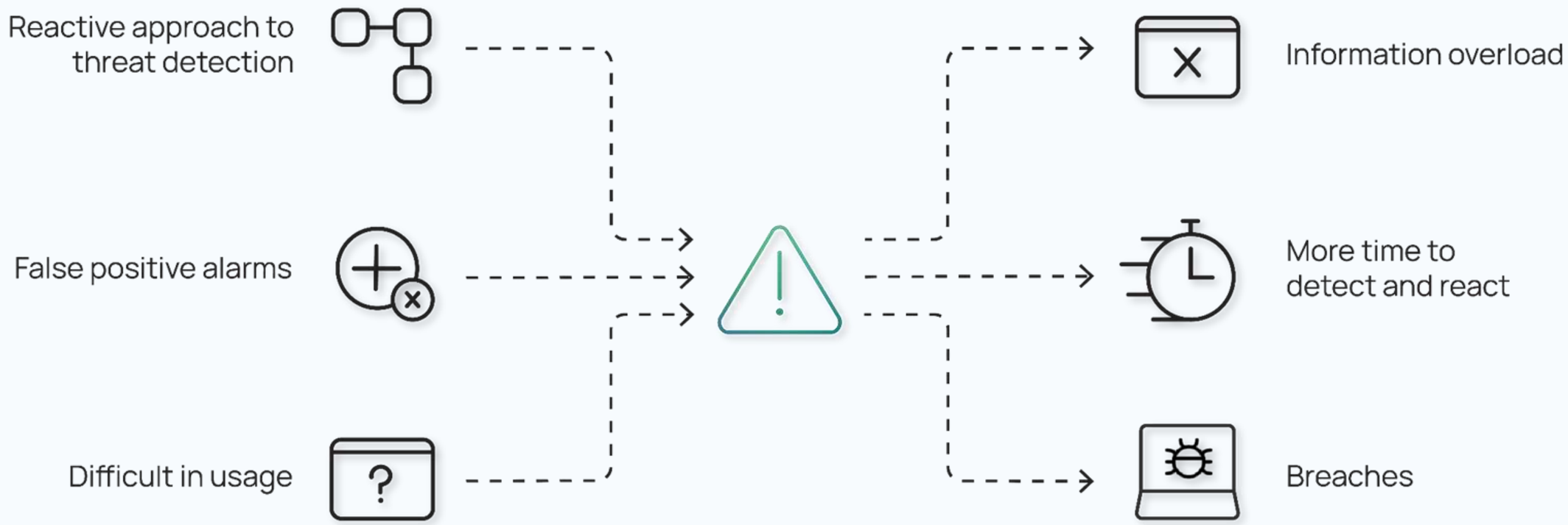
LABYRINTH DECEPTION PLATFORM

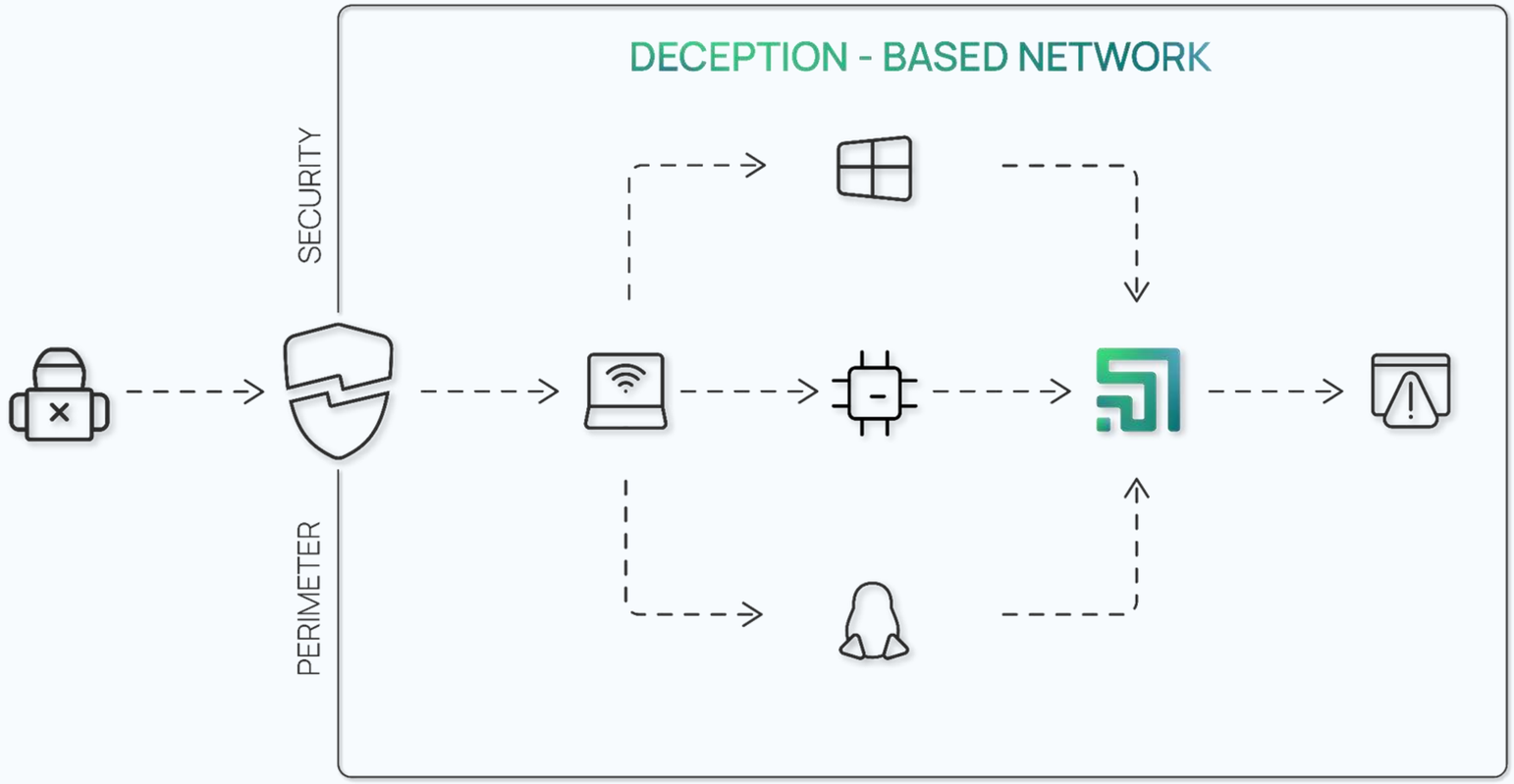
Developed to stop advanced threats

CYBERSECURITY CHALLENGE



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

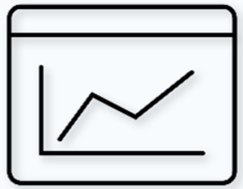
Detects targeted and advanced attacks without requiring prior knowledge of the threat's form, type, or behavior.

ZERO IMPACT ON PERFORMANCE

No negative impact on the performance of network devices, hosts,servers, or applications havior.

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%

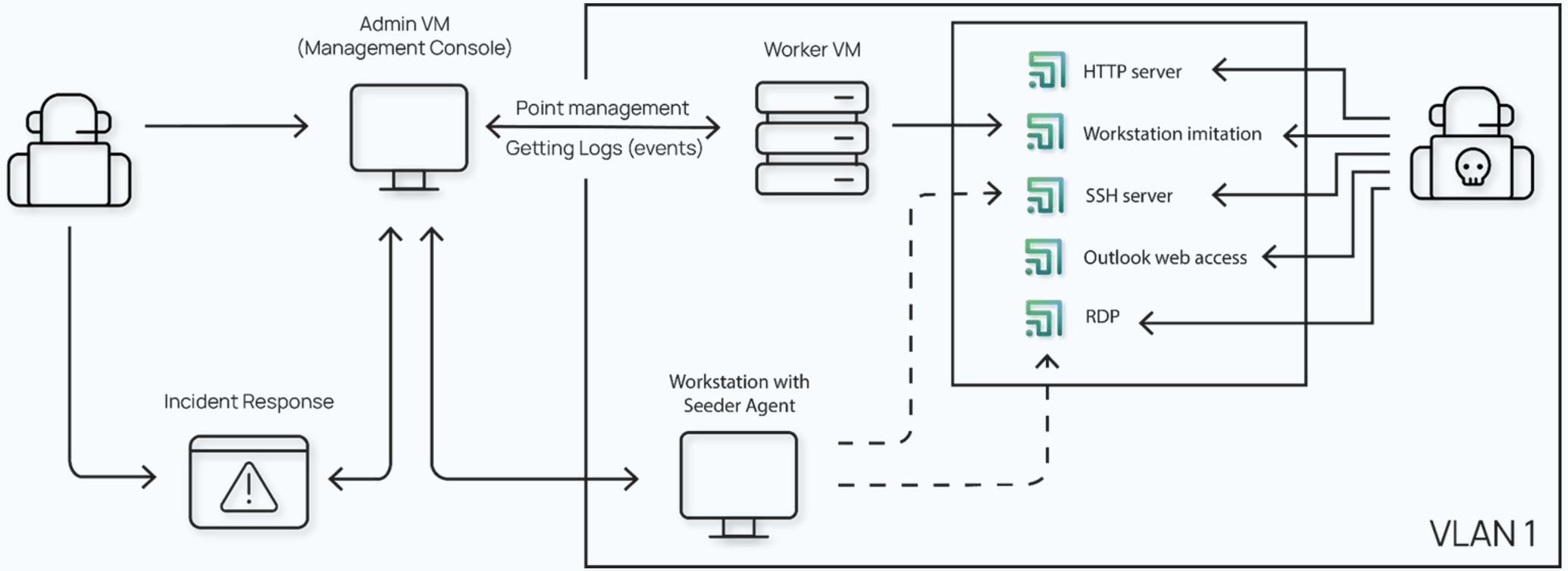
Doesn't collect tons of data, doesn't generate false positive alerts, doesn't require special skills to operate.

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.

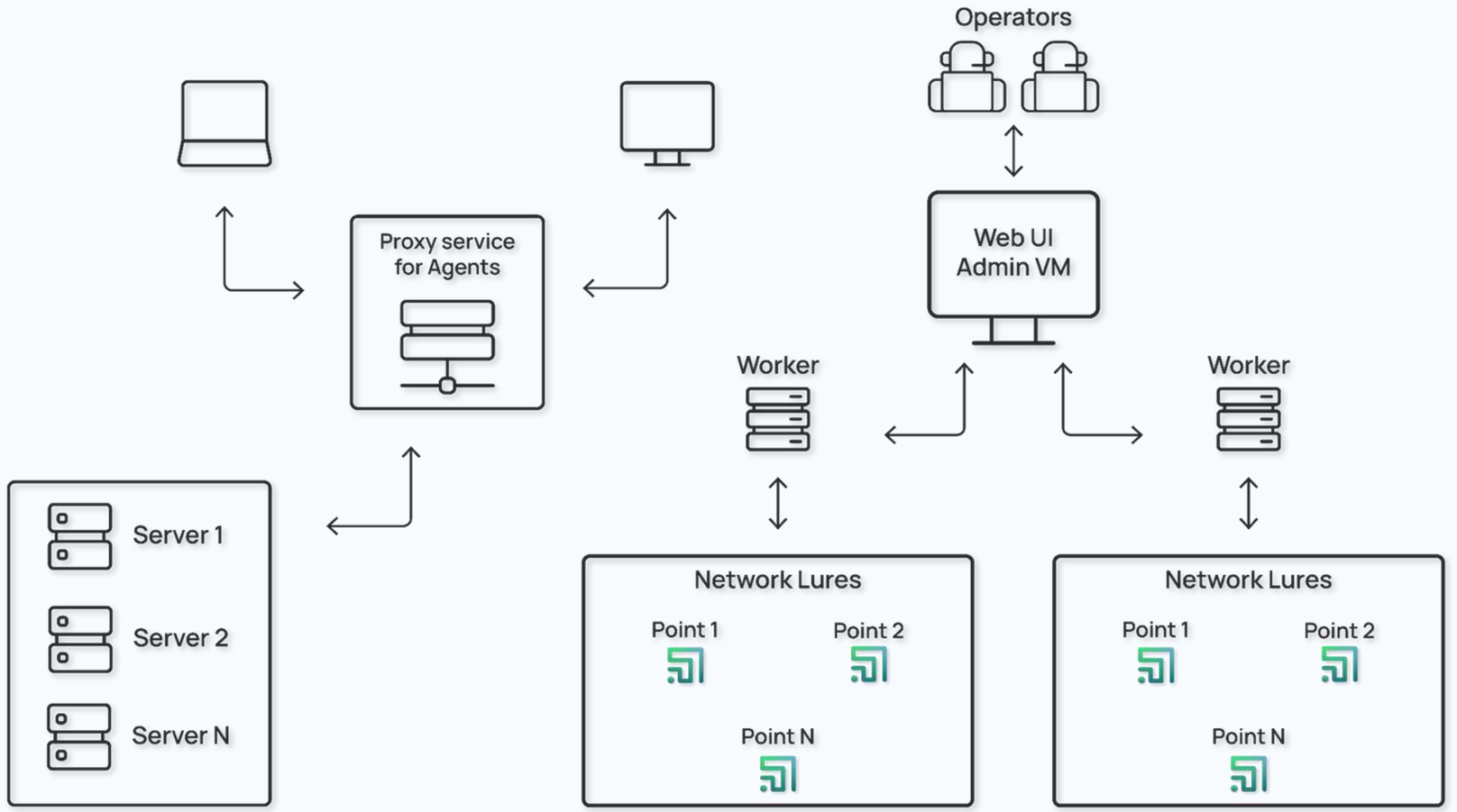
Point

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



Seeder Agent directs the attacker to the Point

Points interact with the attacker and submit warnings to MC

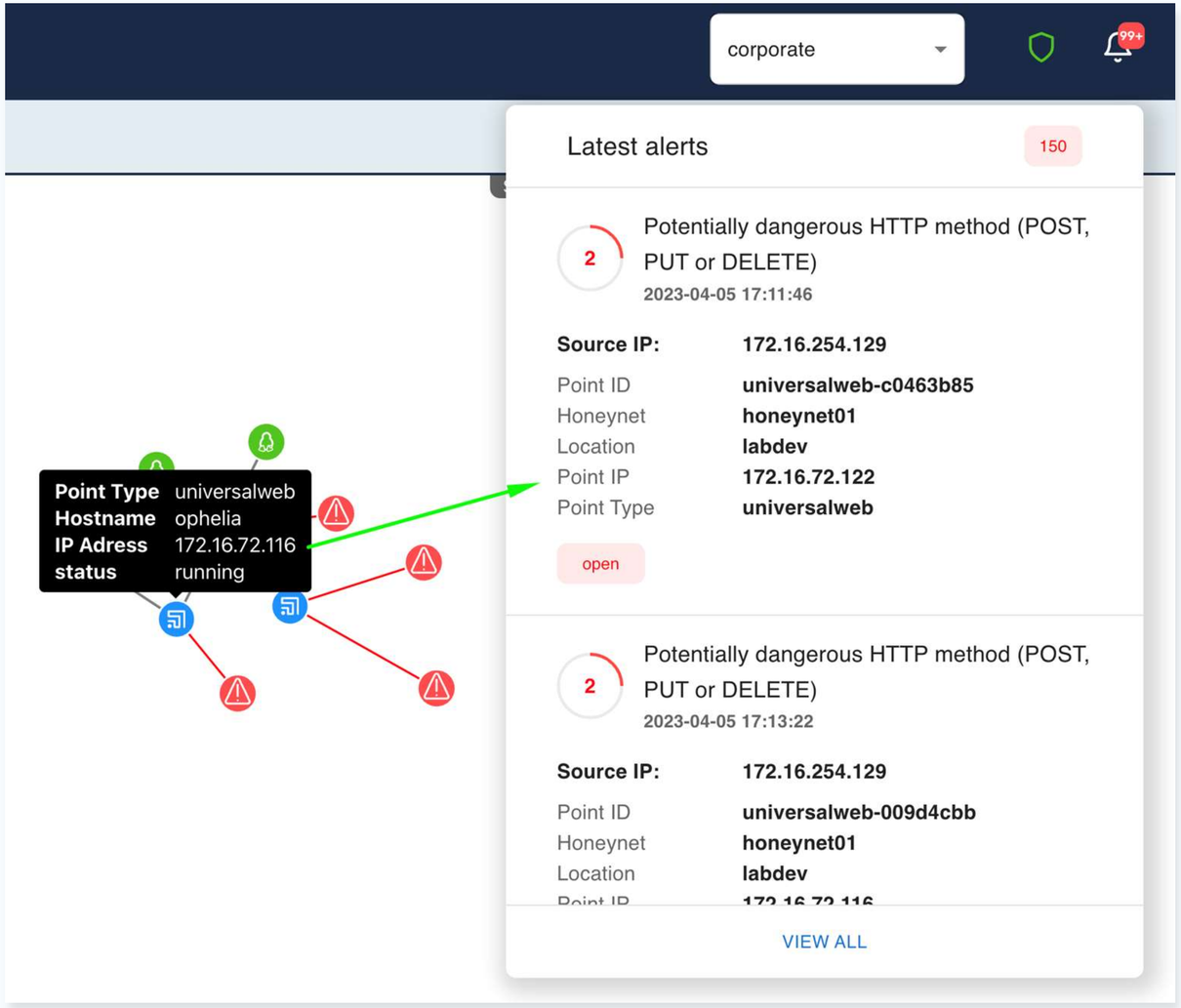
MC notifies the security team and sends metadata for analysis

Seeder Agent directs the attacker to the Point

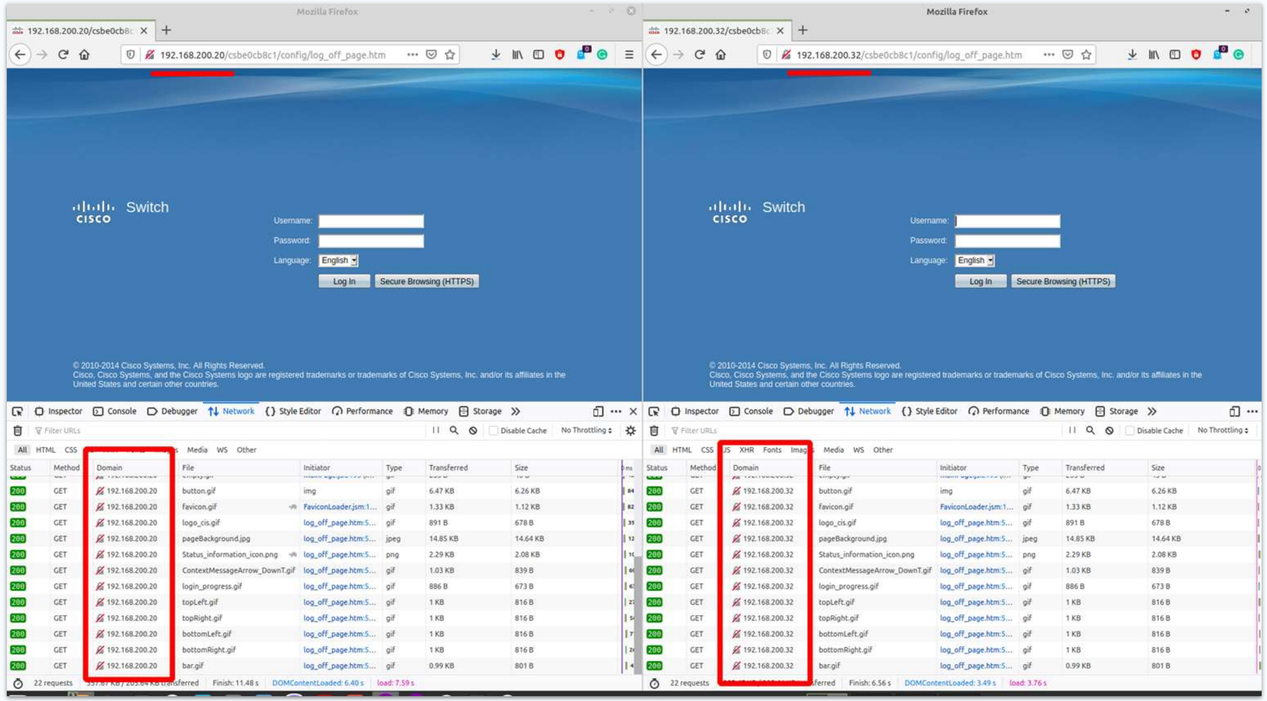
UNIVERSAL WEB POINT

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.

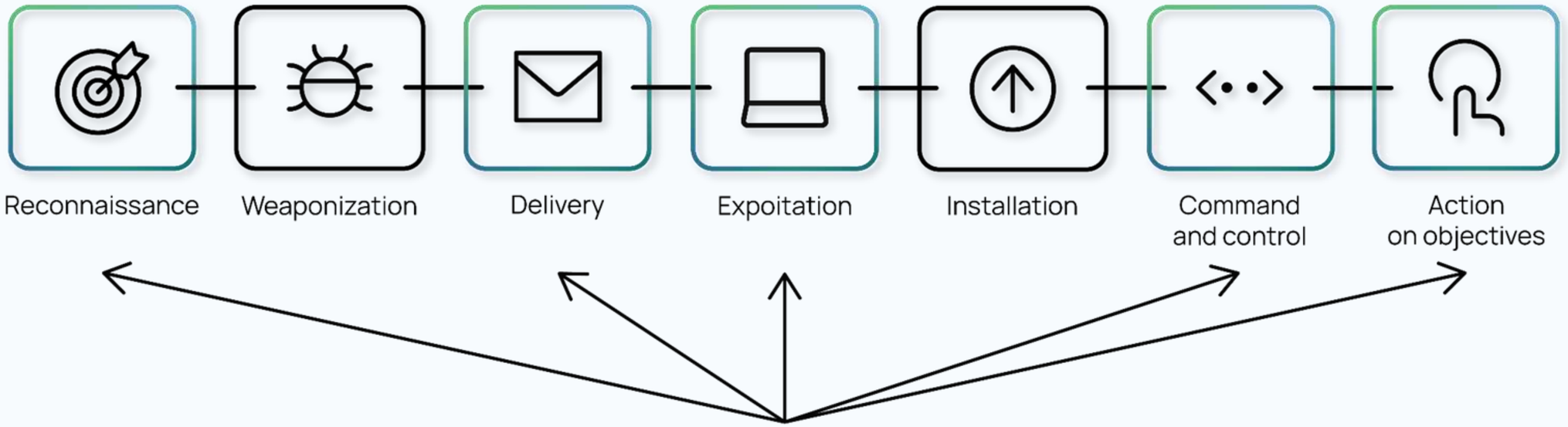


UNIVERSAL WEB POINT



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

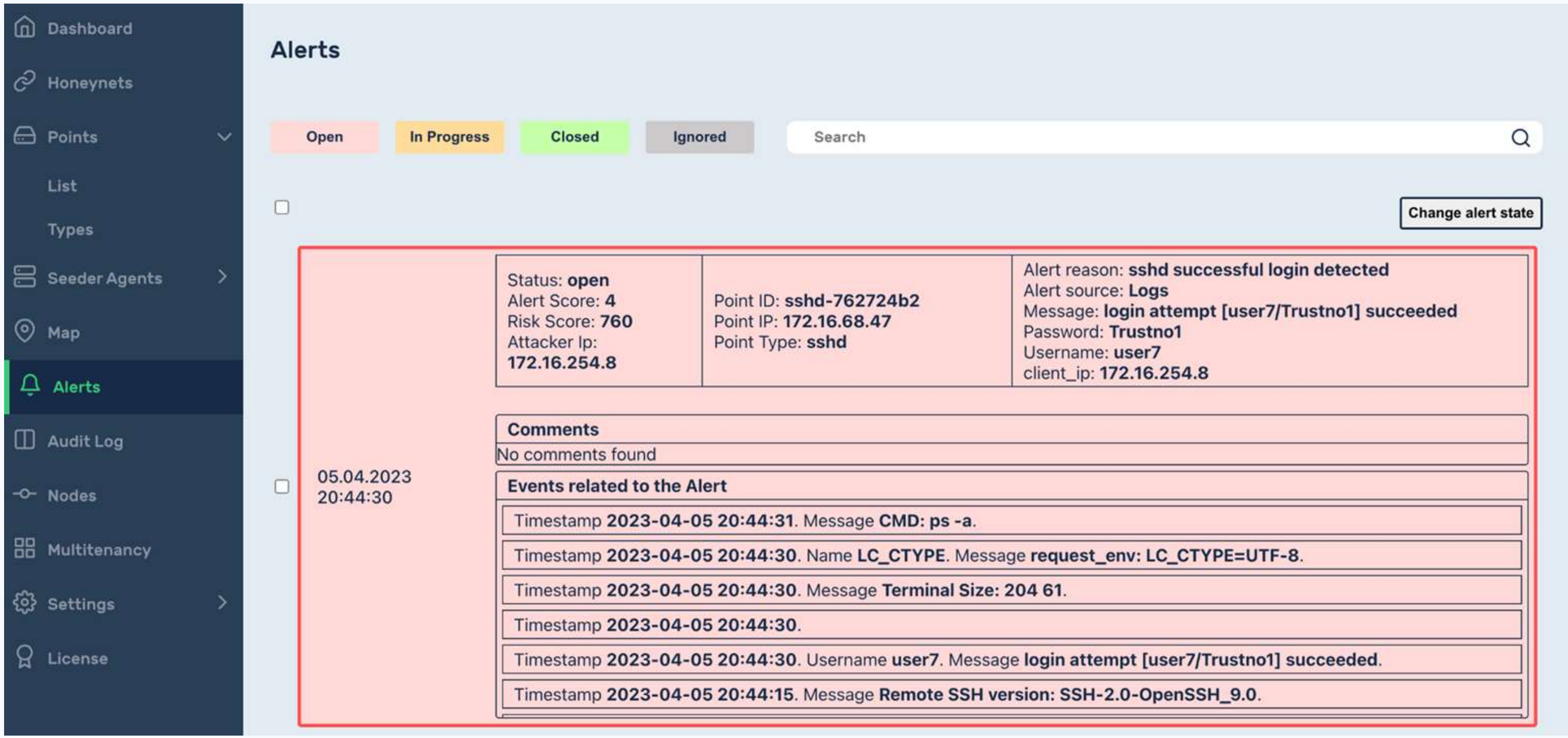


Early detection of network threats
Proactive protection
Targeted attack detection
Reduced Dwell Time

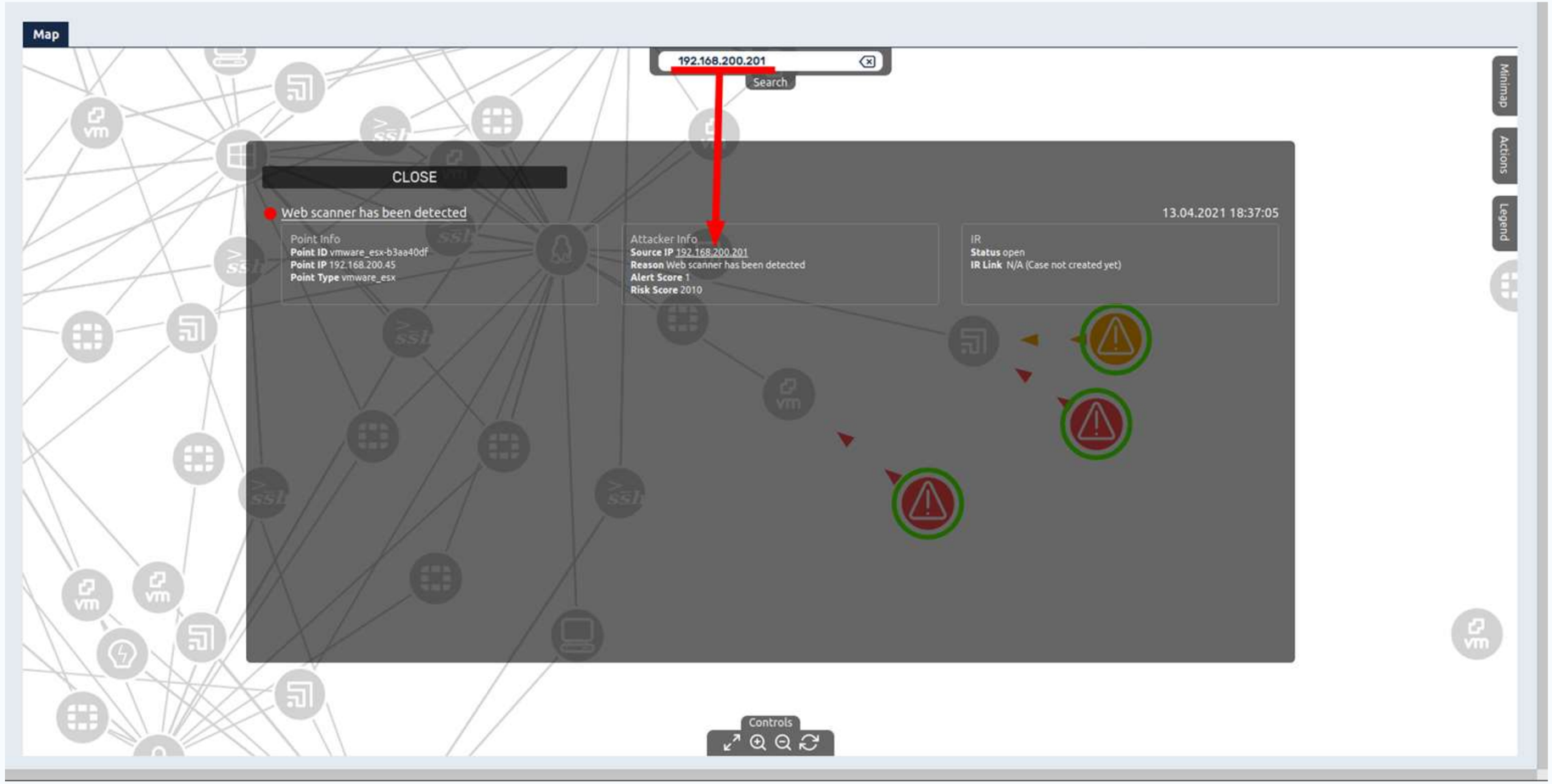
Man-in-the-Middle detection
Lateral Movement identification
Rapid response to incidents
Incident investigation

LABYRINTH

USE CASE SCENARIO: STOLEN CREDENTIALS

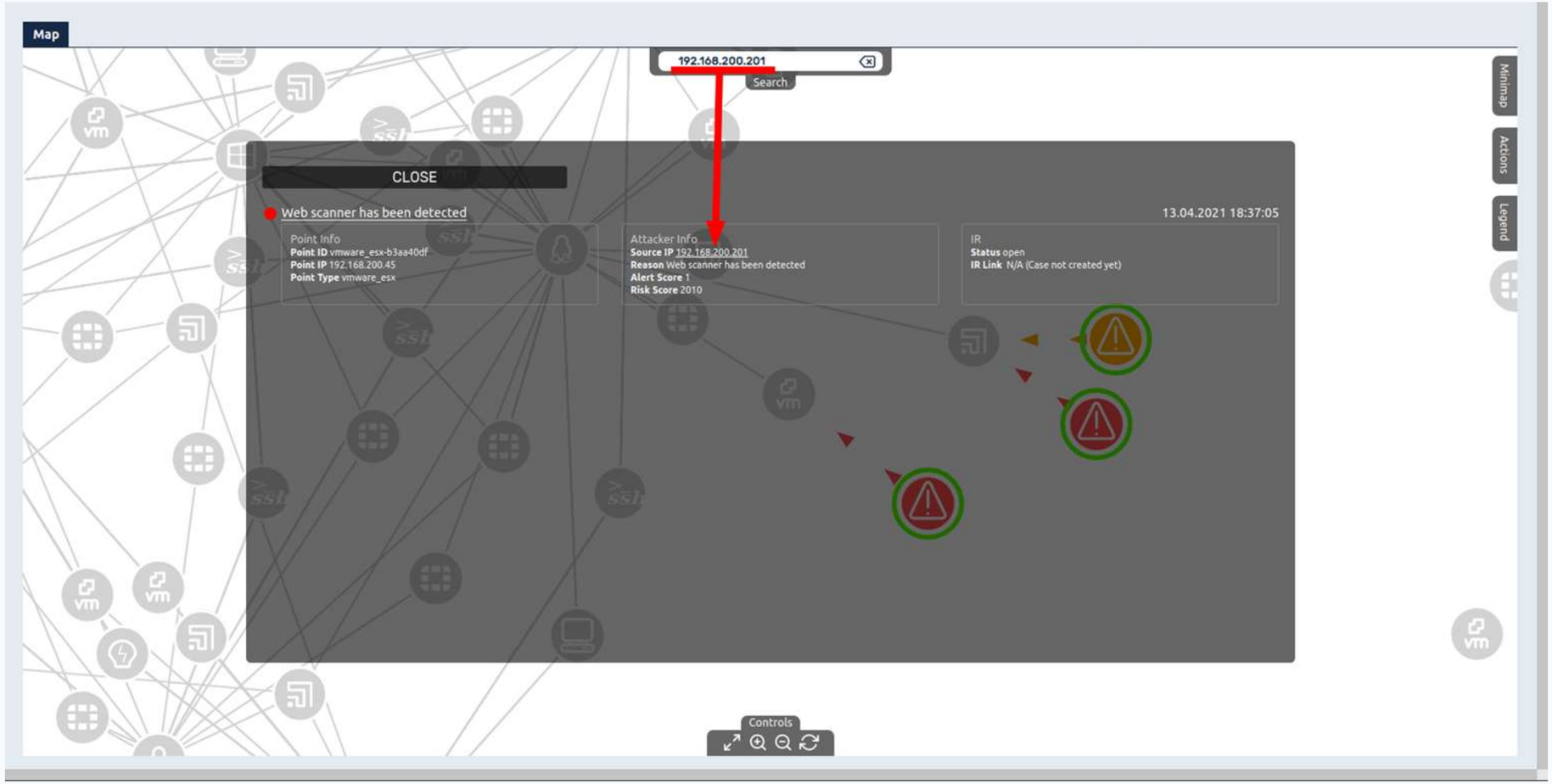


USE CASE SCENARIO: NETWORK SCANNING



LABYRINTH

USE CASE SCENARIO: WEB SCANNING



USE CASE SCENARIO: DETECTING MITM ATTACKS

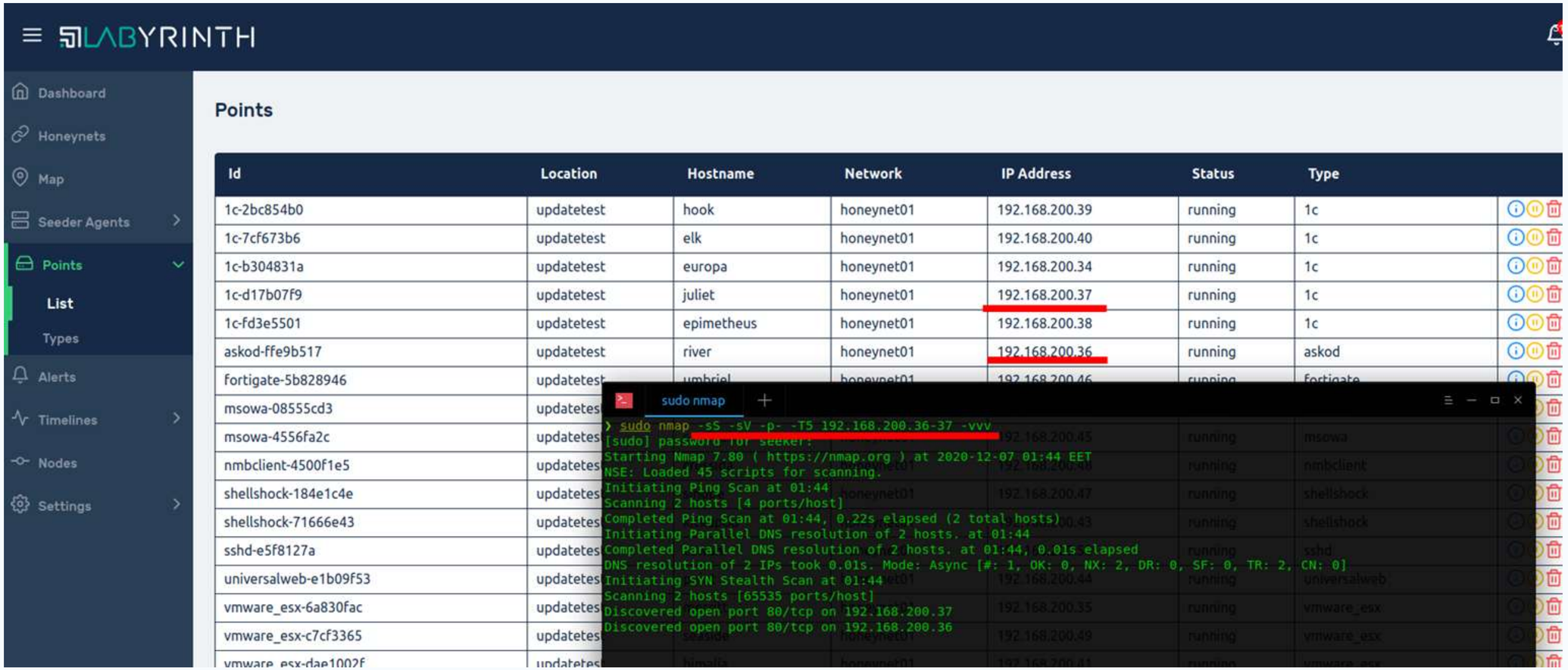
27.03.2023
13:04:36

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**

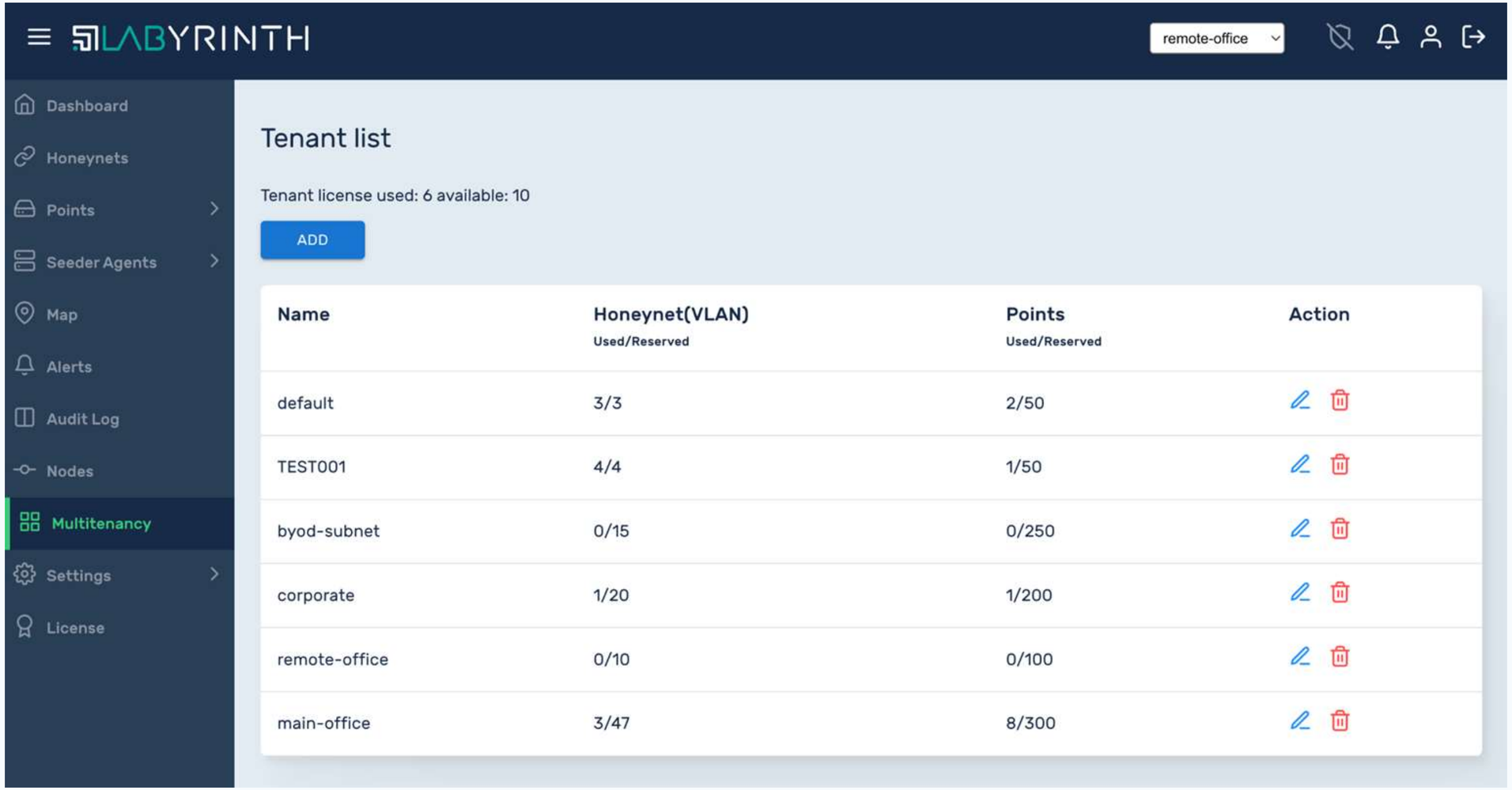
Comments
No comments found

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**. D estination 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

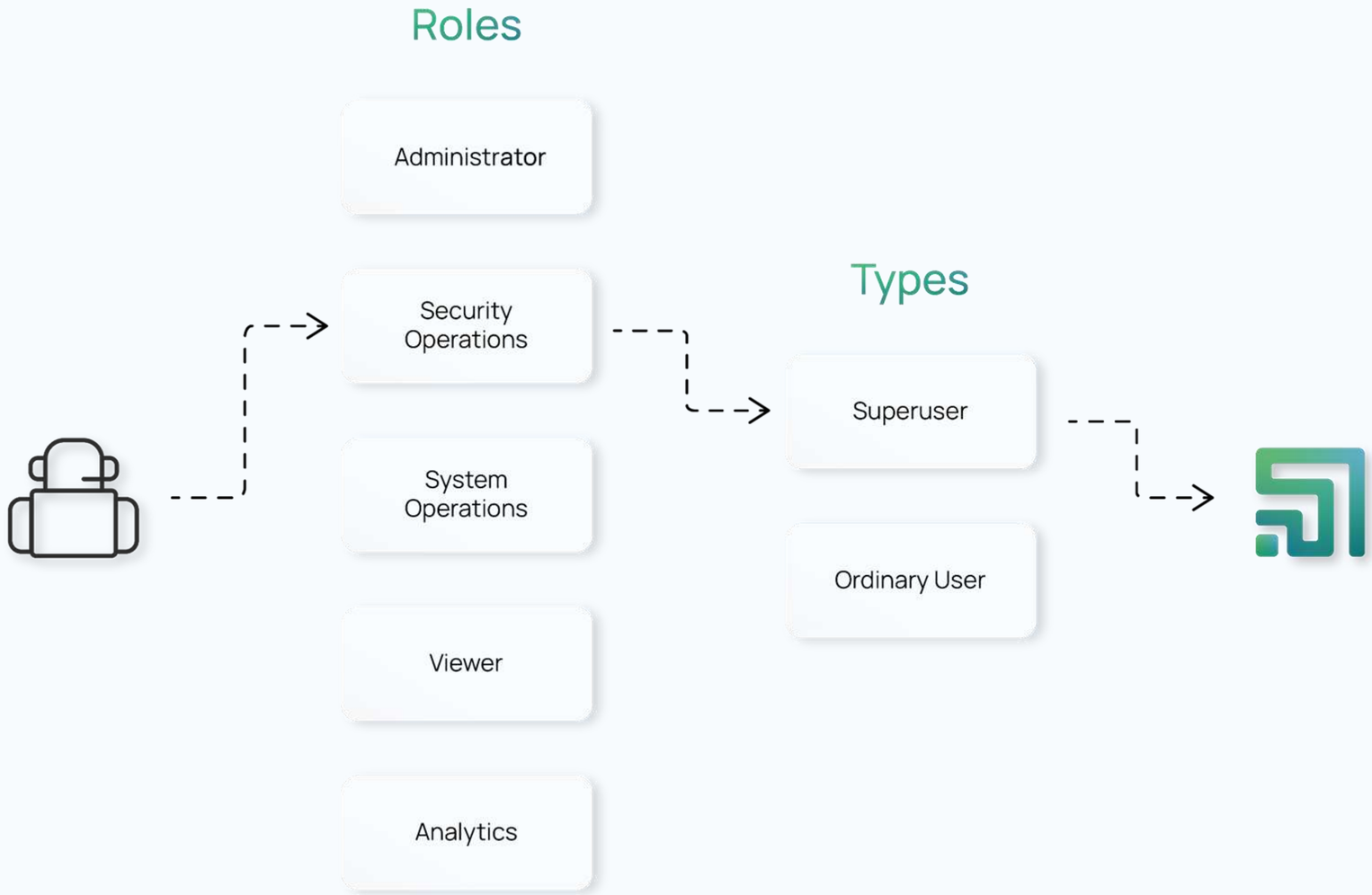
USE CASE SCENARIO: ESCALATION OF PRIVILEGES



MULTITENANCY



SYSTEM USERS



LABYRINTH

INTEGRATIONS

TheHive

CROWDSTRIKE

splunk>

Radar

FORTINET

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

LABYRINTH

info@labyrinth.tech
https://labyrinth.tech