A1 Webinar

Zakaj je Deception Point ena izmed naboljših obrambnih tehnologij?

Združite EDR/XDR s tehnologijo zavajanja in učinkovito odgovorite na kompleksne kibernetske grožnje

LABYRINTH

Kje: **spletni seminar**
Kdaj: **5. junij 2025 ob 10. uri**

A1 ICT Distribucija

Distributer z dodano vrednostjo

- Partnerski program
- Široka mreža partnerjev v Adria regiji
- Prodajna in tehnična podpora partnerjem
- Organizacija tehničnih treningov
- Promocija vendorjev na dogodkih/konferencah
- Širok nabor evropskih rešitev
  - Endpoint zaščita (EPP, EDR, XDR)
  - Zaščita za mrežo (NGFW/UTM, NDR, Deception)
  - Zaščita za elektronsko pošto (Antispam/antiphishing)
  - Upravljanje privilegiranih uporabnikov (PAM)
  - Večnivojska avtentikacija (MFA)
  - Backup (online, offsite)
  - SIEM

A1 ICT Distribucija

Ekipa

Sergeja Cvelfer

Vodja oddelka za distribucijo ICT rešitev

Tadej Križovnik

Ekspert za distribucijo ICT rešitev

Maja Milojević

Ekspert za distribucijo ICT rešitev

Marko Kašić

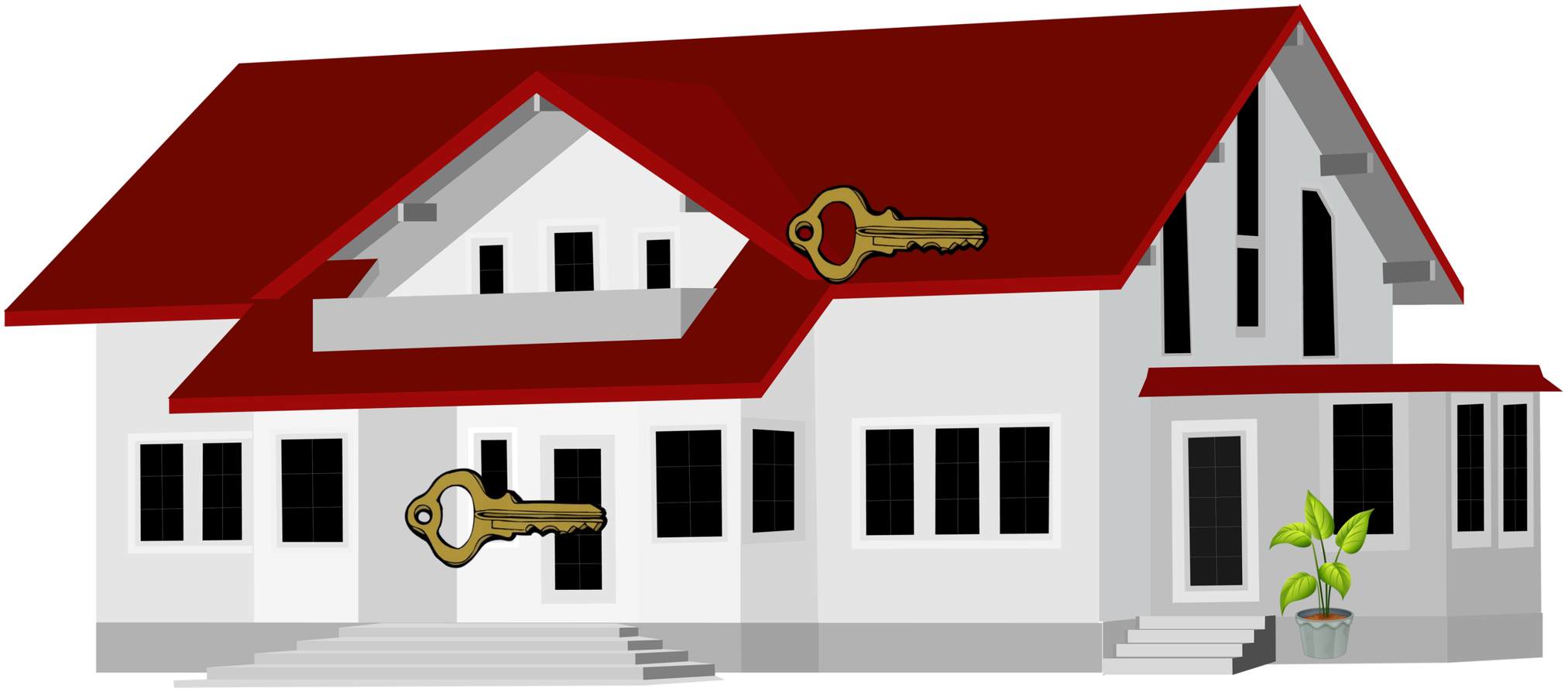
Vodilni ICT inženir

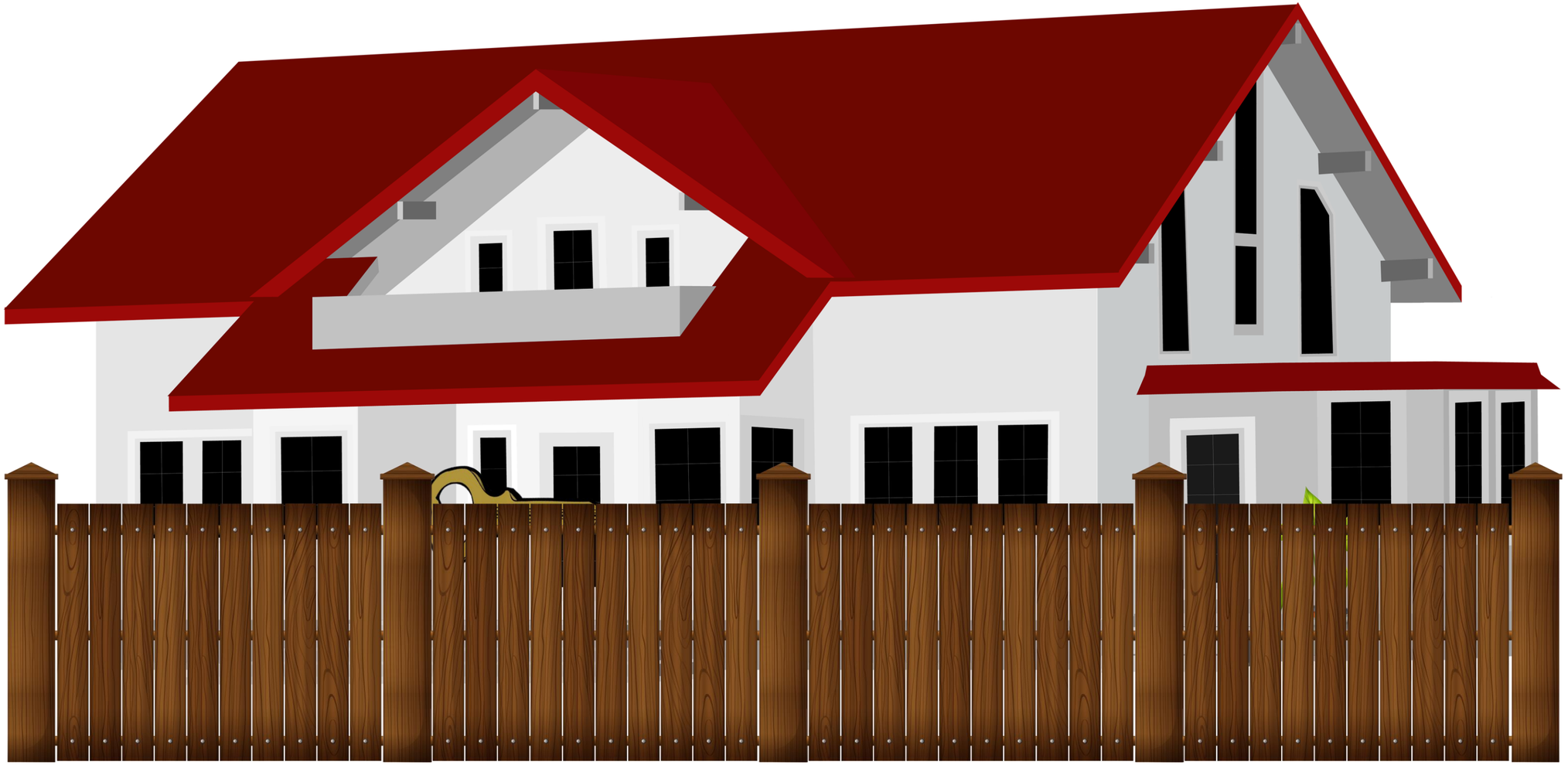
Filip Šimonka

Ekspert za distribucijo ICT rešitev

Amadej Blažinčič

Ekspert za implementacijo ICT rešitev





LABYRINTH

Grožnje in varnost

Naprednost groženj

Pisanje virusov „za zabavo“

Potencialna škoda

Neprijetnost

Zmožnost zaznavanja

Vidne težave, nestabilnosti, o katerih poročajo uporabniki

Dolžina napada

Takojšnji učinek

LABYRINTH

Grožnje in varnost

Naprednost groženj

Pisanje virusov „za zabavo“ → Botneti & kibernetski kriminal v porastu

Potencialna škoda

Neprijetnost → Nekaj finančnih izgub

Zmožnost zaznavanja

Vidne težave, nestabilnosti, o katerih poročajo uporabniki → Analiza podpisov, prometa in dnevnikov za iskanje groženj

Dolžina napada

Takojšnji učinek → Oportunistični napadi, nekaj minut ali ur

LABYRINTH

Grožnje in varnost

Naprednost groženj

Pisanje virusov „za zabavo“ → Botneti & kibernetski kriminal v porastu → Napredni ransomware napadi & vztrajne grožnje(APT)

Potencialna škoda

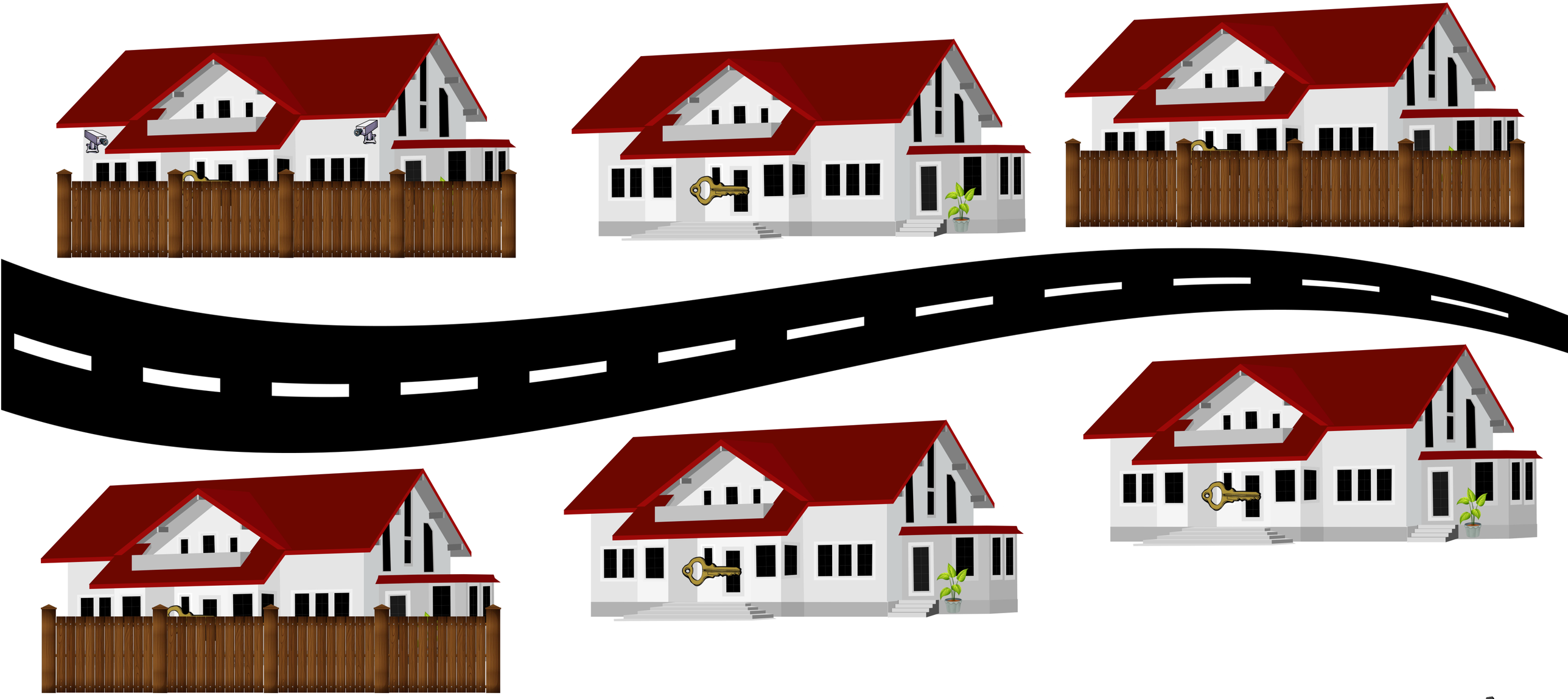
Neprijetnost → Nekaj finančnih izgub → Organizacije se ugasnejo, več dni/tednov zaprtja

Zmožnost zaznavanja

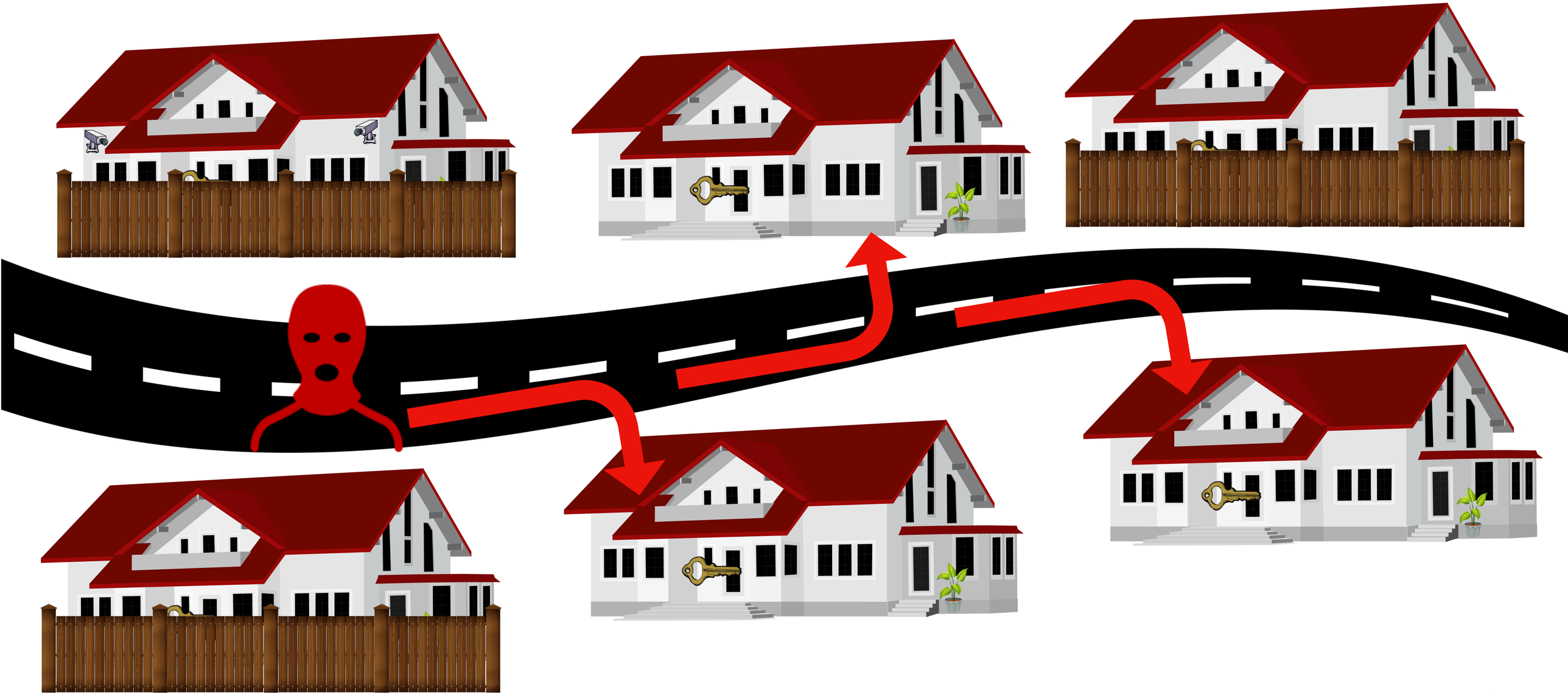
Vidne težave, nestabilnosti, o katerih poročajo uporabniki → Analiza podpisov, prometa in dnevnikov za iskanje groženj → Proaktivni sistemi za zgodnje opozarjanje, 24/7 SOC

Dolžina napada

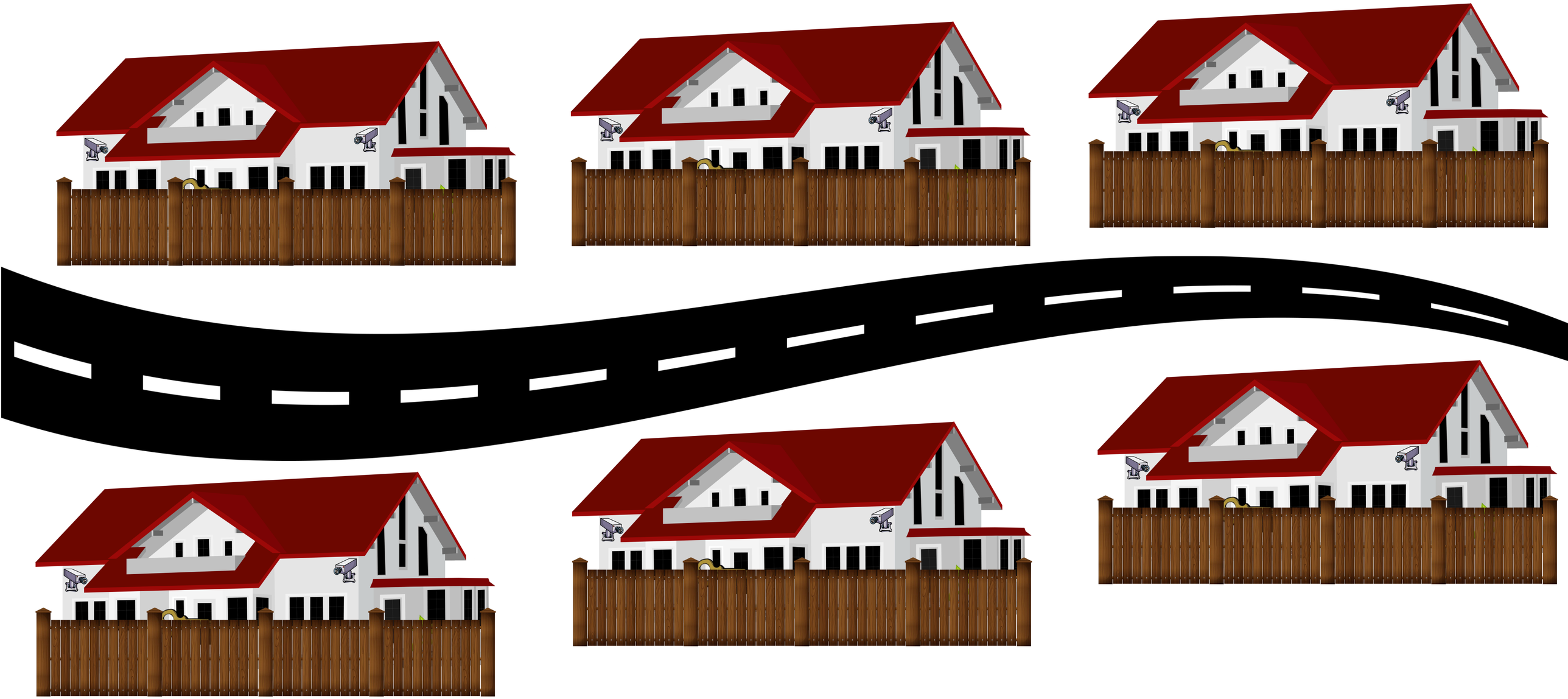
Takojšnji učinek → Oportunistični napadi, nekaj minut ali ur → Tedne ali mesece



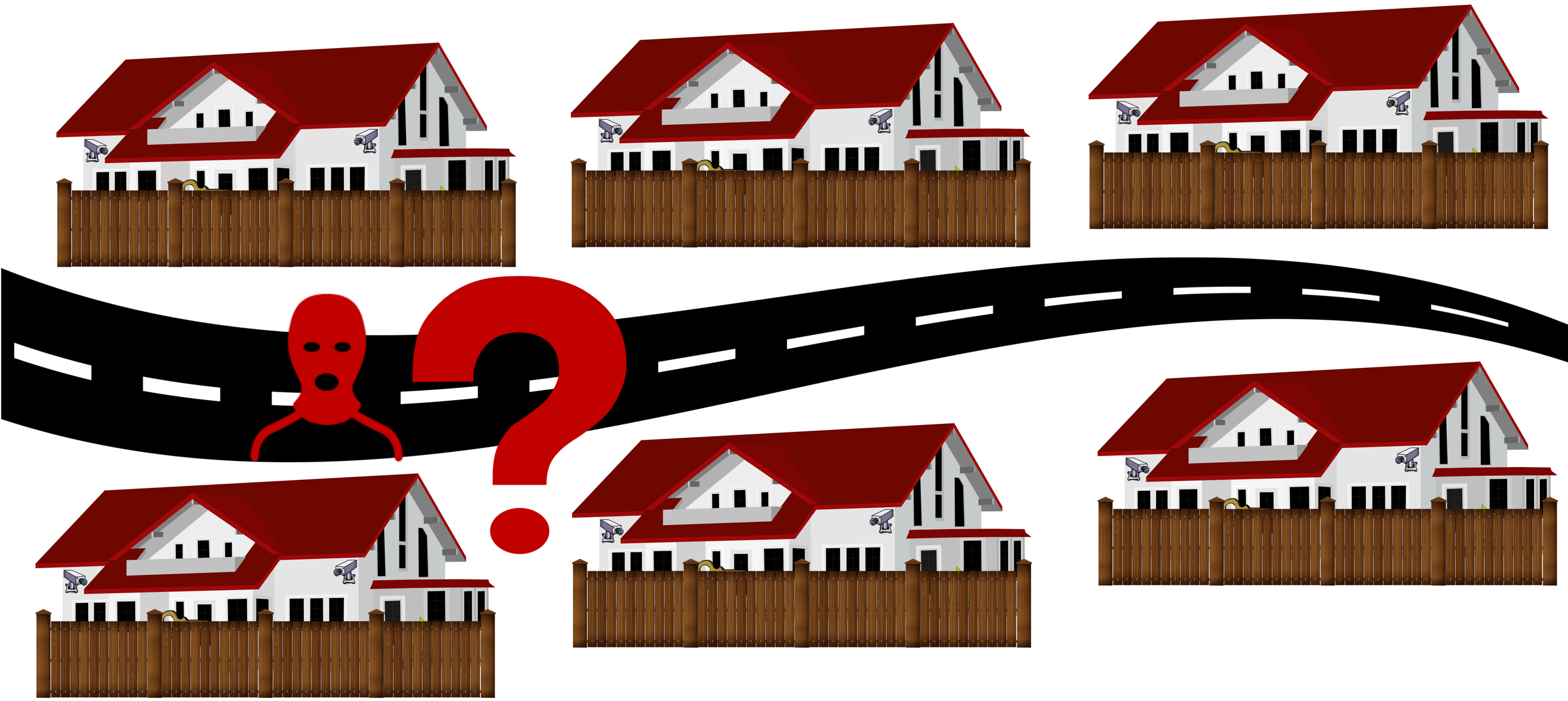
LABYRINTH



LABYRINTH



LABYRINTH



LABYRINTH

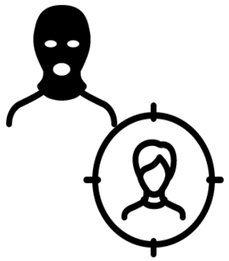
Vedno korak zadaj?

- Virus
- Spyware
- Spam
- Phishing
- Ransomware
- …

- Antivirus
- Antispyware
- Antispam
- Antiphishing
- Antiransomware
- …

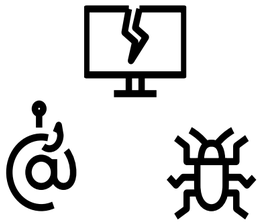
LABYRINTH

Potrebno razumevanje groženj



ČLOVEŠKI NADZOR

TEHNOLOŠKI NADZOR
VELIKEGA ŠTEVILA NAPADOV



DRŽAVE
Neznana 0-day orodja
ter tehnike napadov

OGRANIZIRAN KRIMINAL
Prikriti, organizirani ter
usmerjeni napadi

KRIMINAL
Brezdatotečni
napadi, skripte,
sistemska orodja

RANSOMWARE

PREPROSTI NAPADI
Oportunistični
Phishing
Malware
Spam

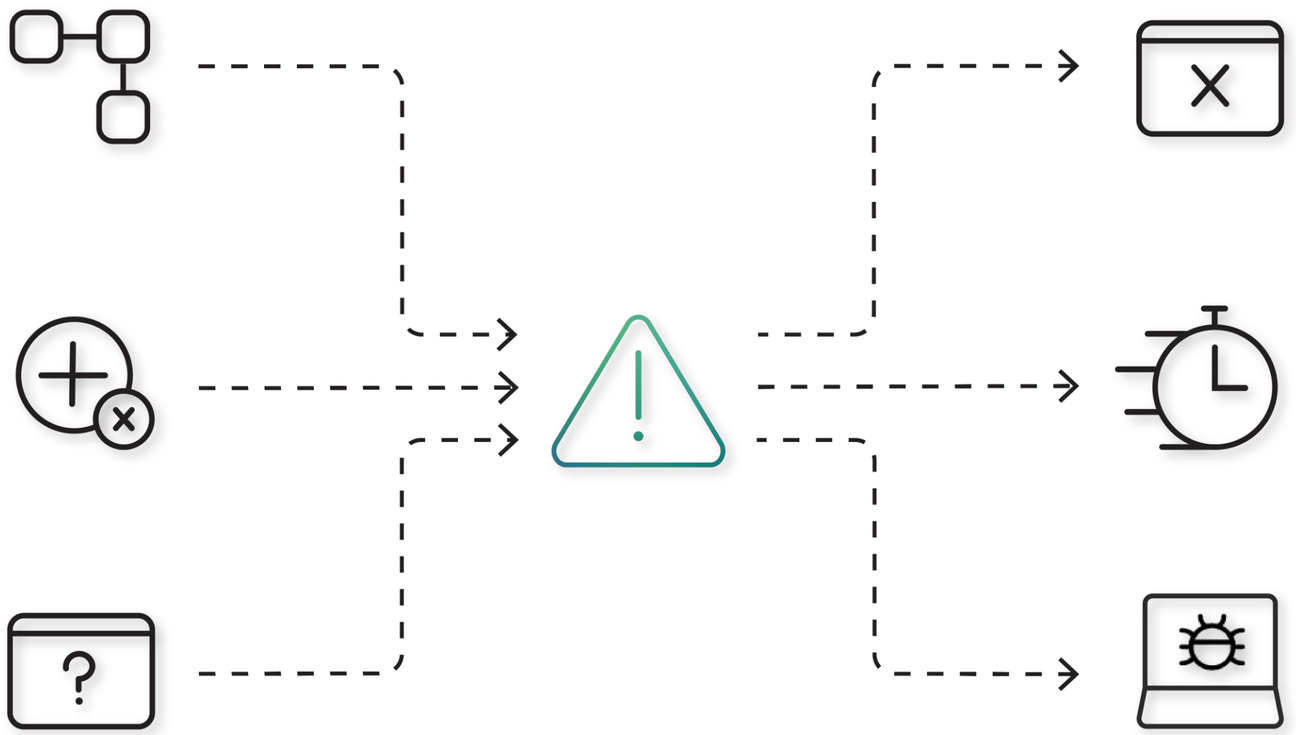
LABYRINTH

Izzivi

Reagiranje na zaznane grožnje

Delo z lažnimi alarmi

Kompleksno delo, dodatni člani ekipe?



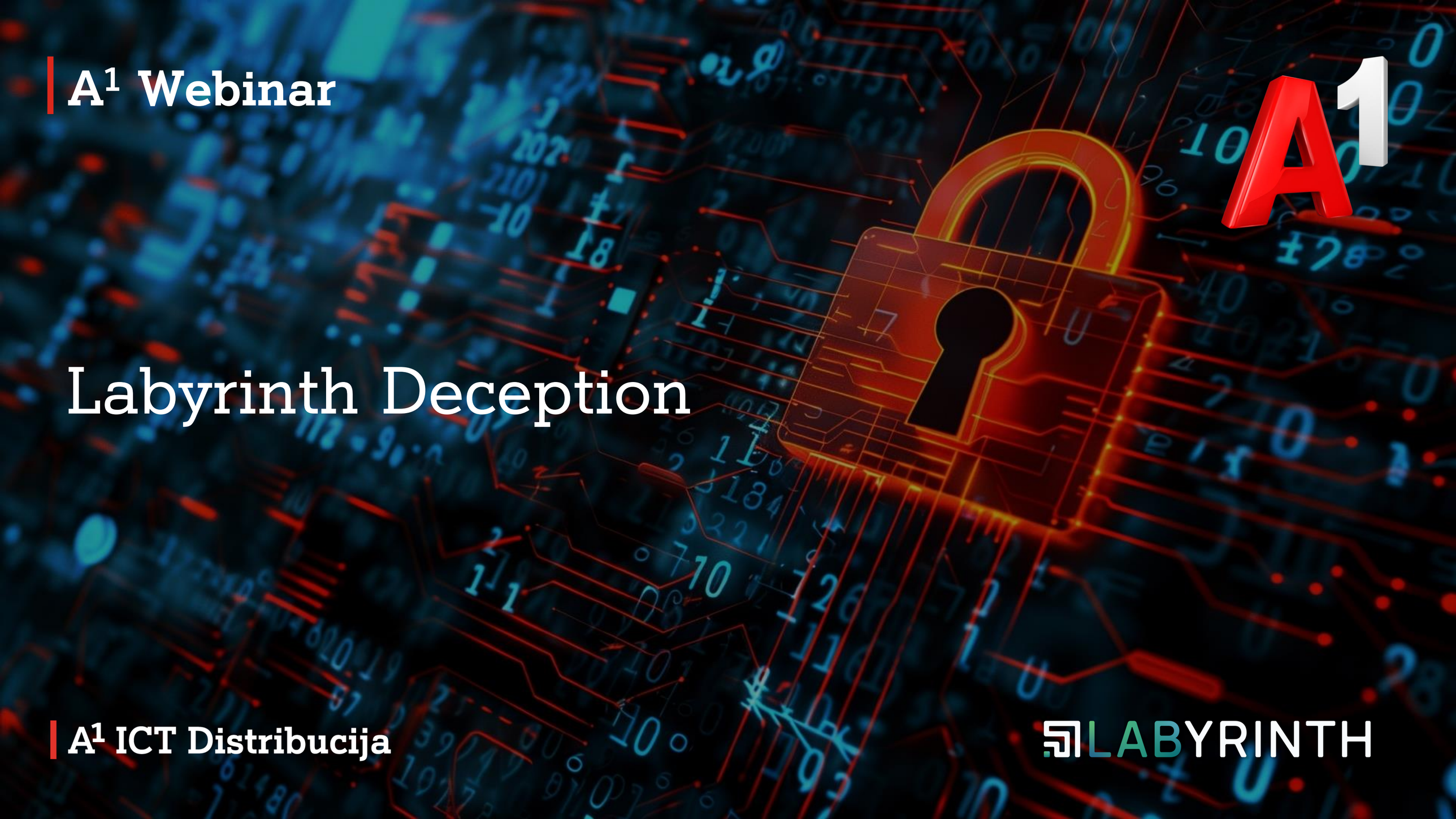
Preobremenitev z informacijami

Daljši čas zaznavanja in odzivanja

Uspešni vdori

A1 Webinar

Labyrinth Deception



A1 ICT Distribucija

LABYRINTH

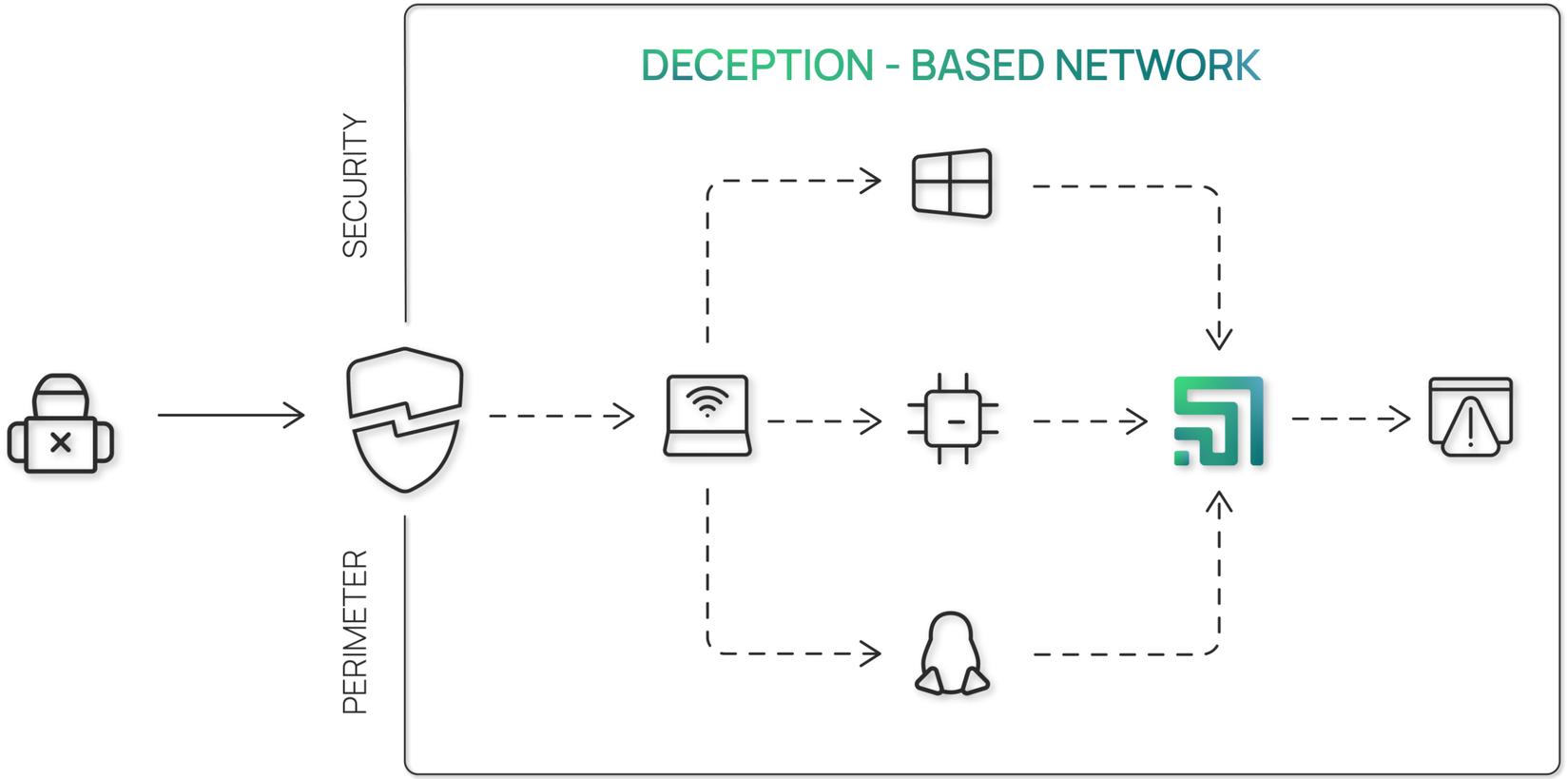
Drugačen pristop za spremljanje omrežja?

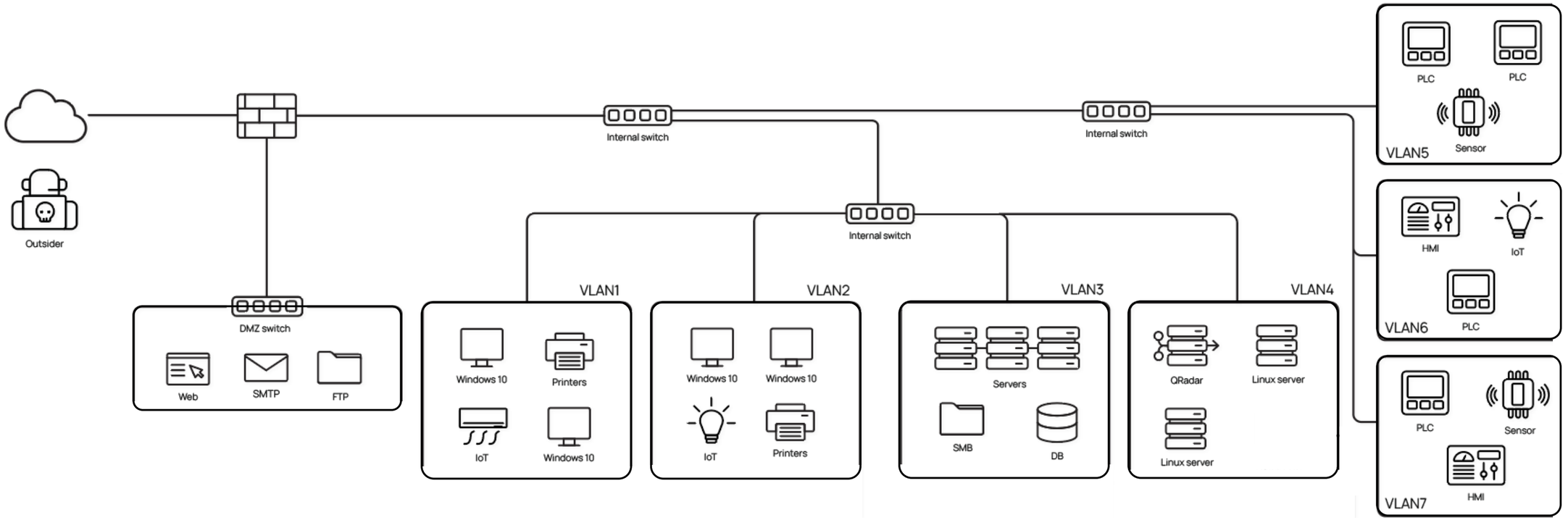
Kdo je Labyrinth?

- **Osnovan u 2019.**
- Sedež v Zabrze, Poljska
- Spletna stran: www.labyrinth.tech
- LinkedIn profil: link
- YouTube kanal: link

Zaznavanje groženj z uporabo tehnologije zavajanja

Platforma Labyrinth spreminja kibernetsko varnost z uporabo proaktivnega pristopa k zaznavanju groženj.




Outsider
Internal switch
Internal switch
Internal switch
DMZ switch
Web
SMTP
FTP
VLAN1
Windows 10
Printers
IoT
Windows 10
VLAN2
Windows 10
Windows 10
IoT
Printers
VLAN3
Servers
SMB
DB
VLAN4
QRadar
Linux server
Linux server
PLC
PLC
Sensor
VLAN5
HMI
IoT
PLC
VLAN6
PLC
Sensor
HMI
VLAN7

LABYRINTH

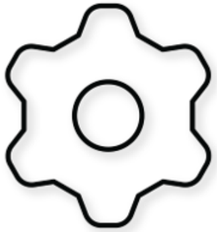
Zakaj Labyrinth

Zaustavitev naprednih groženj

Zaznava usmerjene in napredne napade pred predhodnega poznavanja oblike, tipa ali obnašanja grožnje.

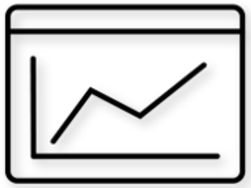
Brez vpliva na delovanje

Brez negativnega učinka na delovanje ostalih naprav v omrežju.



Enostavna implementacija

Hitra in enostavna implementacija brez sistemskih konfliktov in minimalnim vzdrževanjem: brez baz podatkov, podpisov ali pravil, ki jih je potrebno nastavljati ali posodabljati.



Znižanje operativnih stroškov*

Ne zbira velikih količin podatkov, ne ustvarja lažnih alarmov, ne potrebuje specialističnega znanja za upravljanje.

Avtomatizacija odzivanja na incidente

Pospešitev odzivanja na incidente z zniževanjem časa zaznavanja in odzivanja (MTTD, MTTR) do 12-krat**.

* https://www.enterprisemanagement.com/news/press_release.php?p_id=2659

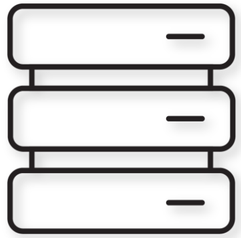
** https://www.bloomberg.com/press-releases/2020-09-14/cyber-deception-reduces-data-breach-costs-by-over-51-and-soc-inefficiencies-by-32

LABYRINTH

Gradniki platforme

Admin VM (Management Console)

Vse informacije zbrane na pasteh (Points) in posredovane na konzolo za upravljanje za nadaljnjo analizo incidenta in odzivanje.



Worker VM

Gradnik, ki gosti vse naprave, na katerih so pasti (Points) Labyrintha. Lahko deluje v več VLAN-ih hkrati.

Point

Point je simulacija aplikacij in storitev iz resničnega IT okolja in ponuja interakcijo z napadalci, s čimer jih drži znotraj Labyrintha.

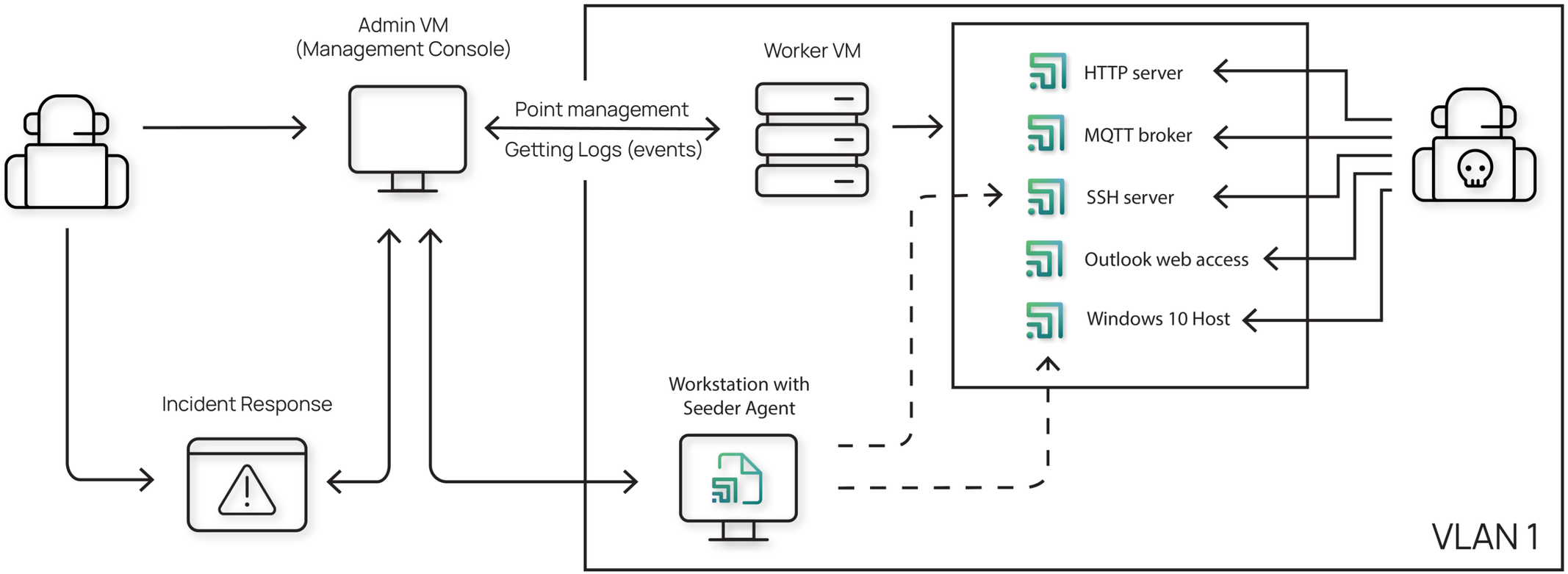
Host with Seeder Agent

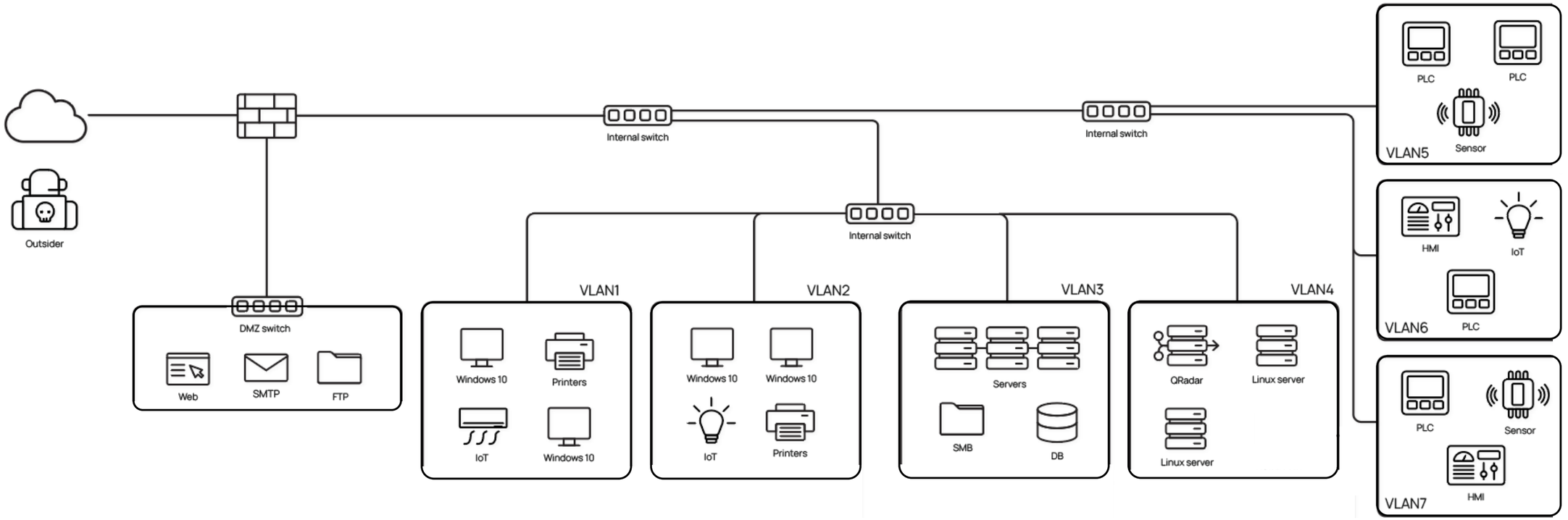
Agente sprožimo na pravih delovnih postajah in porazdelimo zanimive sledi, ki usmerijo napadalca proti postavljenim pastem (Points).

LABYRINTH

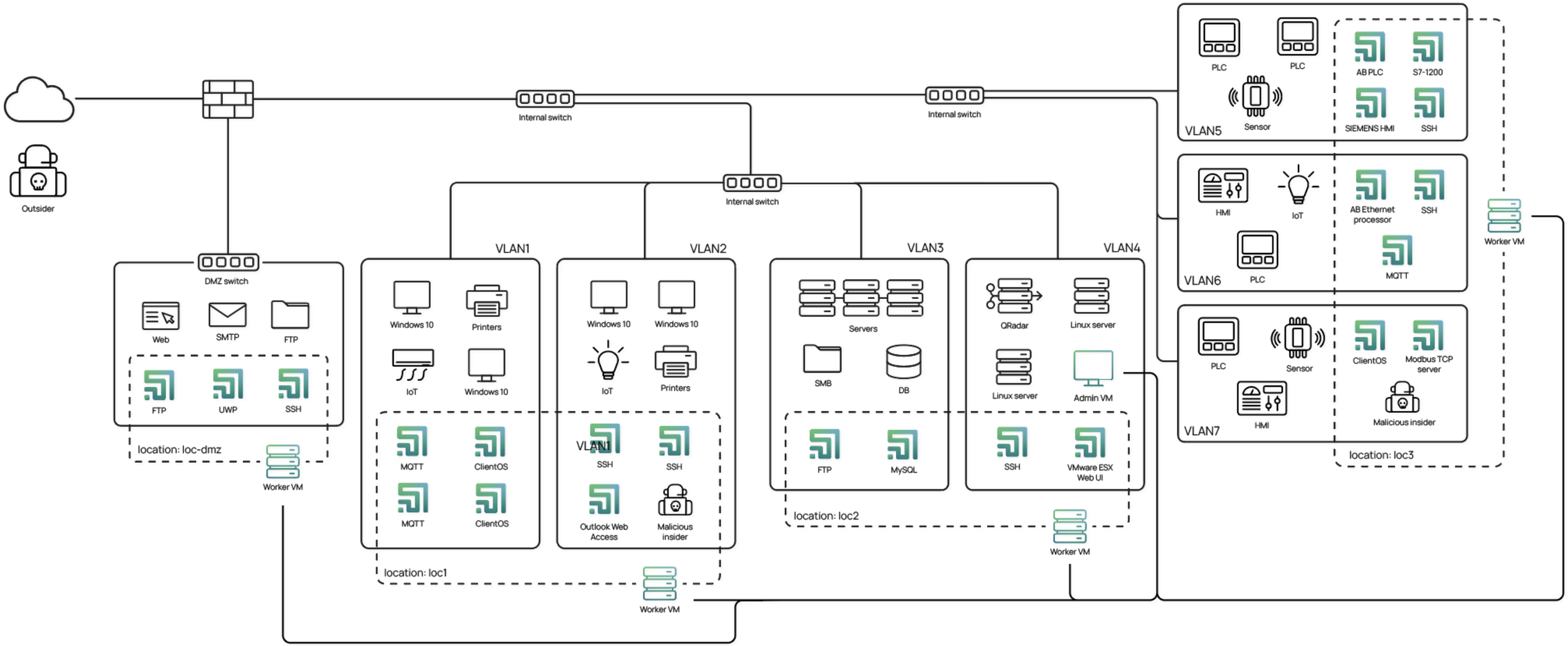
Labyrinth Deception Platform

Platforma ustvari namensko ranljive IT storitve in aplikacije, s čimer poveča število potencialnih tarč v okolju in napadalca preusmerja. Labyrinth izzove napadalca, s čimer zaznava in sledi vsem njihovih aktivnostim ter jih izolira od dejanskega IT okolja.




Outsider
Internal switch
Internal switch
Internal switch
DMZ switch
Web
SMTP
FTP
VLAN1
Windows 10
Printers
IoT
Windows 10
VLAN2
Windows 10
Windows 10
IoT
Printers
VLAN3
Servers
SMB
DB
VLAN4
QRadar
Linux server
Linux server
PLC
PLC
Sensor
VLAN5
HMI
IoT
PLC
VLAN6
PLC
Sensor
HMI
VLAN7

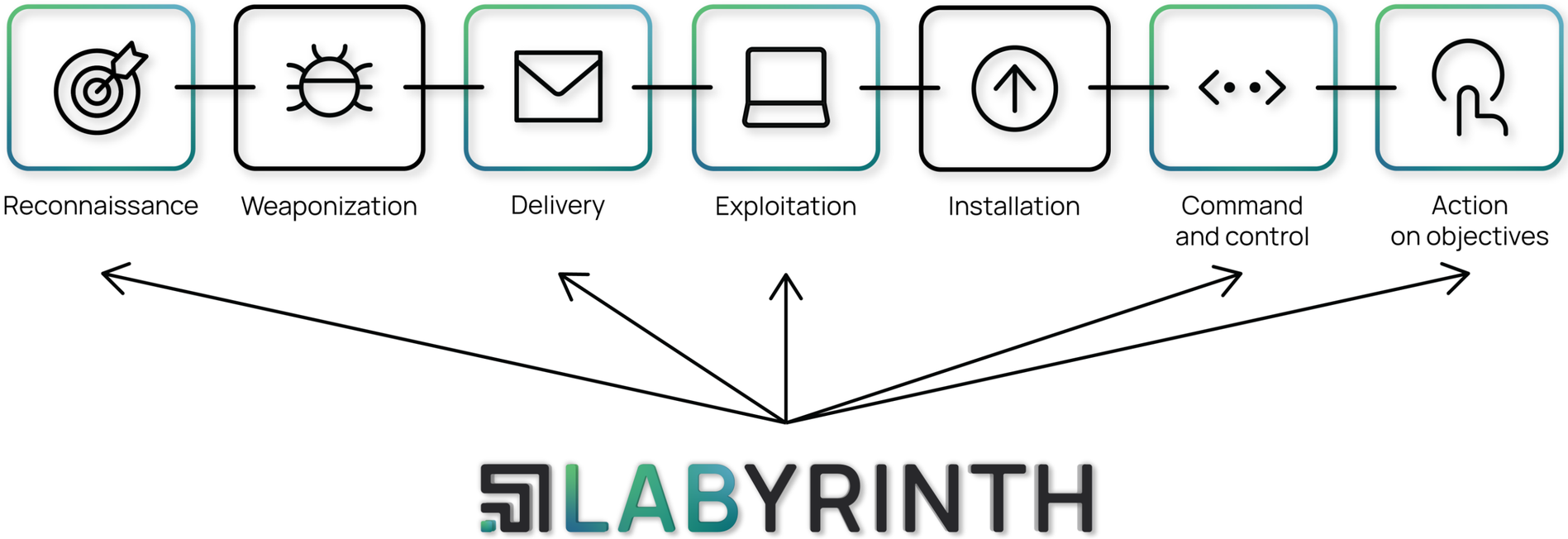
LABYRINTH



A1 ICT Distribucija

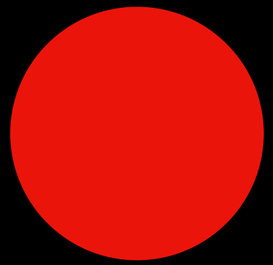
Kibernetski „kill-chain“

Labyrinth je najbolj učinkovit v **zgodnjem odkrivanju napada**



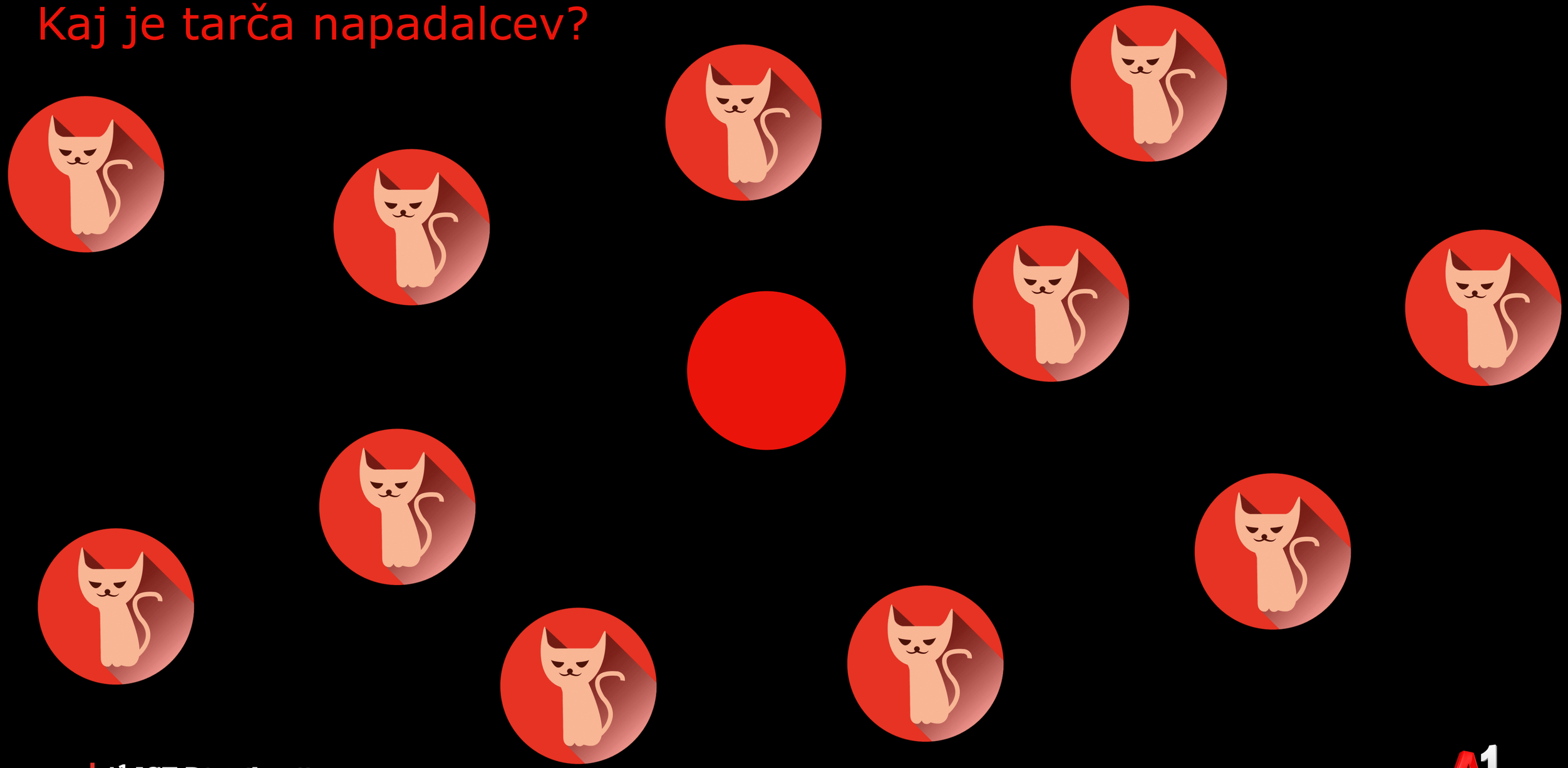
LABYRINTH

Kaj je tarča napadalcev?



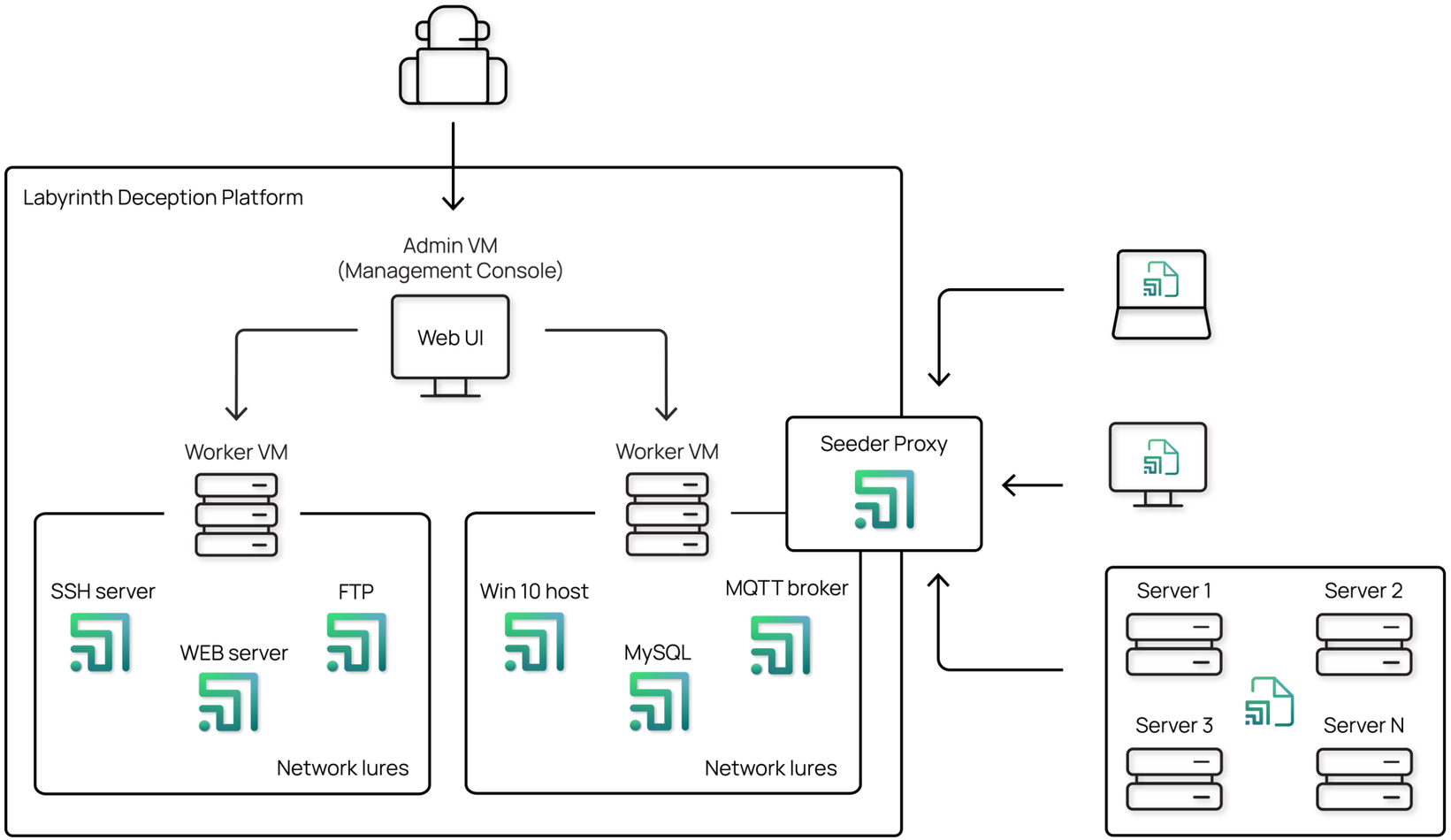
LABYRINTH

Kaj je tarča napadalcev?



LABYRINTH

Pot napadalca



Seeder Agent usmeri napadalca v past (Point)

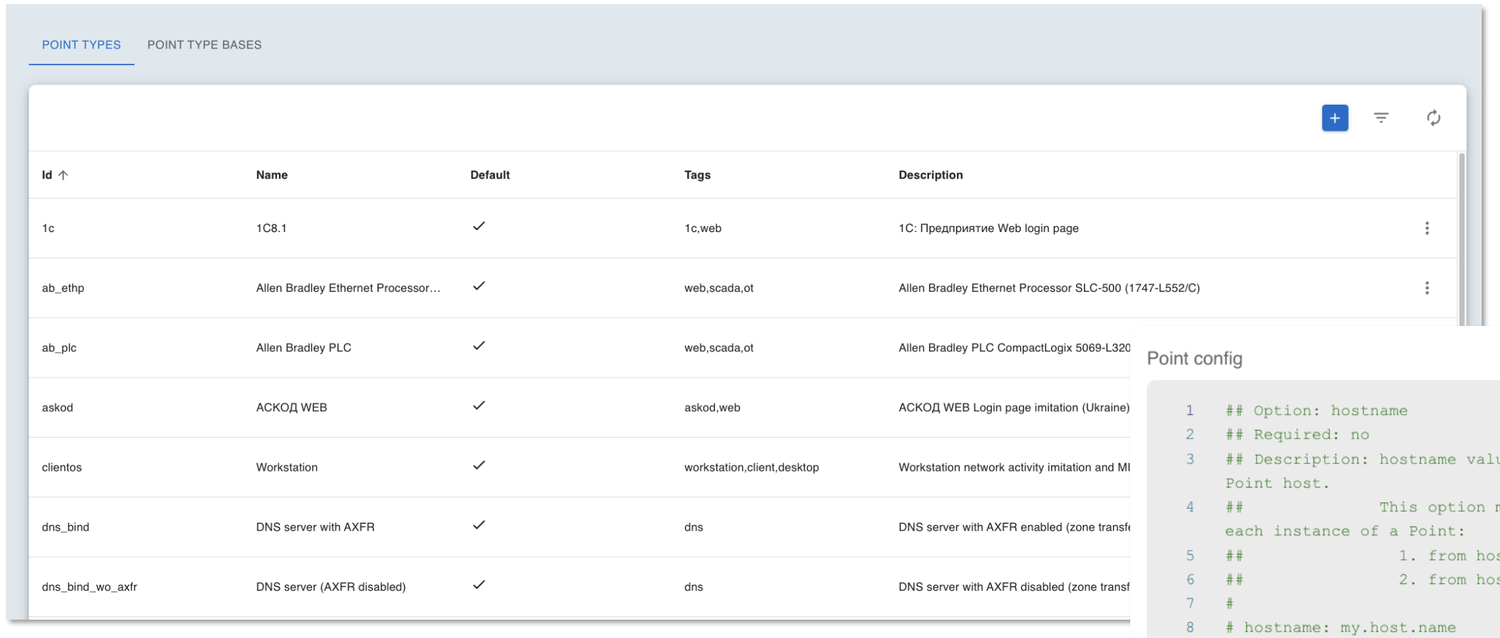
Pas (Point) komunicira s napadalcem i pošlje alarme na konzolo

Konzola alarmira ekipo za odzivanje in pošalje metapodatke za analizo

Ekipa za odzivanje potrdi podatke i zaustavi napad

LABYRINTH

Points



Id	Name	Default	Tags	Description
1c	1C8.1	✓	1c,web	1C: Предприятие Web login page
ab_ethp	Allen Bradley Ethernet Processor…	✓	web,scada,ot	Allen Bradley Ethernet Processor SLC-500 (1747-L552/C)
ab_plc	Allen Bradley PLC	✓	web,scada,ot	Allen Bradley PLC CompactLogix 5069-L320
askod	АСКОД WEB	✓	askod,web	АСКОД WEB Login page imitation (Ukraine)
clientos	Workstation	✓	workstation,client,desktop	Workstation network activity imitation and MI
dns_bind	DNS server with AXFR	✓	dns	DNS server with AXFR enabled (zone transf
dns_bind_wo_axfr	DNS server (AXFR disabled)	✓	dns	DNS server with AXFR disabled (zone transf

Points (pasti) nudijo servise, ki so prilagojene različnim sektorjem uporabnikov – od IT do OT in IoT.

Point config

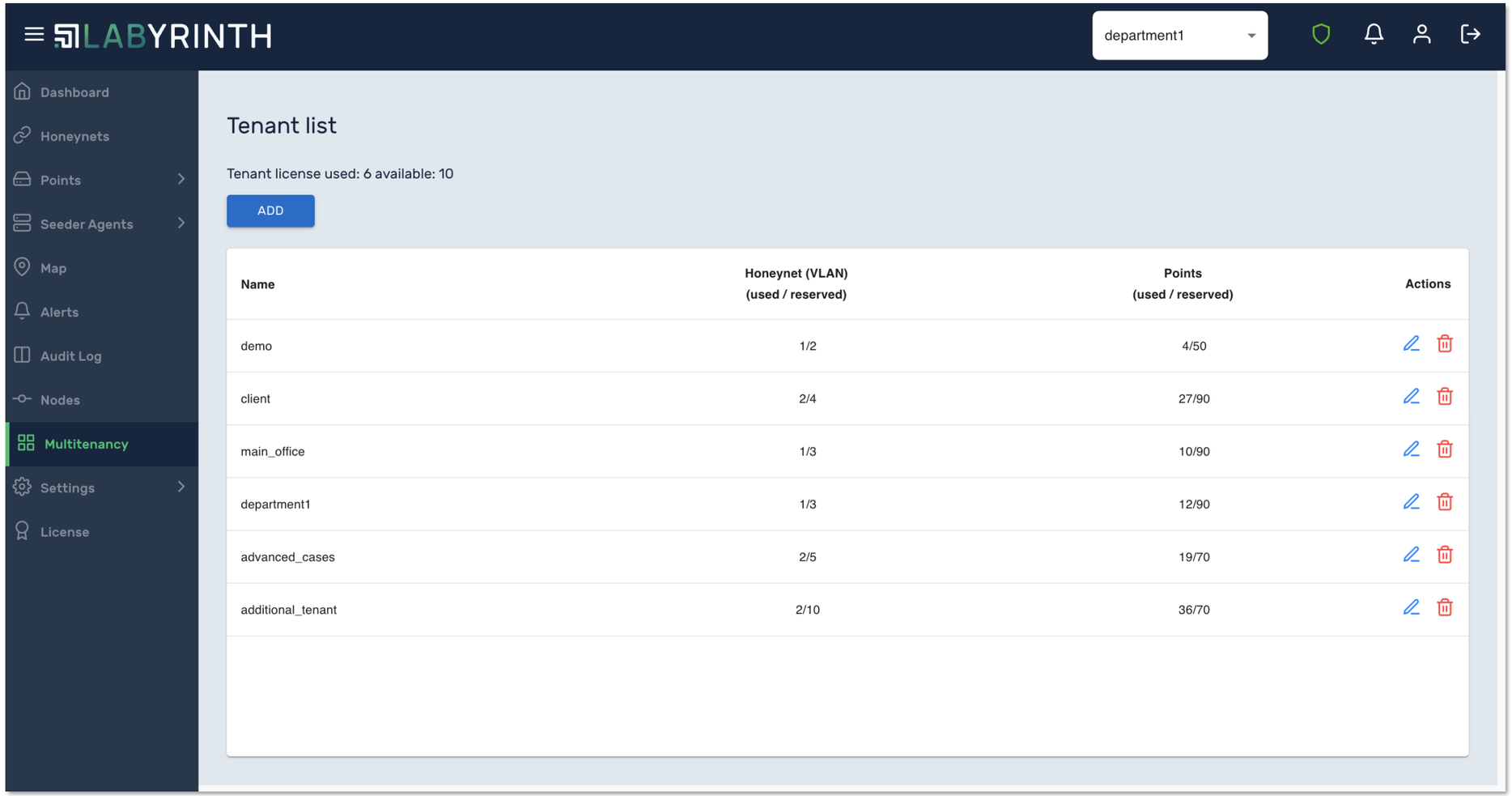
```
## Option: hostname
## Required: no
## Description: hostname value is short domain name or Fully Qualified Domain Name of the Point host.
##              This option may be omitted. In this case hostname value will be generate for each instance of a Point:
##                1. from hostnames wordlist which is specified in Point Type configuration
##                2. from hostnames wordlist which is specified in Honeynet configuration.
#
# hostname: my.host.name
#
## Option: fake_ports
## Required: no
## Description: fake_ports are TCP and UDP ports which will be visible to network scanners as filtered ports.
##              Main goal of fake ports is simulation of 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.
##              fake_ports is a list of objects which have tcp and udp properties or just tcp or udp.
##              During generate process for each instance of Point which uses current configuration will be randomly chosen one of fake ports groups.
#
# fake_ports:
```

Vsako past lahko enostavno prilagodimo preko spletnega vmesnika in YAML konfiguracijo, s čimer prilagodimo past potrebam okolja.

A1 ICT Distribucija

LABYRINTH

Multitenancy



LABYRINTH

The Seeker

Seeker je napredno orodje za **Potrjevanje napadalnih vektorjev (Attack Vector Validation)**, ki ponuja celovito testiranje pripravljenosti na kibernetske grožnje. Ponuja ključne tri lastnosti:

1. Potrditev varnostnih mehanizmov
2. Potrditev varnostnih pravilnikov
3. Potrditev učinkovitosti ekipe SOC

SEEKER DEMO:

LABYRINTH

Podprte platforme

Microsoft Hyper-V

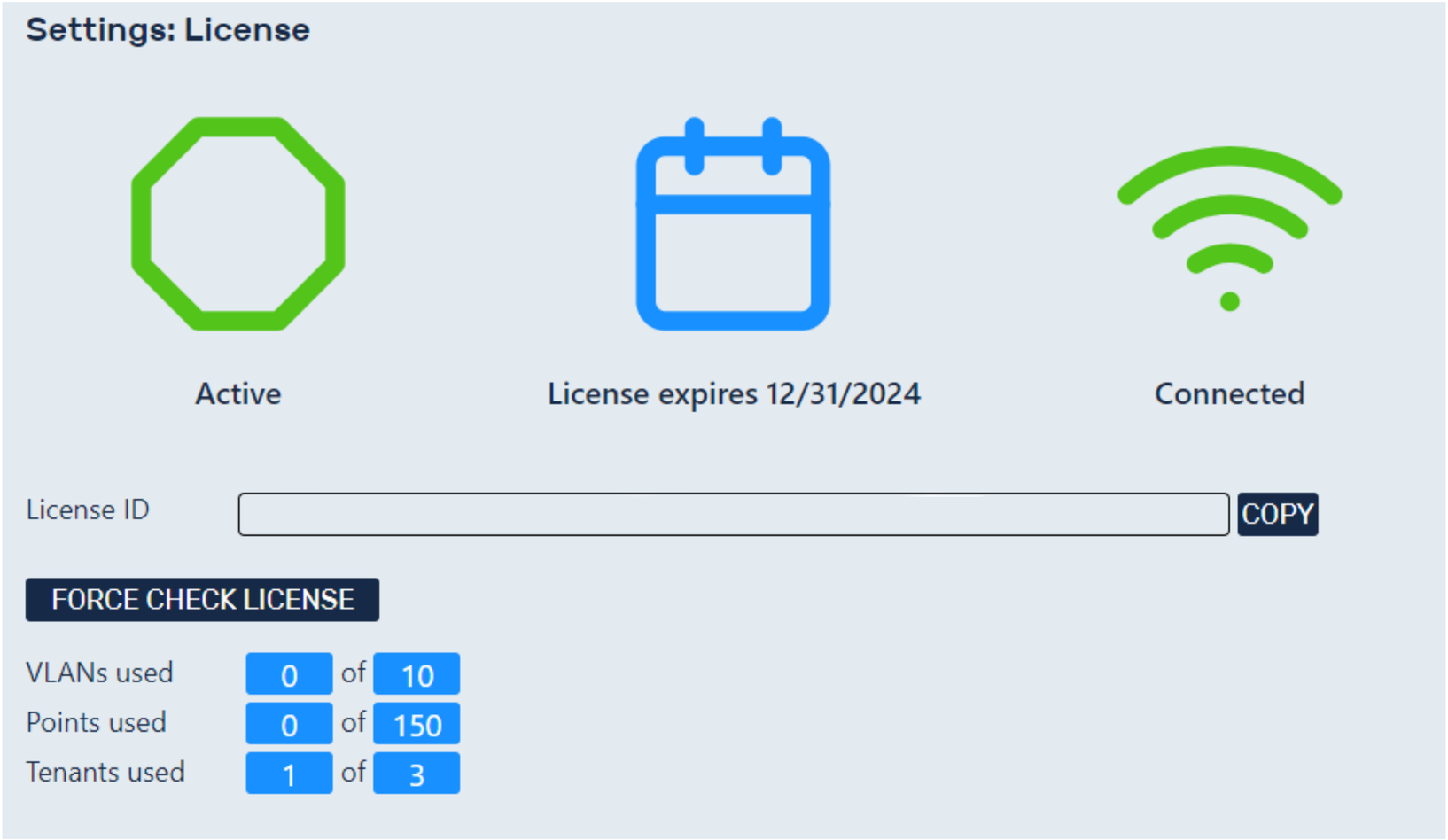
Azure

vmware®

PROXMOX
Proxmox Virtual Environment

LABYRINTH

Licenciranje



A1 Webinar

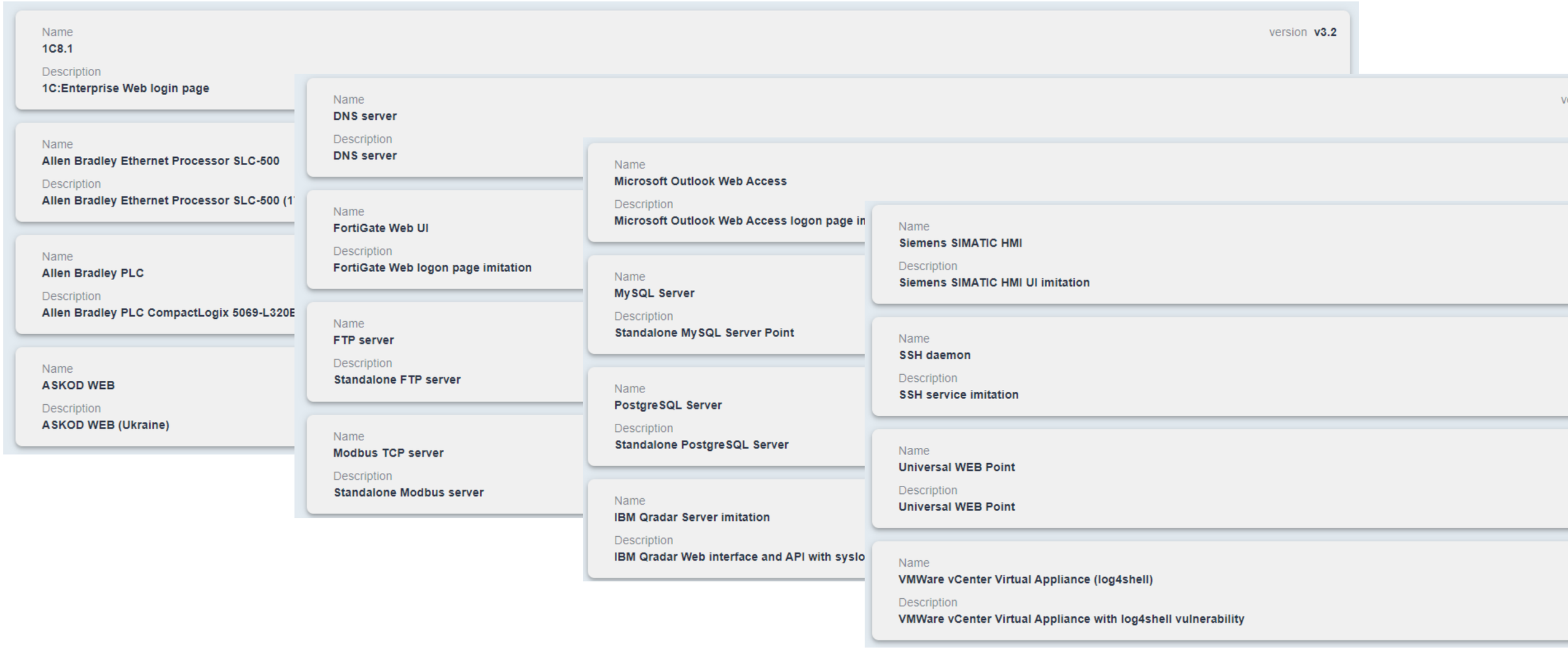
DEMO

A1 ICT Distribucija

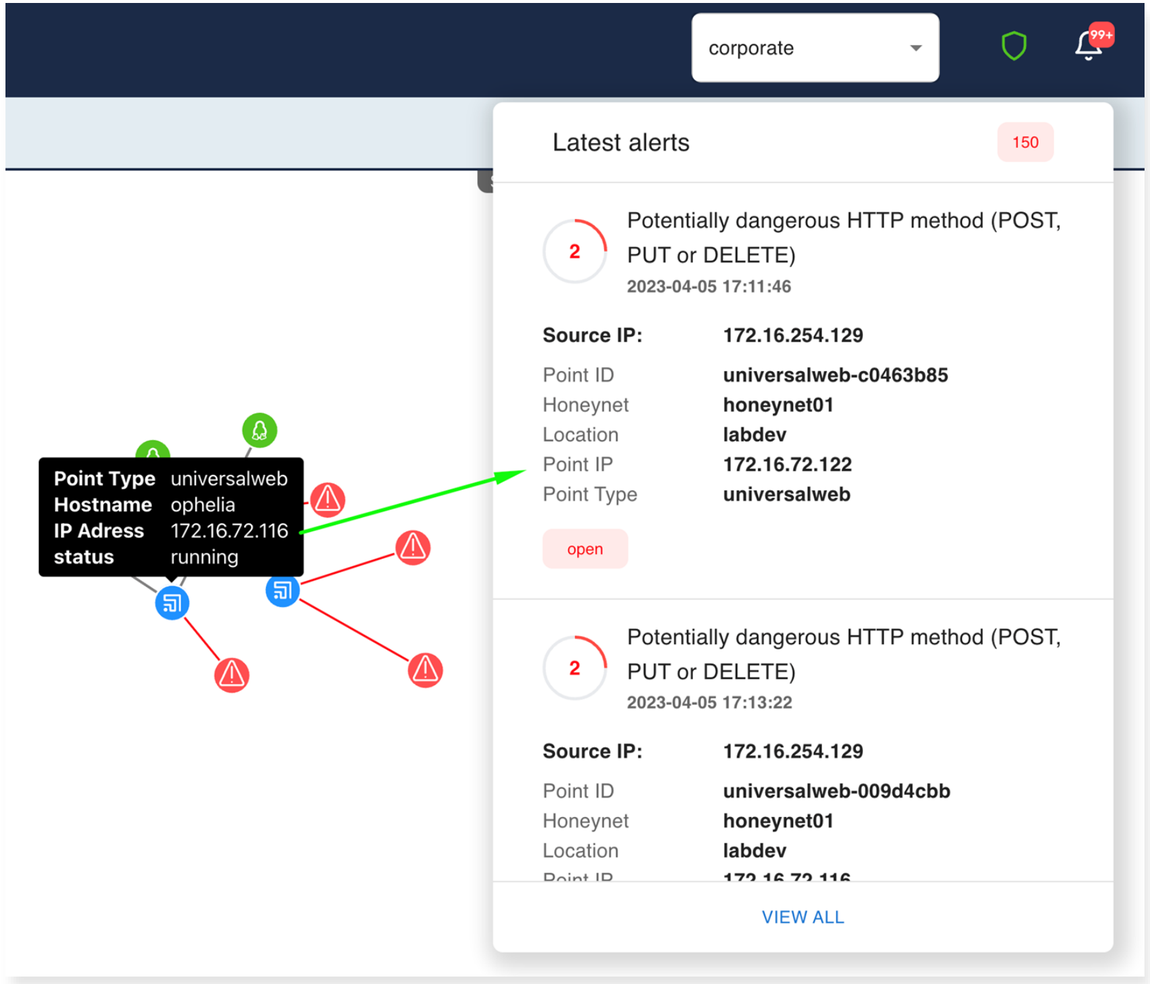
LABYRINTH

LABYRINTH

Deception Point Type Bases



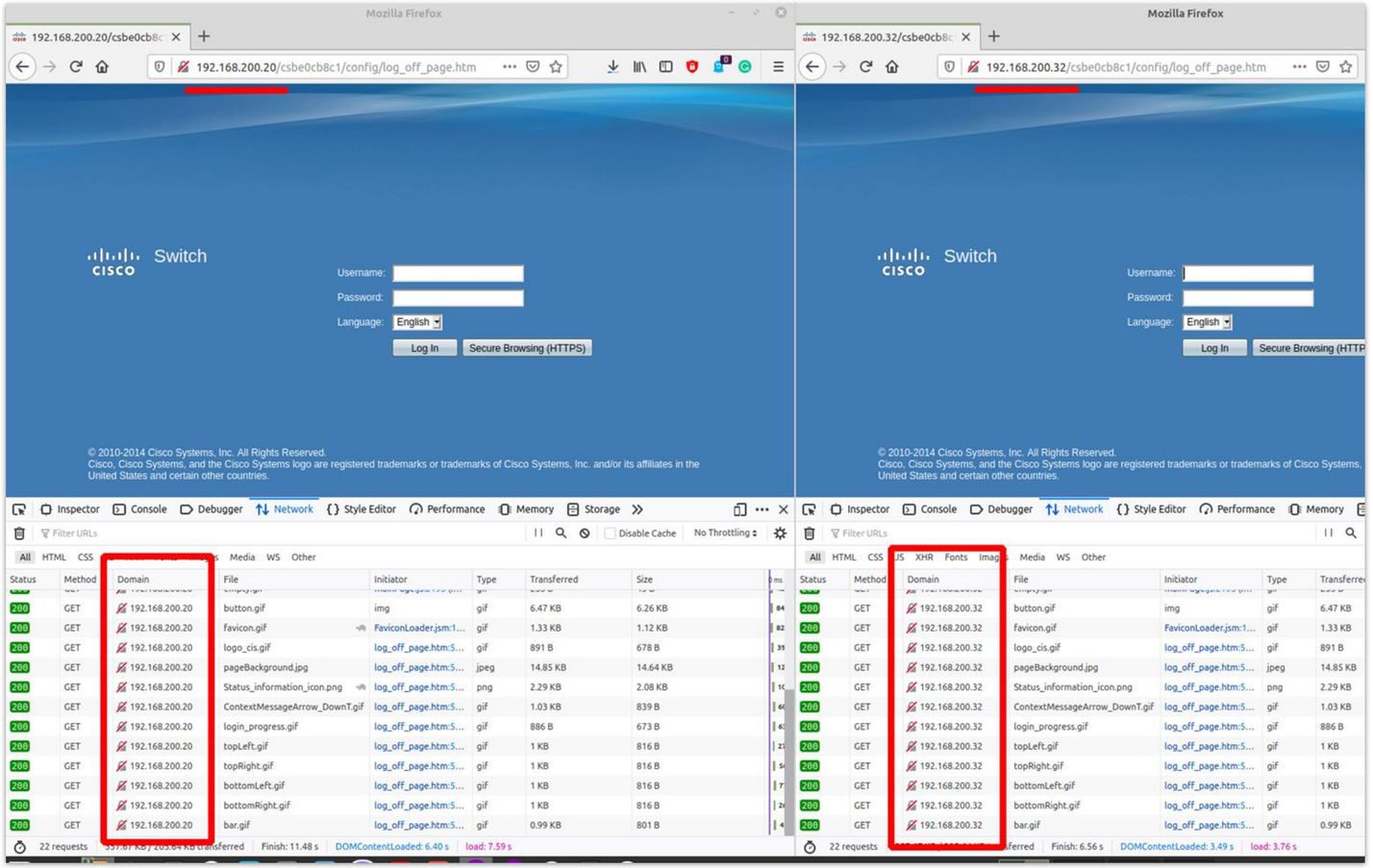
Universal Web Point



LABYRINTH

Universal Web Point

- „Kloniranje“ web aplikacije
- Dodane ranljivosti iz OWASP TOP10
- Deluje kot proxy



LABYRINTH

Primer alarma

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

DETAILS

2024-05-

Alert ID

Alert R

Destin

D

21

File Typ

MD5: d0dfc9beff7552a0af6c142c5da6a885

Additional Info

Username	testol1
Clientip	10.10.10.1
Password	robot
Message	login attempt [testol1/robot] succeeded

Additional Info

Message	login attempt [test_receiver3/tarakan] failed
Clientip	172.16.1.50
Password	tarakan
Username	test_receiver3

LABYRINTH

Podrobnosti alarma

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**

LABYRINTH

Podrobnosti alarma

DETAILS EVENTS ACTIVITY(0)

2024-05-16 11:09:41	Hostname: - Message: **CMD: ps**
2024-05-16 11:09:26	Hostname: - Message: **CMD: cat passwd**
2024-05-16 11:09:19	Hostname: - Message: **CMD: cd /etc**
2024-05-16 11:09:16	Hostname: - Message: **CMD: sudo su**
2024-05-16 11:09:01	Hostname: - Message: **CMD: ping 8.8.8.8**

2024-05-16 11:08:58

2024-05-16 11:08:58

2024-05-16 11:08:58

2024-05-16 11:08:58

2024-05-16 11:08:50

TCP Flags: **SYN**

LABYRINTH

Integracije

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	

A1 Webinar

VPRAŠANJA

A1 ICT Distribucija

LABYRINTH

A1 Webinar

- **Evropska** kibernetska varnost
- Odlična **nadgradnja** obstoječih EDR/XDR rešitev
- **Nadzor omrežja**
- Brez **lažnih alarmov**
- **Učinkovito** zaznavanje s **preprosto** implementacijo
- **Brez vpliva** na aktivno infrastrukturo
- Možnost testiranja (**POC**)

CYBERSECURITY™
MADE IN EUROPE

A1 ICT Distribucija

LABYRINTH

A1 Webinar

Več informacij

https://varnostne-resitve.si/

ict-partners@A1.si

A1 ICT Distribucija

LABYRINTH

Thank you

Marko Kašić

E marko.kasic@A1.si
M +386 40 440 842