A1 Dogodek

SIEM ZA VSAKOGAR

Ljubljana, A1 Konferenčni center, 13. april ob 9. uri

A1 ICT Distribucija

ENERGY LOGSERVER

Koga bomo poslušali?☺

Robert Kąkol
Territory Manager

Energy LogServer

Szymon Ćwieka
Sales Engineer

Energy LogServer

Maja Milojević
ICT Distribution Manager

A1 Slovenija

Marko Kašić
Lead ICT and Cybersecurity Presales Engineer

A1 Slovenija

Vladimir Ban
Cybersecurity and Ethical hacker

A1 Slovenija

Današnja Agenda

09:00 – 09:30	Prihod in jutranja kava
09:30 – 09:45	Uvod in predstavitev podjetja Energy LogServer
09:45 – 10:15	SIEM, kaj je to, zakaj SIEM, zakaj Energy LogServer
10:15 – 10:30	Predstavitev Energy LogServer rešitve
10:30 – 10:45	Odmor
10:45 – 11:45	Demo predstavitev Energy LogServer
11:45 – 12:15	Poslovni model, licenciranje, diskusija…
12:15 – 13:30	Druženje ob kosilu

SIEM in Energy LogServer

Maja Milojević in Marko Kašić

ENERGY LOGSERVER

ENERGY LOGSERVER

A1 ICT Distribucija

ENERGY
LOGSERVER

A1

Izzivi podjetij

Izzivi

- Preveč podatkov z različnih virov
- Alert storm
- Ni mogoče ustaviti napadov, ki jih ne zaznavaš
- Primanjkljaj varnostnih strokovnjakov
- Visoki stroški

SKLADNOST

GDPR
Interni pravilniki
Revizijska sled

Javni sektor
Zdravstvo
Finance in zavarovalništvo
Kritična infrastruktura

ENERGY LOGSERVER

ENERGY LOGSERVER

SLA

Višji nivo poročanja za managerje

Osrednji pogled v SLA statuse

SME segment

Finance in zavarovalništvo

Kritična infrastruktura

A1 ICT Distribucija

SECURITY

Zaznavanje groženj
Kategorizacija dogodkov
Prioritizacija
SOC dashboard
Alarmi v realnem času

Zavezanci k regulaciji
Finance, zavarovalništvo
Kritična infrastruktura
Dobra praksa za SME segment

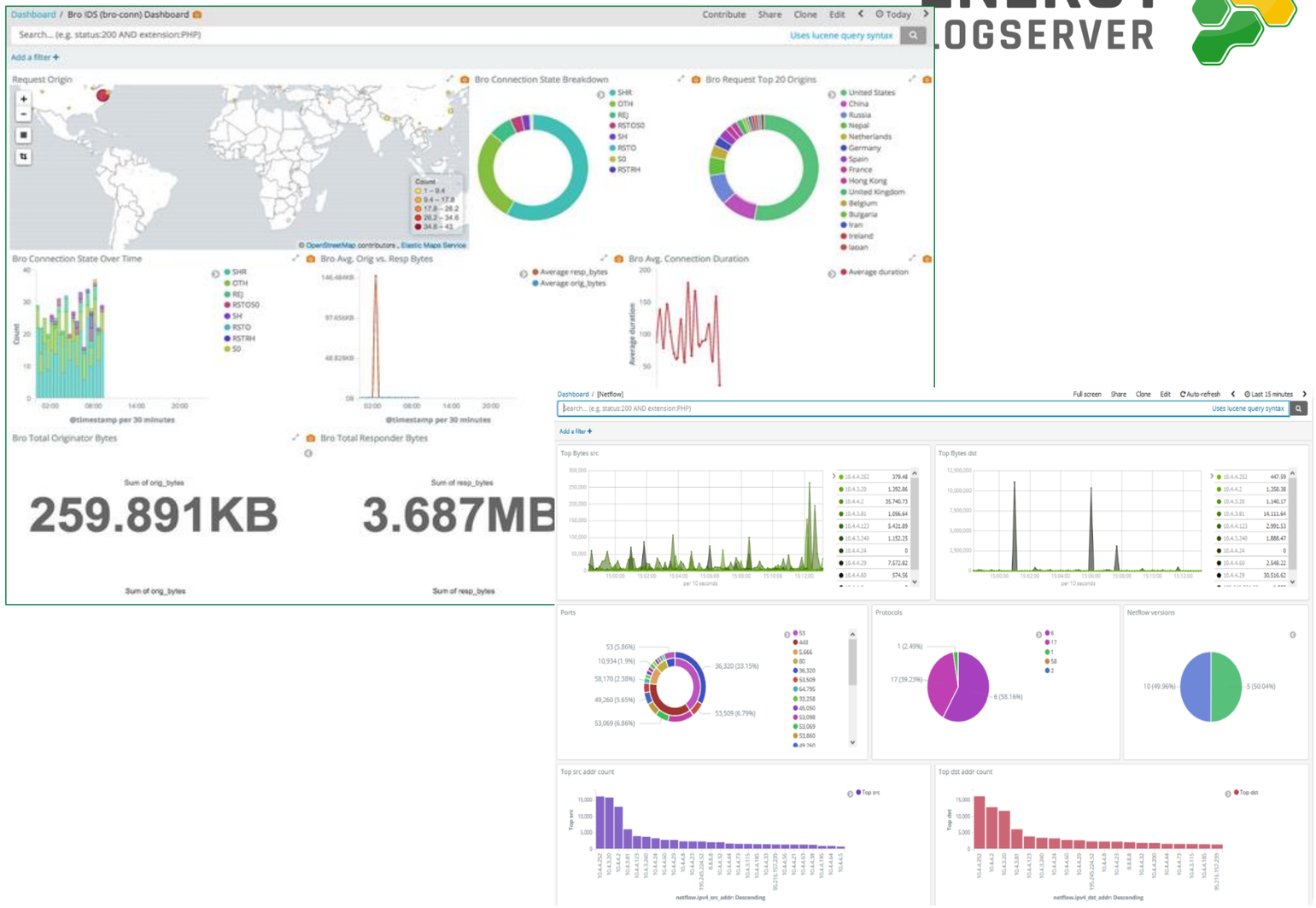
ENERGY LOGSERVER

A1 ICT Distribucija

OMREŽNI PROMET

Zaznavanje prometa
Verifikacija protokolov
Celovit vpogled v dogodke na omrežju

Zavezanci k regulaciji
Finance, zavarovalništvo
Telekomunikacije
Kritična infrastruktura
SME segment



SIEM

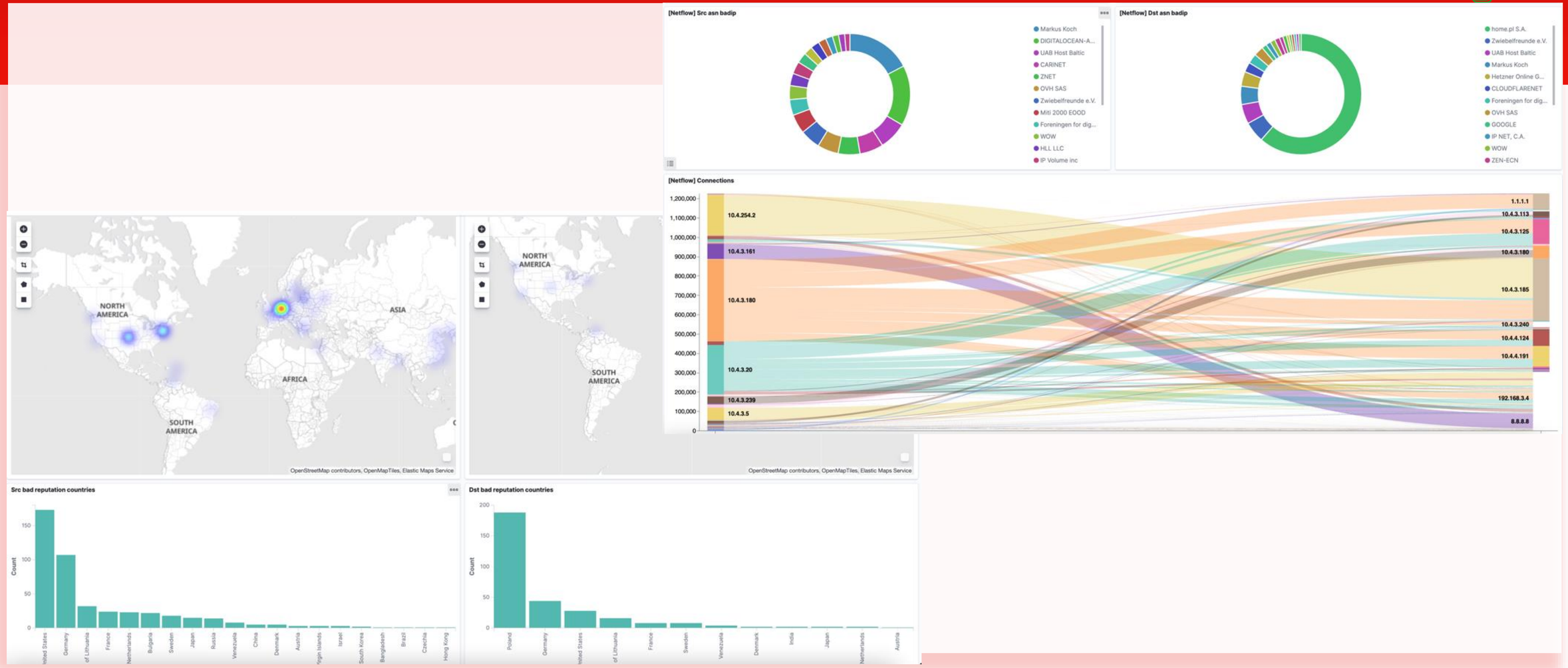
ENERGY
LOGSERVER

Upravljanje dnevnikov in poročanje

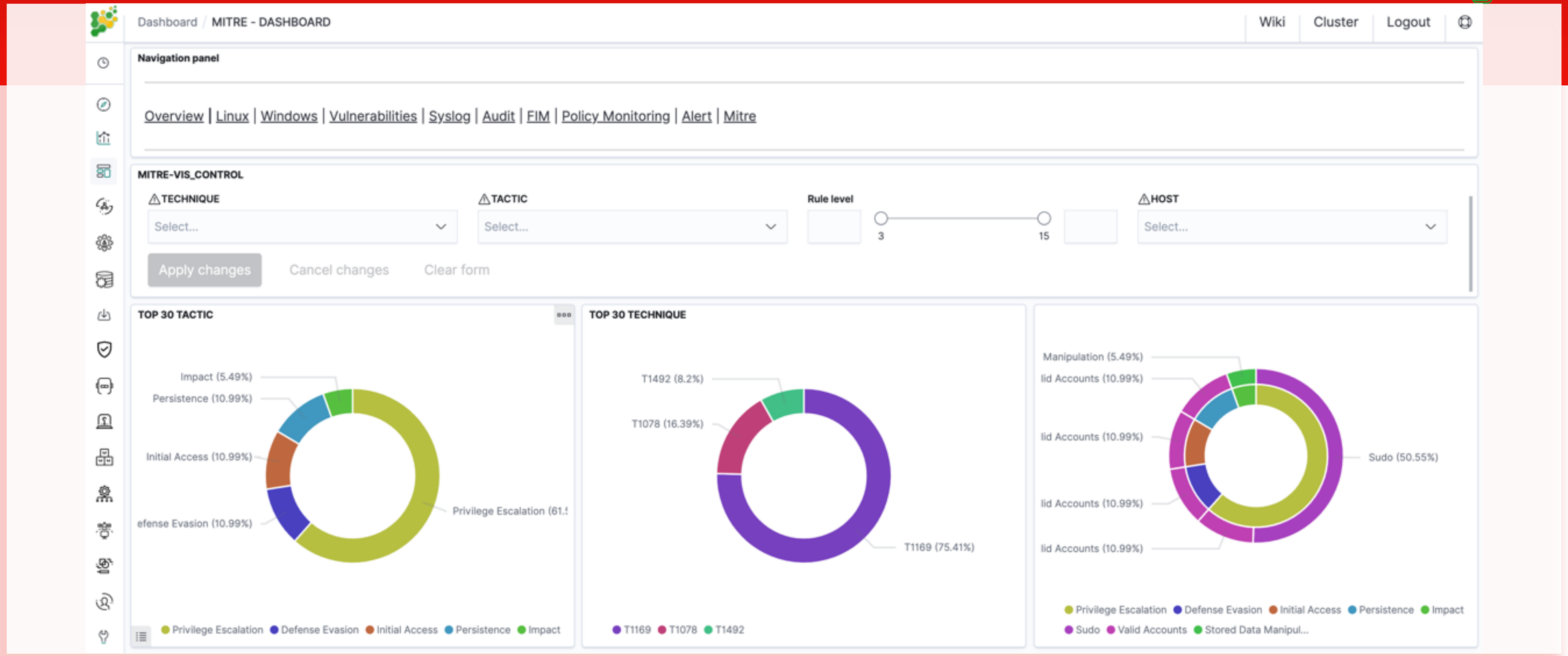
ENERGY LOGSERVER

VSI TEKSTOVNI PODATKI

Spremljanje v realnem času



Nadzorna plošča

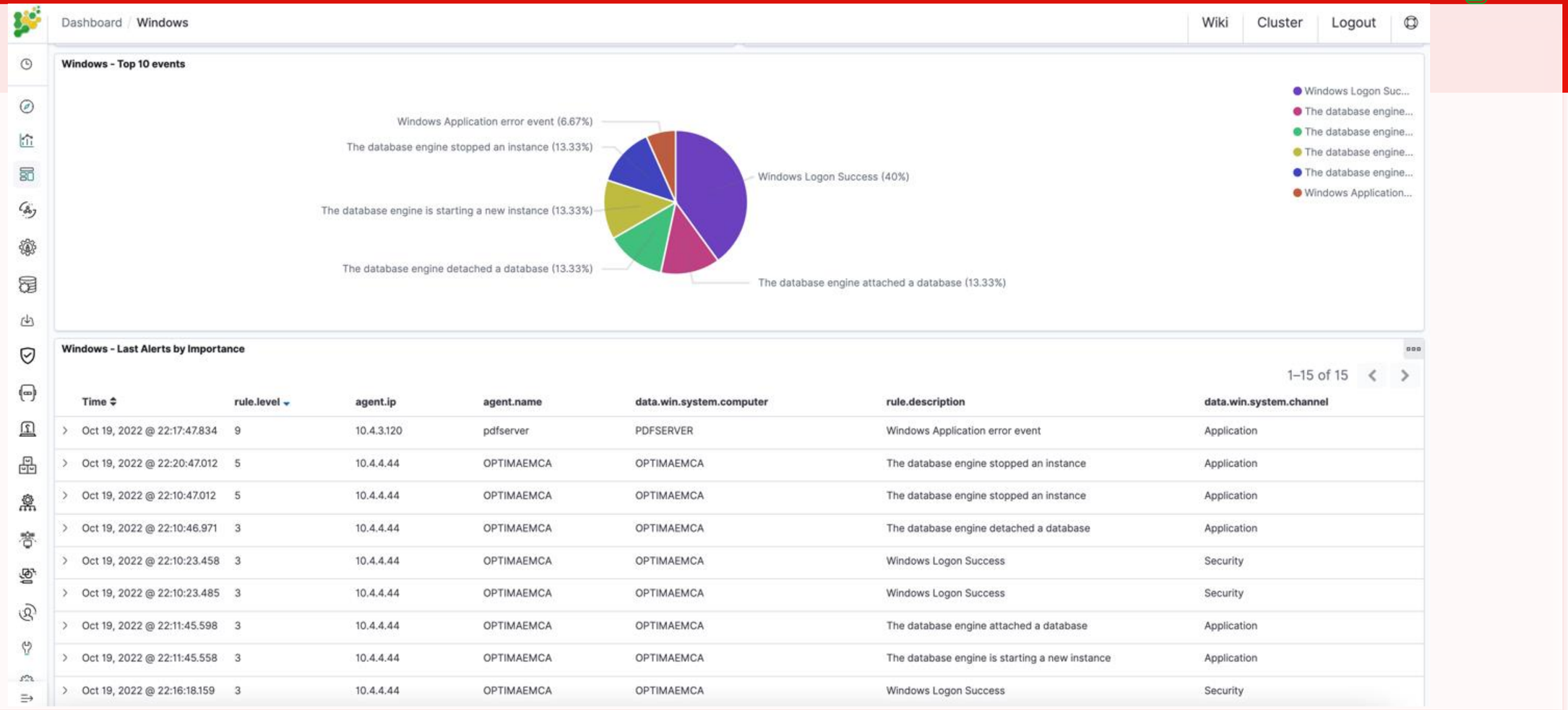


Upravljanje z incidenti

ENERGY LOGSERVER

A1 ICT Distribucija

Spremljanje podatkov/uporabnikov/aplikacij

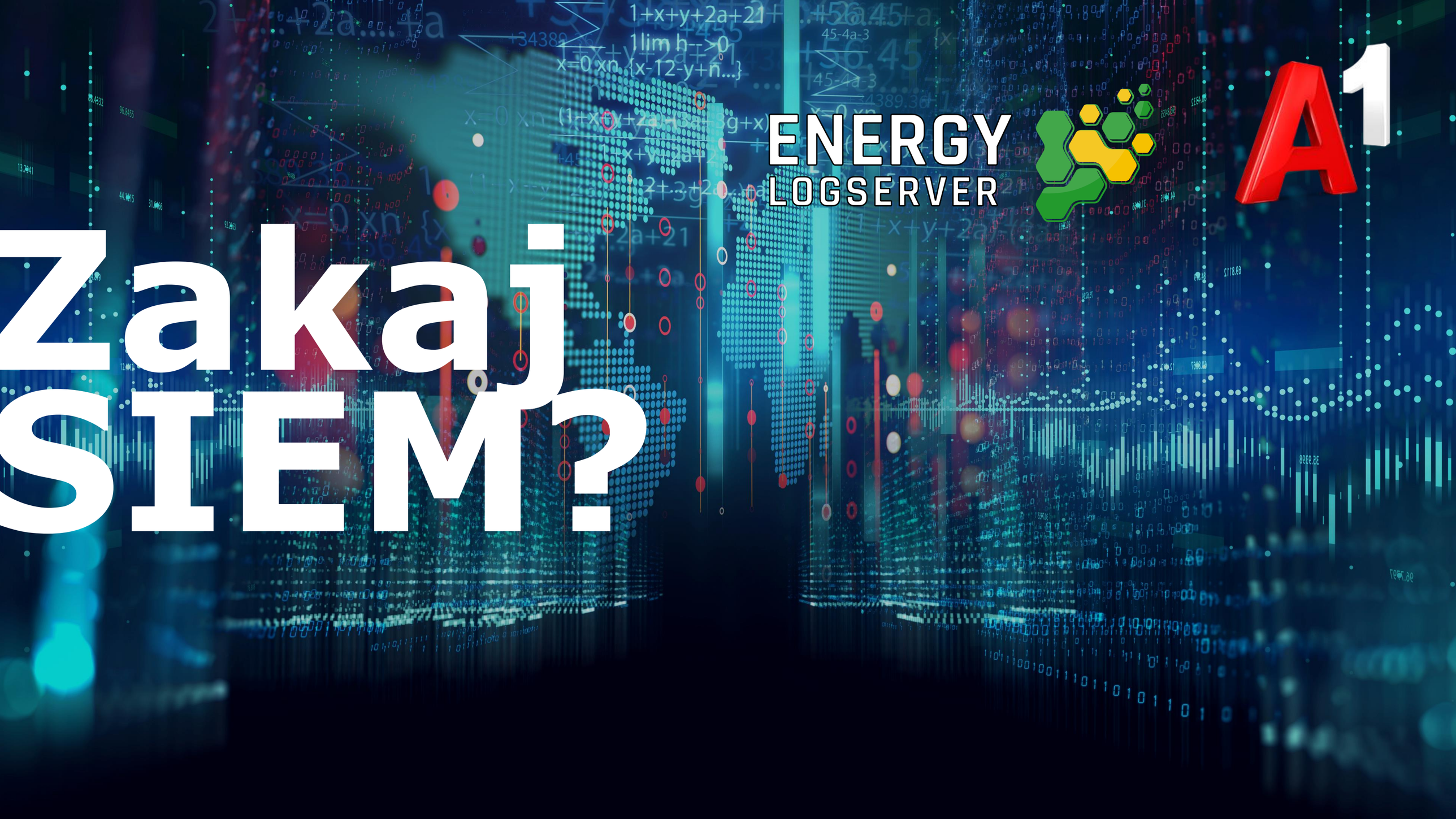


Time	rule.level	agent.ip	agent.name	data.win.system.computer	rule.description	data.win.system.channel
Oct 19, 2022 @ 22:17:47.834	9	10.4.3.120	pdfserver	PDFSERVER	Windows Application error event	Application
Oct 19, 2022 @ 22:20:47.012	5	10.4.4.44	OPTIMAEMCA	OPTIMAEMCA	The database engine stopped an instance	Application
Oct 19, 2022 @ 22:10:47.012	5	10.4.4.44	OPTIMAEMCA	OPTIMAEMCA	The database engine stopped an instance	Application
Oct 19, 2022 @ 22:10:46.971	3	10.4.4.44	OPTIMAEMCA	OPTIMAEMCA	The database engine detached a database	Application
Oct 19, 2022 @ 22:10:23.458	3	10.4.4.44	OPTIMAEMCA	OPTIMAEMCA	Windows Logon Success	Security
Oct 19, 2022 @ 22:10:23.485	3	10.4.4.44	OPTIMAEMCA	OPTIMAEMCA	Windows Logon Success	Security
Oct 19, 2022 @ 22:11:45.598	3	10.4.4.44	OPTIMAEMCA	OPTIMAEMCA	The database engine attached a database	Application
Oct 19, 2022 @ 22:11:45.558	3	10.4.4.44	OPTIMAEMCA	OPTIMAEMCA	The database engine is starting a new instance	Application
Oct 19, 2022 @ 22:16:18.159	3	10.4.4.44	OPTIMAEMCA	OPTIMAEMCA	Windows Logon Success	Security

Upravljanje

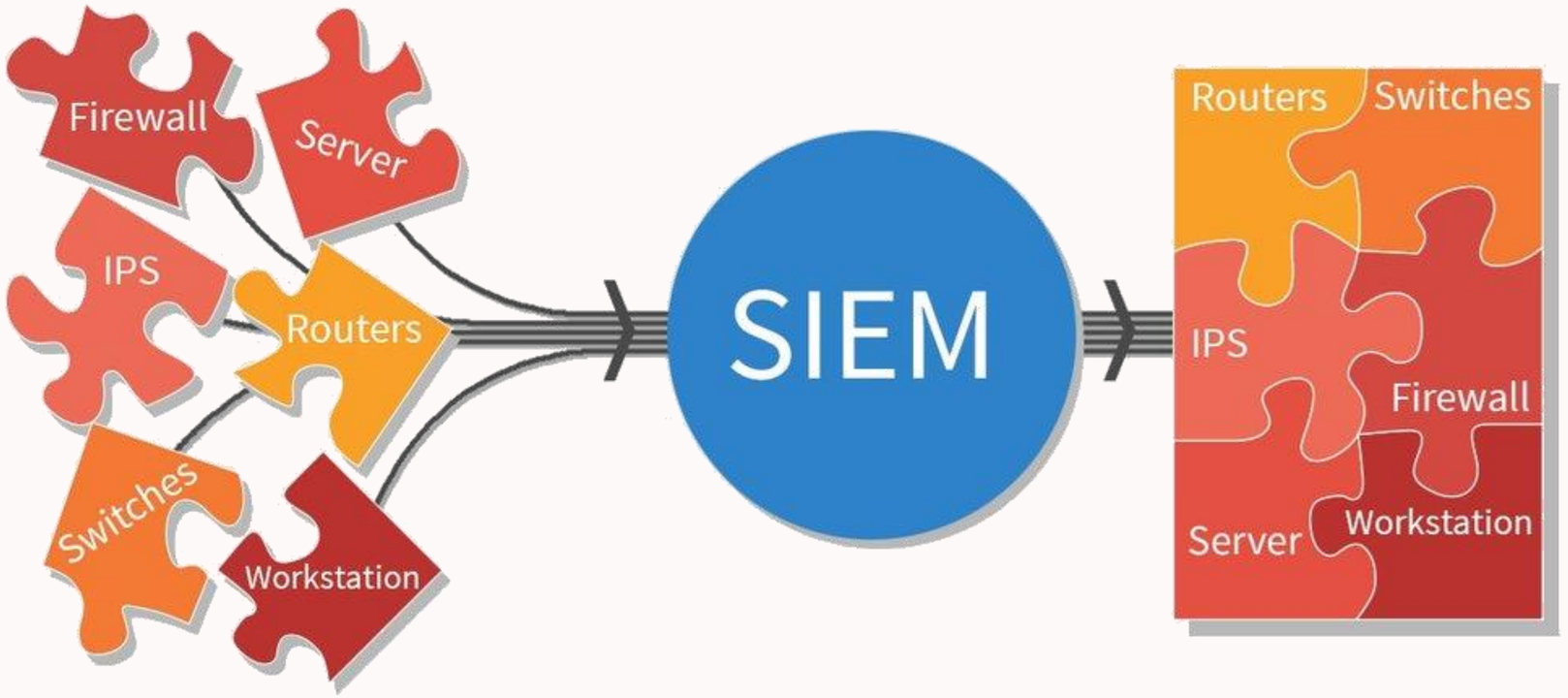
SIEM ali MSSP?

ENERGY LOGSERVER


ENERGY
LOGSERVER
A1
Zakaj SIEM?

Zakaj SIEM?

ENERGY LOGSERVER

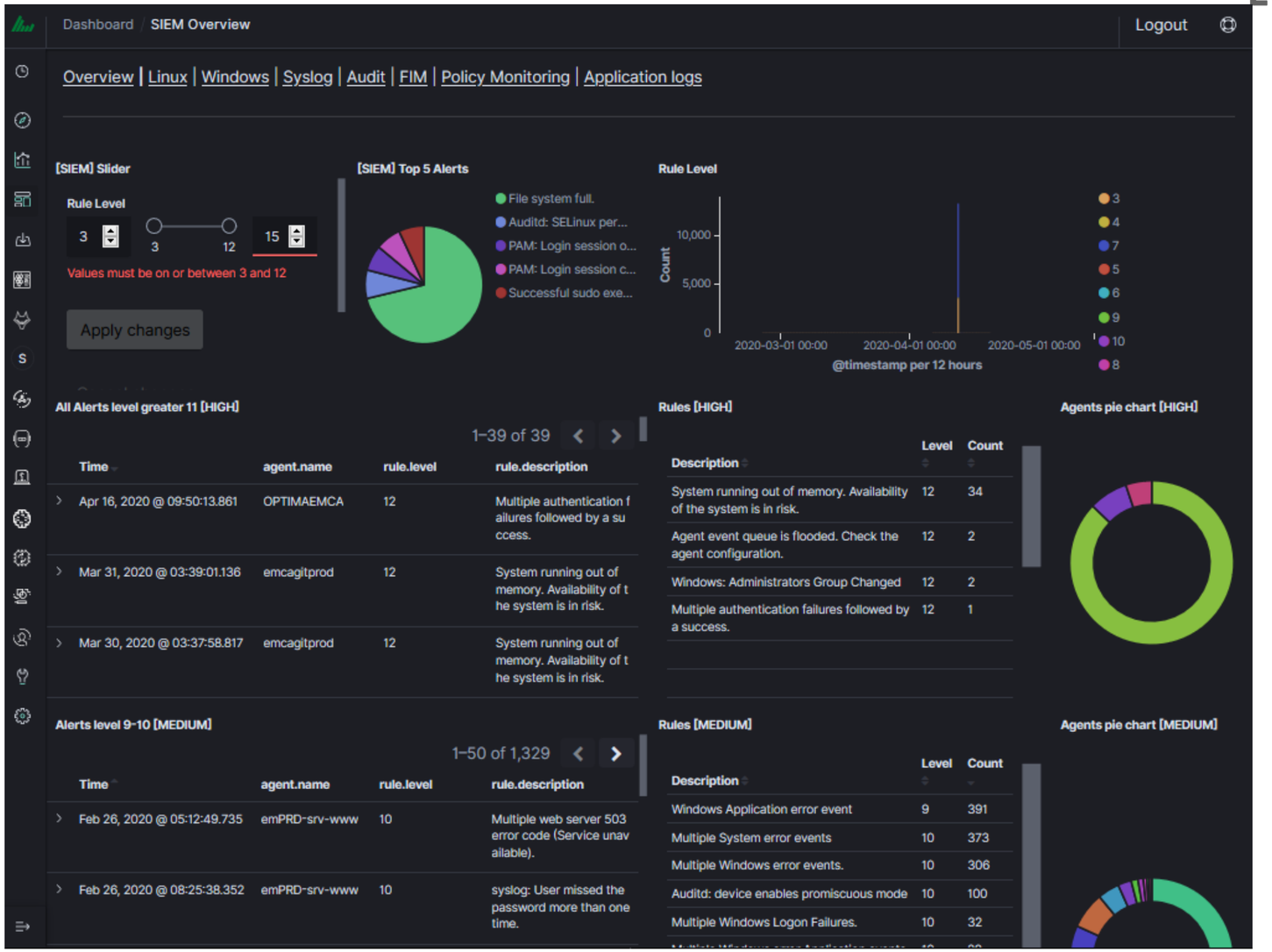


A1 ICT Distribucija

Skladnost

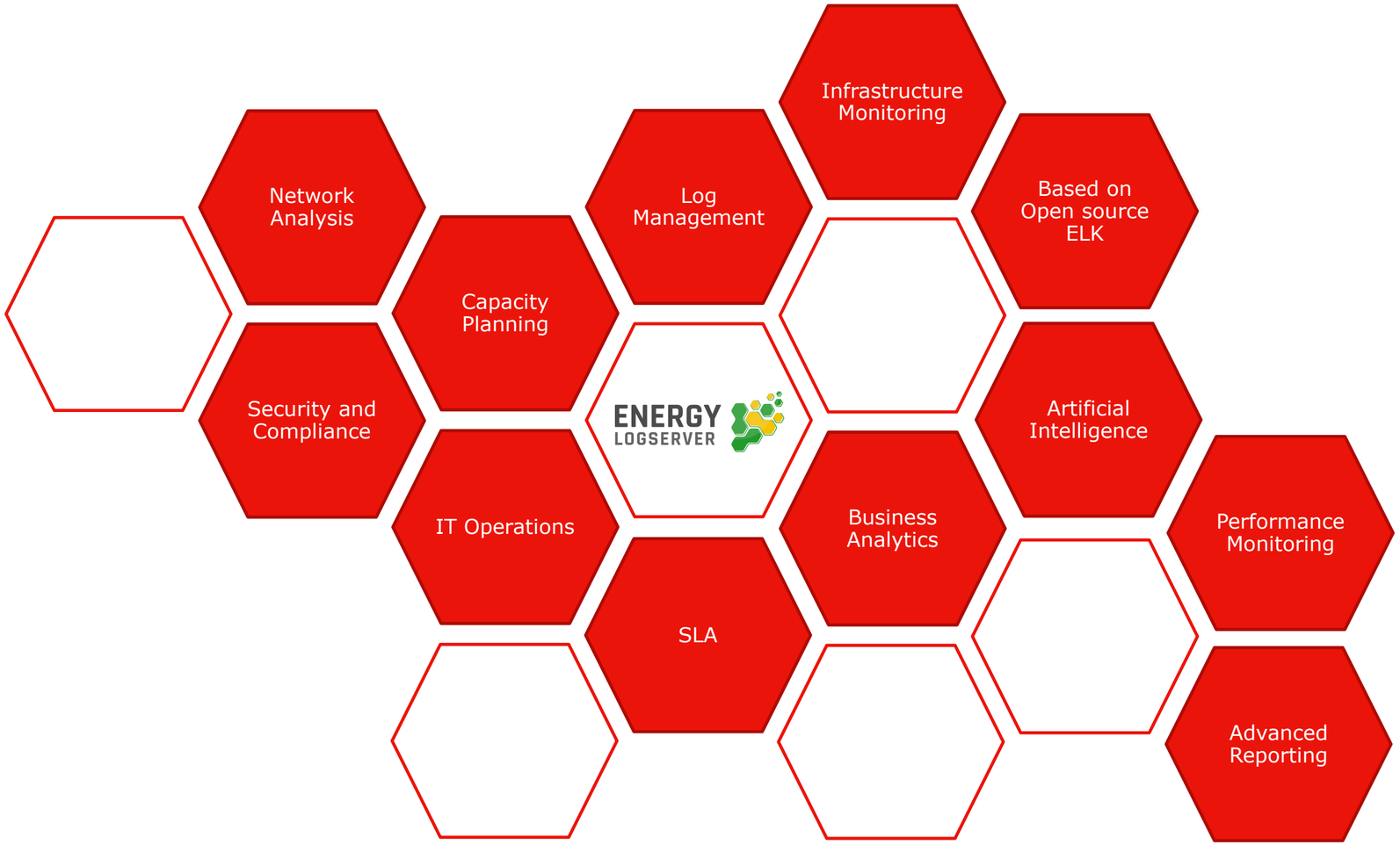
Obvladovanje groženj

ENERGY LOGSERVER

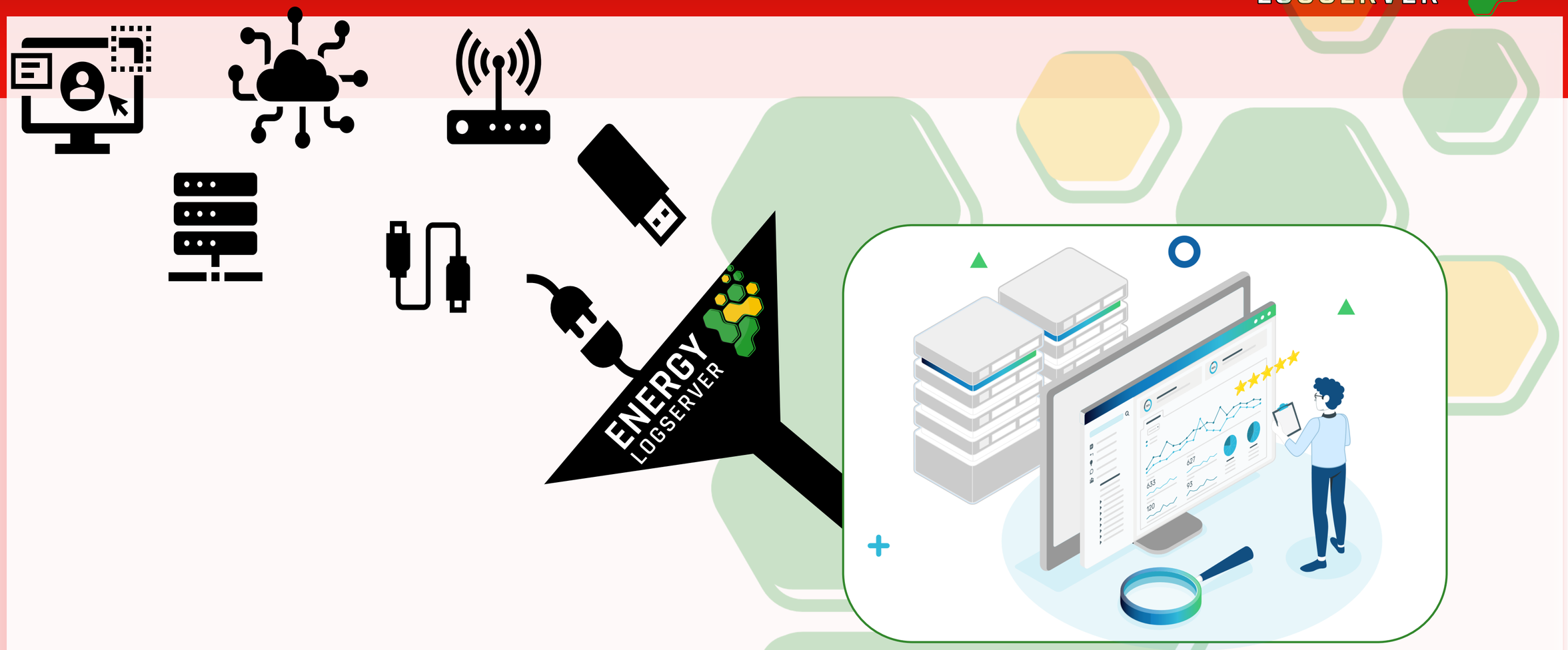


A1 ICT Distribucija

Zakaj Energy LogServer?



Zakaj Energy LogServer?

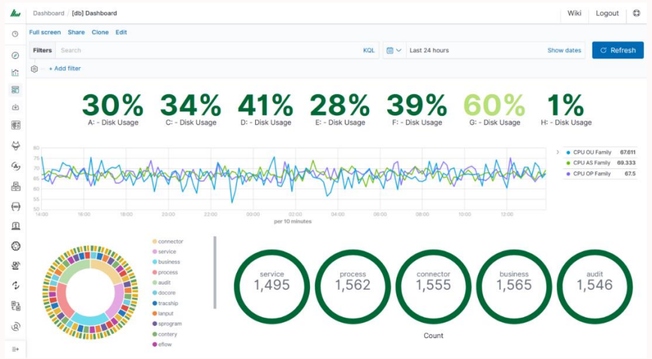


Zakaj Energy LogServer?

IT DATA INPUT

ANY TEXT DATA

- Windows Events
- Application
- Log files
- Syslog
- Exec scripts
- HTTP/JSON/API
- JDBC
- Kafka
- JMX
- Log4j
- SNMPTrap
- TCP/UDP raw



FLEKSIBILNOST

IOT PROTOCOLS

- AB-ETH
- ADS/AMS
- BACnet/IP
- CANopen
- DeltaV
- DF1
- Ethernet/IP
- Firmata
- KNXnet/IP
- Modbus
- OPC UA
- S7
- Simulated

IoT

Zakaj Energy LogServer?

- Energy LogServer **SIEM LITE**

ENERGY LOGSERVER

Thank you

A1 ICT Distribucija

E ict-partners@A1.si
M 040 440 373