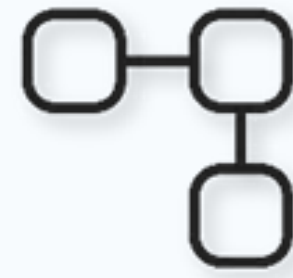


LABYRINTH DECEPTION PLATFORM

Developed to stop advanced threats

CYBERSECURITY CHALLENGE

Reactive approach to
threat detection



False positive alarms



Difficult in usage



Information overload



More time to
detect and react

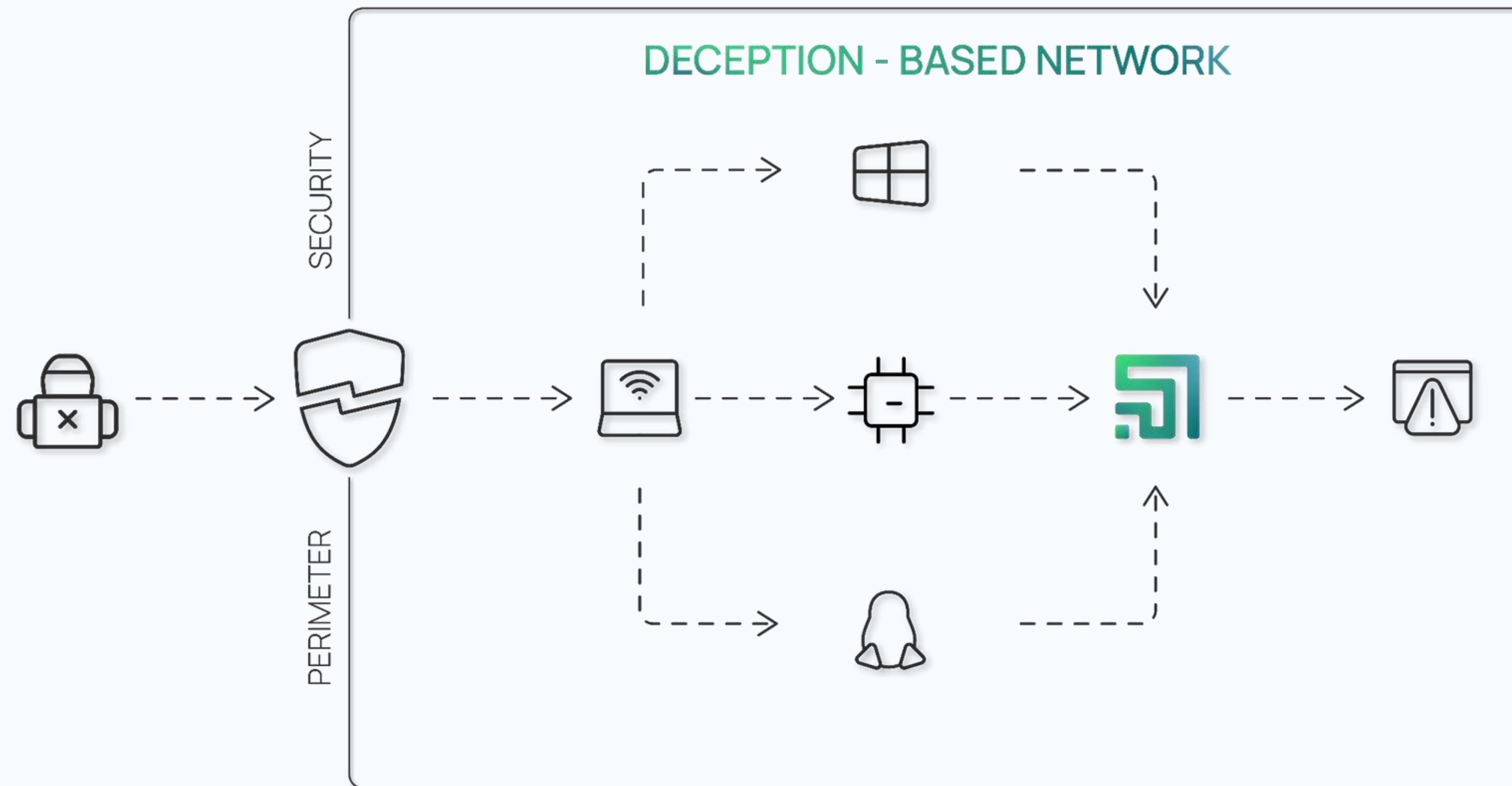


Breaches



DECEPTION-BASED THREAT DETECTION

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

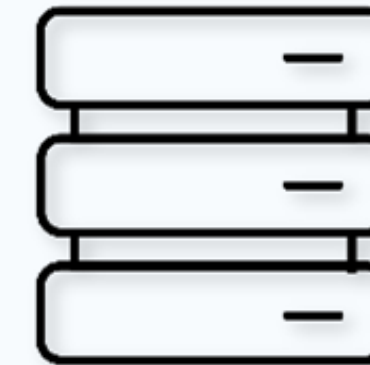


BUSINESS VALUE



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.



OPERATING COSTS REDUCTION OF BY 30%

Doesn't collect tons of data, doesn't generate false positive alerts, doesn't require special skills to operate.

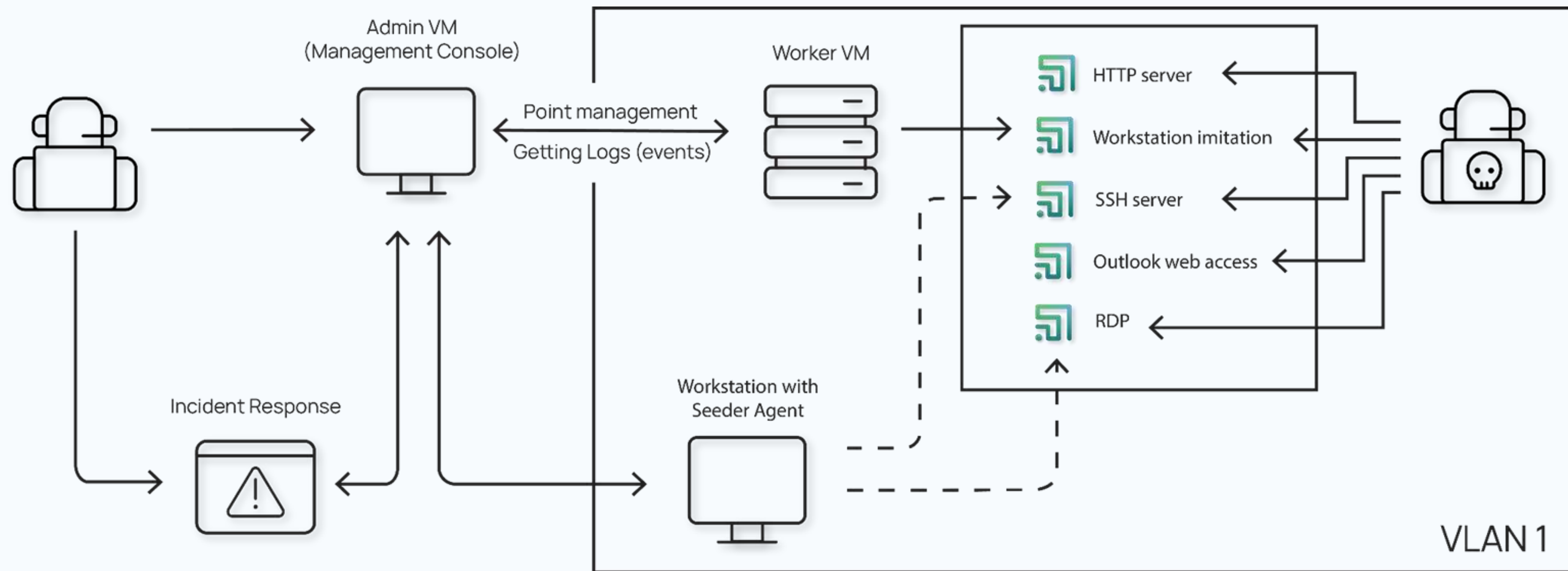


INCIDENT RESPONSE AUTOMATION

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

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.

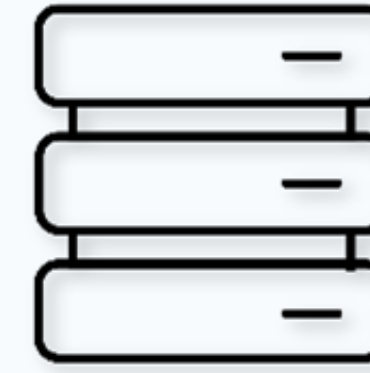


LABYRINTH'S COMPONENTS



Seeder Agent

Agents are deployed on real hosts and distribute attractive artifacts to them. The artifacts used by attackers direct them to Points.



Worker Node

The Worker Node is the host that hosts all the Points in Labyrinth. It is capable of operating in multiple VLANs simultaneously.



Point

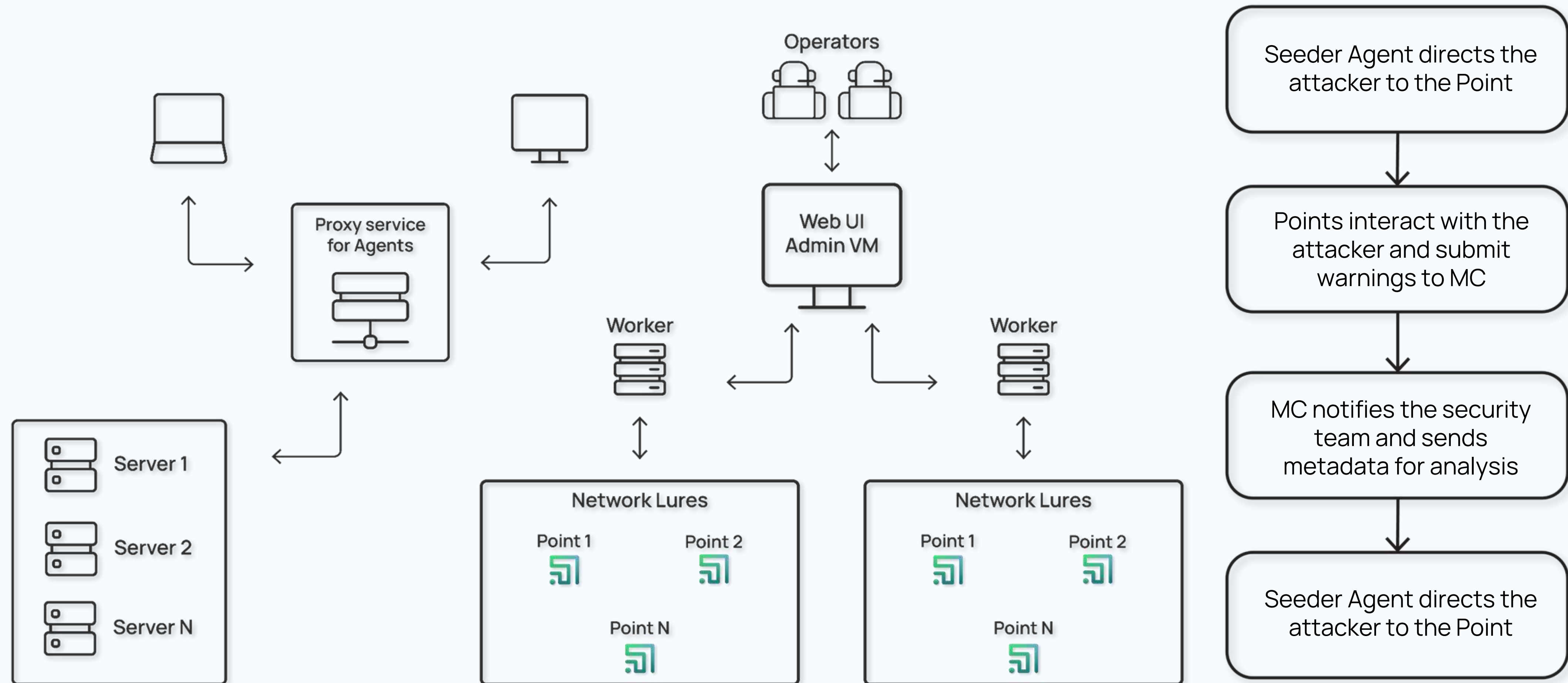
Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.



Management Console

All information collected at the Points is forwarded to the Management Console for incident analysis and response.

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 commonly used targets by hackers - web applications and services.

The screenshot displays the Labyrinth security dashboard. At the top, a dark blue header contains a 'corporate' dropdown menu, a green shield icon, and a red notification bell with '99+'. Below the header, a network diagram on the left shows a central black box with details for a 'universalweb' point: Hostname 'ophelia', IP Address '172.16.72.116', and status 'running'. This box is connected to several other nodes, some marked with red warning triangles. A green arrow points from the IP address in the diagram to the first alert entry on the right. The right side of the dashboard features a 'Latest alerts' panel with a red '150' badge. It lists two identical alerts: 'Potentially dangerous HTTP method (POST, PUT or DELETE)' from source IP '172.16.254.129' on 2023-04-05. Each alert entry includes fields for Point ID, Honeynet, Location, Point IP, and Point Type, followed by an 'open' button. A 'VIEW ALL' link is at the bottom of the alerts panel.

corporate

Latest alerts 150

2 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

open

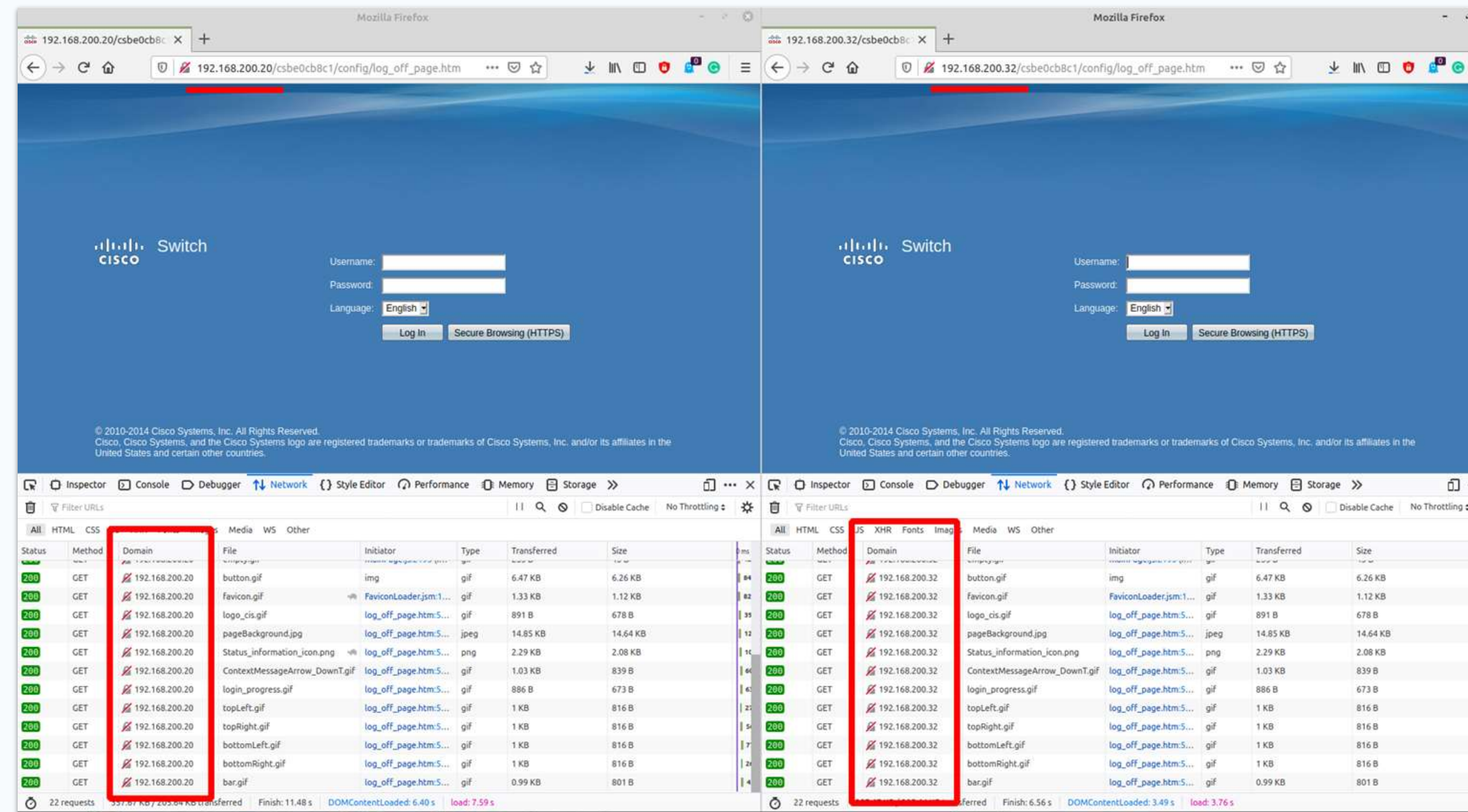
2 Potentially dangerous HTTP method (POST, PUT or DELETE)
2023-04-05 17:13:22

Source IP: 172.16.254.129
Point ID: universalweb-009d4cbb
Honeynet: honeynet01
Location: labdev
Point IP: 172.16.72.116

[VIEW ALL](#)

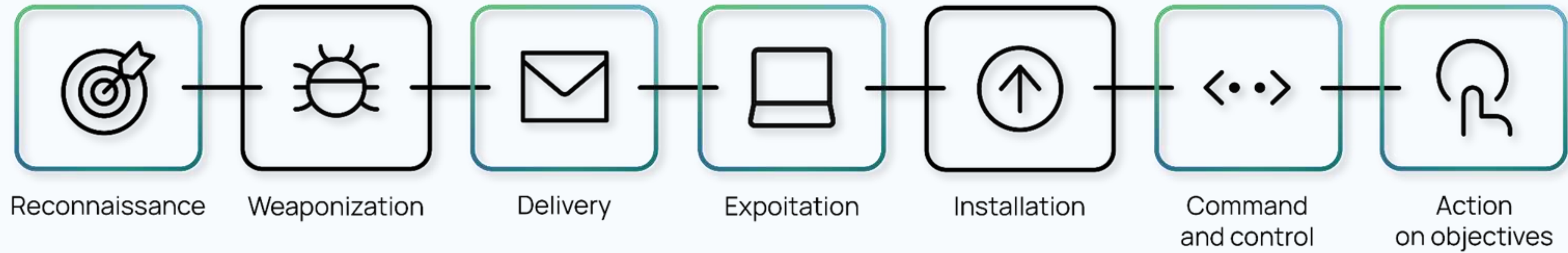
Point Type	universalweb
Hostname	ophelia
IP Address	172.16.72.116
status	running

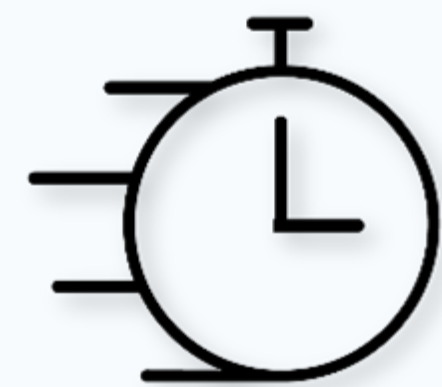
UNIVERSAL WEB POINT



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





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

Dashboard

Honeynets

Points

List

Types

Seeder Agents

Map

Alerts

Audit Log

Nodes

Multitenancy

Settings

License

Alerts

Open

In Progress

Closed

Ignored

Search

05.04.2023 20:44:30

Status: **open**

Alert Score: **4**

Risk Score: **760**

Attacker Ip: **172.16.254.8**

Point ID: **sshd-762724b2**

Point IP: **172.16.68.47**

Point Type: **sshd**

Alert reason: **sshd successful login detected**

Alert source: **Logs**

Message: **login attempt [user7/Trustno1] succeeded**

Password: **Trustno1**

Username: **user7**

client_ip: **172.16.254.8**

Comments

No comments found

Events related to the Alert

Timestamp **2023-04-05 20:44:31**. Message **CMD: ps -a.**

Timestamp **2023-04-05 20:44:30**. Name **LC_CTYPE**. Message **request_env: LC_CTYPE=UTF-8.**

Timestamp **2023-04-05 20:44:30**. Message **Terminal Size: 204 61.**

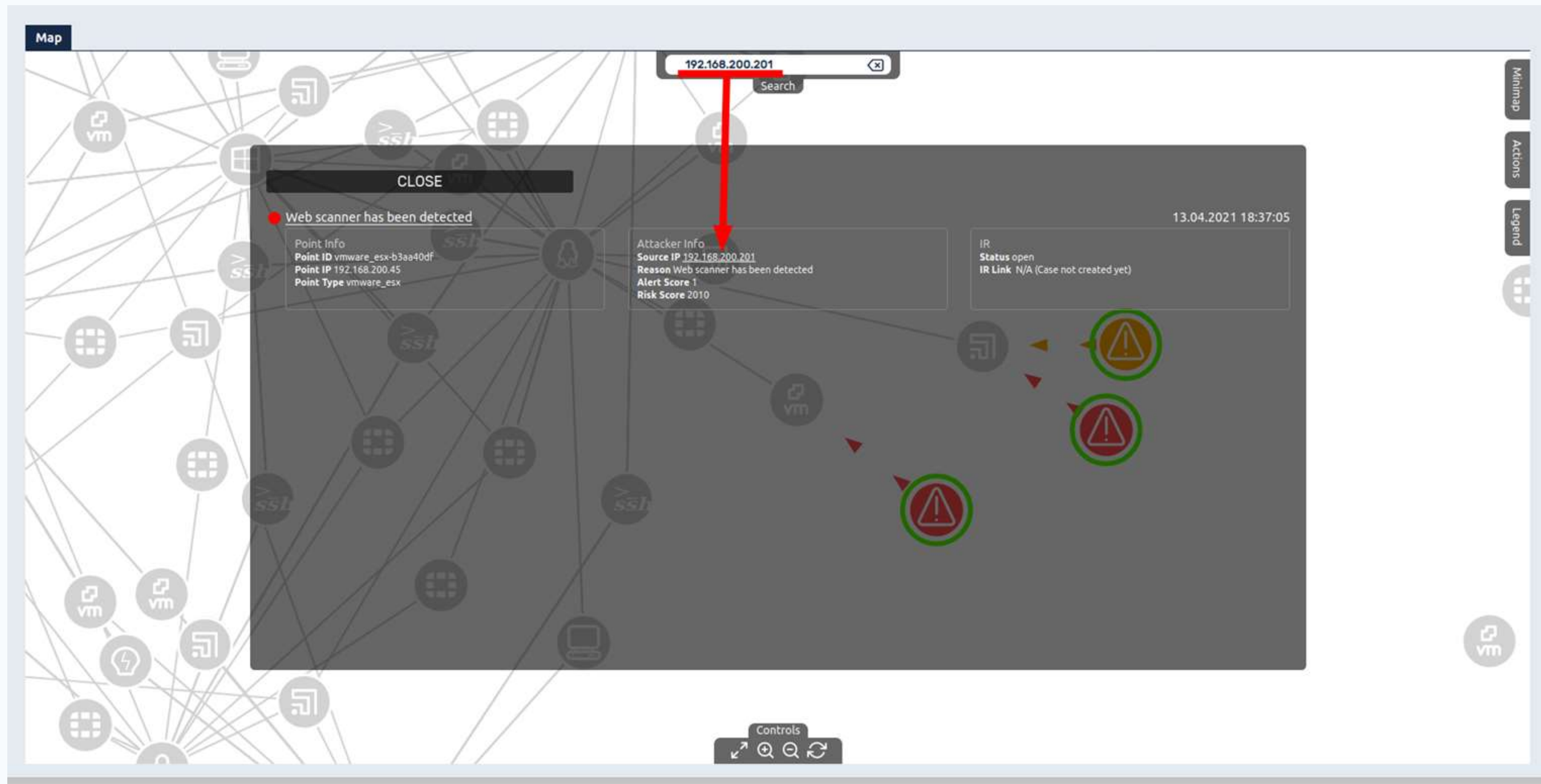
Timestamp **2023-04-05 20:44:30.**

Timestamp **2023-04-05 20:44:30**. Username **user7**. Message **login attempt [user7/Trustno1] succeeded.**

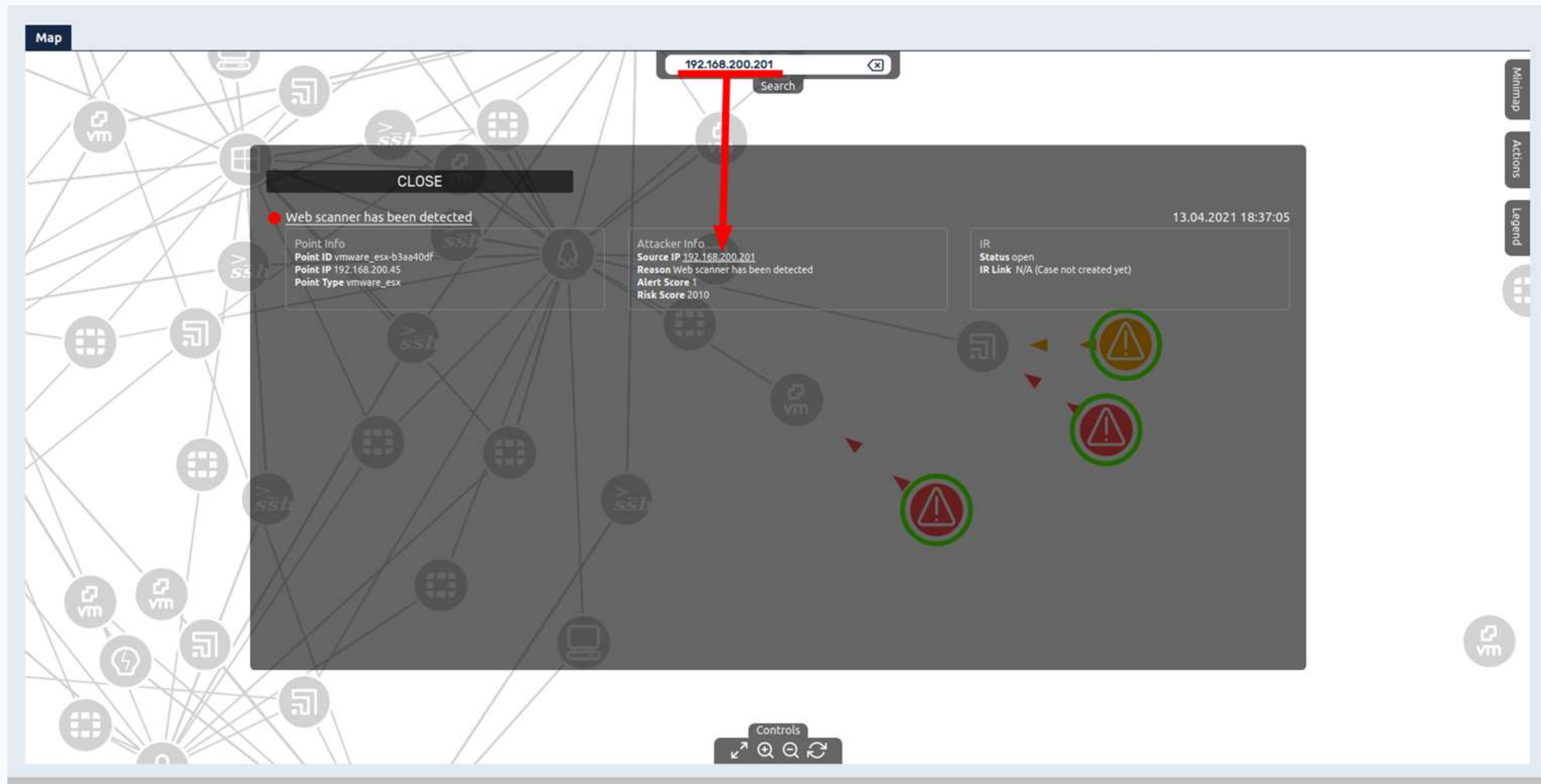
Timestamp **2023-04-05 20:44:15**. Message **Remote SSH version: SSH-2.0-OpenSSH_9.0.**

Change alert state

USE CASE SCENARIO: NETWORK SCANNING



USE CASE SCENARIO: WEB SCANNING



USE CASE SCENARIO: DETECTING MITM ATTACKS



27.03.2023
13:04:36

Status: **open**
Alert Score: **3**
Risk Score: **104**
Attacker Ip:
172.16.65.252

Point ID: **nmbclient-8a5e8a1d**
Point IP: **172.16.65.13**
Point Type: **nmbclient**

Alert reason: **Responder has been detected**
Alert source: **Logs**
Domain: **SMB12**
ResponseName: **jenny<00>**
client_ip: **172.16.65.252**

Comments

No comments found

Events related to the Alert

Timestamp **2023-03-27 13:05:14**. Domain **SMB12**. Hostname **sinope**.

Timestamp **2023-03-27 13:05:14**. Domain **SMB12**. Hostname **sinope**.

Timestamp **2023-03-27 13:05:14**. Domain **SMB12**. Hostname **sinope**.

Timestamp **2023-03-27 13:05:14**. Domain **SMB12**. Hostname **sinope**.

Timestamp **2023-03-27 13:05:11**. Transport **udp**. Source IP **172.16.65.252**. Source Port **137**. Destination IP **172.16.65.13**. Destination Port **43351**.

Timestamp **2023-03-27 13:05:02**. Transport **udp**. Source IP **172.16.65.252**. Source Port **137**. Destination IP **172.16.65.13**. D

USE CASE SCENARIO: ESCALATION OF PRIVILEGES

LABYRINTH

Dashboard

Honeynets

Map

Seeder Agents

Points

List

Types

Alerts

Timelines

Nodes

Settings

Points

Id	Location	Hostname	Network	IP Address	Status	Type
1c-2bc854b0	updatetest	hook	honeynet01	192.168.200.39	running	1c
1c-7cf673b6	updatetest	elk	honeynet01	192.168.200.40	running	1c
1c-b304831a	updatetest	europa	honeynet01	192.168.200.34	running	1c
1c-d17b07f9	updatetest	juliet	honeynet01	192.168.200.37	running	1c
1c-fd3e5501	updatetest	epimetheus	honeynet01	192.168.200.38	running	1c
askod-ffe9b517	updatetest	river	honeynet01	192.168.200.36	running	askod
fortigate-5b828946	updatetest	umbriel	honeynet01	192.168.200.46	running	fortigate
msowa-08555cd3	updatetest				running	msowa
msowa-4556fa2c	updatetest				running	nmbclient
nmbclient-4500f1e5	updatetest				running	shellshock
shellshock-184e1c4e	updatetest				running	shellshock
shellshock-71666e43	updatetest				running	sshd
sshd-e5f8127a	updatetest				running	universalweb
universalweb-e1b09f53	updatetest				running	vmware_esx
vmware_esx-6a830fac	updatetest				running	vmware_esx
vmware_esx-c7cf3365	updatetest				running	vmware_esx
vmware_esx-dae1002f	updatetest				running	vmware_esx

```
sudo nmap -sS -sV -p- -T5 192.168.200.36-37 -vvv
[sudo] password for seeker:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-07 01:44 EET
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 01:44
Scanning 2 hosts [4 ports/host]
Completed Ping Scan at 01:44, 0.22s elapsed (2 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 01:44
Completed Parallel DNS resolution of 2 hosts. at 01:44, 0.01s elapsed
DNS resolution of 2 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 2, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating SYN Stealth Scan at 01:44
Scanning 2 hosts [65535 ports/host]
Discovered open port 80/tcp on 192.168.200.37
Discovered open port 80/tcp on 192.168.200.36
```


MULTITENANCY

≡ LABYRINTH

remote-office ▾

Dashboard

Honeynets

Points >

Seeder Agents >

Map

Alerts

Audit Log

Nodes

Multitenancy

Settings >

License

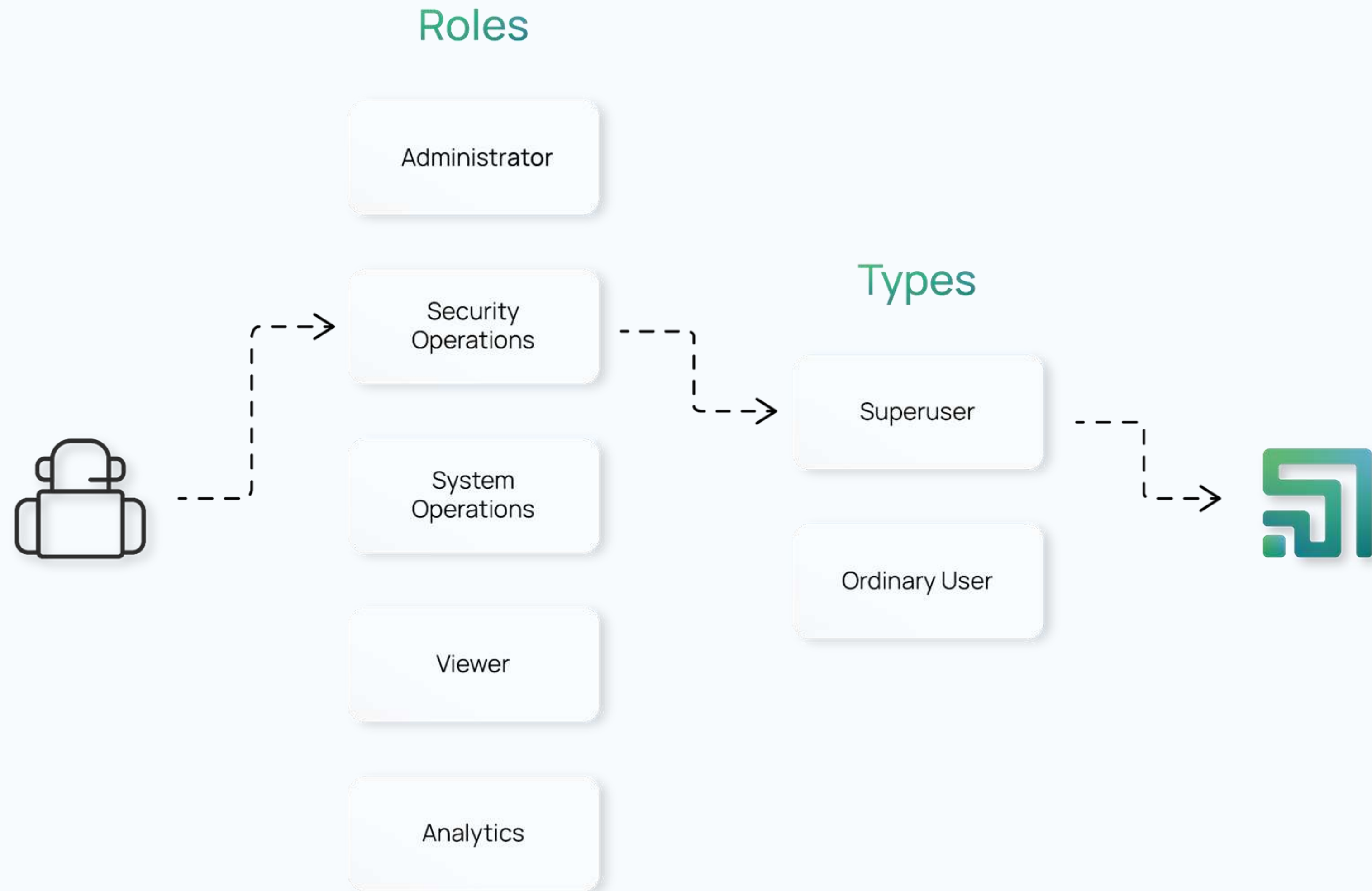
Tenant list

Tenant license used: 6 available: 10

ADD

Name	Honeynet(VLAN) Used/Reserved	Points Used/Reserved	Action
default	3/3	2/50	✎ 🗑
TEST001	4/4	1/50	✎ 🗑
byod-subnet	0/15	0/250	✎ 🗑
corporate	1/20	1/200	✎ 🗑
remote-office	0/10	0/100	✎ 🗑
main-office	3/47	8/300	✎ 🗑

SYSTEM USERS



INTEGRATIONS



State	Name	Edit
	CrowdStrike	Edit
	Cuckoo Sandbox	Edit
	Fortigate	Edit
	Microsoft Teams Notifications	Edit
	IBM-Qradar	Edit
	Slack Notification	Edit
	SMTP Notification	Edit
	Splunk	Edit
	SIEM Integration (Syslog forwarder)	Edit
	TheHive	Edit

LABYRINTH

info@labyrinth.tech

<https://labyrinth.tech>