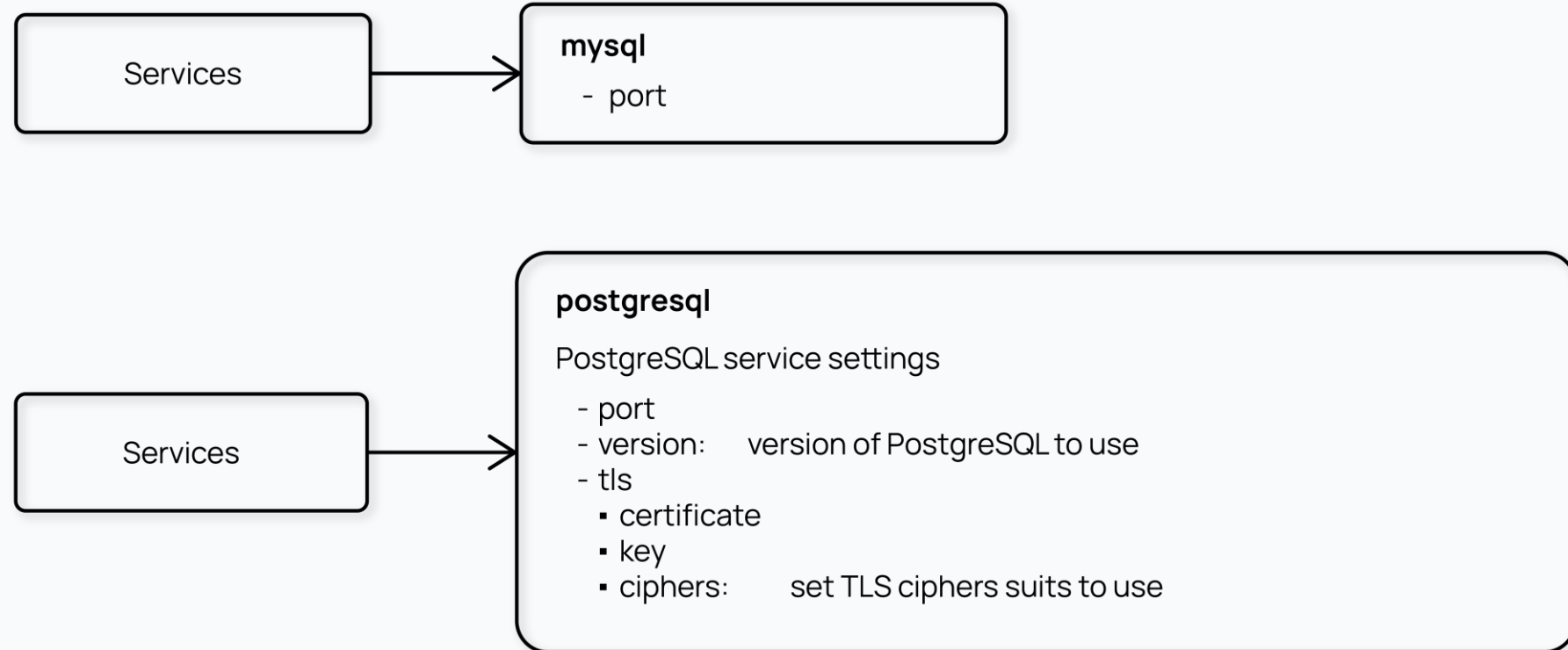
Services

mqtt

MQTT service settings

- port
- enable_auth: enables authentication with user credentials.
- users: allow zone transfer requests for all available zones

MySQL and PostgreSQL



Samba file server

Services



samba

Samba service settings

- netbios_name
- netbios_aliases
- workgroup
- server_string
- max_protocol: maximum supported SMB protocol version
- min_protocol: minimum supported SMB protocol version
- signing
- session_timeout

FTP server

Services

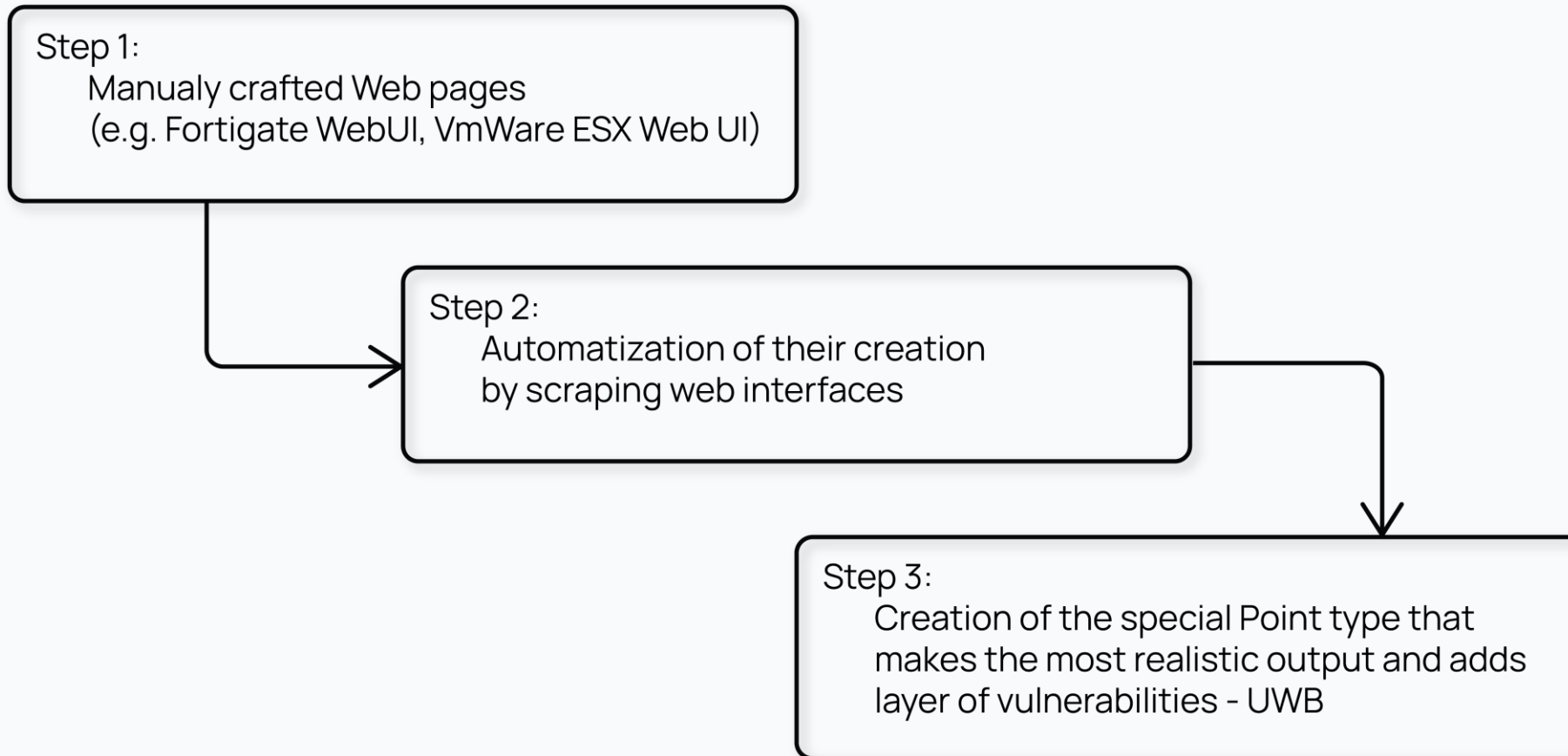


ftp

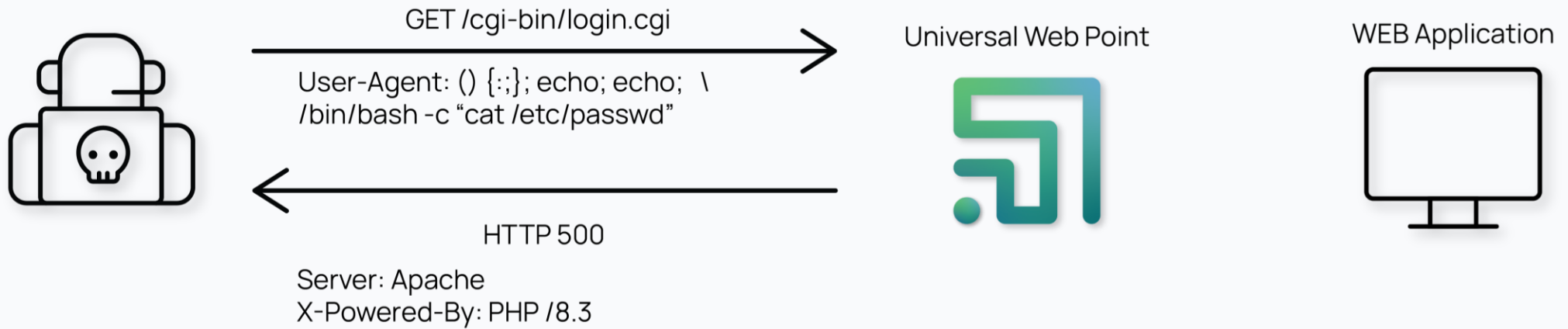
FTP service configuration

- port
- banner
- active_ftp: active FTP settings
 - enable
 - port
- anonymous: enable / disable anonymous access to FTP service
 - allow_upload
 - allow_mkdir
- session_timeout
- allow_recurse_ls: allow / disallow to browse directories recursively
- disable_pasv: disable PASV FTP command
- disable_port: disable PORT FTP command
- commands
- users

WEB deception



Universal Web Point



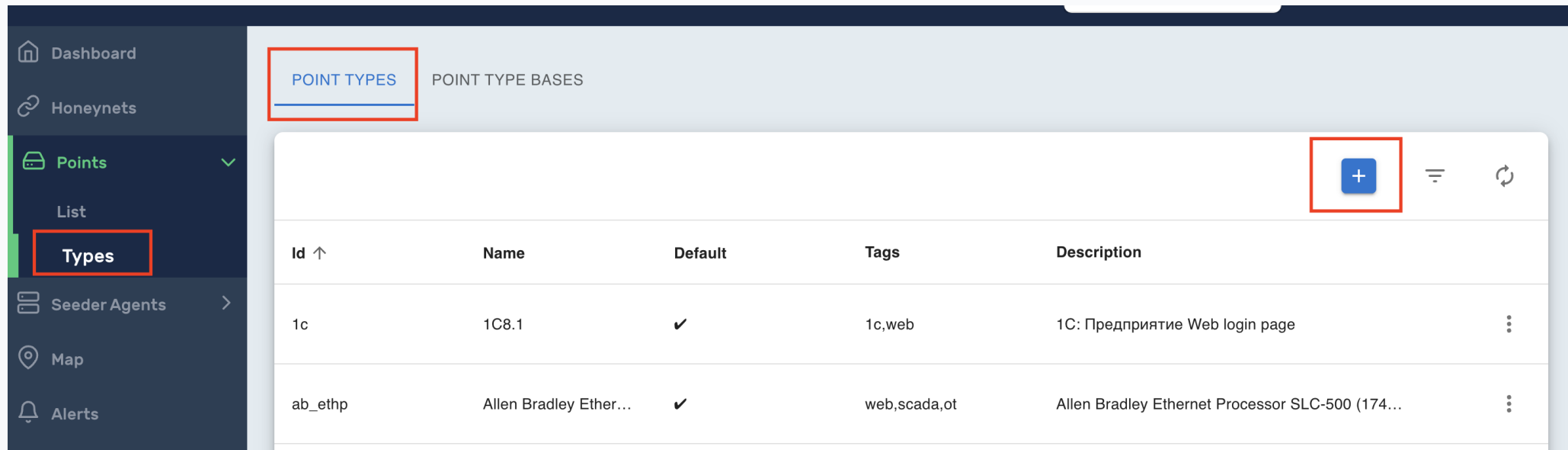
03 - Point customization

Labyrinth Training Program



How to create a new Point type

1. Go to the “Points->Types->Point types”
2. Click on “Add”



The screenshot shows the LABYRINTH interface. On the left sidebar, the 'Points' menu is expanded, and 'Types' is highlighted. The main content area displays 'POINT TYPES' and 'POINT TYPE BASES'. A table lists existing point types, and a blue '+' button is highlighted in the top right corner of the table area, indicating the 'Add' action.

| Id ↑ | Name | Default | Tags | Description |
|---------|------------------------|---------|--------------|--|
| 1c | 1C8.1 | ✓ | 1c,web | 1C: Предприятие Web login page |
| ab_ethp | Allen Bradley Ether... | ✓ | web,scada,ot | Allen Bradley Ethernet Processor SLC-500 (174... |

Configuration pattern

| Options | Required | Description |
|------------------|----------|---|
| Hostnames | No | Hostname value is short domain name or Fully Qualified Domain Name of the Point host. If omitted, hostname value will be generate for each instance of a Point: <ol style="list-style-type: none">1. from hostnames wordlist which is specified in Point Type configuration;2. from hostnames wordlist which is specified in Honeynet configuration. |
| Fake_ports | No | Fake_ports are TCP and UDP ports which will be visible to network scanners as filtered ports. Although main goal is to simulate 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. You may specify fake port group, which will be randomly chosen for each Point of that type. |
| Mac_oui_prefixes | No | Gives an ability to specify preferred MAC address OUI prefixes. The rest of the address is generated in a random manner. |
| Services | Yes | Contains configuration of services which are supported by the Point Type. |

Case 1

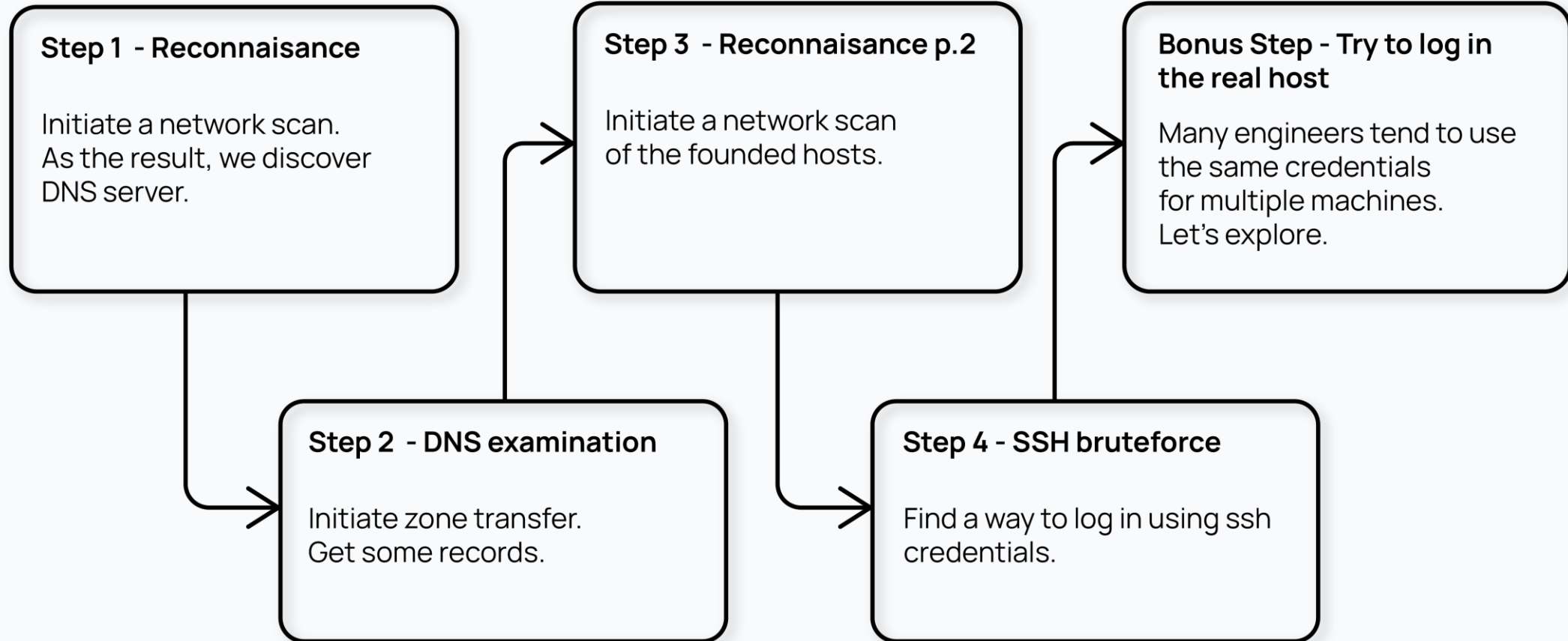
Use DNS as the starting point

Preparation

1. Create a Honeynet with a SSH Point in it
2. Create new DNS Point type with custom records
3. Create another Honeynet with the new DNS Point type

```
Type: dns_ed7
Configuration:
10 - name: tyrell.corp
11   records:
12   - name: ssh1
13     ttl: 300
14     type: A
15     value: 172.16.4.134
16   - name: yours
17     ttl: 300
18     type: CNAME
19     value: ssh
20   - name: ab_ethp
21     ttl: 300
22     type: A
23     value: 172.16.4.138
24   - name: ftp
25     ttl: 300
```

Action plan



Case 2

Use FTP as the starting point

Preparation

1. Create FTP server with disabled anonymous access
2. Put there file that leads to another Point

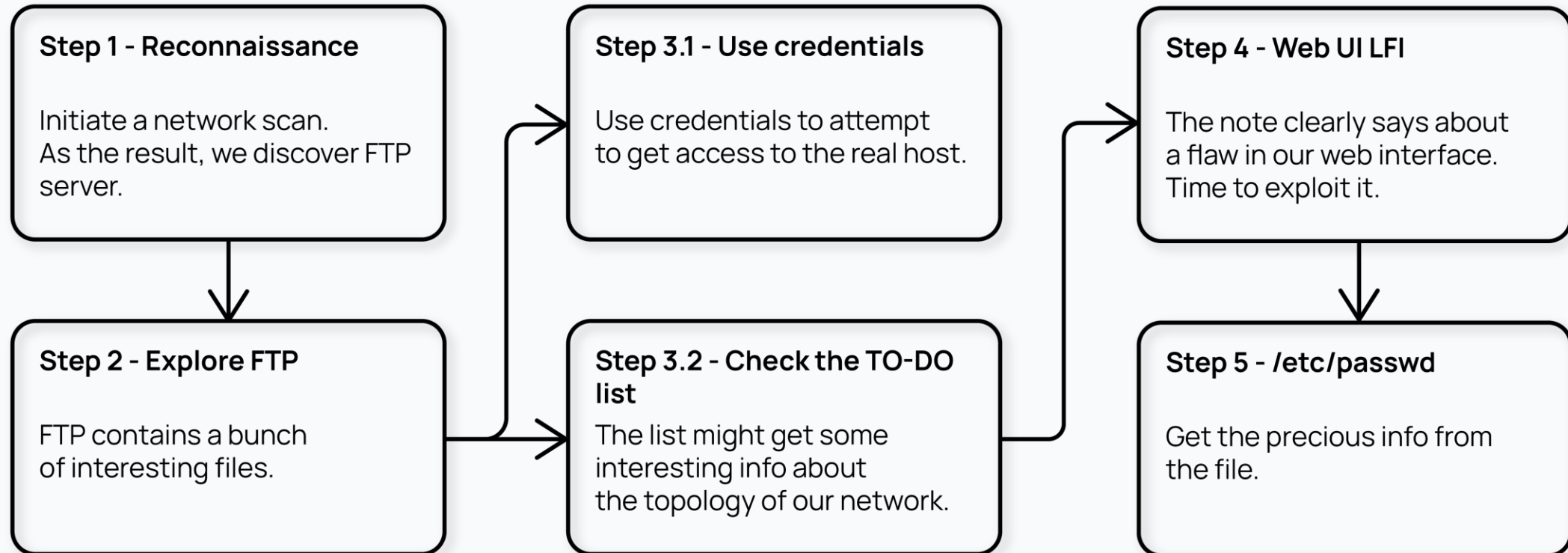
The screenshot displays the Labyrinth web interface. On the left is a dark sidebar with navigation options: Dashboard, Honeynets, Points (selected), List, Types, Seeder Agents, Map, Alerts, Audit Log, Nodes, Multitenancy, Settings, and License. The main content area shows a 'Point info' modal window for a point with ID 'ftpd-07d7f6eb'. The modal lists the following details:

- Id:** ftpd-07d7f6eb
- Location:** office
- Hostname:** fallriver
- Honeynet:** basic_hon
- IP address:** 172.16.4.140
- MAC address:** b4:7a:f1:20:cd:7b
- Status:** running
- Type:** ftp_ed7
- Configuration:** A code block showing the configuration for the ftp_ed7 type, including settings for anonymous access (disabled), banner, port, session timeout, and a list of users with their passwords.

```
15     enable: false
16     banner: Tyrell Corporation
17     disable_pasv: false
18     disable_port: false
19     port: 21
20     session_timeout: 200
21     users:
22     - password: welcome
23       username: rachael
24     - password: iloveyou
25       username: elder
26     - password: '12345678'
27       username: mariette
28     - password: '1234567'
29       username: decker
```

In the background, a table lists various point types: ab_plc, dns_ed7, fortigate, ftp_ed7, modbus, and modbus.

Action plan























04 – Integrations and API

Labyrinth Training Program



Integrations: overview

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

Classification



| Type | Integration name |
|--|-------------------------------------|
| Integrations that perform host isolation | CrowdStrike |
| | FortiGate |
| Two-way integration | Splunk |
| | IBM QRadar |
| Notifications | Slack |
| | Microsoft Teams |
| | SMTP |
| | Webhook |
| Log forwarding to SIEM | Syslog Forwarder (SIEM integration) |
| IR platforms | The Hive |

Labyrinth Deception Platform YouTube

<https://www.youtube.com/@labyrinthdeceptionplatform7278>

CrowdStrike



CrowdStrike Edit

* Denotes required field

State

API Host

Client ID *

API Token *

Network containments/ Isolation

1. Enriching the alert using the data about the attacking host from the system;
2. Isolating the host that appears in the Source IP of the alert (optional).

API Token *

Network containments/ Isolation

FortiGate



Isolates the host that appears in the Source IP of the alert.

YouTube Labyrinth Deception Platform

<https://www.youtube.com/watch?v=nLXkgwzZw4>

FortiGate Edit

* Denotes required field

State

API Host*

https://192.168.200.213

Vdom

Access token*

.....



Host isolation

Verify TLS

Test

Save

Trellix

- Integration with Trellix ePO
- Performs Host isolation based on your policies

Trellix

The screenshot displays the Trellix web interface for managing Policy Assignment Rules. The navigation bar includes 'Dashboards', 'System Tree', 'Queries & Reports', and 'Policy Catalog'. The main content area is titled 'Policy Assignment Rules' and features a 'New Assignment Rule' button. A table lists two rules, with their names and details highlighted by red boxes.

| Priority | Name | Type | Actions |
|----------|---|--------|--|
| 1 | Transfer to isolate group | System | Duplicate Delete Disable |
| | Type: System | | |
| | System Criteria: System descends from: My Organization | | |
| | Tag Criteria: <u>Has tag:</u> <u>isolate_host</u> | | |
| | User Criteria: No user criteria selected | | |
| | Assigned Policies: <u>Endpoint Security Firewall: Firewall > Rules > Block ICMP</u> | | |
| 2 | Release isolated host | System | Duplicate Delete Disable |
| | Type: System | | |
| | System Criteria: System descends from: My Organization | | |
| | Tag Criteria: <u>Does not have tag:</u> <u>isolate_host</u> | | |
| | User Criteria: No user criteria selected | | |
| | Assigned Policies: <u>Endpoint Security Firewall: Firewall > Rules > My Default</u> | | |

Some notes

1. Isolation requirements
2. Custom timeout for FortiGate integration

CrowdStrike Edit

* Denotes required field

State

API Host *

Client ID *

API Token *

Network containments/ Isolation

Expiry

Severity

FortiGate Edit

* Denotes required field

State

API Host *
192.168.200.213

Vdom

Access token *
.....

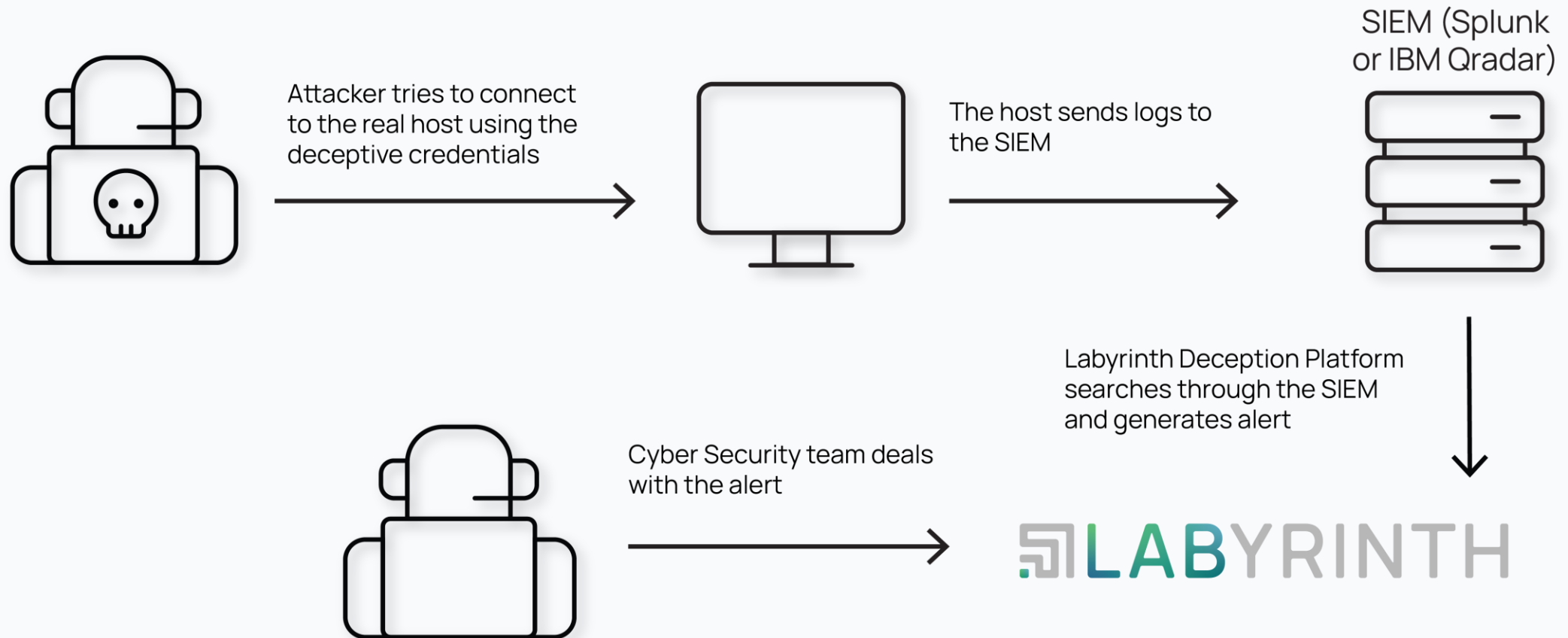
Verify TLS

Host isolation

Expiry

Severity

What is two-way integration?



Splunk



1. Search in the SIEM for attempts to use logins and passwords that are not valid and appear in Seeder Tasks (breadcrumbs), that is, these logins and passwords are used in the configuration of network decoys (Points) and should not be used when trying to log in to real servers.
2. Enrichment of the alert that occurred on Point.

Since Splunk query in the integration setup form is not a query, but a template, these templates support the following template variables:

1. **`\${usernames}`** - a template variable that contains a list of usernames that are part of the Seeder Tasks.
2. **`\${source_ip}`** - IP address of an attacker. It should mostly be used for Alert enrichment.

| <input type="checkbox"/> | Severity | Status | Timestamp | Point ID |
|--------------------------|----------|--------|---------------------|-----------------------|
| <input type="checkbox"/> | H | open | 2024-04-09 13:59:31 | universalweb-bd072a55 |

| DETAILS | | EVENTS | ACTIVITY |
|-----------------|-----------------------|--------|----------|
| Tactic | TA0001 | | |
| Point Info | | | |
| ID | universalweb-bd072a55 | | |
| IP | 172.16.136.6 | | |
| Type | uwp-lab | | |
| Honeynet | honeynet2 | | |
| Hostname | Not set | | |
| Location | demo | | |
| Additional Info | | | |
| Username | test_esxi | | |
| Hostname | 172.16.128.101 | | |

IBM QRadar



- Allows to detect usage of credentials from breadcrumbs

The screenshot shows the IBM QRadar interface for an alert. At the top, there is a header bar with a close button, a red 'H' icon, an 'open' button, the timestamp '2024-04-10 08:46:20', the source 'universalweb-bd072a55', the destination IP '172.16.254.4', and the alert name 'Bad Username'. Below the header, there are three tabs: 'DETAILS' (selected), 'EVENTS', and 'ACTIVITY'. The main content area displays the following information:

| | |
|----------------------------|--------------------------------------|
| 2024-04-10 08:46:20 | |
| Alert ID | 01691856-94c1-4399-a5a0-b16cc0eea46c |
| Alert Reason | Bad Username |
| Destination IP | Not set |
| MITRE | |
| Technique | T1078 |
| Tactic | TA0001 |
| Point Info | |
| ID | universalweb-bd072a55 |
| IP | 172.16.136.6 |

SIEM integration (syslog forwarder)

Test message:

```
> 4/10/24 9:03:20.000 AM Apr 10 09:03:20 192.168.200.231 2024-04-10T06:03:05Z AdminConsole CEF:v2.0.54-18|Labyrinth Technologies|Point|0|LAB_TESTING_ALERT|This is your test message. The parameters are correct.|1|src=192.168.1.2 dst=192.168.1.1 pointType=sshd honeynetID=honeyNet01 location=the_location dvc=192.168.1.1 dvchost=test.host deviceExternalId=sshd-123456 severity=Low cs1=Action has been occurred that fails to be categorised. cs1Label=Description cs2=Investigate surrounding alerts to identify potential source of and attack. Contact support of Labyrinth Technoog ies. cs2Label=Playbook
host = 192.168.200.231 | source = udp:514 | sourcetype = syslog
```

Alerts:

```
> 4/10/24 9:05:48.000 AM Apr 10 09:05:48 192.168.200.231 2024-04-10T06:05:02Z AdminConsole CEF:v2.0.54-18|Labyrinth Technologies|Point|0|LAB_ALERT|Port scan detected (TCP SYN e.g. nmap -sS -T4)|1|src=172.16.254.4 dst=172.16.132.10 pointType=ab_ethp honeynetID=honeyNet3 location=demo dvc=172.16.132.10 dvchost=hermes deviceExternalId=ab_ethp-7949fe95 severity=Low cs3=TA0043 cs3Label=Tactic cs4=T1595 cs4Label=Technique cs1=Port scan on specific Point has been deteced cs1Label=Description cs2=Identify the host of the source IP. Identify the owner of this host. Recommendation: Verify previous activity from Source IP. Continue monitoring Source IP activity. cs2Label=Playbook
host = 192.168.200.231 | source = udp:514 | sourcetype = syslog
```

Audit Log:

```
> 4/10/24 8:58:14.000 AM Apr 10 08:58:14 192.168.200.231 2024-04-10 05:57:59 AdminConsole CEF:0|Labyrinth Technologies|Tenant|0|LAB_AUDIT|change_state_for_integrations|10|src=172.16.254.4 event_type=change_state_for_integrations tenant=additional_tenant username=meow event_status=success
host = 192.168.200.231 | source = udp:514 | sourcetype = syslog
```

Syslog: message fields

1. **Timestamp** - ISO 8601 format (always UTC);
2. **(UTC) AdminConsole CEF:<version>** - always static and indicates Labyrinth version;
3. **Labyrinth Technologies** - vendor, always static;
4. **Point** - Alert info always contains Point keyword;
5. **LAB_ALERT** - indicates that the source is Alerts;
6. **<Alert reason>**;
7. **<Severity in numerical form>** - may be from 0 to 10. 0 Low severity, 10 High Severity;
8. **CEF Extensions:**
 1. CEF Extensions:
 2. src - Source IP address of an attacker;
 3. dst - Destination IP address. In most cases it is the IP address of the attacked Point. In some cases it may differ from Point's for example during outgoing connections attempts.
 4. pointType - Point Type of the attacked Point.
 5. honeynetID - the Honeynet to which the attacked Point belongs.
 6. location - Honeynet location to which the attacked Point belongs.
 7. dvc - actual IP address of the Point / network decoy which has been attacked.
 8. dvchost - hostname of the Point / network decoy
 9. deviceExternalId - unique ID of the Point in Labyrinth.
 10. severity – severity level;
 11. cs1 - details of an Alert / Description
 12. cs2 – recommendations
 13. cs3 - MITRE ATT&CK tactics
 14. cs4 - MITRE ATT&CK techniques

Webhooks

Webhook Edit

* Denotes required field

State

Webhook URL *

<https://webhook.site/673c8887-0f81-4ce8-8d8f-61ac1a63ccef>

Verify TLS


Test

Save

```
{
  "alert": {
    "reason": "DNS Query attempt detected",
    "timestamp": "2024-04-10T06:08:19Z",
    "destination_ip": "172.16.132.12",
    "id": "8e02da3f-fb79-4550-ae3a-12d4384b9eed",
    "source_ip": "172.16.254.4",
    "honeynet": "honeynet3",
    "location": "demo",
    "hostname": "stephano",
    "point_id": "dns-7b3769d4",
    "point_ip": "172.16.132.12",
    "point_type": "dns_bind",
    "severity": "Low",
    "mitre_te": "T1590.002",
    "mitre_ta": "TA0043"
  },
  "link": "https://192.168.200.231/lab/alerts?id=8e02da3f-fb79-4550-ae3a-12d4384b9eed"
}
```

Slack and Microsoft Teams



 **incoming-webhook** APP 9:47 AM

! Potentially dangerous HTTP method (POST, PUT or DELETE)

Timestamp: 2023-10-25T06:47:13Z

Destination IP: 172.16.73.2

ID: 0afafdbc-a540-4ddf-9efa-7865113c6ebd

Source IP: 172.16.254.129

Point Honeynet: test_test

Point Location: labdev

Point Hostname: candlewood

Point ID: 1c-8661929a


Point IP: 172.16.73.2

Point Type: 1c

Mitre te: T1078

Mitre ta: TA0001

[Details](#)

 **Labyrinth Bubble** 6/9, 11:13 AM

Connection to sshd port detected

Source IP: 172.16.254.3

Timestamp: 2023-06-09 11:13:39.907000 (UTC)

Destination IP: 172.16.72.101

ID: 355c6ce6-972f-4904-b67b-60ccf27c7ced

Point Honeynet: honeynet01

Point Location: labdev

Point Hostname: patoka

Point ID: sshd-35570720

[See more](#)

[Details](#)

SMTP



Labyrinth ALERT - Test message Inbox x

[Redacted]

to me ▾

This is your test message. The parameters are correct.

← Reply

→ Forward

Alert: Port scan detected (TCP SYN, e.g. nmap -sS -T4) Inbox x

[Redacted]

to me ▾

Labyrinth Alert

Reason: Port scan detected (TCP SYN, e.g. nmap -sS -T4)

Timestamp: 2023-09-27T10:18:10Z

Destination IP: 172.16.12.31

ID: 100c3379-e352-4ead-9615-cdce25c33145

Point Honeynet: demo_hn

Point Location: labtest

Point Hostname: echo

Point ID: clientos-0a3320e5

Point IP: 172.16.12.31

Point Type: clientos

Mitre te: T1595

Mitre ta: TA0043

Details

REST API

Overview ▼

Resource Group ▼

- Get status ↓
- Get License Info ↓
- List All Tenants ↓
- List All Nodes ↓
- List All Honeynets ↓

Points

- List All Points ↓
- Get Point Details ↓
- Manage Point ✎
- Delete Point ✖

Alerts

- List All Alerts ↓
- Get Alert Details ↓
- Manage Alert ✎

- 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 | | |
| <code>GET</code> | <code>https://your-provider-host.com/api/v1/status</code> | |
| Response 200 | | Show |
| Response 401 | | Show |
| Response 429 | | Show |

LICENSE

MFA

Two-factor authentication

Secure your account with two-factor authentication (2FA).

status: **Disabled**

Enable Two-Factor Authentication



Two-factor authentication



Two-factor authentication gives you an extra layer of security to the account.



Please, check if you already installed an authenticator app on your device and enter your password to continue.

Current Password *



Continue

Roadmap



1. Adding new integrations:
 1. Checkpoint
 2. Integrations with Sandboxes (R&D)
 3. Integrations suggested by the customers
2. Updating the existing ones



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

