

01. LISTOPADA 2026. · 12:40 — 13:00 · MAGUS CYBER WORLD

INTEGRIRANA KOMUNIKACIJSKA RJEŠENJA

i budućnost poslovne suradnje

Od uređaja do clouda - jedna sigurna komunikacijska infrastruktura

Matija Matijevac



Komunikacija više nije telefon, Teams ili e-mail.

Budućnost poslovne suradnje nije još jedna aplikacija. Budućnost je infrastruktura u kojoj ljudi, uređaji, lokacije, cloud i industrijski sustavi mogu sigurno i neprekidno komunicirati.



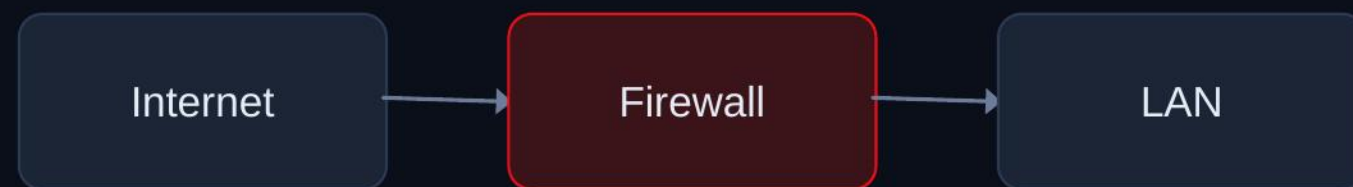
Sve to je jedna organizacija. Sve to mora komunicirati — sigurno, i onda kad nešto zakaže.

Kad kažemo komunikacijska infrastruktura, ne pričamo o tome kako će dva čovjeka razgovarati.

VIŠE NE POSTOJI JEDNA MREŽA

postoji jedno poslovanje preko mnogo okruženja

NEKAD



Jedan ulaz. Jedan zid. Sve iza njega je „naše“.

Nešto u uredu, nešto u AWS-u, ERP negdje treće, remote korisnik, serviser, laboratorij, OT uređaj, API prema partneru. Jedna organizacija — sedam okruženja.

DANAS



Korisnika ne zanima gdje aplikacija živi. Sigurnost to mora znati.

OMNI-NETWORK SECURITY

jedna sigurnosna arhitektura, gdje god sustav živi

- **Lokalni firewall**

štiti fizičku lokaciju i segmentira lokalnu infrastrukturu.

- **Cloud firewall**

isti sigurnosni koncept u AWS-u, Azureu, Hetzneru ili privatnom cloudu.

- **Sigurna međusobna povezanost**

lokacije i cloud instance postaju dio kontrolirane privatne infrastrukture.

- **Jedinstvena pravila**

nije AWS „jedna priča“, ured druga, a Hetzner treća.

- **EU-first gdje ima smisla**

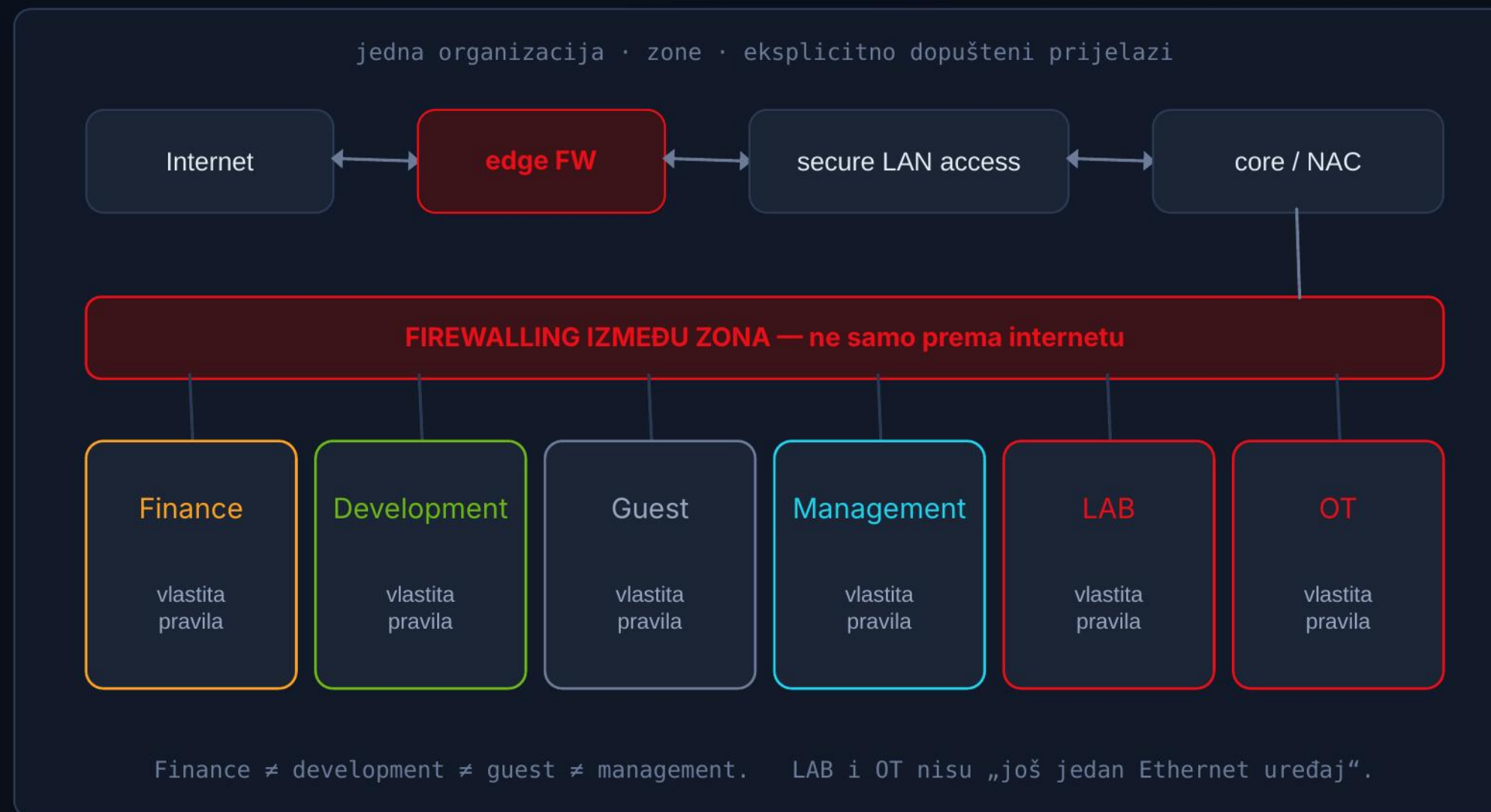
kontrola lokacije podataka, infrastrukture i jurisdikcije.



Cloud nije izvan vaše mreže. Cloud je samo druga lokacija vaše mreže.

LAN NIJE „ONO IZA FIREWALLA“

sigurnost počinje unutar mreže

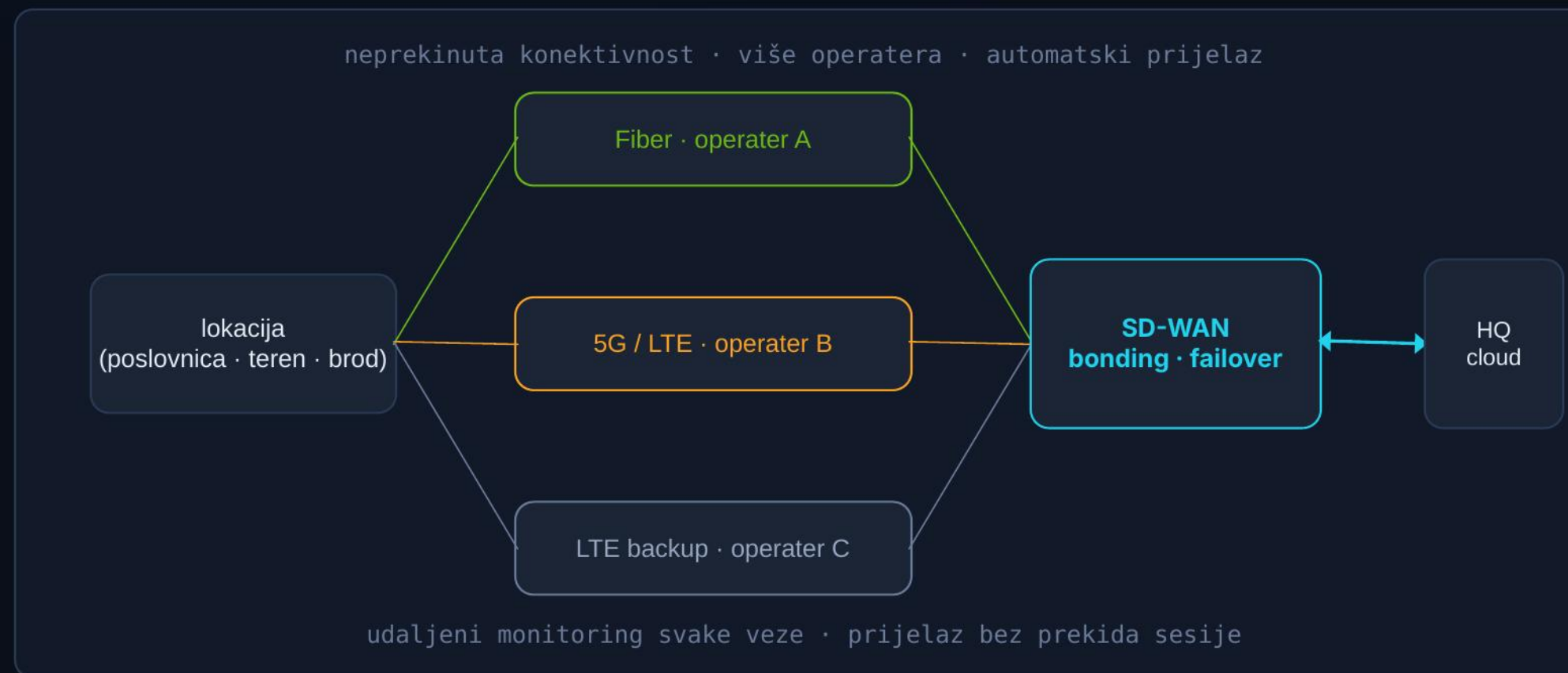


- **Secure LAN access**
tko se spoji, na što i pod kojim uvjetima.
- **Department segregation**
odjeli su zasebne zone, ne jedan VLAN.
- **LAB segregation**
firewall dolazi prije laboratorijske opreme, ne poslije.
- **OT segregation**
proizvodnja ima vlastite zone i pravila.
- **Firewalling između zona**
štitimo i organizaciju od same sebe.

Ako LAB oprema vrijedi 500.000 €, zašto joj vjerujemo samo zato što ima RJ45 konektor?

SIGURNA MREŽA KOJA NE RADI NIJE OTPORNA

komunikacija mora preživjeti kvar



GDJE TO ODLUČUJE

poslovnica izgubi primarni Internet

teren / servisna ekipa

brod, vozilo, mobilna jedinica

proizvodni pogon

privremena lokacija / event

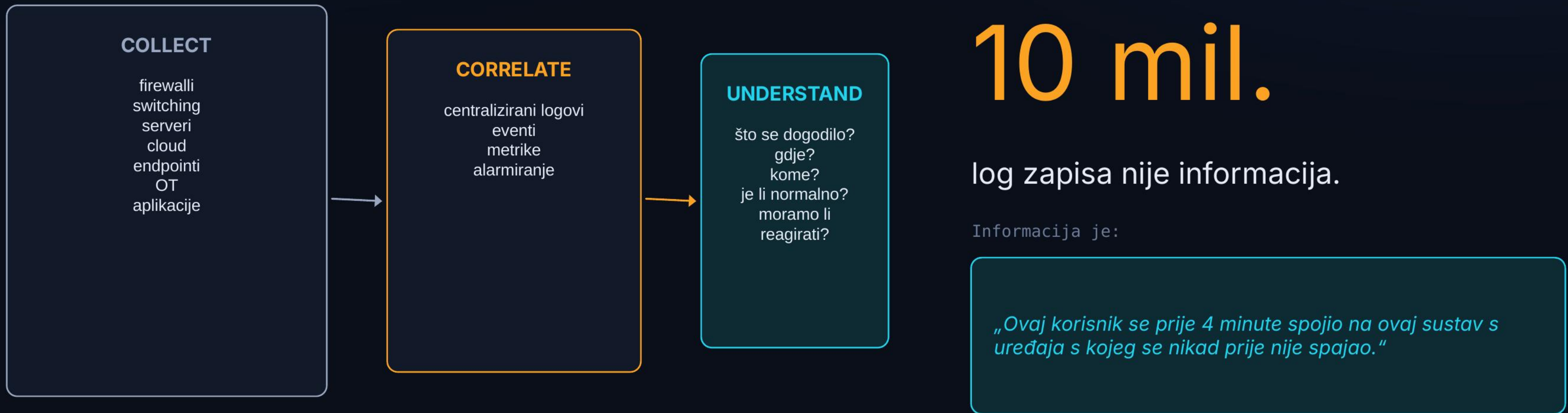
krizna situacija

Za taj sloj koristimo rješenja poput Peplinka — ali ključ nije proizvod, nego dizajn: dvije neovisne putanje i sustav koji sam odlučuje.

Cybersecurity štiti komunikaciju. Resilience osigurava da komunikacija uopće postoji.

ŠTO NE VIDIMO — NE MOŽEMO ŠTITITI

lokalni sustavi + cloud + jedna okolina za nadzor



AI ovdje kao alat: korelacija, anomalije, sumarizacija — ne kao zamjena za arhitekturu.

Problem više nije nedostatak podataka. Problem je količina podataka.

UREĐAJ JE DIO SIGURNOSNE ARHITEKTURE

mreža završava tek na endpointu

01 poznaj uređaj
inventar, vlasnik, stanje, verzija

02 kontroliraj konfiguraciju
politike se guraju, ne mole

03 kontroliraj aplikacije
što smije biti instalirano i pokrenuto

04 odvoji poslovne podatke
poslovno i privatno nisu isti spremnik

05 udaljeno reagiraj
zaključaj, obriši, izoliraj — s bilo kojeg mjesta

06 povuci pristup
kad uređaj više nije pouzdan, mreža ga više ne zna

identitet korisnika

+

povjerenje u uređaj

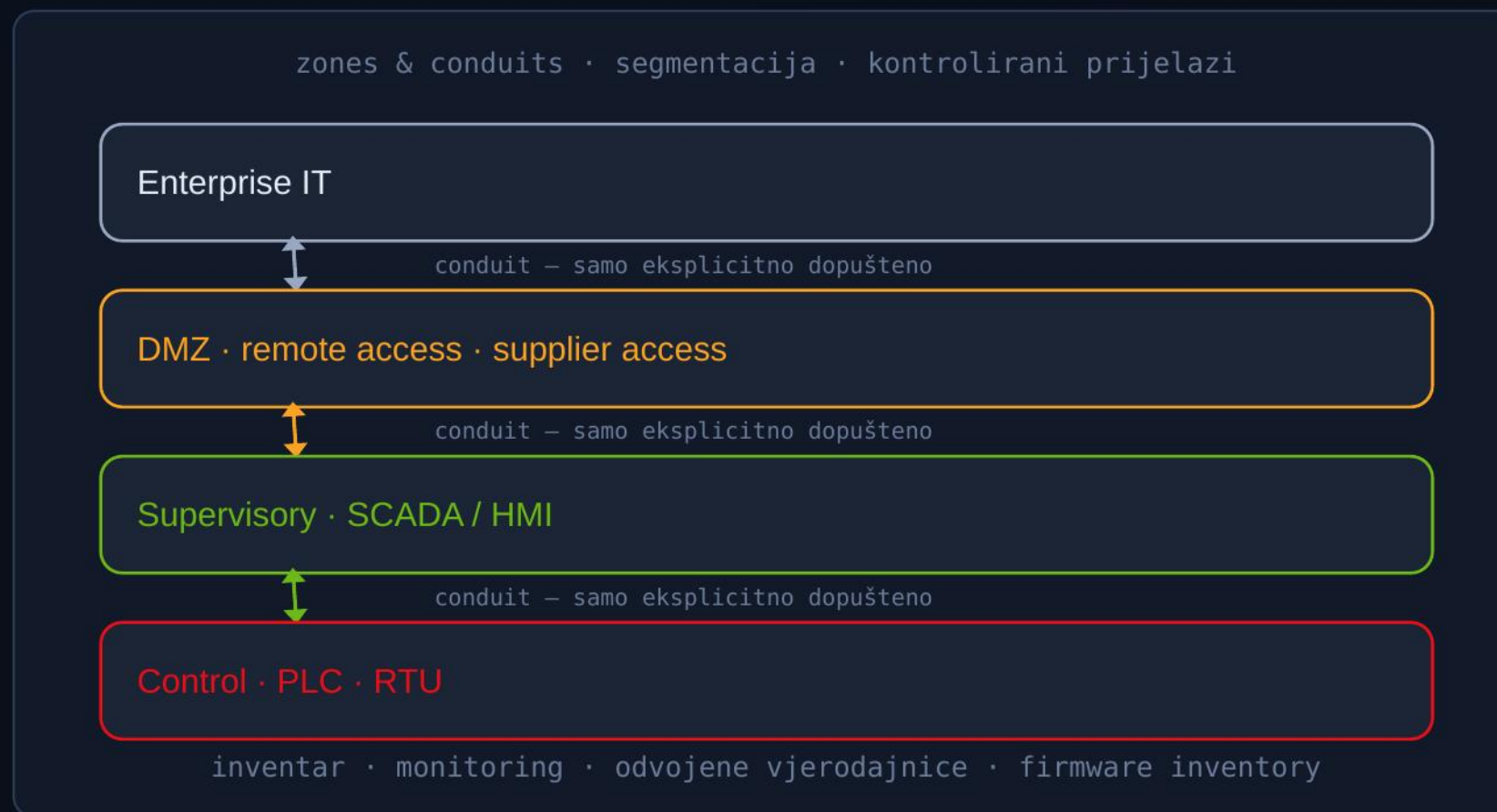


pristup sustavu

SOTI kao sloj upravljanja uređajima — uklopljen u istu arhitekturu, iste zone, isti nadzor.

Identitet korisnika nije dovoljan. Moramo vjerovati i uređaju s kojeg dolazi.

IT pravila ne možemo samo kopirati u OT



IZAŠAO JE CVE ZA PLC. ŠTO SAD?

IT

patch

utorak navečer, gotovo.

OT

procijeni

izoliraj

kompenziraj

planiraj
intervenciju

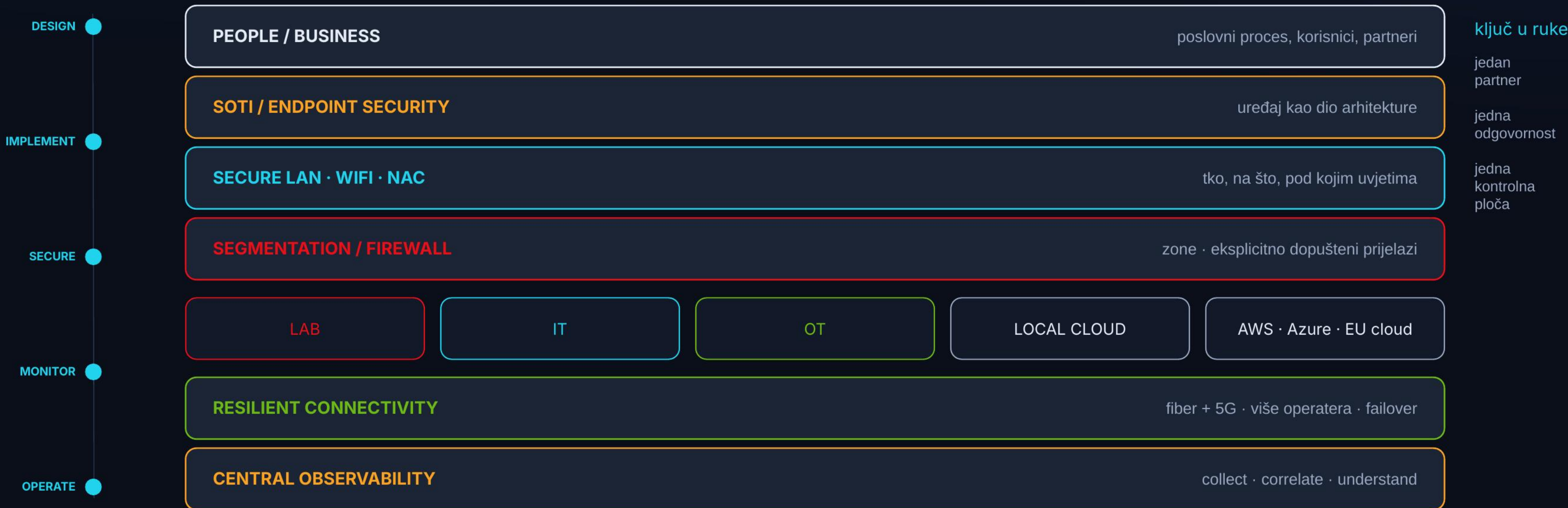
PLC ne možemo nužno patchirati u utorak navečer samo zato što je izašao CVE. Linija stoji, ljudi na smjeni, certifikacija stroja. Zato: procijeni što je izloženo, izoliraj zonu, dodaj kompenzacijsku kontrolu, i planiraj zahvat u sljedeći remont.

Full-blown implementacija: od procjene rizika i dizajna zona do nadzora i kontroliranog pristupa dobavljača.

Industrijska sigurnost nije firewall ispred tvornice. To je arhitektura cijele tvornice.

JEDNA KONTROLNA PLOČA

od komunikacije do poslovnog procesa



Pet tehničkih disciplina. Korisniku — jedna kontrolna površina i jedan odgovoran partner.



Naša vizija nije prodati firewall, switch, MDM ili cloud.

Naša vizija je preuzeti odgovornost da sve to zajedno radi.

Ključ u ruke više ne znači samo „radi“. Znači: radi, povezano je, zaštićeno je i znamo što se događa.



pitanja

Matija Matijevac · Magus Komunikacije · MAIDEA