LABYRINTH

Zaznavanje groženj z nastavljanjem pasti

Učinkovito orodje za odkrivanje in zaustavitev napadalcev v omrežju podjetja

16. maj 2024 | Ljubljana

A1 ICT Distribucija

A1 ICT Distribucija

- **Distributer z dodano vrednostjo** že od leta 2005 (F-Secure v okviru Amis d.o.o.)
- Znotraj A1 Slovenija **namenska ekipa** s prodajnimi in tehničnimi kompetencami
- Široka **partnerska mreža**
- Pokrivamo obsežen **nabor rešitev**
  - Zaščita delovnih postaj in strežnikov
  - Zaščita poslovno kritičnih podatkov
  - Zaščita omrežja
  - Zaščita elektronske pošte
  - Sistemi za zaznavanje in odzivanje na vdore (omrežje in end-point)
  - Omrežne rešitve (brezžična in žična omrežja)

A1 ICT Distribucija

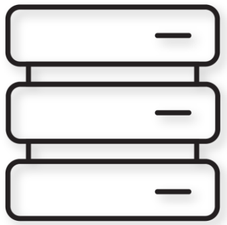
naši dobavitelji

Komponente platforme

LABYRINTH

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.

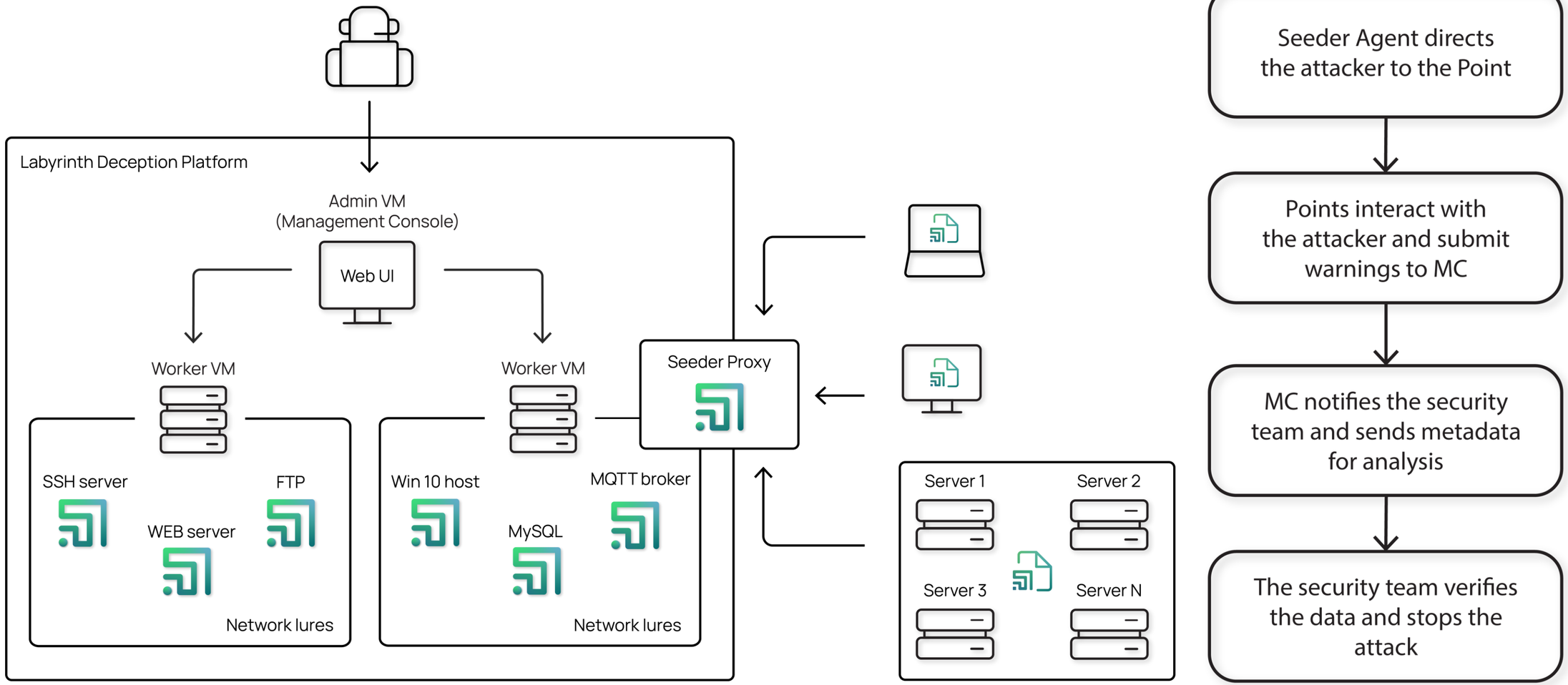
Point

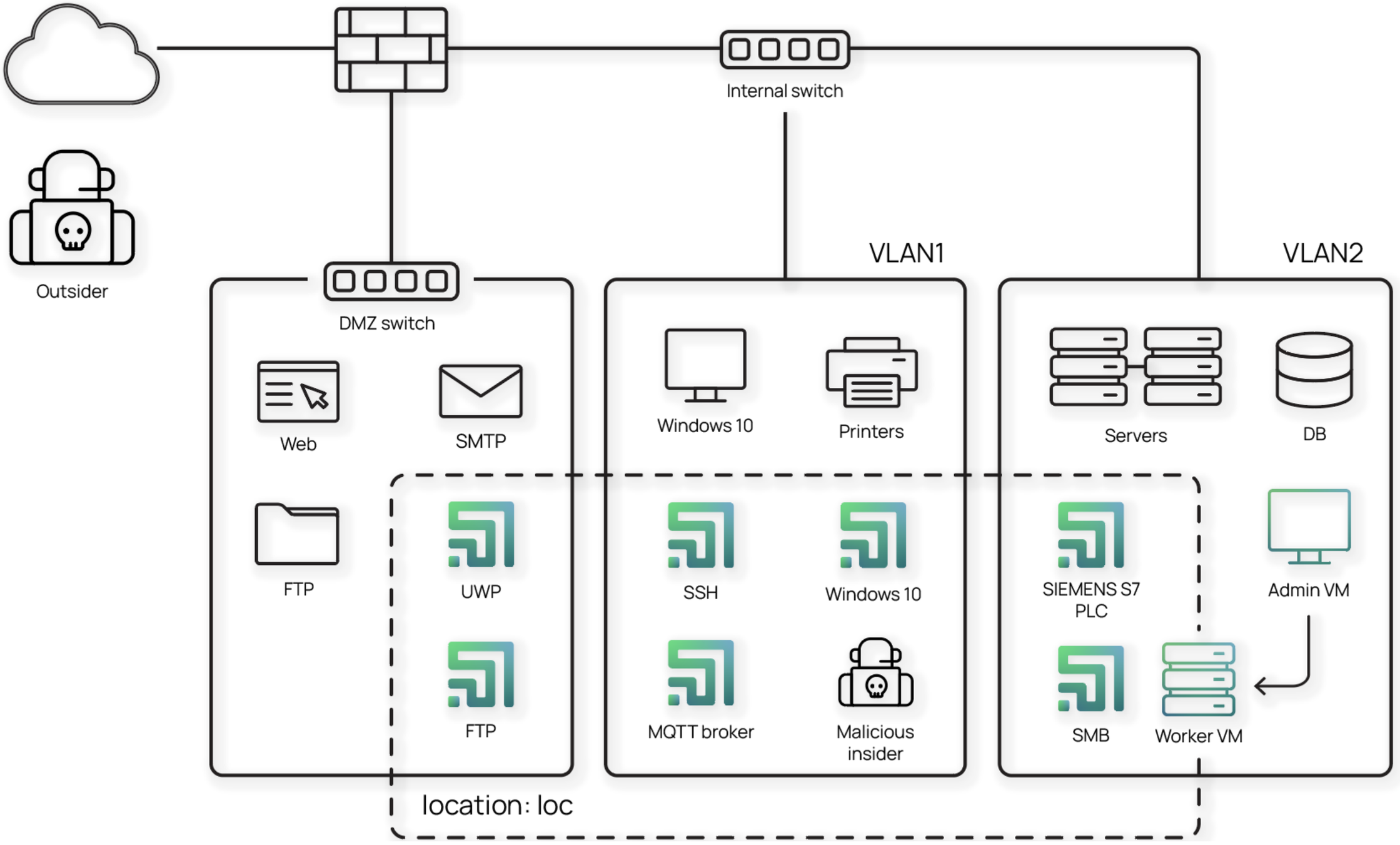
Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.

Host with Seeder Agent

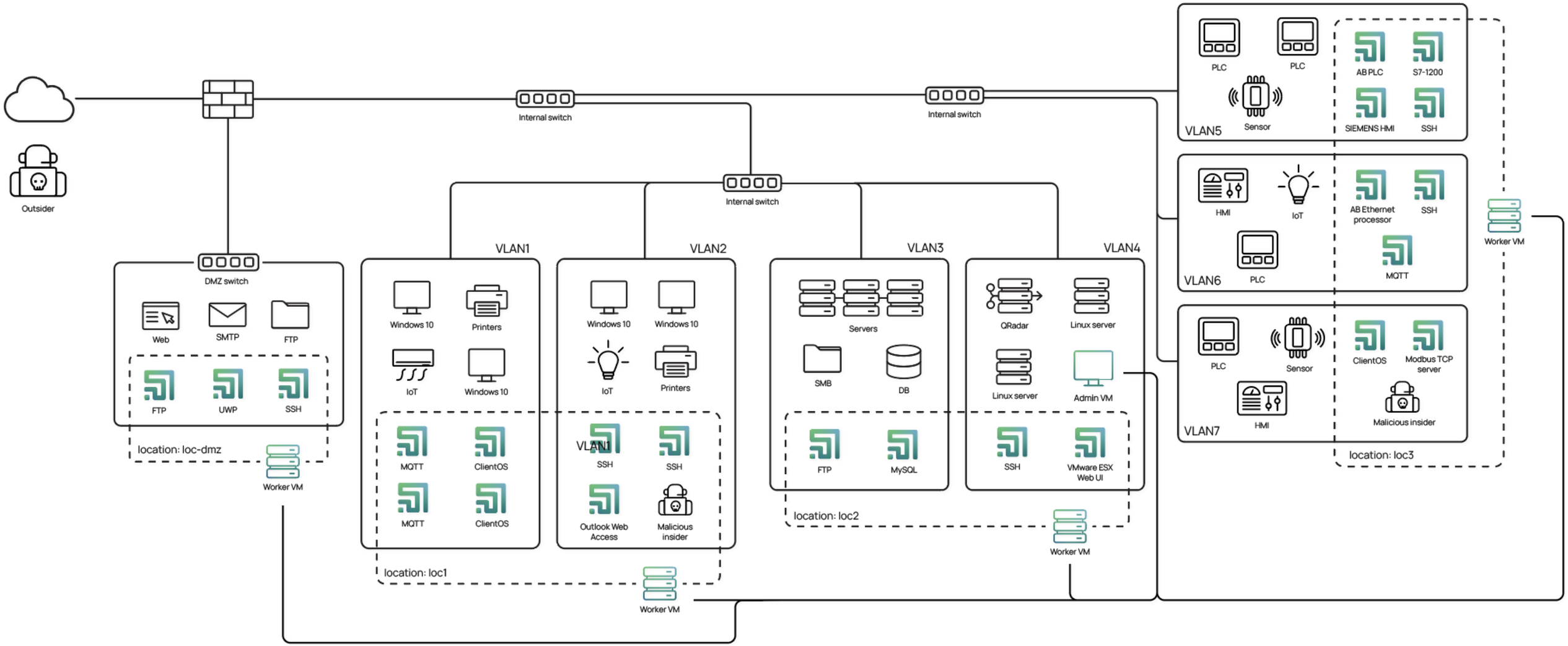
Agents are deployed on real hosts and distribute attractive artifacts to them. The artifacts used by attackers direct them to Points.

Arhitektura platforme



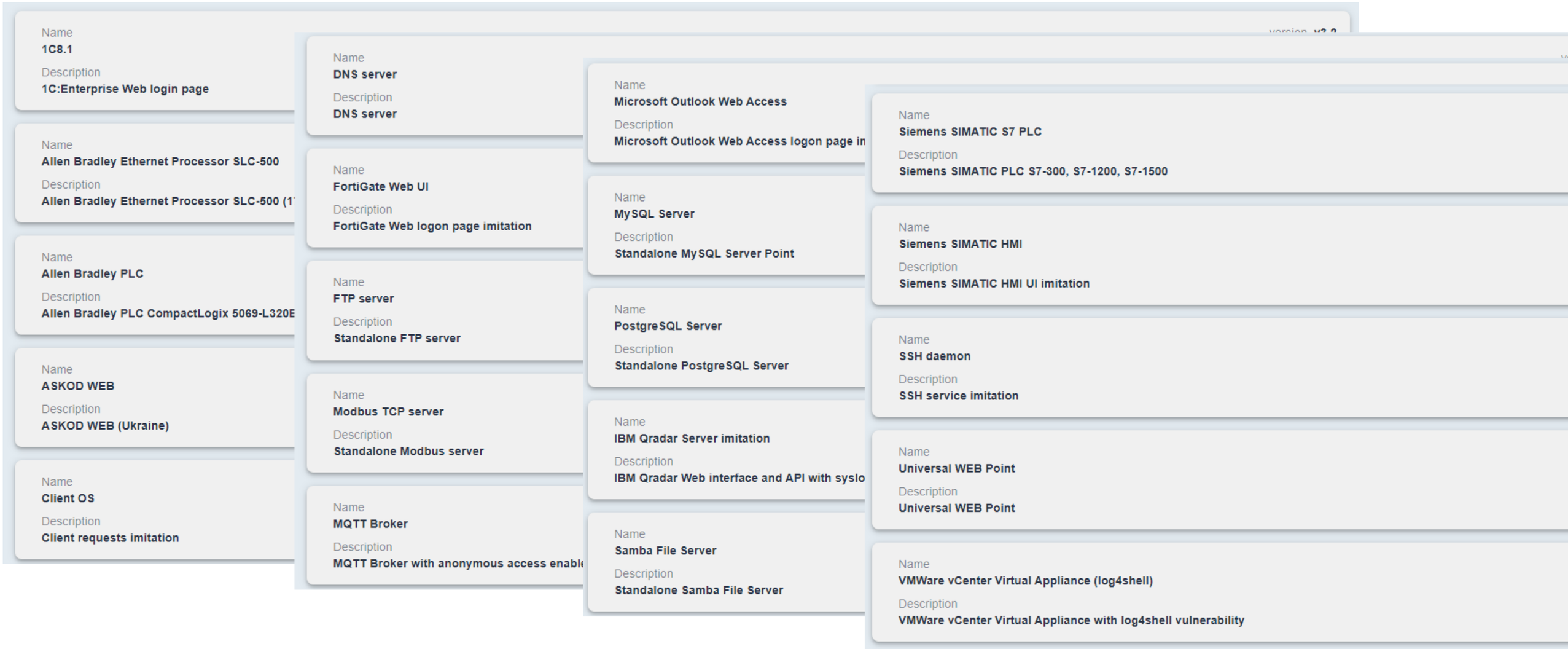

Internal switch
Outsider
DMZ switch
VLAN1
VLAN2
Web
SMTP
Windows 10
Printers
Servers
DB
FTP
UWP
SSH
Windows 10
SIEMENS S7
PLC
Admin VM
FTP
MQTT broker
Malicious
insider
SMB
Worker VM
location: loc

LABYRINTH

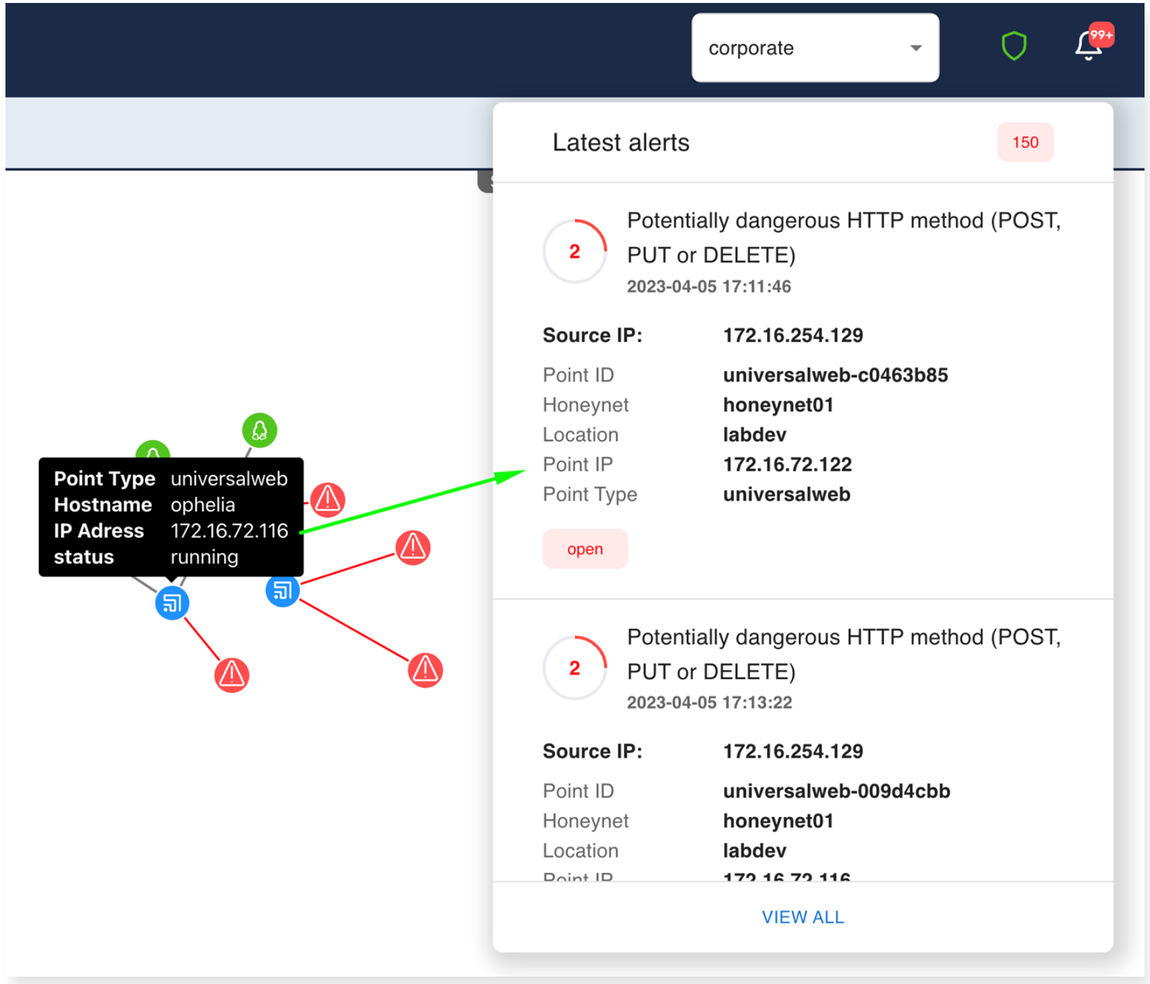


A1 ICT Distribucija

Deception Point Type Bases

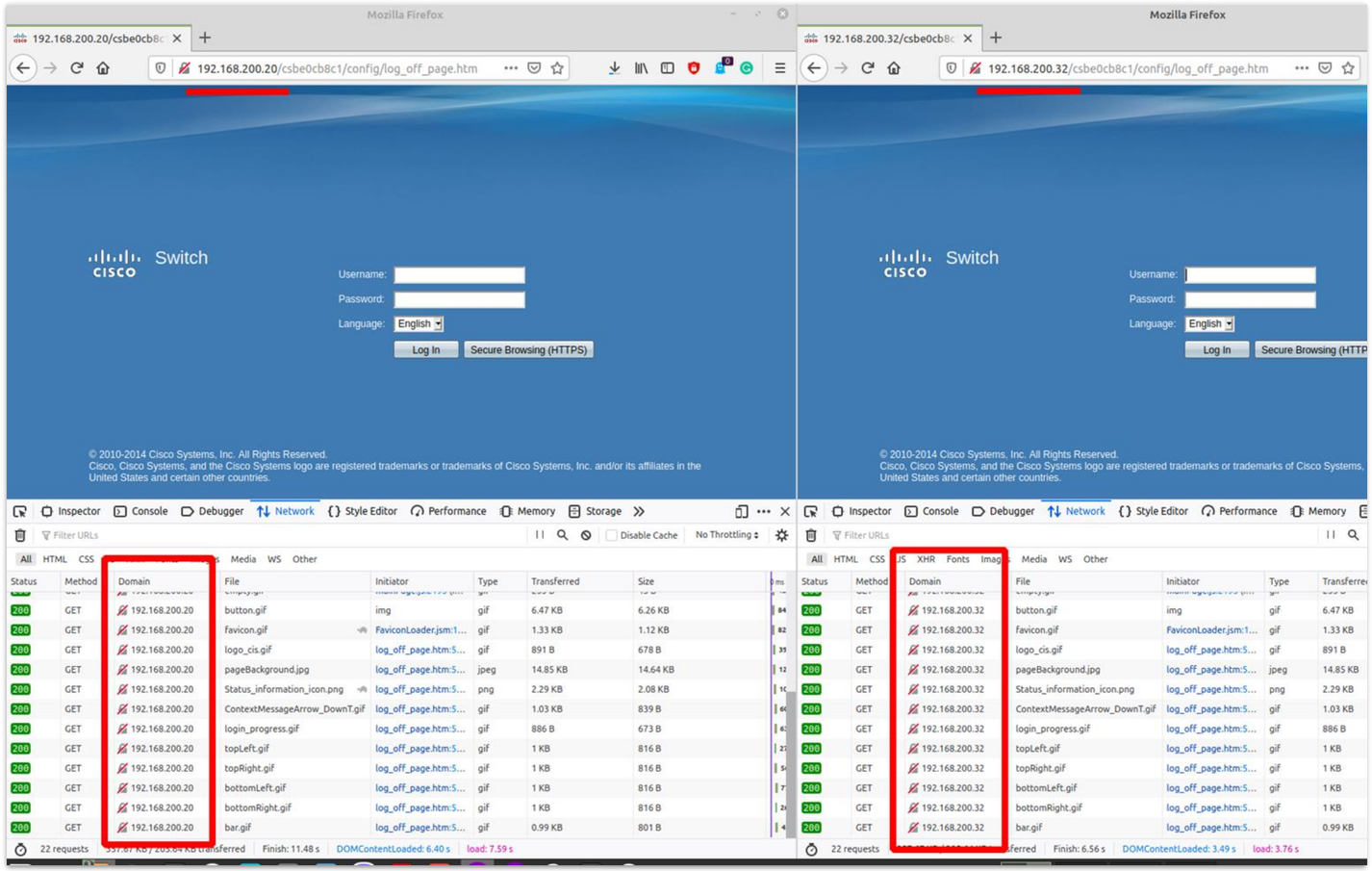


Universal Web Point

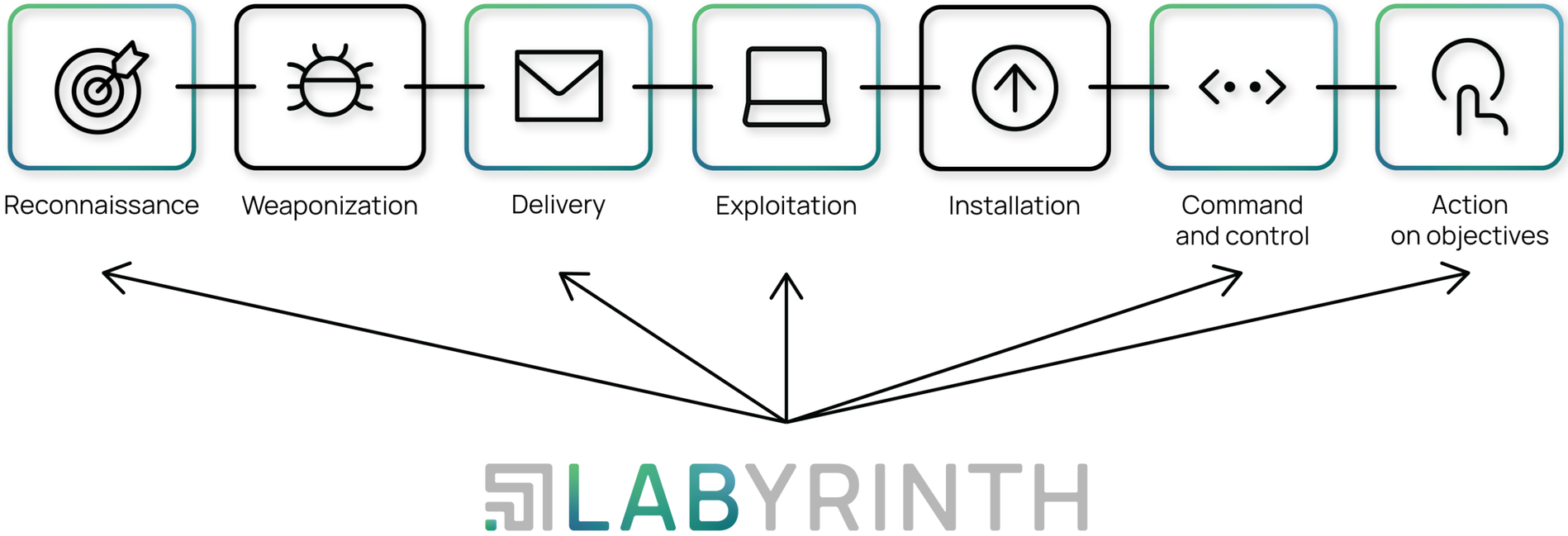


A1 ICT Distribucija

Universal Web Point



Zgodnje zaznavanje grožnje



Primer alarma

LABYRINTH

Severity	Status	Timestamp	Point ID	Attacker IP	Alert Reason
H	open	2024-05-16 11:08:58	sshd-3eae0458	10.10.10.1	sshd successful login detected

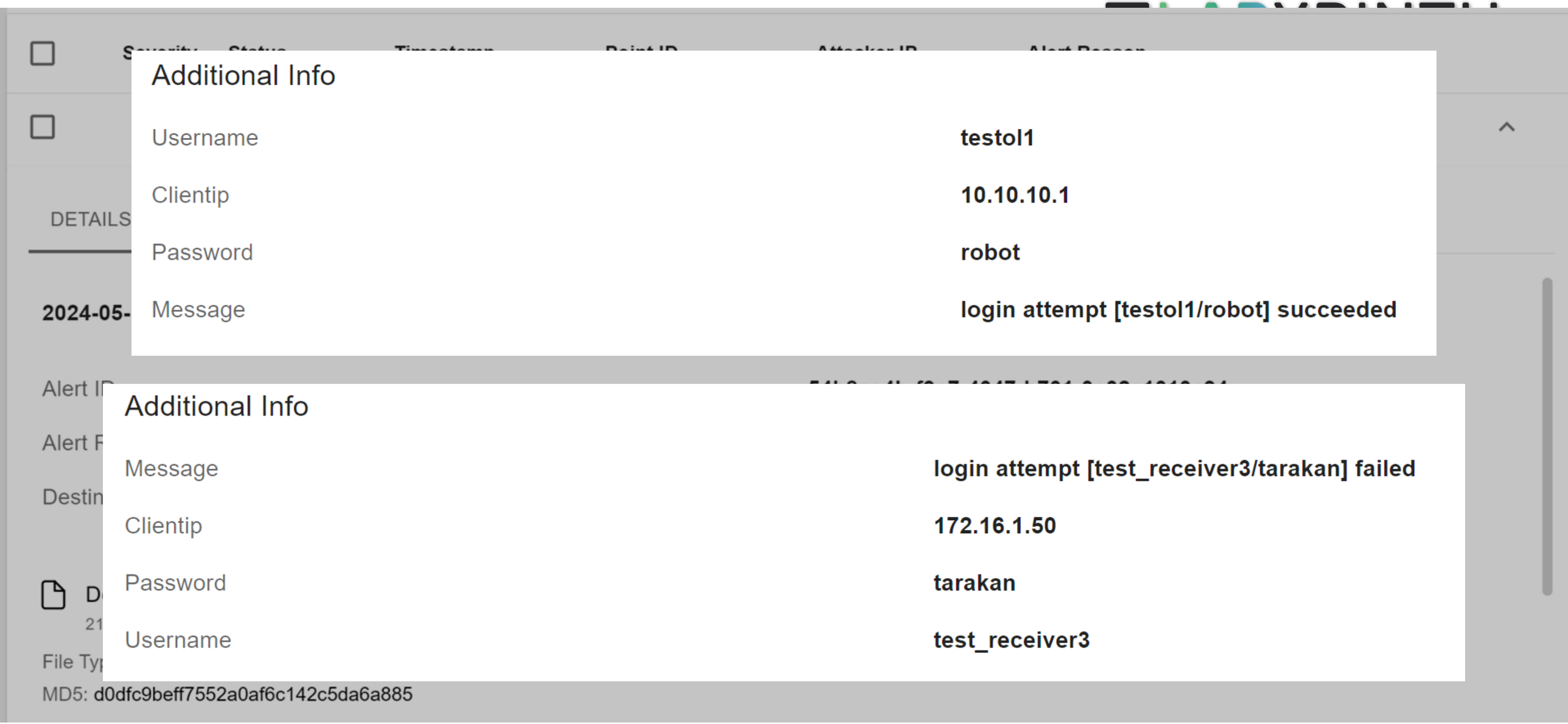
DETAILS EVENTS ACTIVITY(0)

2024-05-16 11:08:58

Alert ID	**54b8ce4b-f9e7-4047-b731-3e02e1010c94**
Alert Reason	**sshd successful login detected**
Destination IP	**10.10.10.71**

Download PCAP
21.31 KB

File Type: pcap
MD5: d0dfc9beff7552a0af6c142c5da6a885


Additional Info
Username
testol1
Clientip
10.10.10.1
Password
robot
Message
login attempt [testol1/robot] succeeded
DETAILS
2024-05-
Alert ID
Alert F
Destin
Additional Info
Message
login attempt [test_receiver3/tarakan] failed
Clientip
172.16.1.50
Password
tarakan
Username
test_receiver3
File Typ
MD5: d0dfc9beff7552a0af6c142c5da6a885

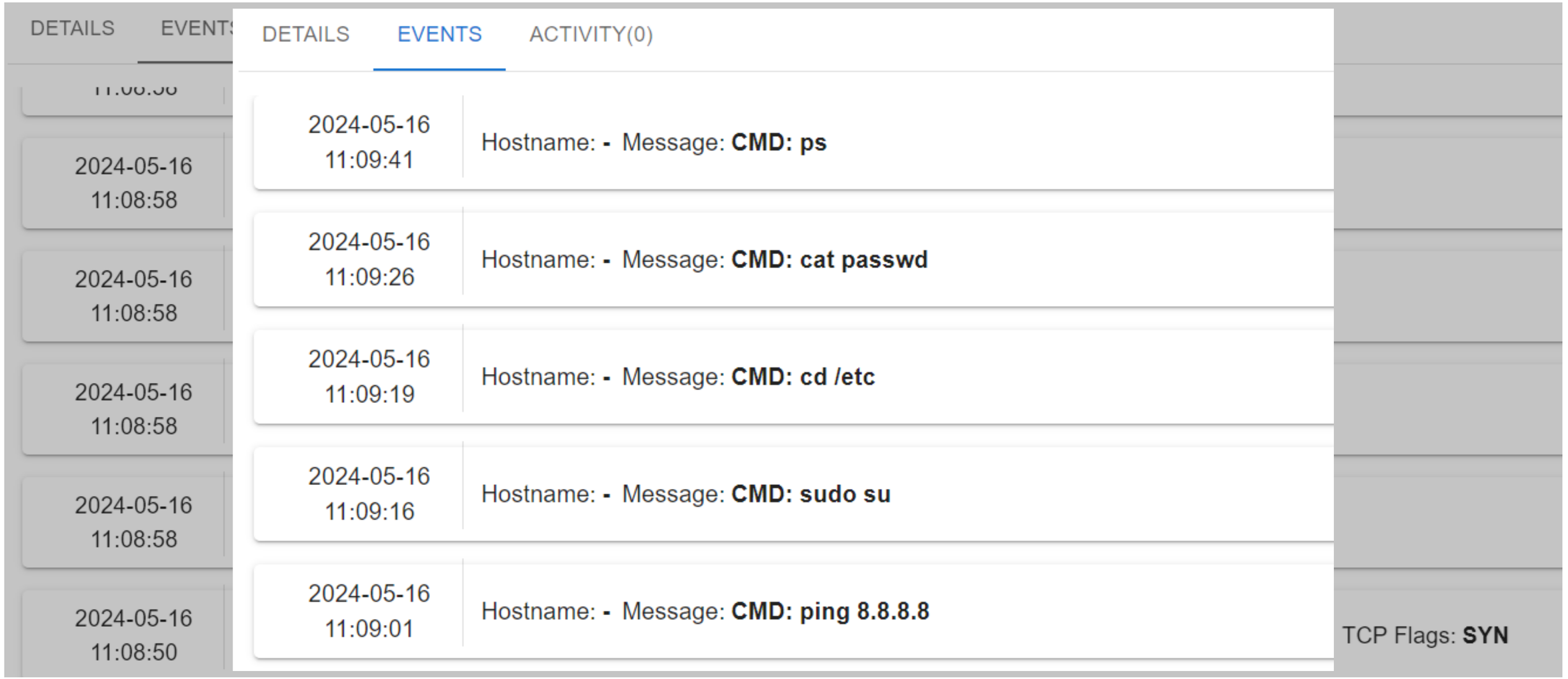
Podrobnosti alarma

LABYRINTH

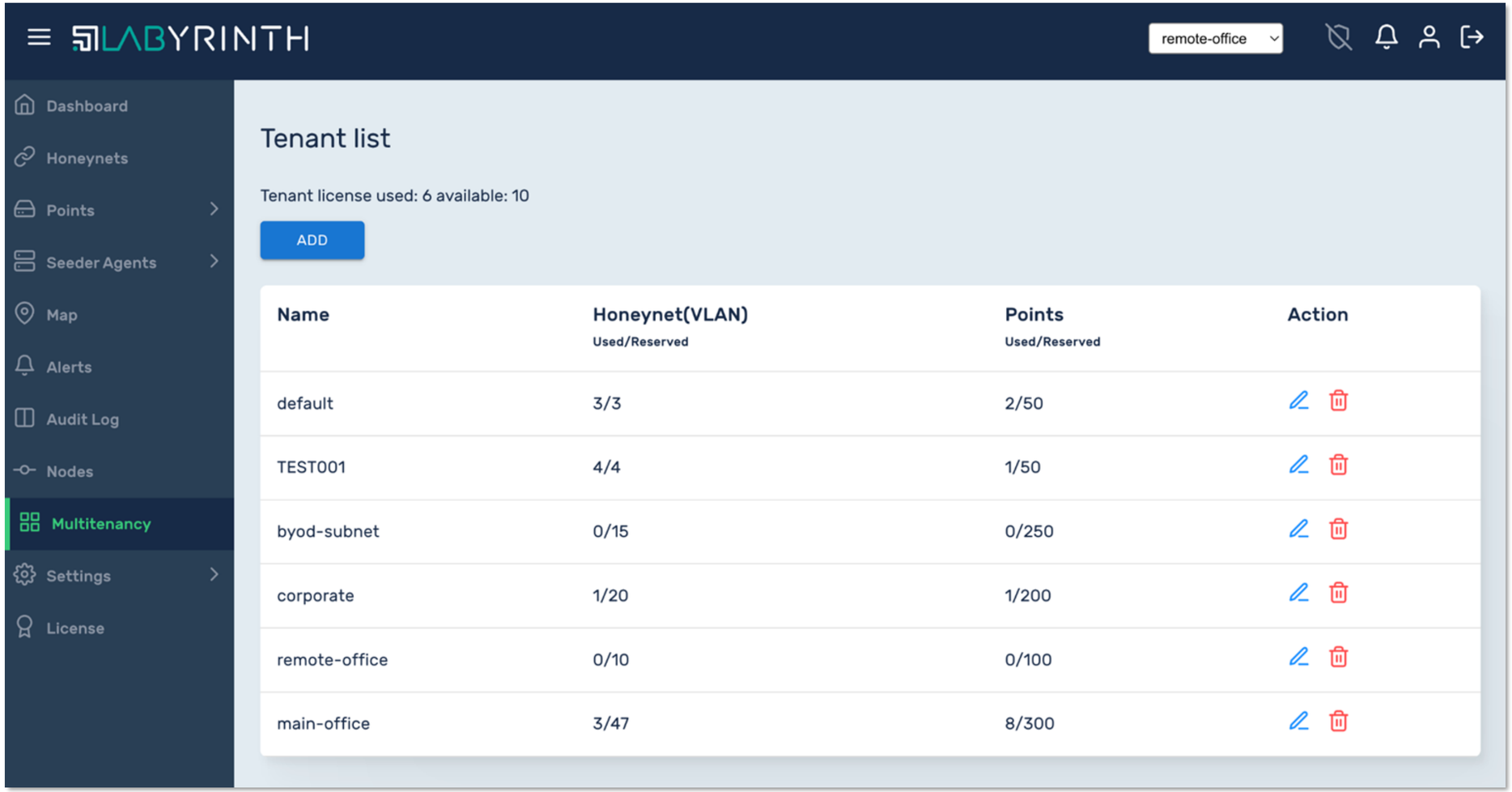
DETAILS | EVENTS | ACTIVITY(0)

11:08:56	
2024-05-16 11:08:58	Hostname: **-** Username: **testol1** Message: **login attempt [testol1/robot] succeeded**
2024-05-16 11:08:58	Hostname: **-** Message: **SSH client hassh fingerprint: 55b7fab6f5d2b485a6773eee233e4a52**
2024-05-16 11:08:58	Hostname: **-** Message: **New connection: 10.10.10.1:12033 (10.10.10.71:22) [session: 8495d6e5e930]**
2024-05-16 11:08:58	Hostname: **-** Message: **Remote SSH version: SSH-2.0-OpenSSH_7.8 FreeBSD-20180909**
2024-05-16 11:08:50	Transport: **tcp** Source IP: **10.10.10.1** Source Port: **12033** Destination IP: **10.10.10.71** Destination Port: **22** TCP Flags: **SYN**

Podrobnosti alarma



Multi-tenant sistem



Integracije z obstoječimi sistemi

LABYRINTH

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	

Zakaj Labyrinth?

- **Vir detekcij** za varnostno-operativni center (SOC)
- Vir informacij **o tehnikah napadov**
- **Network** monitoring
- **Komplementarno** z EDR / XDR rešitvami

Zakaj Labyrinth?

LABYRINTH

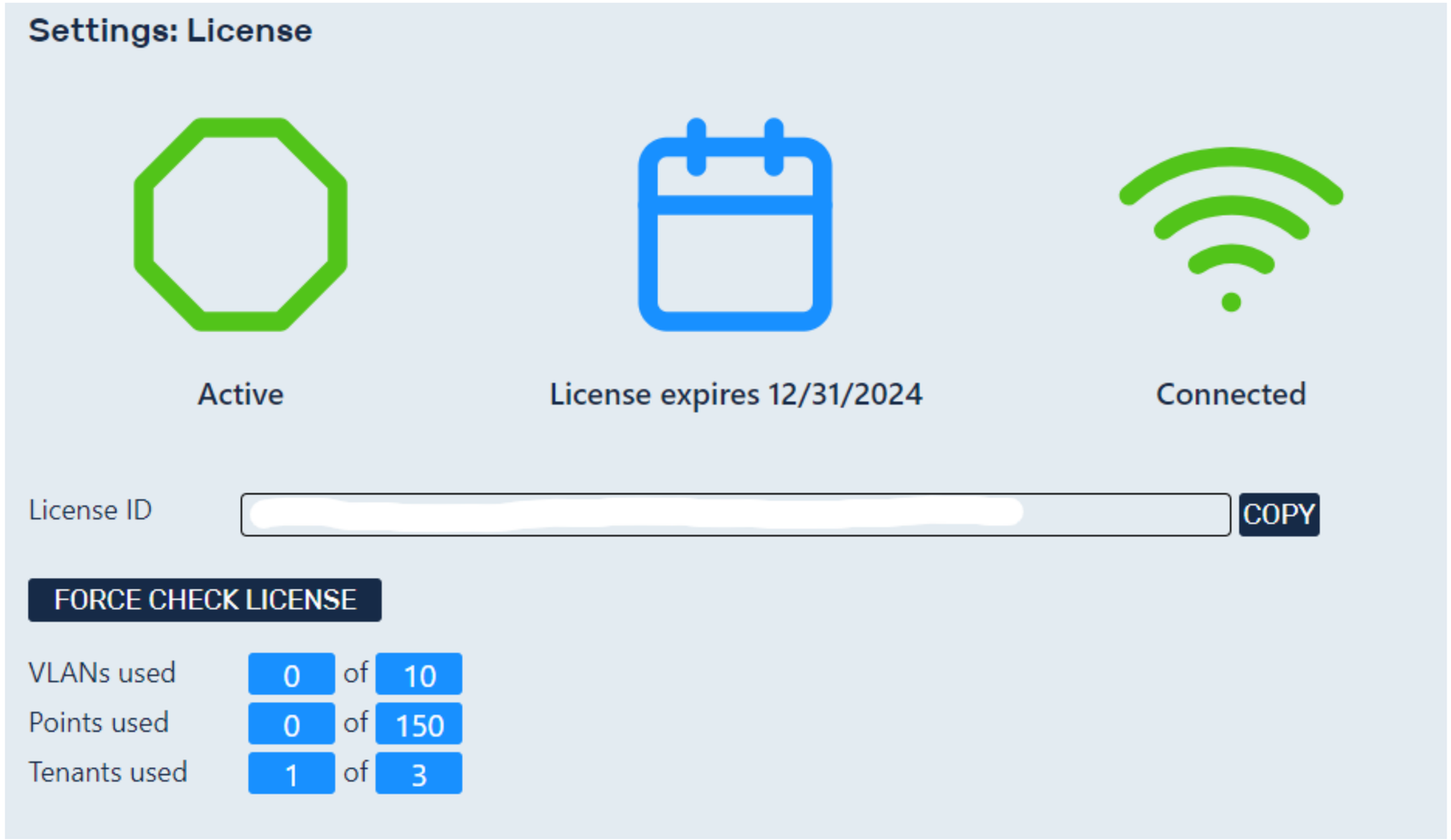
- Hitra in enostavna **implementacija**
- **Brez vpliva** na aktivno infrastrukturo
- Brez **lažnih alarmov**
- Brezplačen **POC** (proof-of-concept)
- Pripravljeno za ponudnike storitev (**MSSP**)
- **Multi-tenant** opcije vgrajene

Thank you

A1 ICT Distribucija

ict-partners@A1.si

Licenciranje



VM dimenzioniranje

LABYRINTH

Requirements for production environment:

Components	Up to 150 Points Up to 15 VLANs	Up to 300 Points Up to 50 VLANs	Up to 500 Points Up to 100 VLANs	More than 500 Points More than 100 VLANs
	vCPU(cores), RAM(GB),HDD(GB)	vCPU(cores), RAM(GB),HDD(GB)	vCPU(cores), RAM(GB),HDD(GB)	vCPU(cores), RAM(GB),HDD(GB)
Admin VM (Management Console)	4 vCPU(cores) 28 GB RAM 500 GB HDD	4 vCPU(cores) 28 GB RAM 500 GB HDD	4 vCPU(cores) 32 GB RAM 800 GB HDD	Contact the manufacturer's representative
Worker VM	8 vCPU(cores) 16 GB RAM 200GB HDD	12 vCPU(cores) 24 GB RAM 250GB HDD	16 vCPU(cores) 40 GB RAM 500GB HDD	
Total	12 vCPU(cores) 44 GB RAM 700 GB HDD	16 vCPU(cores) 52 GB RAM 750 GB HDD	20 vCPU(cores) 72 GB RAM 1300 GB HDD	