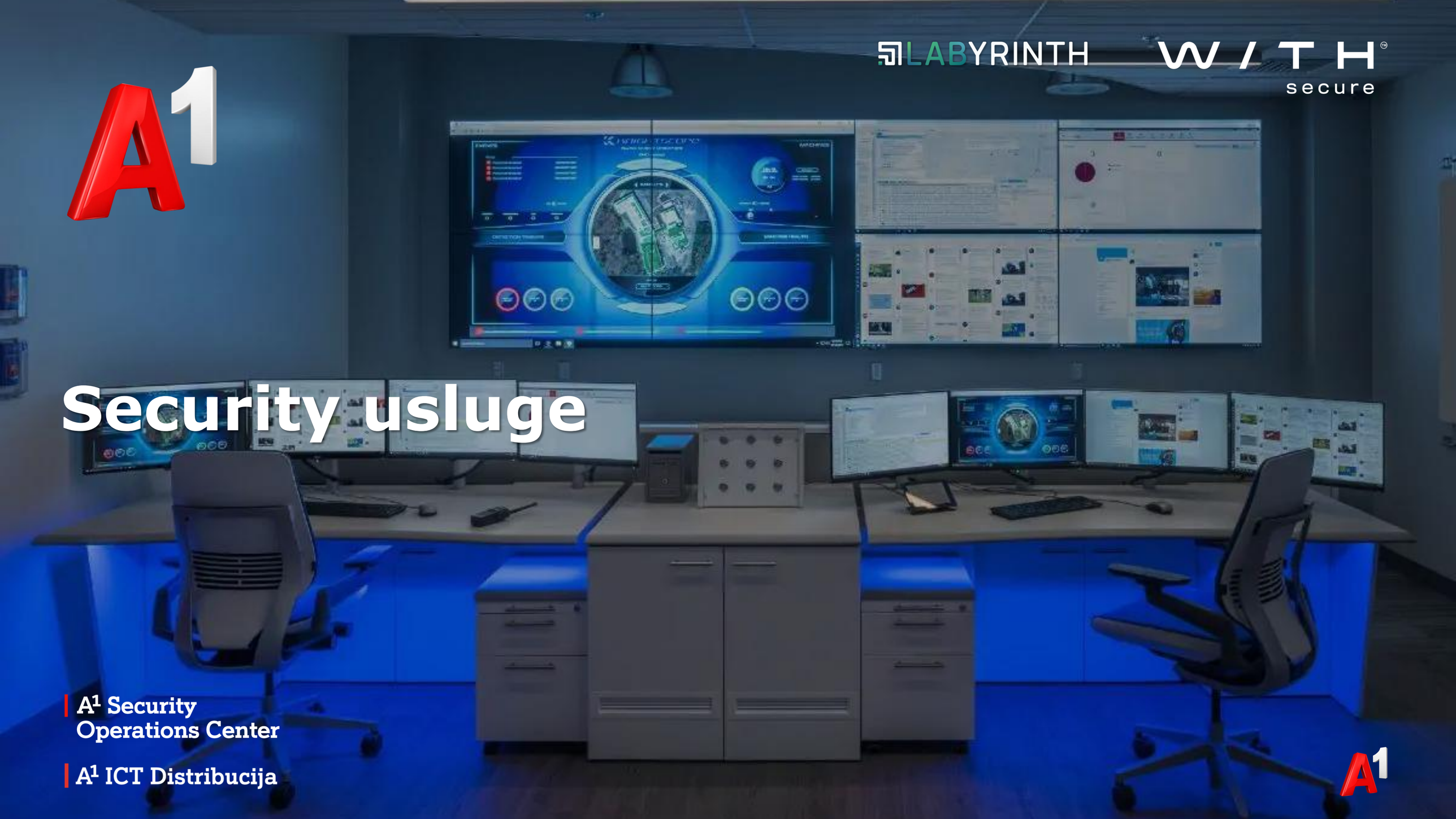


LABYRINTH

WITH secure

Security usluge

- A1 Security Operations Center
- A1 ICT Distribucija

Penetration testing

Penetration testing

Penetration testing

Penetration test pokaže realno stanje bezbjednosti i lokaciju ranjivosti.

Standardi, zakoni, regulative i ostala pravila postavljaju obaveze, da se penetration test odradi redovito

Tipovi pentesta

INTERNAL

- Metodologija „otvorenog“ testa
- Prisutni na lokaciji
- Hek „iznutra“
- Hakerske akcije + otvoren pregled sistema
- Report

EXTERNAL

- Metodologija „sljepog“ testa
- Nismo na lokaciji
- Hek „z interneta“
- Hekerske metode
- Report

A1 Security Operations Center

A1 Security Operations Center

A1 ICT Distribucija

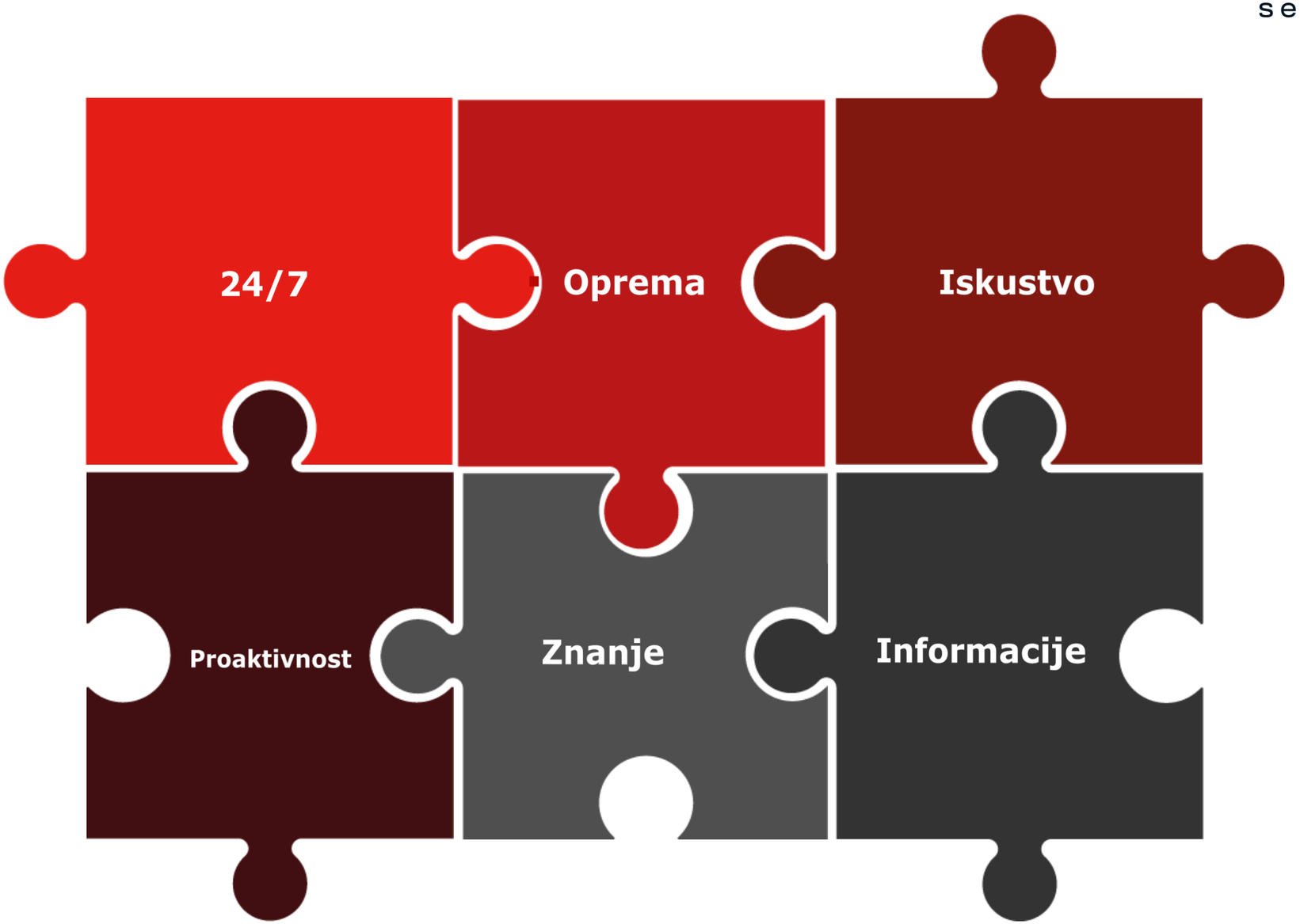

A1 Business
Zašto SOC?
A1 Security
Operations Center

LABYRINTH W/TH secure

A1 Security Operations Center

abacus computing A1

A1 Security Operations Center



A1 Business

Generalni pogled u SOC

A1 Security Operations Center

A1 Security Operations Center

- Aktivan od: 2020
- Broj klienata: 100+ (cca. 9000 endpointa)
- Core ekipe: 10 stručnjaka
  - + 1st level
  - + A1 grupa

1. nivo

24/7 dežurstvo on-premise
Prijam i detekcija alarma
Osnovna triaža

2. nivo

24/7 dežurstvo on-call
Dublja triaža
Komunikacija s klientima

3. nivo

Specifička znanja za posebne situacije

A1 Business

Detajlniji pogled u SOC

A1 Security Operations Center

Odabir opreme

SIEM, Honey Pot, EDR, ...

Penetration test

Security checklist, dižemo nivo cybersecurity, ...

Onboarding proces

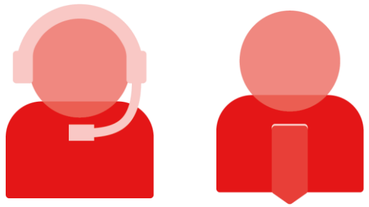
Prijam podataka, dogovor o implementaciji, ...

Playbook definicije

Kada se reagira, kada se javlja, ...

Dark Web
(threat hunting)

Infrastruktura klienta



Slanje alarma

Proaktivne akcije dogovorone uz definiciju playbooka

E-mail / telefon komunikacija

1.nivo

Prijem alarma
Osnovna triaža

2.nivo

2.nivo

Podaci:
- Alarm
- SIEM
- 360 pogled klienta

Detajlnija triaža

Po potrebi se uključuje 3. nivo

3.nivo

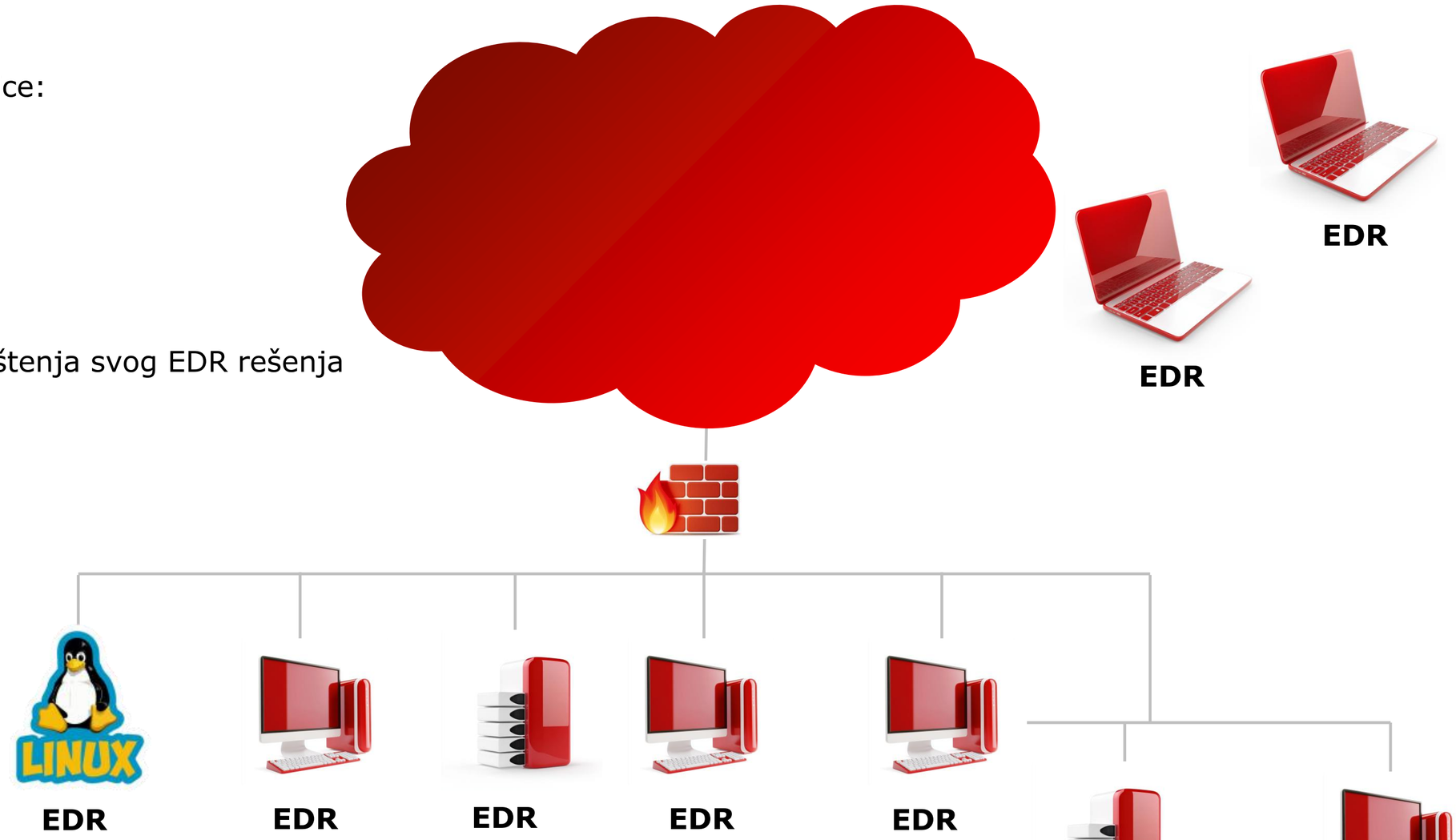
Različiti statusi:
- Monitoring
- Alarmiranje
- Uključiti u report
- Ignore

A1 Business

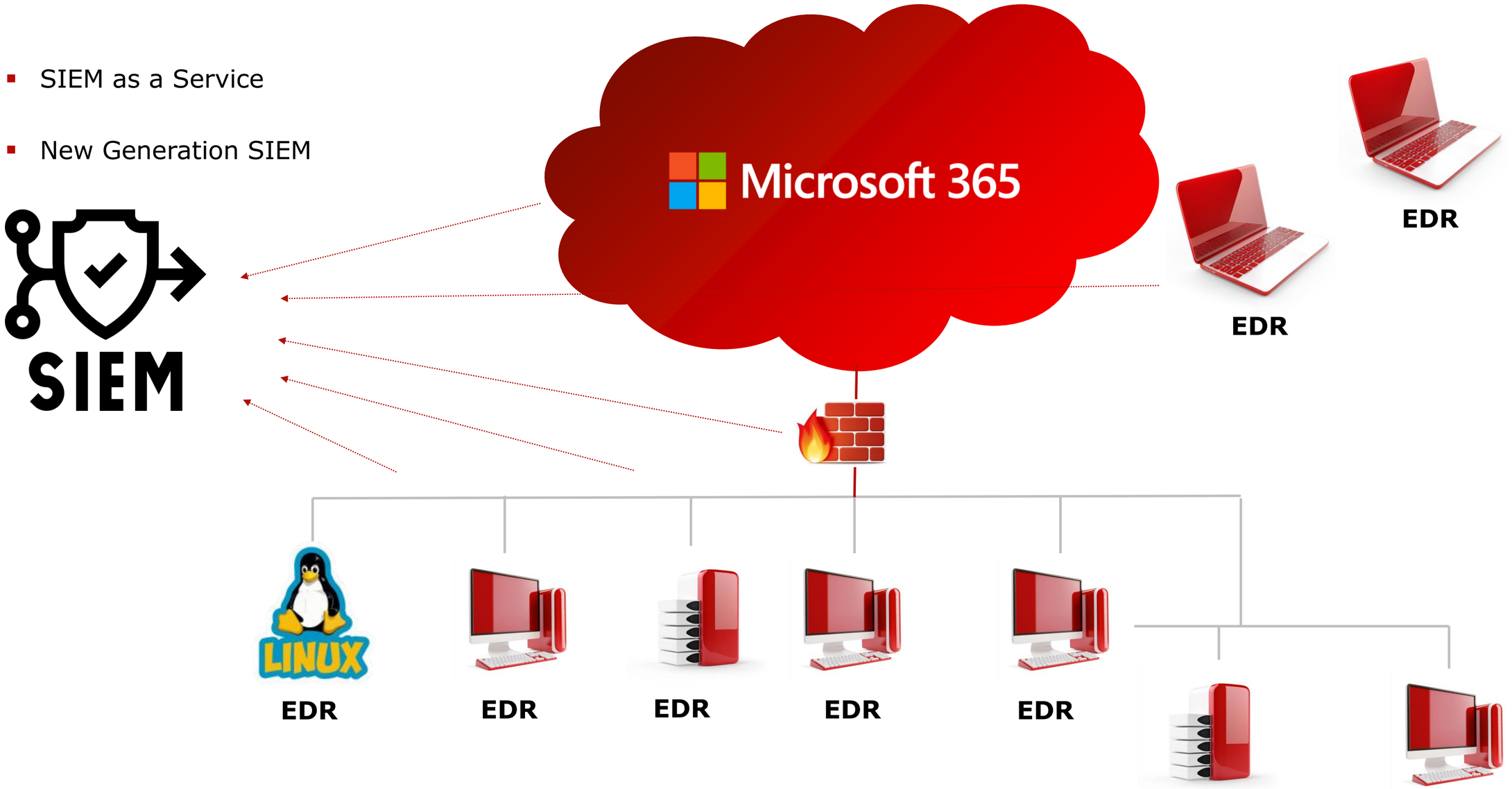
Oprema

A1 Security Operations Center

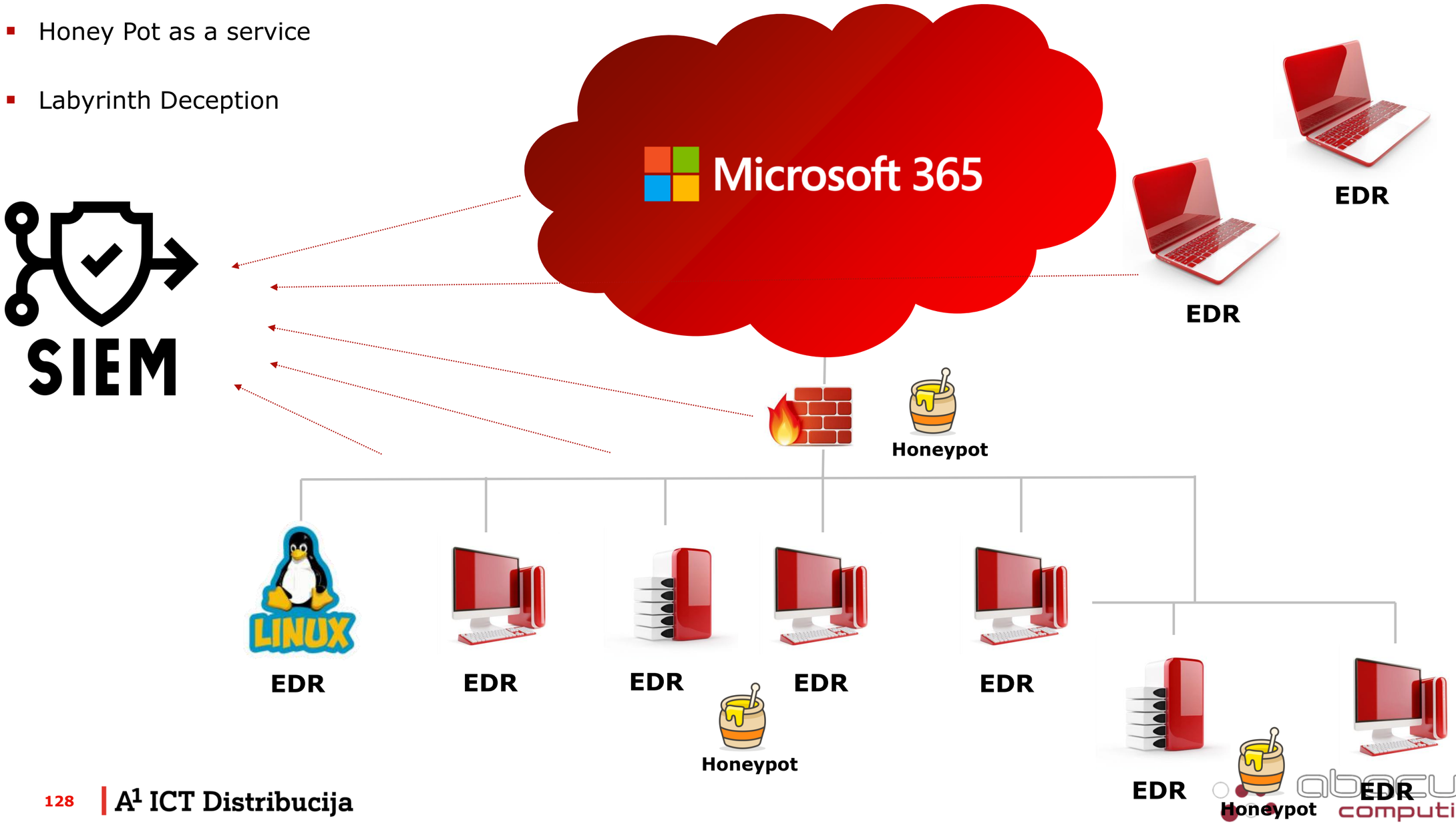
- EDR-AS-A-Service:
  - Cynet
  - Sentinel
- Partneri
  - WithSecure
- Mogućnost korištenja svog EDR rešenja



- SIEM as a Service
- New Generation SIEM



- Honey Pot as a service
- Labyrinth Deception



Pojmovi tehnologije u SOCu

- **SOC** = **S**ecurity **O**perations **C**enter = usluga, koja koristi različite cybersecurity i IT alate za aktivno praćenje svih aktivnosti i odazivanje na sve detektirane pretnje

- **SIEM** = **S**ecurity and **I**nformation **E**vent **M**anager = alat za skupljanje svih događaja u IT infrastrukturi, koja ekipi SOC pomaže korelacijom svih aktivnosti i nudi forenzičke mogućnosti otkrivanja svih detajla aktivnih pretnji. Na SIEM šalju se svi eventi security alata (WithSecure, Labyrinth, Stormshield, Proofpoint) i servera (Windows i Linux login, VPN login, cloud…)

- **EDR/XDR** = **E**ndpoint/E**x**tended **D**etection & **R**esponse = osnova za svaku SOC ekipu, kako bi imala pristup do najviše detajla aktivnosti na radnim stanicama i serverima

- **Honeypot / Deception Point** = namjerno ranjiv server, servis, aplikacija u internoj mreži, kako bi hekera usmerili prema lakim metama, da ne diraju pravih servera