

A1

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 (brežžična in žična omrežja)



A1 ICT Distribucija

naši dobavitelji

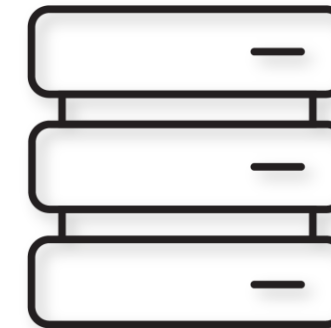


Komponente platforme



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

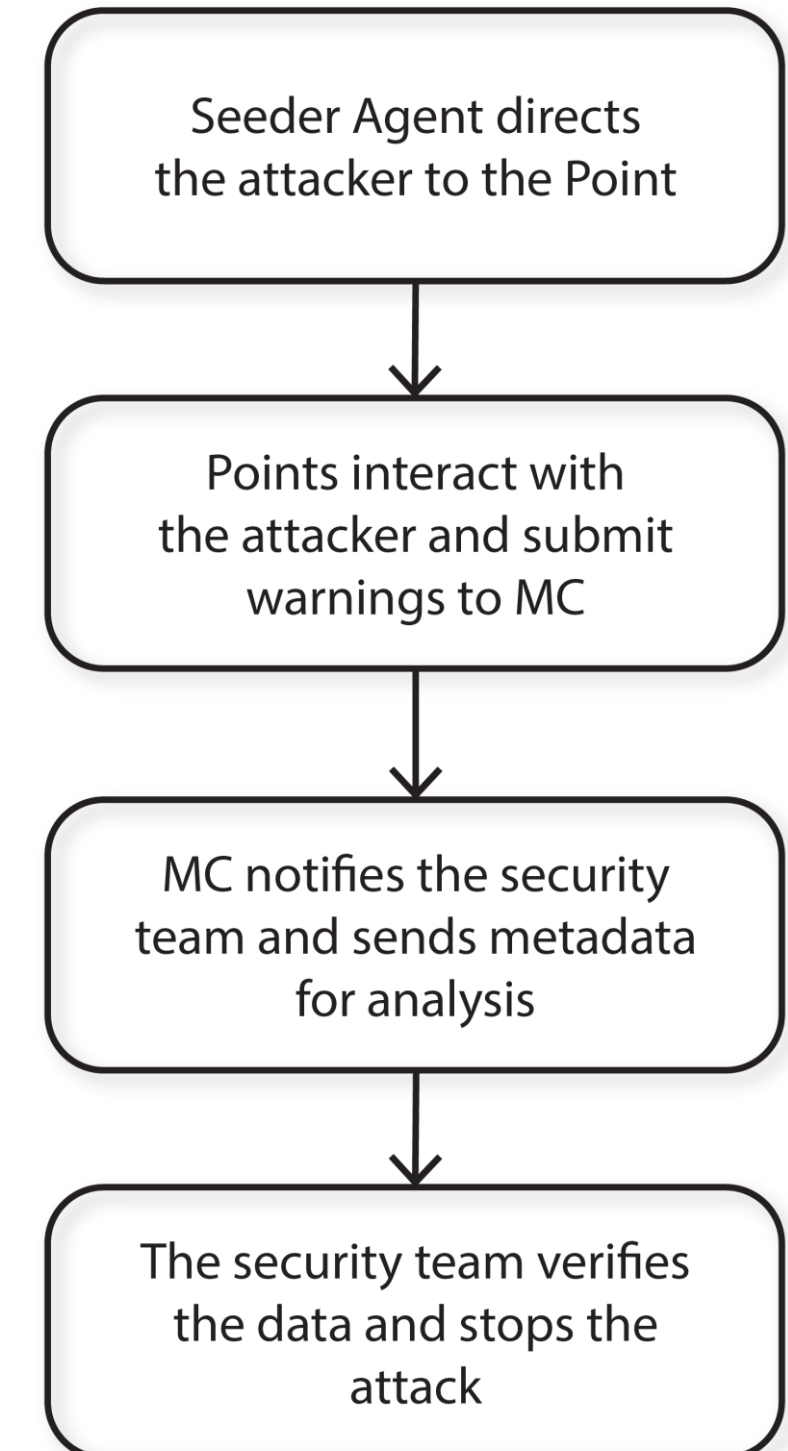
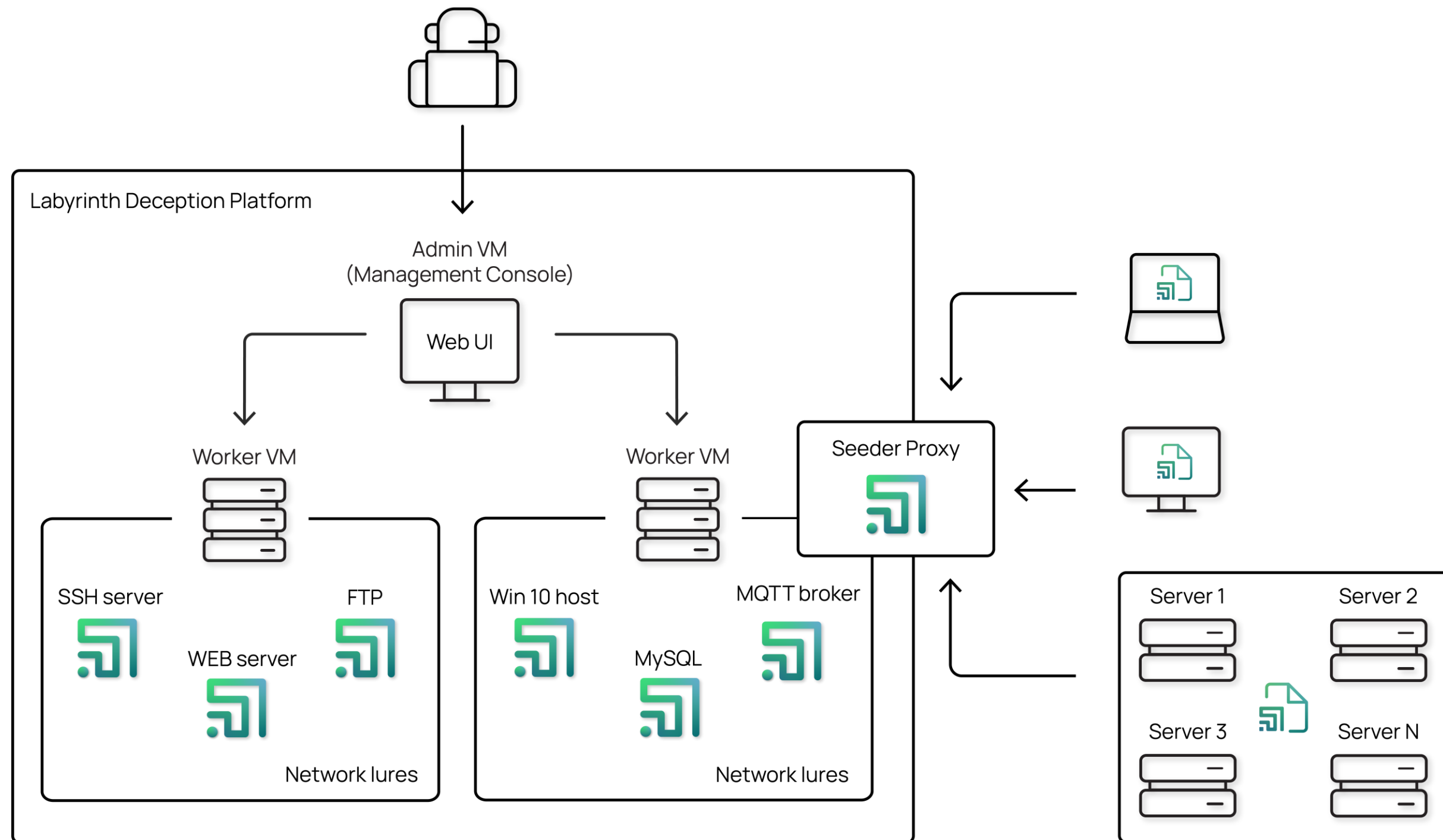
Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.

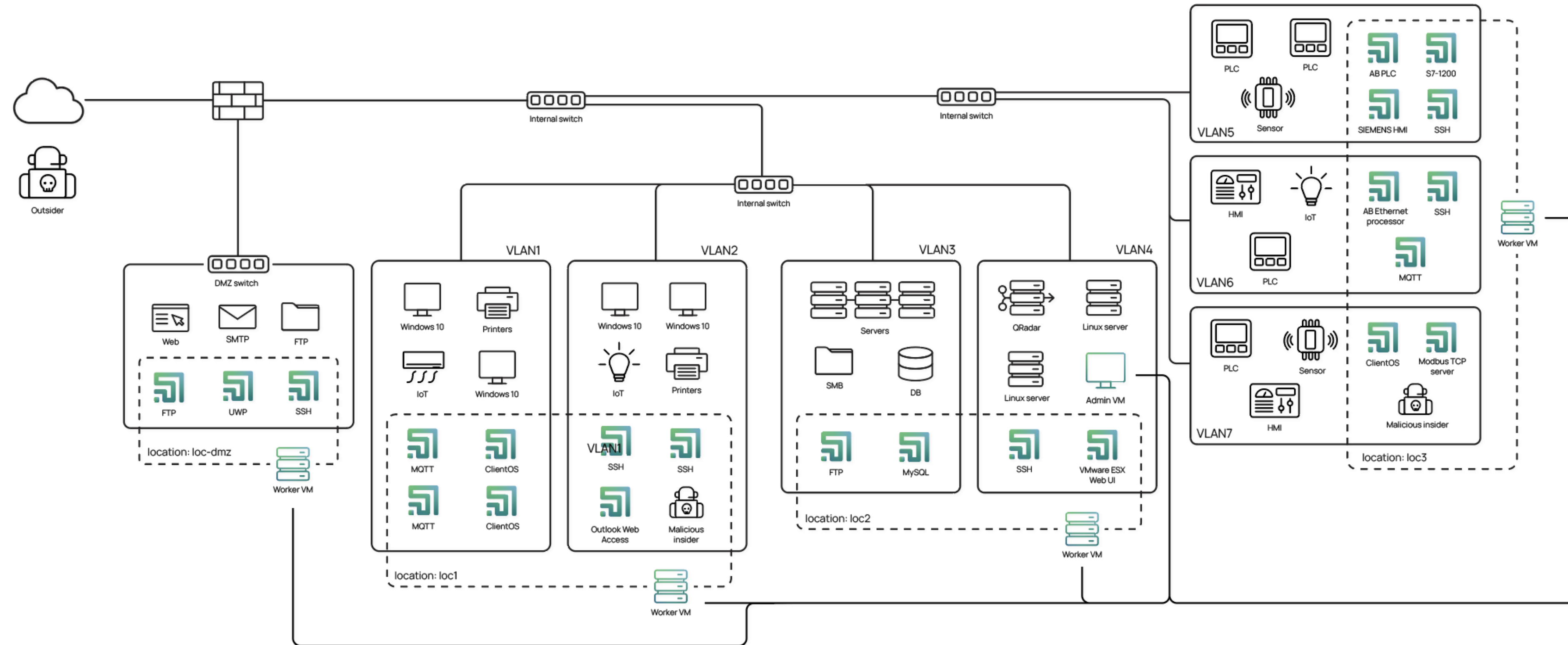


Host with Seeder Agent

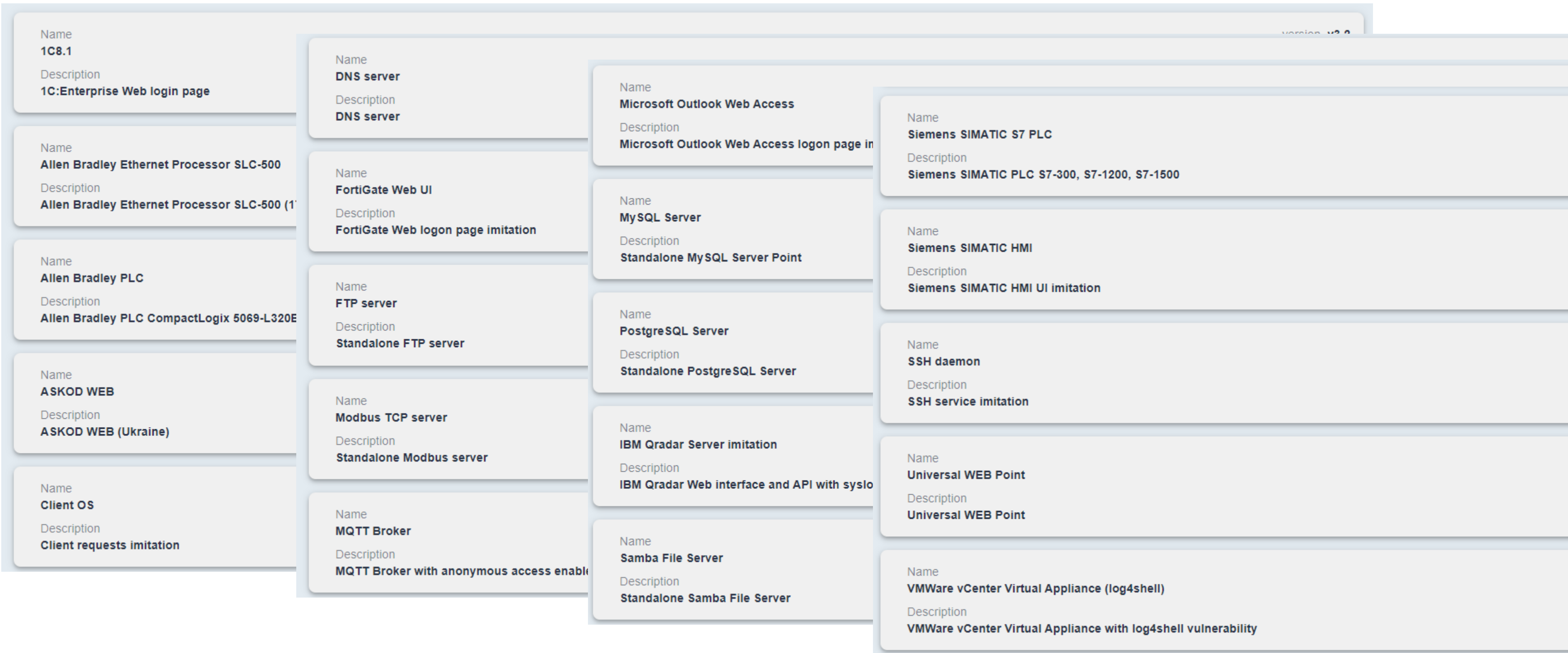
Agents are deployed on real hosts and distribute attractive artifacts to them. The artifacts used by attackers direct them to Points.

Arhitektura platforme





Deception Point Type Bases



Universal Web Point



The screenshot displays the LabYrinth security dashboard. At the top, there is a navigation bar with a dropdown menu set to 'corporate', a shield icon, and a notification bell with '99+' alerts. The main content area is divided into two sections. On the left, a network diagram shows a central node with a tooltip for 'universalweb' containing the following details:

Point Type	universalweb
Hostname	ophelia
IP Adress	172.16.72.116
status	running

On the right, a 'Latest alerts' panel shows two identical alerts. The first alert is titled 'Potentially dangerous HTTP method (POST, PUT or DELETE)' and occurred on 2023-04-05 at 17:11:46. It has a severity of 2. The details for this alert are:

Source IP:	172.16.254.129
Point ID	universalweb-c0463b85
Honeynet	honeynet01
Location	labdev
Point IP	172.16.72.122
Point Type	universalweb

The second alert is identical but occurred at 17:13:22 and has a Point ID of 'universalweb-009d4cbb'. A 'VIEW ALL' link is located at the bottom of the alert panel.

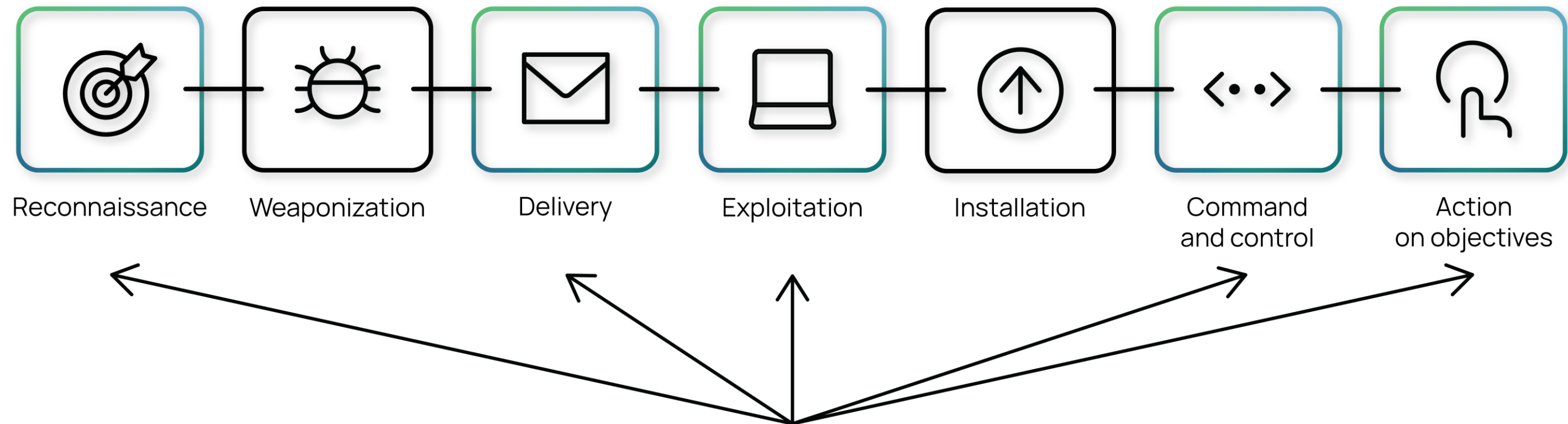
Universal Web Point



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.200.20	button.gif	img	gif	6.47 KB	6.26 KB
200	GET	192.168.200.20	favicon.gif	FaviconLoader.jsm:1...	gif	1.33 KB	1.12 KB
200	GET	192.168.200.20	logo_cis.gif	log_off_page.htm:5...	gif	891 B	678 B
200	GET	192.168.200.20	pageBackground.jpg	log_off_page.htm:5...	jpeg	14.85 KB	14.64 KB
200	GET	192.168.200.20	Status_information_icon.png	log_off_page.htm:5...	png	2.29 KB	2.08 KB
200	GET	192.168.200.20	ContextMessageArrow_DownT.gif	log_off_page.htm:5...	gif	1.03 KB	839 B
200	GET	192.168.200.20	login_progress.gif	log_off_page.htm:5...	gif	886 B	673 B
200	GET	192.168.200.20	topLeft.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.20	topRight.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.20	bottomLeft.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.20	bottomRight.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.20	bar.gif	log_off_page.htm:5...	gif	0.99 KB	801 B

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.200.32	button.gif	img	gif	6.47 KB	6.26 KB
200	GET	192.168.200.32	favicon.gif	FaviconLoader.jsm:1...	gif	1.33 KB	1.12 KB
200	GET	192.168.200.32	logo_cis.gif	log_off_page.htm:5...	gif	891 B	678 B
200	GET	192.168.200.32	pageBackground.jpg	log_off_page.htm:5...	jpeg	14.85 KB	14.64 KB
200	GET	192.168.200.32	Status_information_icon.png	log_off_page.htm:5...	png	2.29 KB	2.08 KB
200	GET	192.168.200.32	ContextMessageArrow_DownT.gif	log_off_page.htm:5...	gif	1.03 KB	839 B
200	GET	192.168.200.32	login_progress.gif	log_off_page.htm:5...	gif	886 B	673 B
200	GET	192.168.200.32	topLeft.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.32	topRight.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.32	bottomLeft.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.32	bottomRight.gif	log_off_page.htm:5...	gif	1 KB	816 B
200	GET	192.168.200.32	bar.gif	log_off_page.htm:5...	gif	0.99 KB	801 B

Zgodnje zaznavanje grožnje



Primer alarma

<input type="checkbox"/>	Severity	Status	Timestamp	Point ID	Attacker IP	Alert Reason	
<input type="checkbox"/>	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

Severity	Status	Timestamp	Host ID	Attacker IP	Alert Reason
Additional Info					
				testol1	
				10.10.10.1	
				robot	
2024-05-					login attempt [testol1/robot] succeeded

Alert ID	Alert F	Destin	File Typ	MD5
Additional Info				
				login attempt [test_receiver3/tarakan] failed
				172.16.1.50
				tarakan
				test_receiver3

MD5: d0dfc9beff7552a0af6c142c5da6a885

Podrobnosti alarma



DETAILS **EVENTS** ACTIVITY(0)

11:08:58	
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

DETAILS	EVENTS	ACTIVITY(0)
11:08:50	2024-05-16 11:08:58	Hostname: - Message: CMD: ps
2024-05-16 11:08:58	2024-05-16 11:09:26	Hostname: - Message: CMD: cat passwd
2024-05-16 11:08:58	2024-05-16 11:09:19	Hostname: - Message: CMD: cd /etc
2024-05-16 11:08:58	2024-05-16 11:09:16	Hostname: - Message: CMD: sudo su
2024-05-16 11:08:50	2024-05-16 11:09:01	Hostname: - Message: CMD: ping 8.8.8.8

TCP Flags: **SYN**

Multi-tenant sistem



Tenant list

Tenant license used: 6 available: 10

[ADD](#)

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

Integracije z obstoječimi sistemi



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

Zakaj Labyrinth?

 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


A1


**Thank
you**


A1 ICT Distribucija

ict-partners@A1.si

Settings: License

 Active

 License expires 12/31/2024

 Connected

License ID **COPY**

FORCE CHECK LICENSE

VLANs used of

Points used of

Tenants used of

VM dimenzioniranje



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	