A1 Security Operations Center

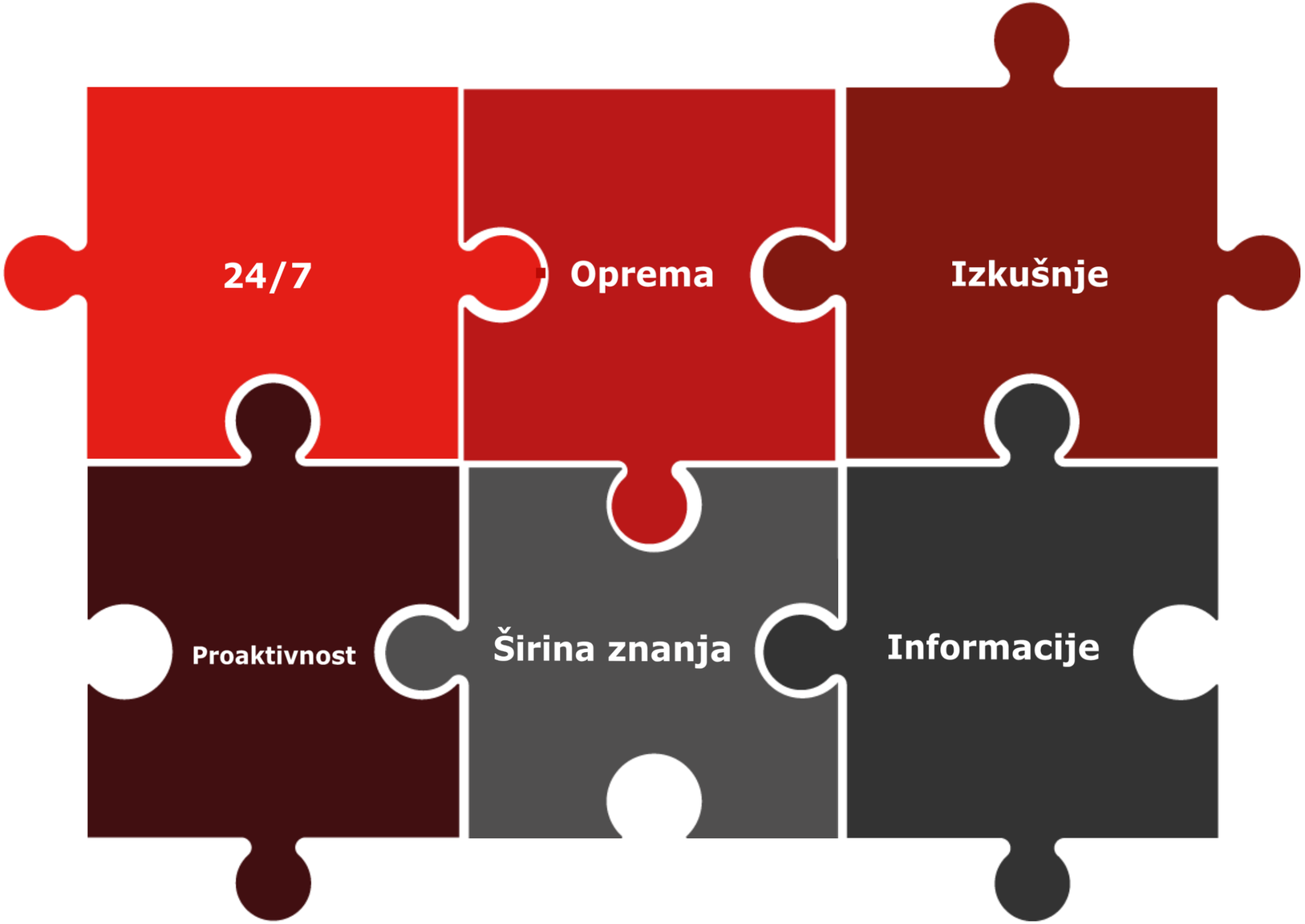
Vladimir Ban

Vodja SOC @A1 Slovenija d.d.
Etični heker
CEH, OSCP, OSEP


A1 Business
Zakaj sploh SOC?
A1 Security
Operations Center

A1 Security Operations Center

A1 Security Operations Center



A1 Business

Generalni oris delovanja

A1 Security Operations Center

A1 Security Operations Center

- Začetek delovanja: 2020
- Število naročnikov: 80+ (cca. 7000 točk)
- Jedro ekipe: 10 strokovnjakov
  - + 1st level
  - + grupa

1. nivo

24/7 dežurstvo na lokaciji
Sprejem in detekcija alarmov
Osnovna triaža

2. nivo

24/7 dežurstvo na klic
Poglobljena triaža
Komunikacija z naročniki

3. nivo

Specifična in poglobljena znanja za posebne primere

A1 Business

Podrobnejši opis delovanja

A1 Security Operations Center

Postavitev opreme
SIEM, Honey Pot, EDR, ipd.

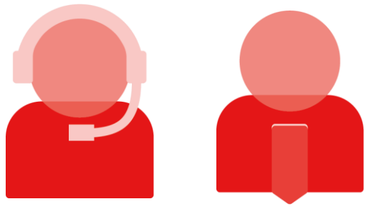
Varnostni pregled
Security checklist, dvig nivoja varnosti, ipd.

Onboarding proces
Prejem podatkov, dogovor o namestitvah, ipd.

Playbook definicije
Kdaj se reagira, kdaj se javlja, ipd.

Dark Web
(threat hunting)

Okolje naročnika



Pošiljanje alarmov

1.nivo

Prejem alarmov
Osnovna triaža

Proaktivne akcije z vnaprej dogovorjenimi playbooki

Prehod v 2.nivo

Podatki:
- Alarm
- SIEM
- 360 vpogled v naročnika

2.nivo

Podrobnejša triaža

E-mail / klic komunikacija

Po potrebi se vključi 3.nivo

Različni statusi:
- Spremljanje
- Alarmiranje
- Za v poročilo
- Ignore

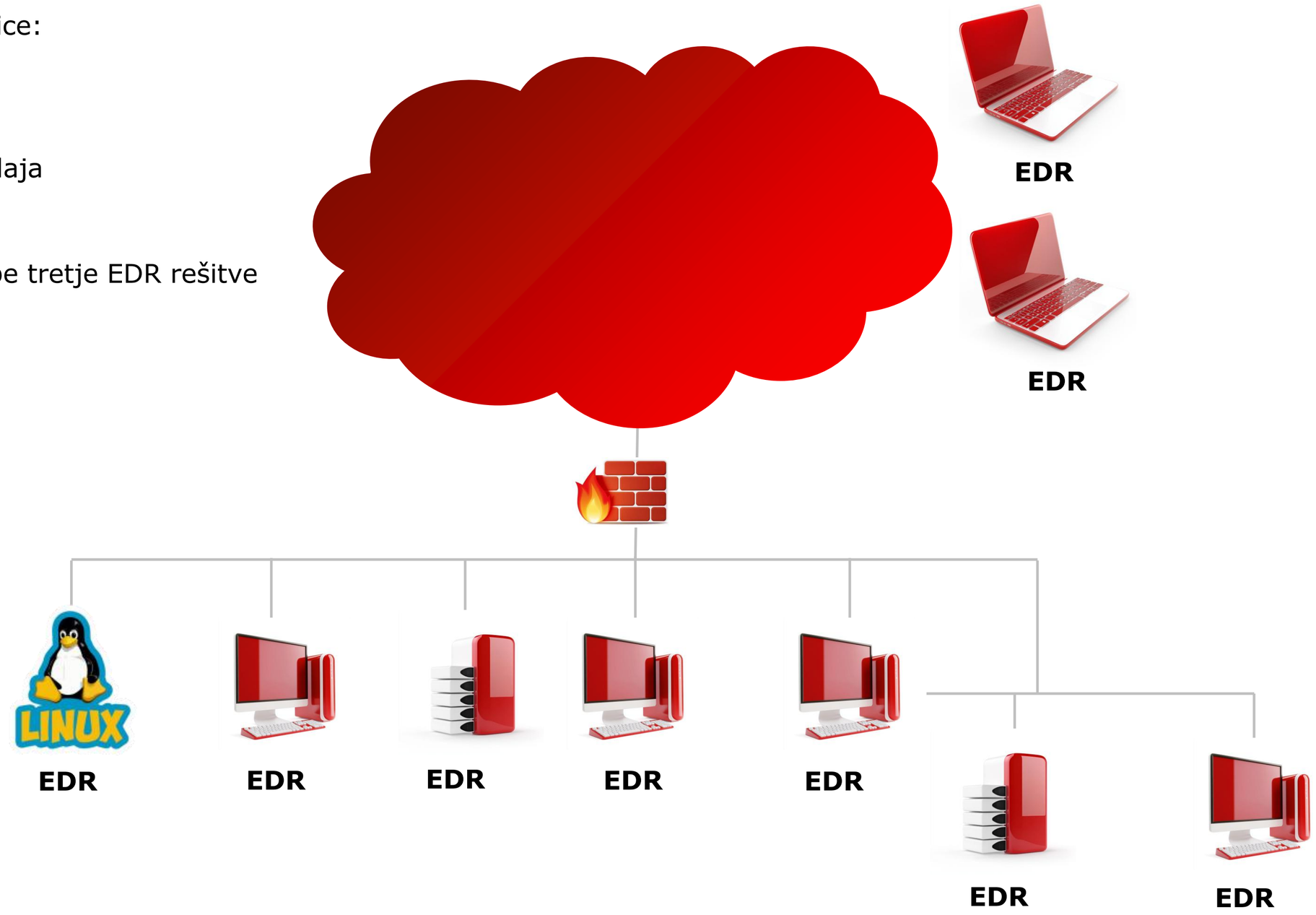
3.nivo

A1 Business

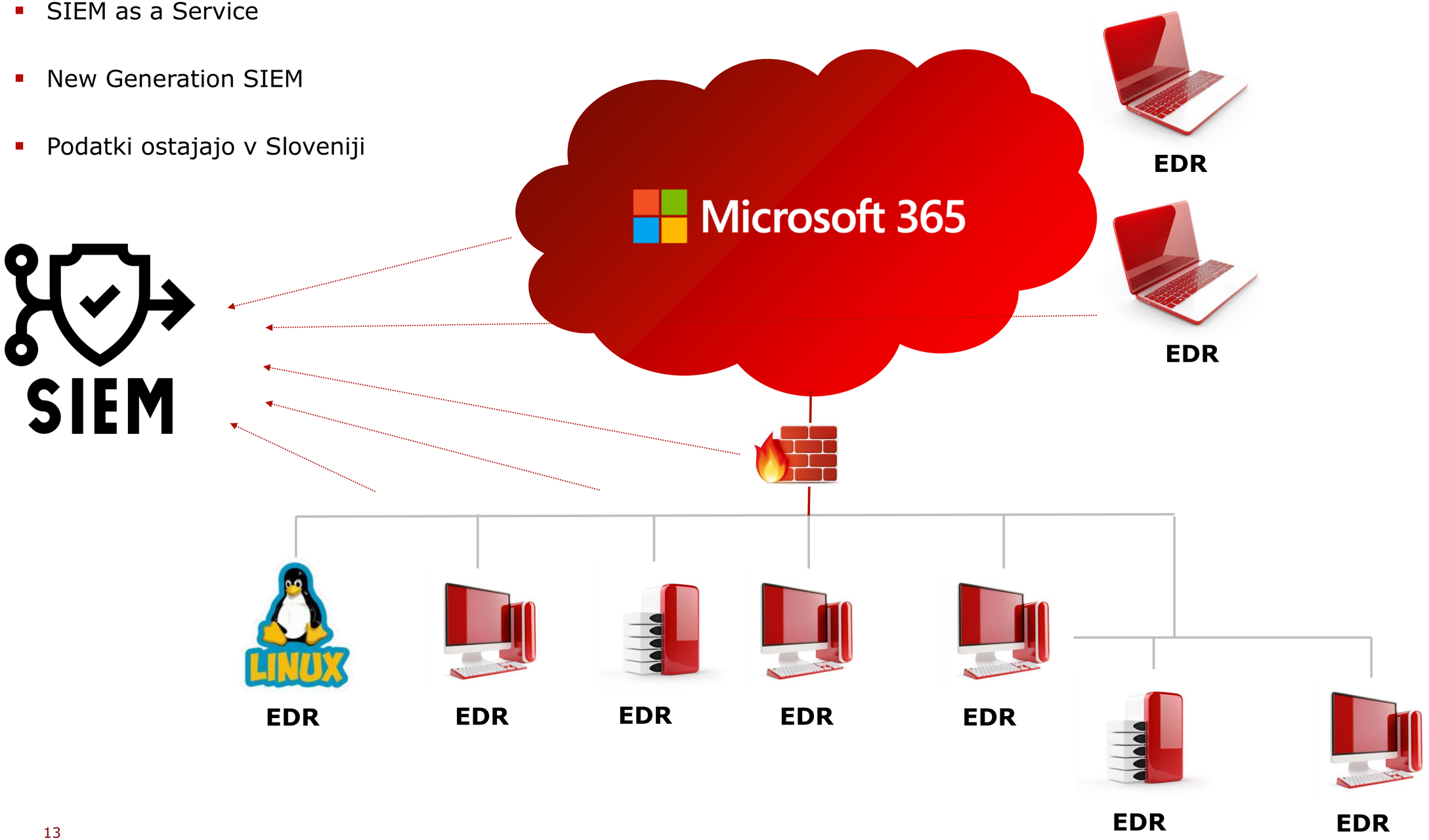
Oprema

A1 Security Operations Center

- EDR-AS-A-Service:
  - Cynet
  - Sentinel
- Partnerska prodaja
  - WithSecure
- Možnost uporabe tretje EDR rešitve

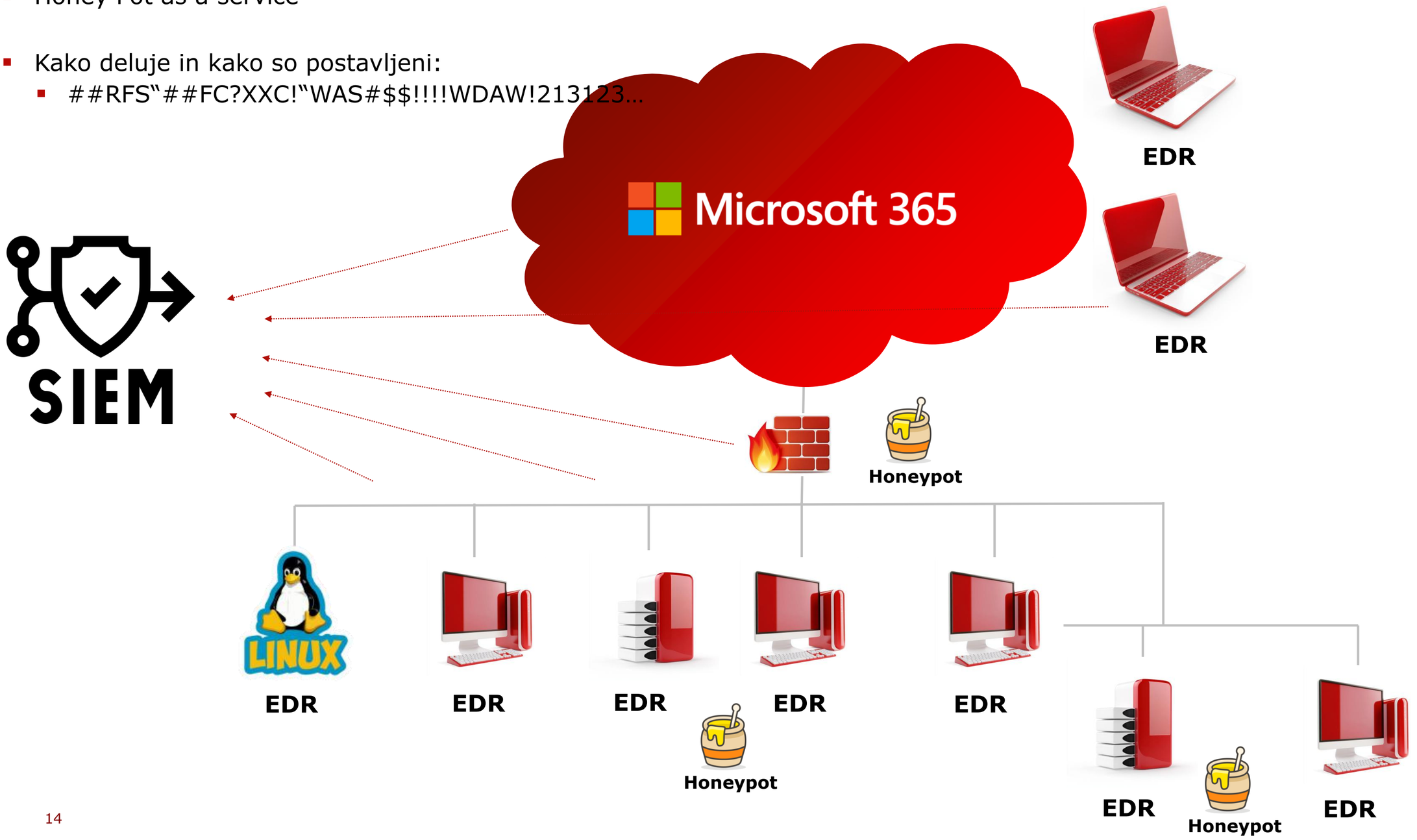


- SIEM as a Service
- New Generation SIEM
- Podatki ostajajo v Sloveniji



- Honey Pot as a service

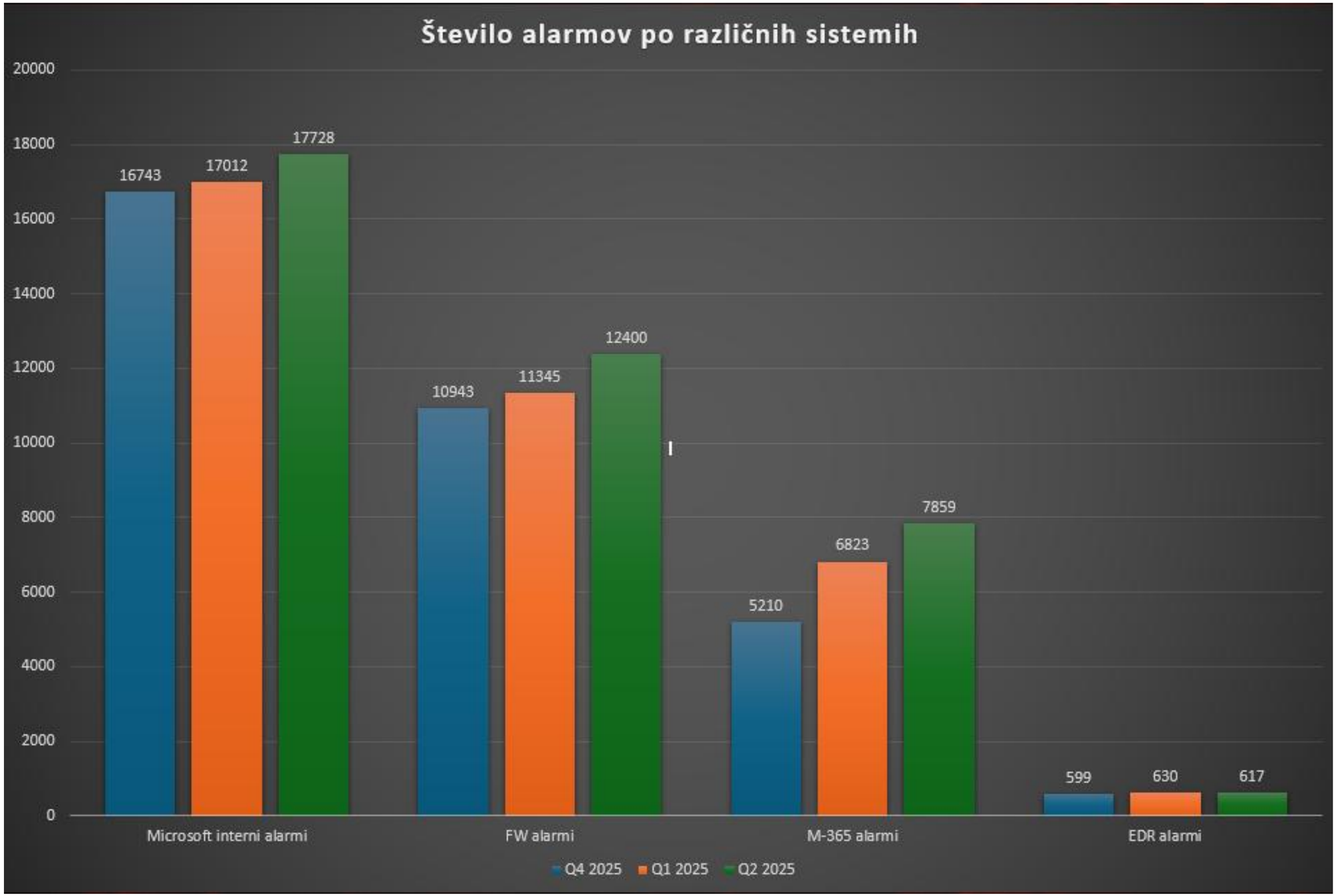
- Kako deluje in kako so postavljeni:
  - ##RFS"##FC?XXC!"WAS#$$!!!!WDAW!213123…



A1 Business

Statistika in konkretni primeri

A1 Security
Operations Center


Število alarmov po različnih sistemih
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
16743
17012
17728
10943
11345
12400
5210
6823
7859
599
630
617
Microsoft interni alarmi
FW alarmi
M-365 alarmi
EDR alarmi
Q4 2025
Q1 2025
Q2 2025


Število dogodkov na mesec na naročnika
4
3,5
3
2,5
2
1,5
1
0,5
0
Q1 2024
Q2 2024
Q3 2024
Q4 2024
Q1 2025
Q2 2025
Število dogodkov

A1 Business

Let's work together in this fast-evolving world of security threats.

A1 Security Operations Center