LABYRINTH

28.05.2026, Zagreb, Croatia

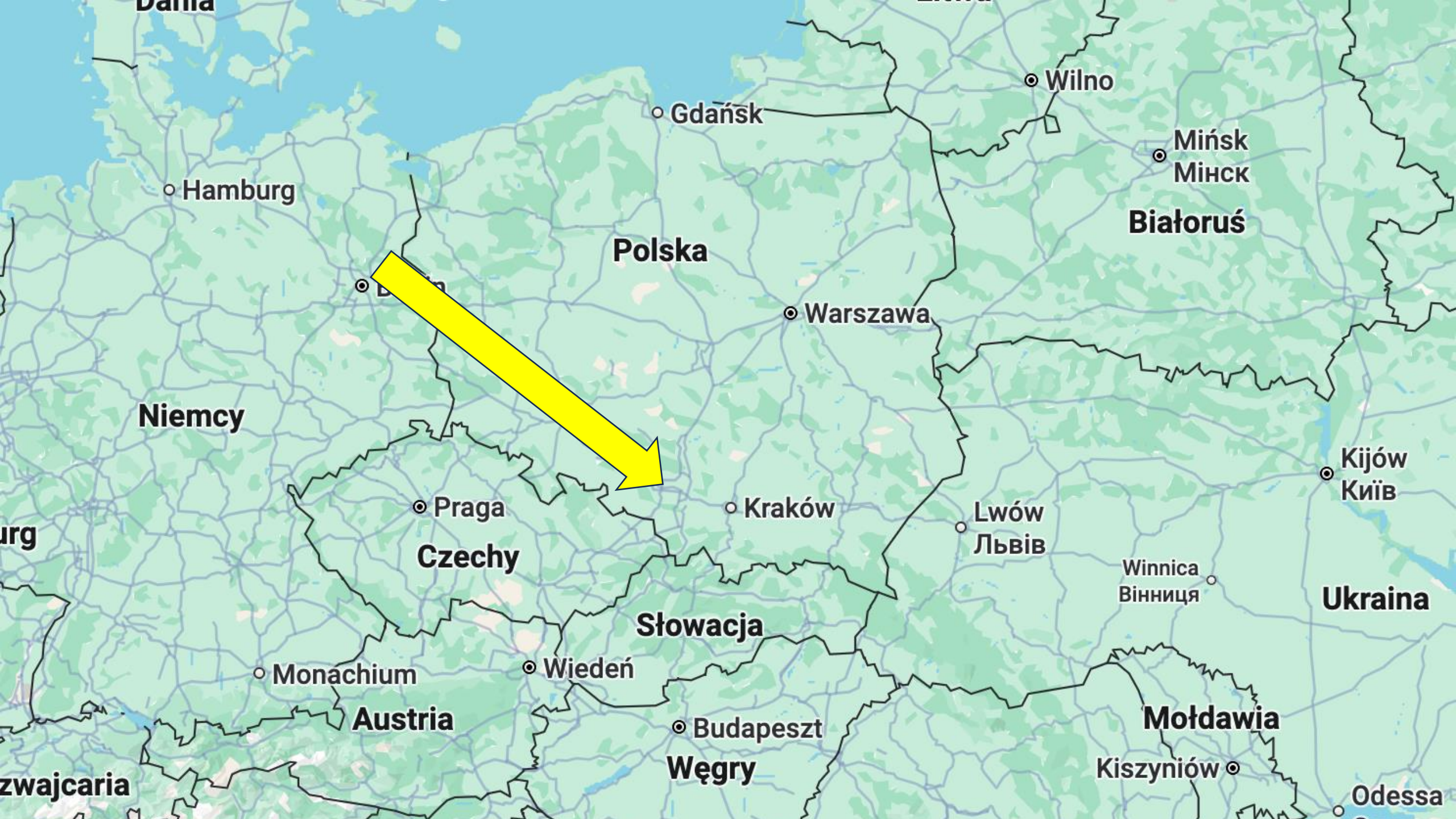
Paweł Rybczyk, CEO

pawel.rybczyk@labyrinth.tech

+48 664 300 375

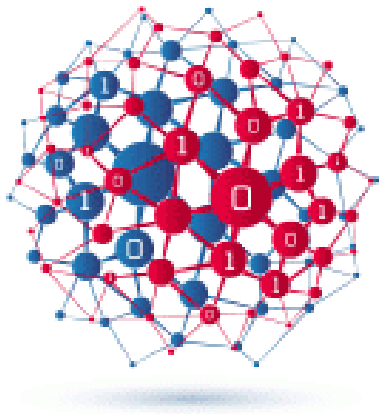
A1 Slovenija
ICT Distribucija

Cybersecurity
MADE IN EUROPE


Wilno
Gdańsk
Mińsk
Мінск
Hamburg
Białoruś
Polska
Warszawa
Niemcy
Kijów
Київ
Praga
Kraków
Lwów
Львів
Czechy
Winnica
Вінниця
Ukraina
Słowacja
Monachium
Wiedeń
Austria
Budapeszt
Mołdawia
Węgry
Kiszyniów
Odessa

ECS

EUROPEAN CYBER SECURITY ORGANISATION



#CyberMadeInPoland

cyberhive
Powered by ECSO

Solutions Vendors Investors Community About Matrix™ Register

Filter

Search a vendor...

Country of HQ

- [ ] Austria
- [ ] Belgium
- [ ] Bulgaria
- [x] Croatia
- [ ] Cyprus
- [ ] Czech Republic
- [ ] Denmark
- [ ] Estonia

1 Vendors found

Croatia

PROMDM

ProMDM d.o.o.

ProMDM is a trusted provider of cybersecurity solutions, helping organizations secure their digit

https://thecyberhive.eu/solutions

Sort solutions by Most popular

94 results found

Find your solutions

'ISO27001', 'UK', 'German', ...

Solution category

- European Regulatory Compliance
- Govern
- Identify
  - Asset Mangement
  - Risk Assessment
  - Improvement
- Protect
  - Identity Management, Authentication, & Access Control
  - Human Risk Management
  - Data security
  - Protective Technology
- Platform Security
- Technology Infrastructure Resilience

AIT Austrian Institute of Technology

Taranis AI - OSINT Analysis

Taranis AI is an advanced Open-Source Intelligence (OSINT) tool, leveraging Artificial Intelligence...

Sekoia.io

Sekoia Defend

Sekoia Defend (Next-Gen SIEM) is an eXtended Detection and Response (XDR) SOC platform available in...

Labyrinth Security Solutions

Cyber Deception platform

Labyrinth creates the illusion of a real infrastructure vulnerability for an attacker. The solution...

WithSecure

BforeAI

Atos Group


LABYRINTH


W / T H
secure


wallix


STORMSHIELD


ENERGY
LOGSERVER


PORT
DESIGNS


TrustLayer


axence®

Think globally act locally


TARNOWSKIE GÓRY
LABYRINTH

LABYRINTH

28.05.2026, Zagreb, Croatia

Paweł Rybczyk, CEO

pawel.rybczyk@labyrinth.tech

+48 664 300 375

A1 Slovenija

ICT Distribucija

LABYRINTH

Napastnik mora uspjeti samo jednom,

branitelj svaki put.

LABYRINTH

Naša je vizija pomaknuti ravnotežu snaga u korist branitelja.

LABYRINTH

Naša je misija svim organizacijama pružiti jednostavan i učinkovit alat za otkrivanje napadača unutar korporativne mreže.

LABYRINTH

PREVENCIJA
NADZOR – DETEKCIJA – REAKCIJA
OPORAVAK

LABYRINTH

2026?

LABYRINTH

Vrijeme proboja: samo 29 minuta

od kompromitacije do lateralnog kretanja napadača.

LABYRINTH

Brzina napada:

+65% u odnosu na 2024. godinu.

LABYRINTH

Napadi uz korištenje umjetne inteligencije:

porast od +89%.

LABYRINTH

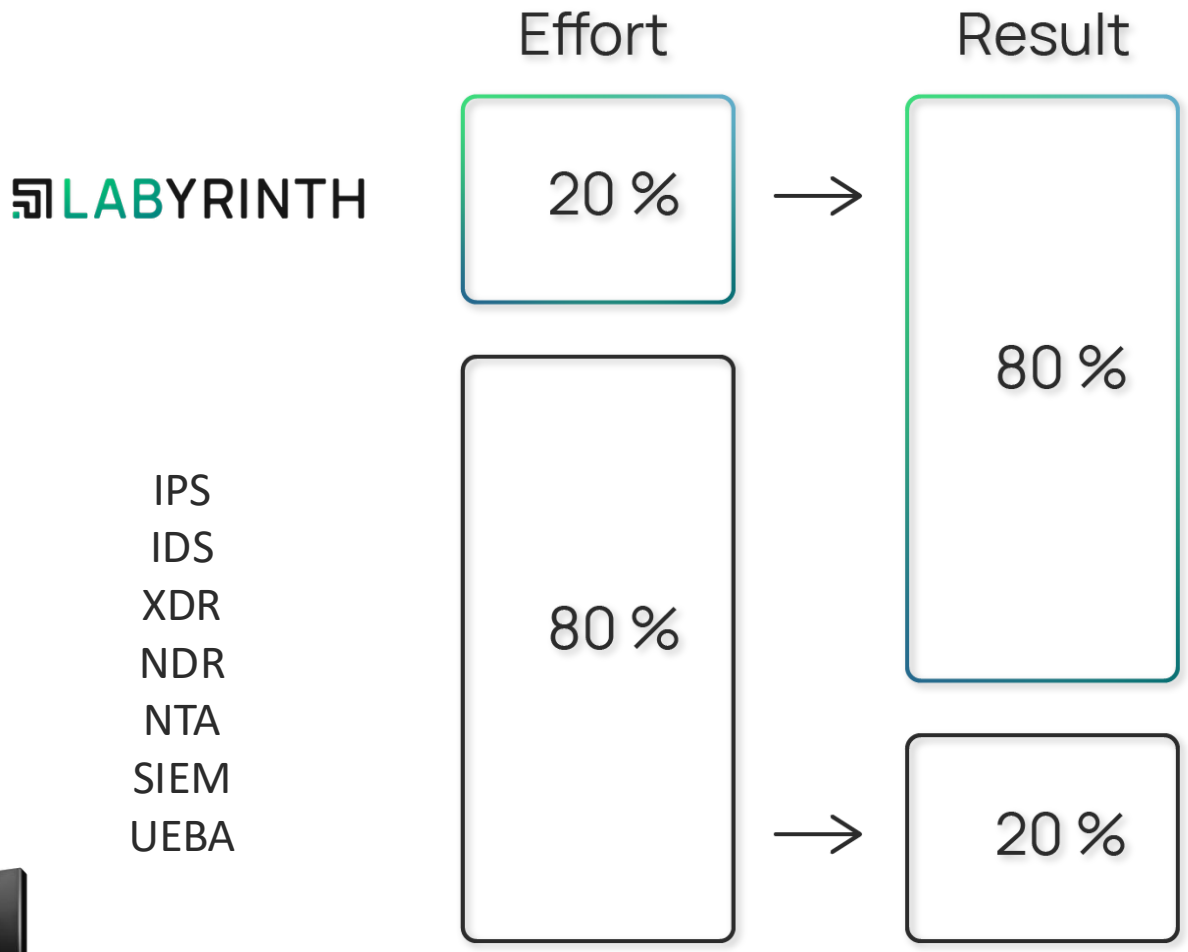
Koji je cilj napadača?

Uvod

Kontekst za LABYRINTH:

- NETWORK MONITORING
- INSTRUSTION DETECTION
- EARLY THREAT DETECTION

Uvod



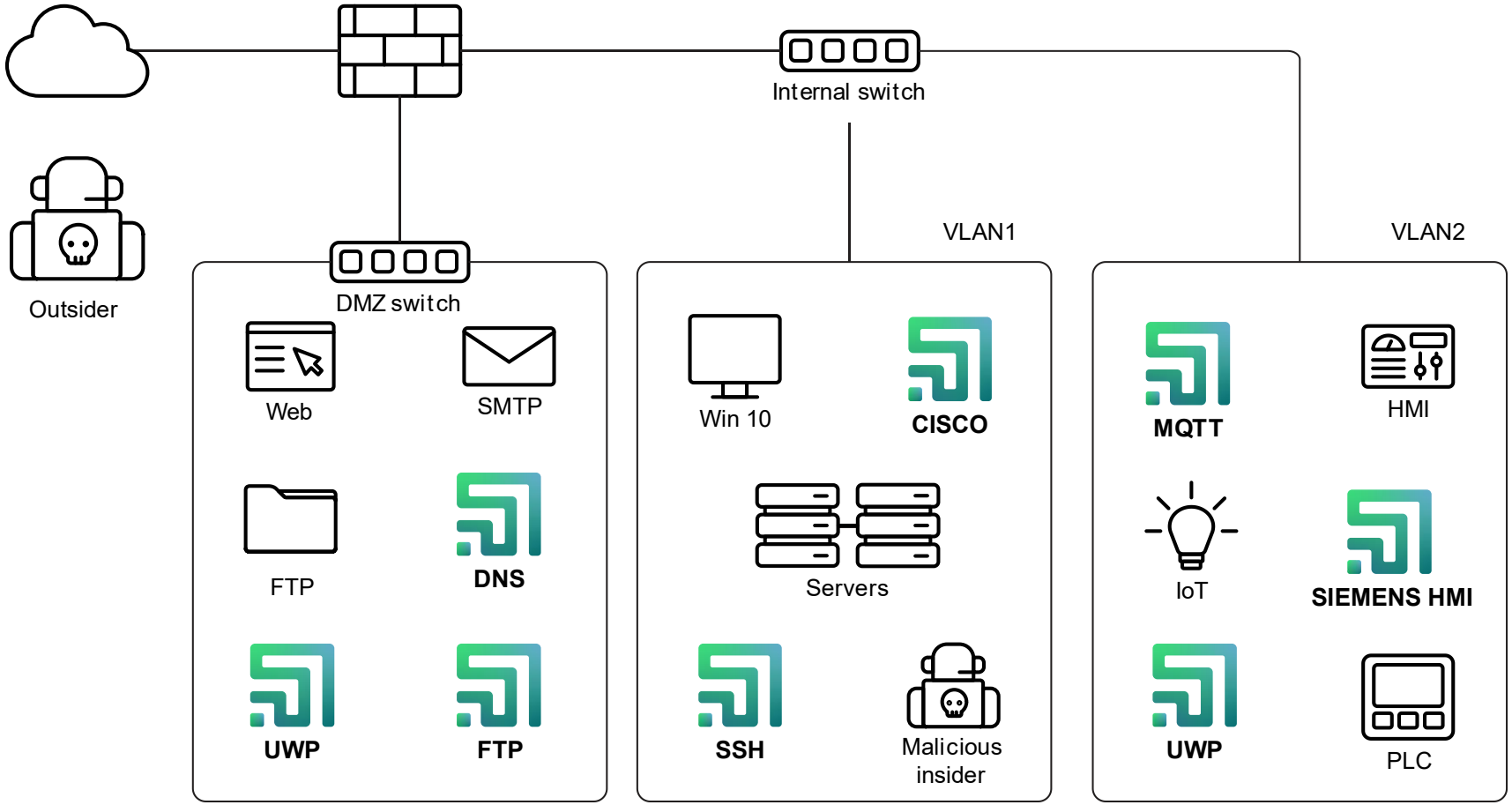
Trenutačna reakcija na svaku aktivnost napadača.

Preuzima udar na sebe i istovremeno dobiva vrijeme za reakciju.

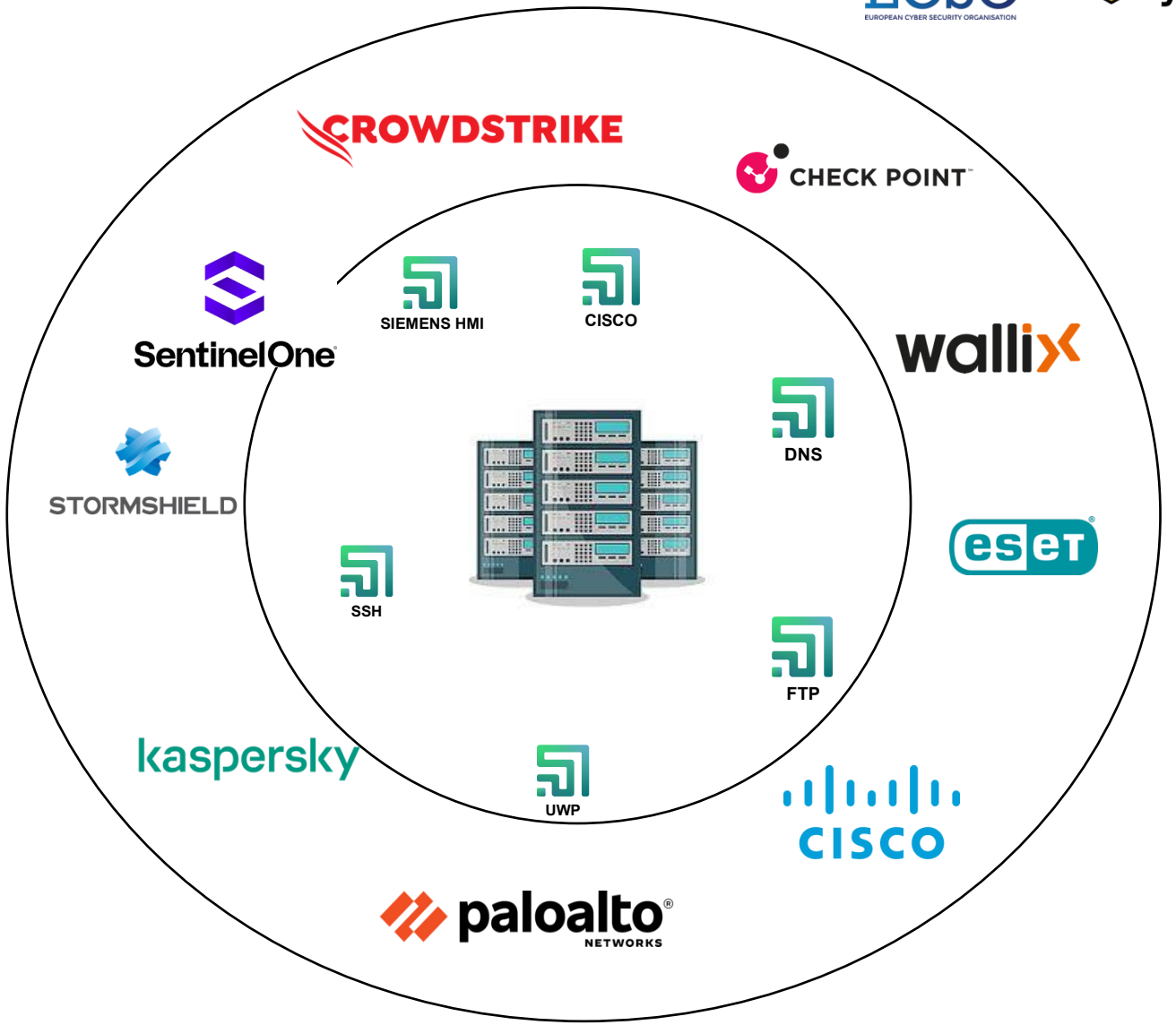
Jasne i detaljne informacije o napadu i napadaču.

Prikupljanje logova, informacija o prijenosu i mrežnim tokovima, što pruža dodatni kontekst.

Uvod


Internal switch
Outsider
DMZ switch
VLAN1
VLAN2
Web
SMTP
FTP
DNS
UWP
FTP
Win 10
CISCO
Servers
SSH
Malicious insider
MQTT
HMI
IoT
SIEMENS HMI
UWP
PLC

Uvod



Slovenija – ICT Distribucija

Dodana vrijednost za korisnika.

1. Veći troškovi djelovanja za napadača
2. Ranije otkrivanje prijetnji
3. Usporavanje napada i prikupljanje obavještajnih informacija o napadaču
4. Praktički nula lažnih alarma
5. Visoko učinkovita strategija nadzora (IT/OT)
6. 100% on-premise implementacija

Slovenija – ICT Distribucija

Podržane platforme

- Virtual: Microsoft Hyper-V, Broadcom VMware, PROXMOX
- Cloud: Microsoft Azure, Amazon Web Services
- Hardware (BareMetal):

Slovenija – ICT Distribucija

LABYRINTH

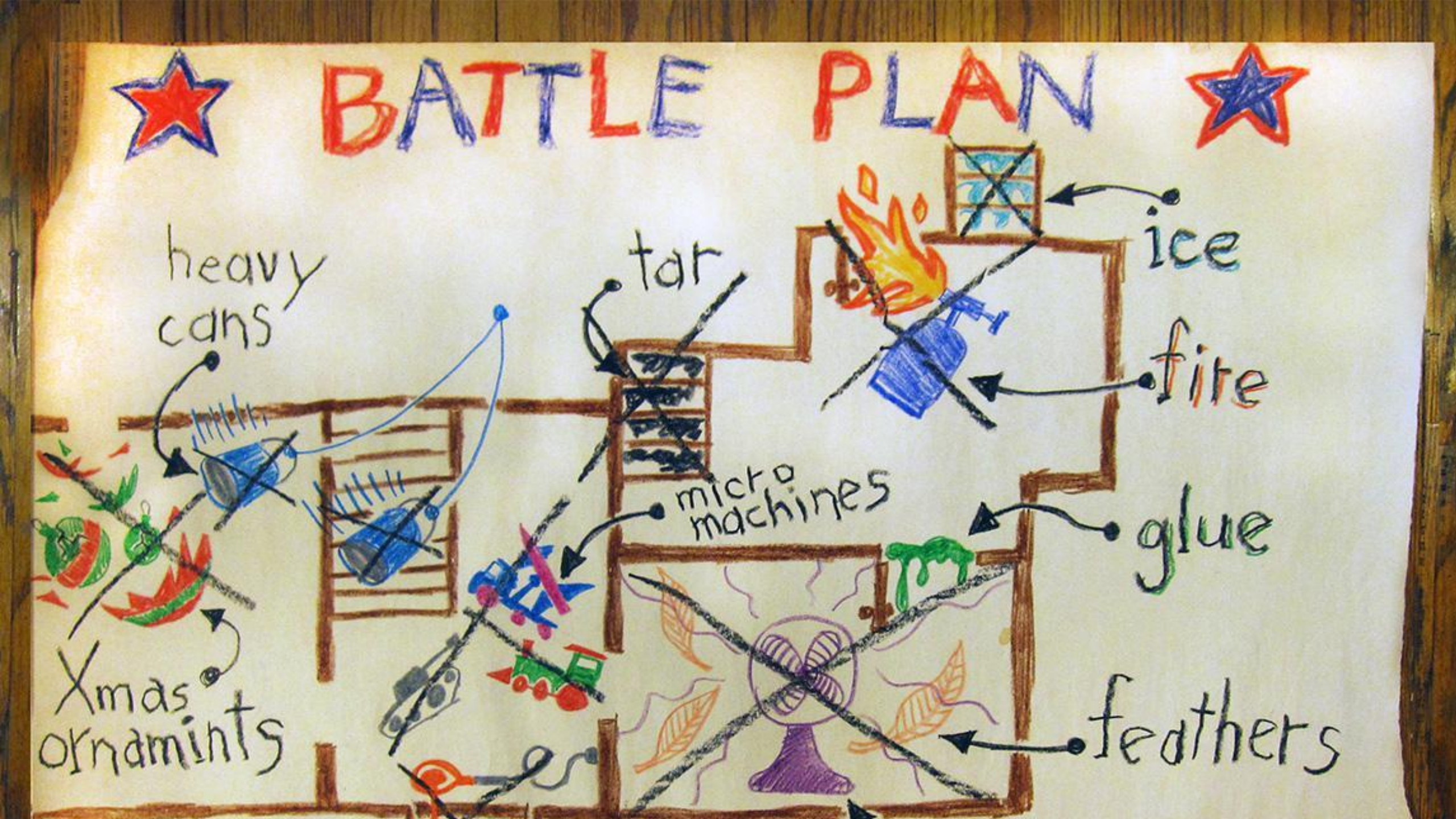
Napastnik mora uspjeti samo jednom,

branitelj svaki put.

LABYRINTH

Snaga analogije


DANGER
MINES


BATTLE PLAN
heavy cans
tar
ice
fire
micro machines
glue
Xmas ornaments
feathers

Usklađenost sa zakonodavstvom.

Napredna detekcija i rano upozoravanje
/NIS2, Zakon o kibernetičkoj sigurnosti, NN 14/24; Uredba o kibernetičkoj sigurnosti, NN 135/24/

LABYRINTH dodaje aktivni deception sloj koji otkriva nepoznate i „0-day" napade unutar mreže, pretvarajući okruženje u kontrolirano minsko polje za napadača. Time organizacijama pomaže primijeniti suvremene mjere kibernetičke sigurnosti, a ne oslanjati se samo na osnovne alate temeljene na potpisima.

Kontinuirana procjena rizika i nadzor ICT okruženja

Deception senzori djeluju kao stalne „oči" u IT i OT segmentima te u stvarnom vremenu otkrivaju lateralno kretanje i neovlaštene aktivnosti. To organizacijama olakšava ispunjavanje zahtjeva za kontinuiranim nadzorom, ranom detekcijom incidenata i pravodobnim izvješćivanjem prema hrvatskom NIS2 okviru.

Usklađenost sa zakonodavstvom.

Sigurnost opskrbnog lanca i zaštita podataka
/NIS2, DORA, Zakon o kibernetičkoj sigurnosti, NN 14/24; Uredba o kibernetičkoj sigurnosti, NN 135/24/

LABYRINTH može otkriti zlouporabu vjerodajnica, sumnjive pristupe i pokušaje izvlačenja osjetljivih ili poslovno kritičnih informacija putem deception aktiva. Time podržava zahtjeve NIS2 okvira za sigurnost opskrbnog lanca, kao i zahtjeve DORA uredbe za upravljanje ICT rizicima i zaštitu kritičnih podatkovnih tokova.

Dokazi za revizije i provjeru učinkovitosti
/NCSC-HR, nadležna sektorska tijela, NIS2, DORA/

LABYRINTH generira precizan trag incidenta: tko je, kada i odakle pristupio kojem deception aktivu te koje je tehnike koristio. Organizacija tako dobiva konkretne dokaze da detekcijske mjere postoje, funkcioniraju u produkcijskom okruženju i mogu se redovito provjeravati, što pomaže pri revizijama, samoprocjenama i nadzoru prema hrvatskom okviru kibernetičke sigurnosti, NIS2 i DORA.

Manje lažnih alarma, učinkovitiji SOC
/NIS2 i DORA/

Budući da legitimni korisnici ne bi trebali pristupati deception aktivima, svaki alert ima visoku relevantnost, a broj lažnih alarma ostaje minimalan. To podržava zahtjeve za učinkovitim procesima upravljanja incidentima: bržu trijažu, kvalitetniju analizu i jasnije izvještavanje prema nadležnim tijelima.

Povijest tvrtke

- Sjedište: Poljska / Zabrze
- 18 zaposlenika
- 100% prodaja putem partnerskog kanala
- Softver
- Hardver isporučuju partneri

Slovenija – ICT Distribucija

Nagrade

- 2024 Startup
- 2025 CISO ch
- 2026 Rising S
- 2026 Securit

Slovenija – ICT

Reference

- GARTNER: https://www.gartner.com/reviews/product/labyrinth-deception-platform
- G2.com: https://www.g2.com/products/labyrinth-cyber-deception-platform/reviews
- GigaOM: https://portal.gigaom.com/report/gigaom-radar-for-deception-technology-5

Okvirna kalkulacija cijene

Primjer 1 - Tvrtka s 200 radnih stanica, 20 poslužitelja, 10 pisača i 3 IP kamere. Ukupno: 233 aktiva.

15% preporučenih deception točaka = 15% × 233 = 35 točaka /zamki / mamaca / honeypotova/

Preporučena cijena za krajnjeg korisnika:

- 1 godina = 4 × 10 × 399 EUR = **15.960 EUR** za 40 zamki / mamaca / honeypotova.
- 3 godine = 4 × 10 × 959 EUR = **38.360 EUR** za 40 zamki / mamaca / honeypotova.

Okvirna kalkulacija cijene

Primjer 2 Tvrtka s 1.000 radnih stanica, 50 poslužitelja, 10 pisača, 20 IP kamera i 20 IoT uređaja. Ukupno: 1.100 aktiva.

15% preporučenih deception točaka = 15% × 1.100 = 165 točaka /zamki / mamaca / honeypotova/

Preporučena cijena za krajnjeg korisnika:

- 1 godina = 17 × 3.490 EUR = **59.330 EUR** za 170 zamki / mamaca / honeypotova.
- 3 godine = 17 × 8.390 EUR = **142.630 EUR** za 170 zamki / mamaca / honeypotova.

Slovenija – ICT Distribucija

LABYRINTH kao komplementarno rješenje

Sigurnost krajnjih točaka / Endpoint Security
Dodaje unutarnji sloj zamki i rane detekcije napada koji zaobiđu EDR/XDR.

Sigurnost mrežnog perimetra / Firewall, UTM
Otkriva napade koji su prošli kroz perimeter ili su ušli drugim vektorom, primjerice putem VPN-a, dobavljača ili insidera.

SIEM / SOC
Djeluje kao dodatni detekcijski engine s malim brojem lažnih alarma i jasnom identifikacijom kompromitiranih hostova.

APT kontekst
Otkriva prisutnost i zadržavanje napadača u okruženju te podržava pristup aktivne obrane i koncept moving target defense.

Organizacije koje preferiraju rješenja „razvijena u Europi”
Tehnologija razvijena u Europi bolje se uklapa u zahtjeve povjerenja, podatkovnog suvereniteta i regulatorne usklađenosti.

Otváracie otázky

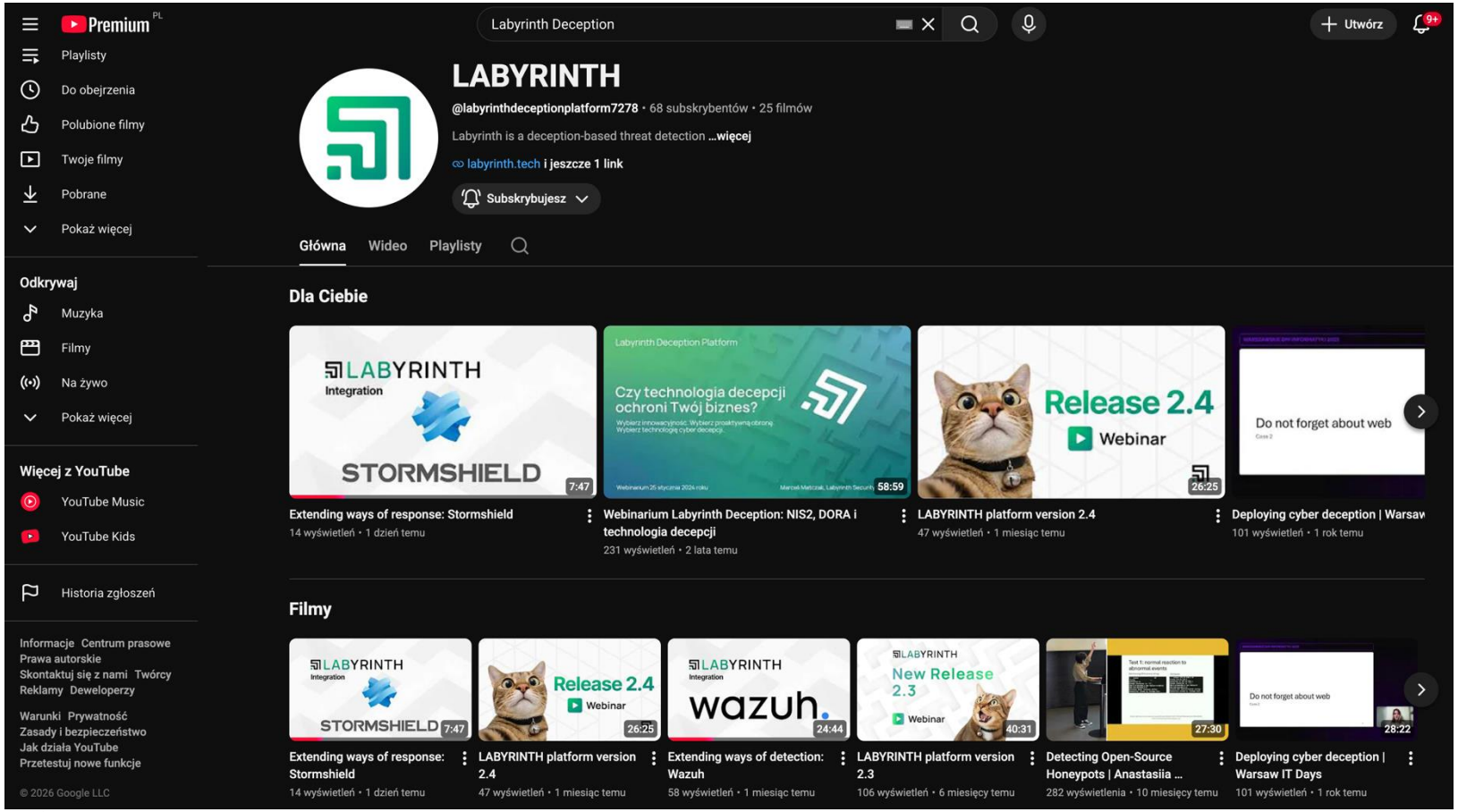
- Što se događa kod vas u trenutku kada je napadač već unutar mreže? Koliko brzo to možete otkriti?
- Koliko rano možete otkriti napadača ako zaobiđe firewall ili endpoint security?
- Želite poboljšati detekciju, ali brine vas prevelik broj lažnih alarma?
- Ima li vaš tim dovoljno kapaciteta za podizanje razine detekcije bez dodavanja novih ljudi u SOC ili IT?
- Tražite li rješenje koje nadopunjuje vaš postojeći sigurnosni stack, a ne zahtijeva zamjenu postojećih alata?

Kako vas možemo podržati?

- Prezentacija
- Proof of Concept (PoC)
- Obuka
- Sastanci s potencijalnim korisnicima
- Tehnički opis rješenja za RFI/RFP
- Projekti izvan Hrvatske
- Podrška distribuciji: PoC / PoV / implementacija

Slovenija – ICT Distribucija

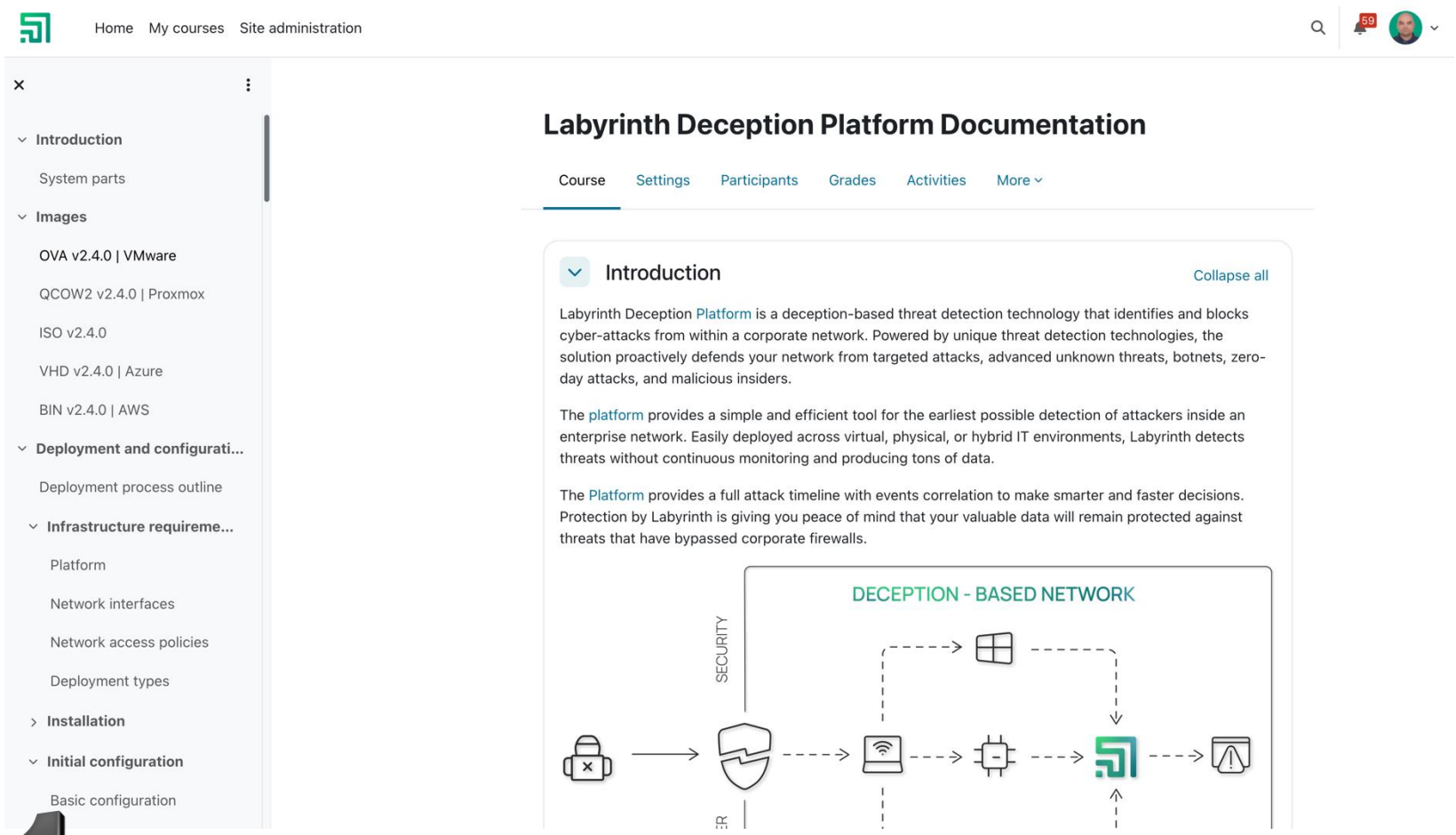
Kako vas možemo podržati?



https://www.youtube.com/@labyrinthdeceptionplatform7278

Slovenija – ICT Distribucija

Kako vas možemo podržati?



https://kb.labyrinth.tech

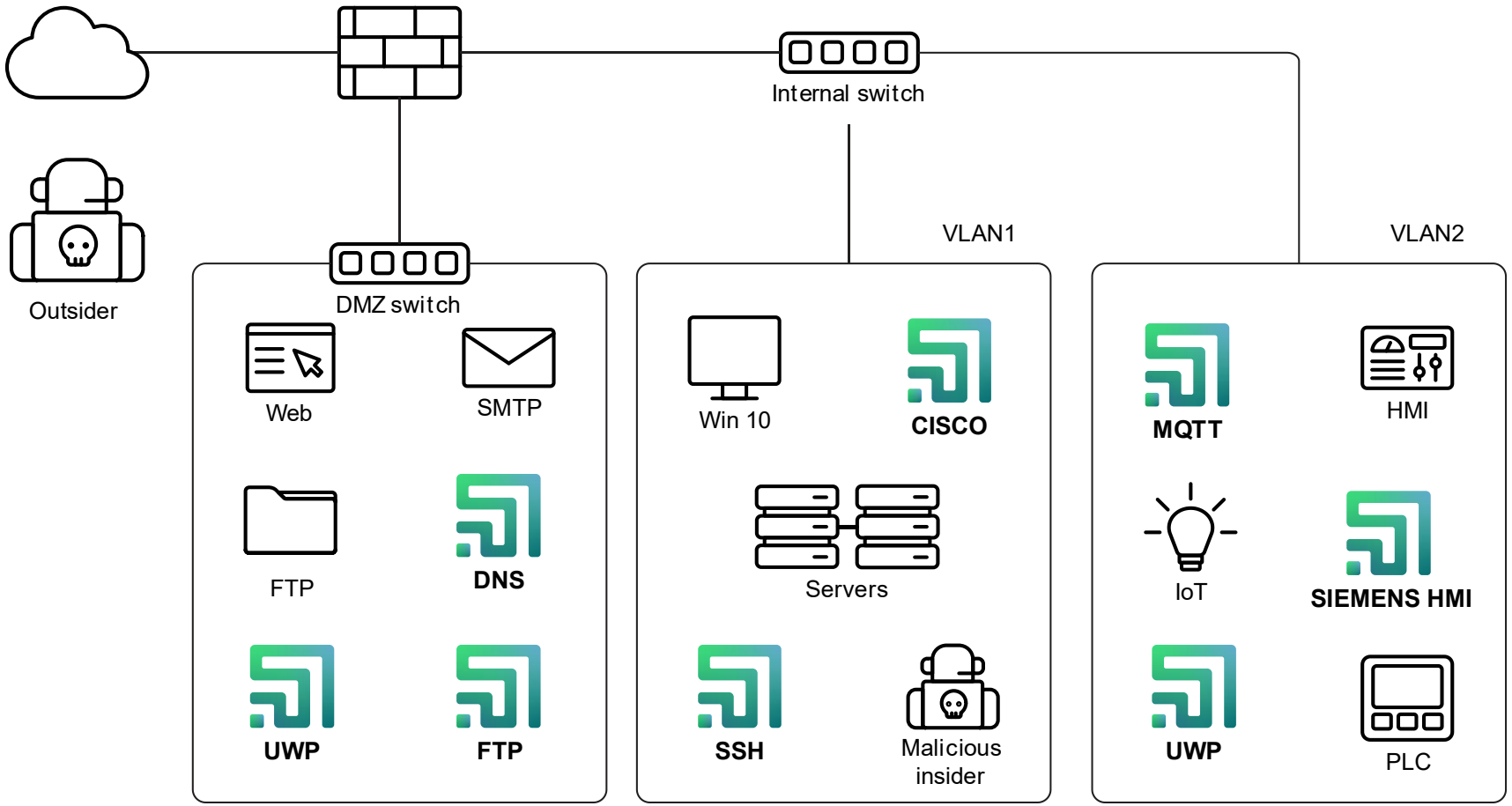
Slovenija – ICT Distribucija

Pitanja vezana uz cjenovnu ponudu

- Koliko sustava / aktiva imate unutar mreže? /radne stanice, poslužitelji, IP pisači, IP kamere, IoT uređaji: hladnjaci, TV uređaji i sl./
- Koliko mrežnih segmenata danas koristite?
- Preferirate li licencu u obliku pretplate / subscription ili vam je potrebna trajna licenca?
- Ako je riječ o pretplati, koje razdoblje za vas ima smisla:

1, 2, 3, 4 ili 5 godina?

Pitanja vezana uz cjenovnu ponudu



Slovenija – ICT Distribucija

Prodaja kroz integracije

- STORMSHIELD
- CROWDSTRIKE
- FORTIGATE
- WAZUH
- SPLUNK / QRADAR / TRELLIX

Hvala na pažnji!

info@labyrinth.tech

Slovenija – ICT Distribucija