

A1 Dogodek

**A1**

# **SIEM** ZA VSAKO GAR

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

**A<sup>1</sup> 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 Kašič**  
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

**A1**

# SIEM in Energy LogServer

Maja Milojević in Marko Kašić

**ENERGY  
LOGSERVER**





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

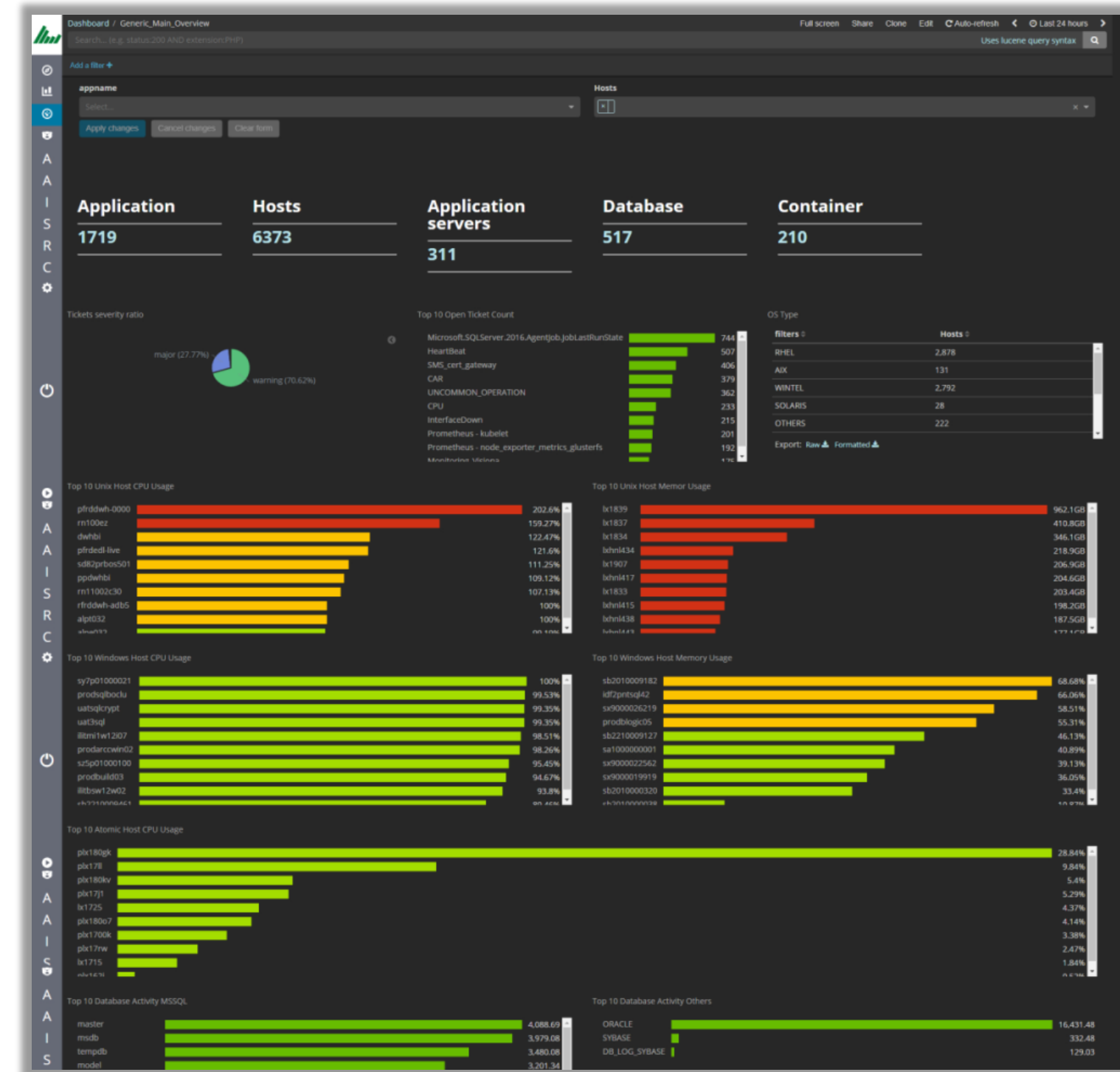
Javni sektor  
Zdravstvo  
Finance in  
zavarovalništvo  
Kritična infrastruktura



# SLA

Višji nivo poročanja  
za managerje  
Osrednji pogled v  
SLA statuse

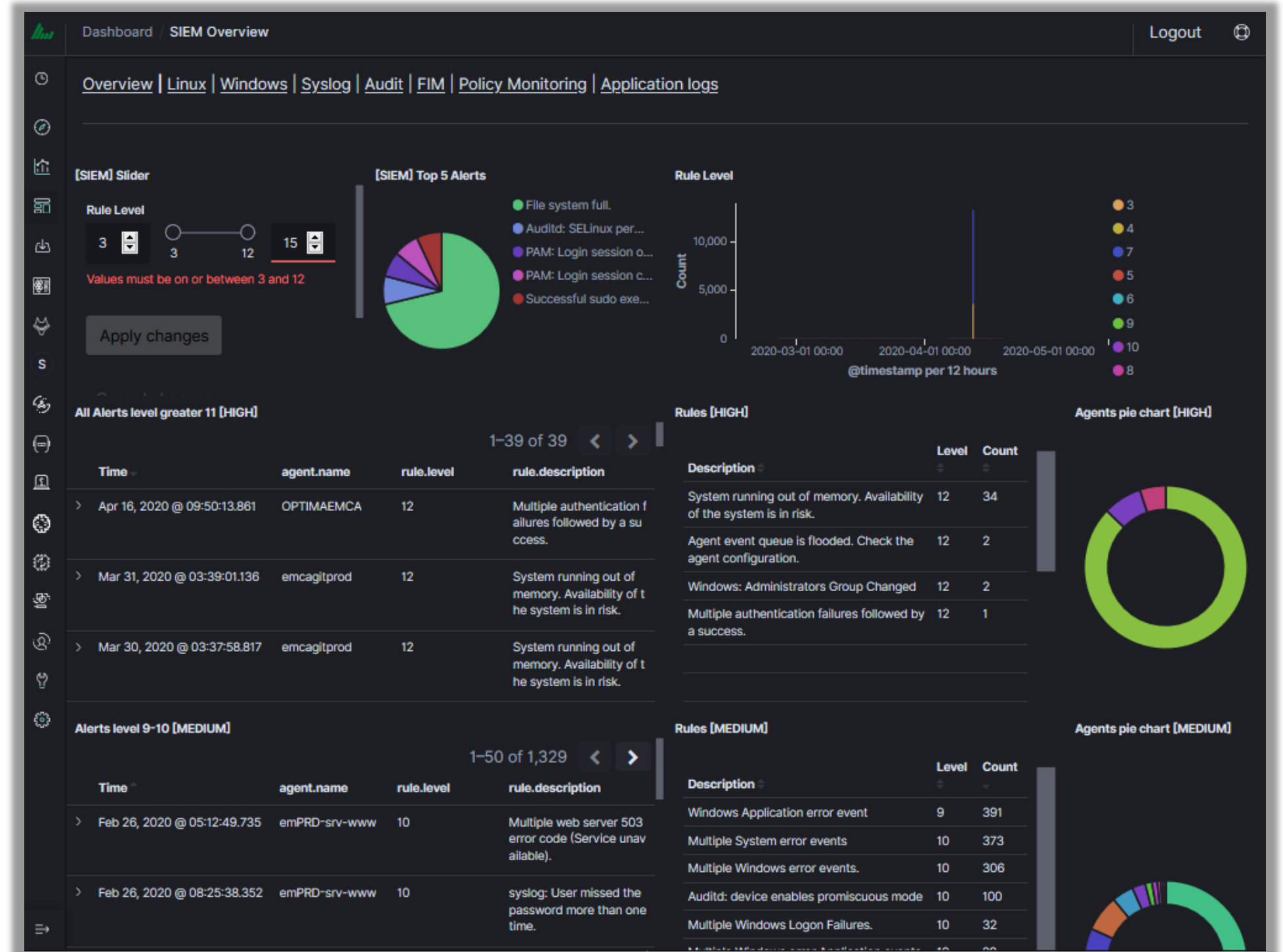
SME segment  
Finance in  
zavarovalništvo  
Kritična  
infrastruktura



# SECURITY

Zaznavanje groženj  
 Kategorizacija dogodkov  
 Prioritizacija  
 SOC dashboard  
 Alarmi v realnem času

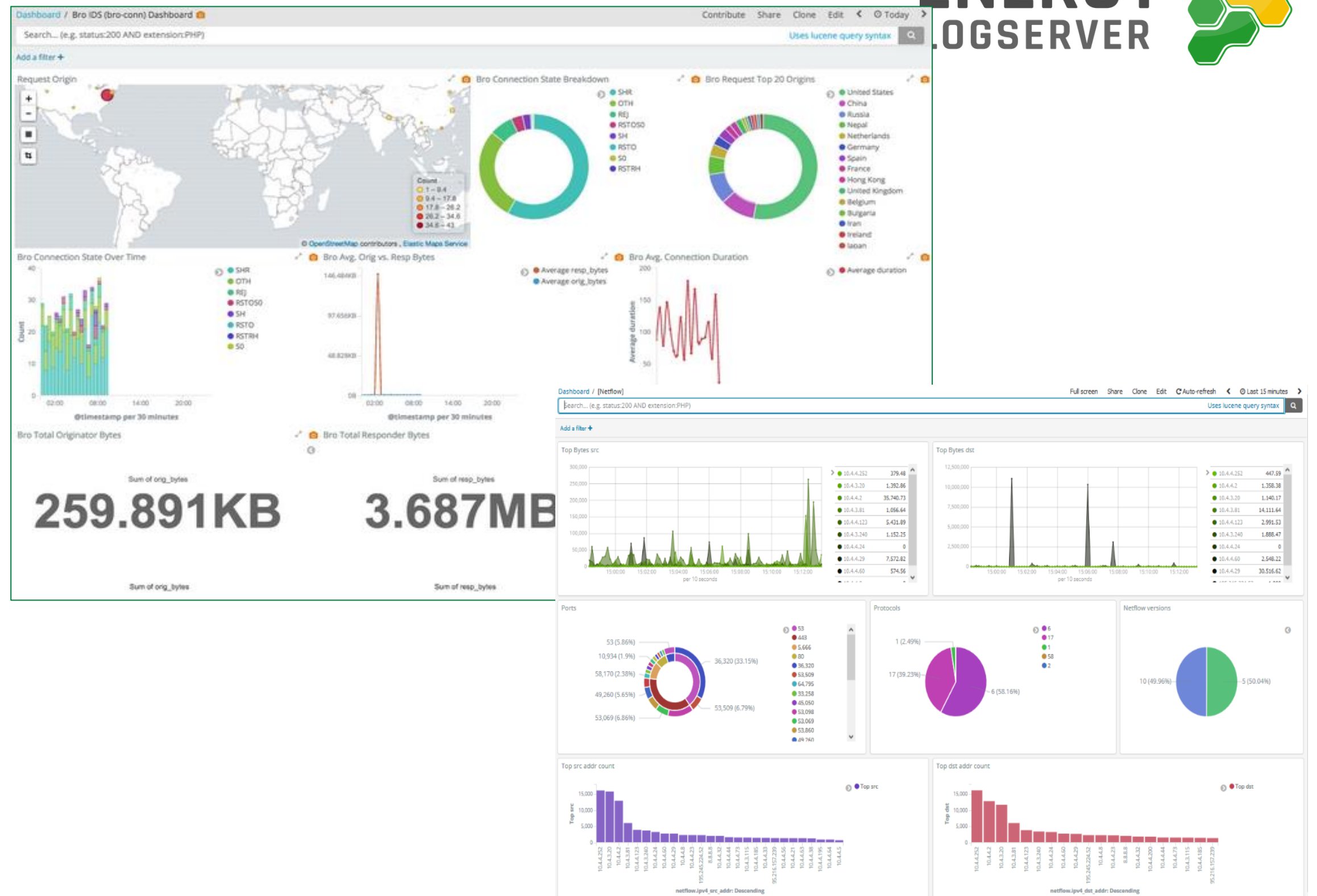
Zavezanci k regulaciji  
 Finance, zavarovalništvo  
 Kritična infrastruktura  
 Dobra praksa za SME  
 segment



# OMREŽNI PROMET

Zaznavanje prometa  
Verifikacija protokolov  
Celovit vpogled v  
dogodke na omrežju

Zavezanci k regulaciji  
Finance, zavarovalništvo  
Telekomunikacije  
Kritična infrastruktura  
SME segment



**A1**

# SIEM

**ENERGY  
LOGSERVER**



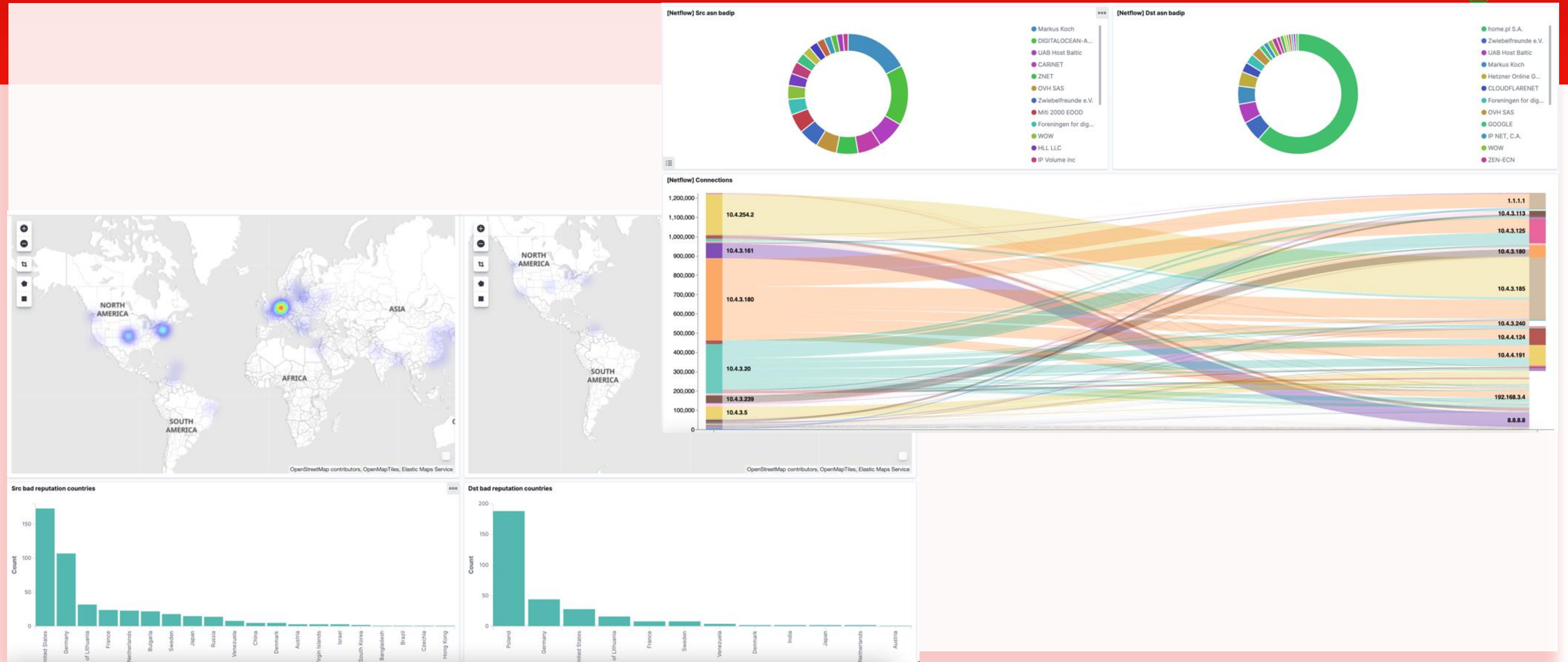
# Upravljanje dnevnikov in poročanje



**VSI  
TEKSTOVNI  
PODATKI**



# Spremljanje v realnem času



# Nadzorna plošča



Dashboard / MITRE - DASHBOARD Wiki Cluster Logout

Navigation panel

[Overview](#) | [Linux](#) | [Windows](#) | [Vulnerabilities](#) | [Syslog](#) | [Audit](#) | [FIM](#) | [Policy Monitoring](#) | [Alert](#) | [Mitre](#)

MITRE-VIS\_CONTROL

TECHNIQUE: Select... TACTIC: Select... Rule level: 3 to 15 HOST: Select...

Apply changes Cancel changes Clear form

TOP 30 TACTIC

Tactic	Percentage
Privilege Escalation	61.1%
Defense Evasion	10.99%
Initial Access	10.99%
Persistence	10.99%
Impact	5.49%

TOP 30 TECHNIQUE

Technique	Percentage
T1169	75.41%
T1078	16.39%
T1492	8.2%

Legend: Privilege Escalation, Defense Evasion, Initial Access, Persistence, Impact

Legend: T1169, T1078, T1492

Legend: Sudo (50.55%), Valid Accounts (10.99%), Stored Data Manipul... (10.99%), Manipulations (5.49%), lid Accounts (10.99%), lid Accounts (10.99%), lid Accounts (10.99%), lid Accounts (10.99%)

# Upravljanje z incidenti



Dashboard / SIEM Overview Logout

Overview | Linux | Windows | Syslog | Audit | FIM | Policy Monitoring | Application logs

**[SIEM] Slider**

Rule Level

3 3 12 15

Values must be on or between 3 and 12

Apply changes

**[SIEM] Top 5 Alerts**

- File system full.
- Auditd: SELinux per...
- PAM: Login session o...
- PAM: Login session c...
- Successful sudo exe...

**Rule Level**

**All Alerts level greater 11 [HIGH]**

1-39 of 39

Time	agent.name	rule.level	rule.description
> Apr 16, 2020 @ 09:50:13.861	OPTIMAEMCA	12	Multiple authentication failures followed by a success.
> Mar 31, 2020 @ 03:39:01.136	emcagltprod	12	System running out of memory. Availability of the system is in risk.
> Mar 30, 2020 @ 03:37:58.817	emcagltprod	12	System running out of memory. Availability of the system is in risk.

**Rules [HIGH]**

Description	Level	Count
System running out of memory. Availability of the system is in risk.	12	34
Agent event queue is flooded. Check the agent configuration.	12	2
Windows: Administrators Group Changed	12	2
Multiple authentication failures followed by a success.	12	1

**Alerts level 9-10 [MEDIUM]**

1-50 of 1,329

Time	agent.name	rule.level	rule.description
> Feb 26, 2020 @ 05:12:49.735	emPRD-srv-www	10	Multiple web server 503 error code (Service unavailable).
> Feb 26, 2020 @ 08:25:38.352	emPRD-srv-www	10	syslog: User missed the password more than one time.

**Rules [MEDIUM]**

Description	Level	Count
Windows Application error event	9	391
Multiple System error events	10	373
Multiple Windows error events.	10	306
Auditd: device enables promiscuous mode	10	100
Multiple Windows Logon Failures.	10	32

# Spremljanje podatkov/uporabnikov/aplikacij



Dashboard / Windows
Wiki Cluster Logout

### Windows - Top 10 events

Event Description	Percentage
Windows Logon Success	40%
The database engine stopped an instance	13.33%
The database engine is starting a new instance	13.33%
The database engine detached a database	13.33%
The database engine attached a database	13.33%
Windows Application error event	6.67%

### Windows - Last Alerts by Importance

1-15 of 15 < >

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

ENERGY  
LOGSERVER



A1



# SIEM ali MSSP?



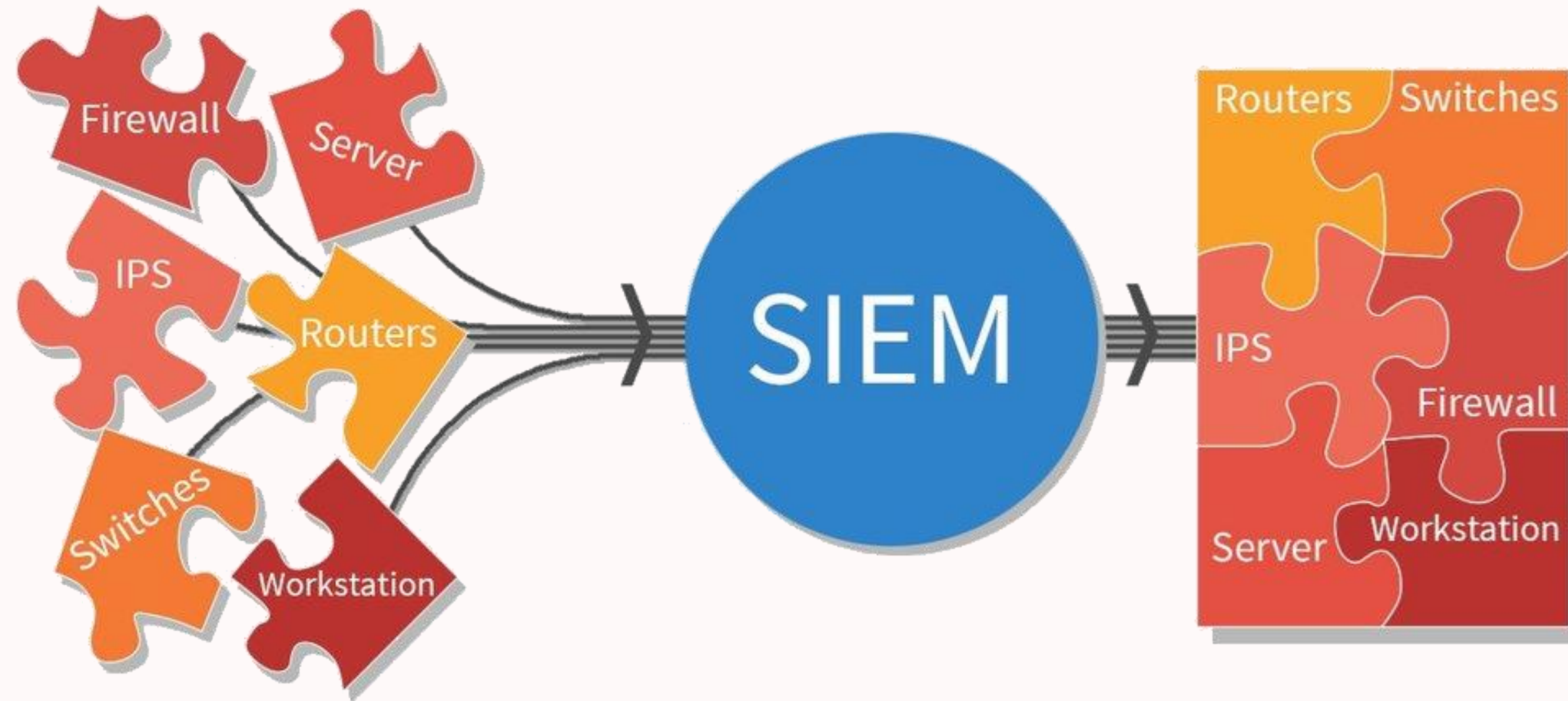
Zakaj  
SIEM?

ENERGY  
LOGSERVER



A1

# Zakaj SIEM?



# Skladnost



# Obvladovanje groženj



Dashboard / SIEM Overview Logout

Overview | Linux | Windows | Syslog | Audit | FIM | Policy Monitoring | Application logs

**[SIEM] Slider**

Rule Level

3 3 12 15

Values must be on or between 3 and 12

Apply changes

**[SIEM] Top 5 Alerts**

- File system full.
- Auditd: SELinux per...
- PAM: Login session o...
- PAM: Login session c...
- Successful sudo exe...

**Rule Level**

**All Alerts level greater 11 [HIGH]**

1-39 of 39

Time	agent.name	rule.level	rule.description
> Apr 16, 2020 @ 09:50:13.861	OPTIMAEMCA	12	Multiple authentication failures followed by a success.
> Mar 31, 2020 @ 03:39:01.136	emcagltprod	12	System running out of memory. Availability of the system is in risk.
> Mar 30, 2020 @ 03:37:58.817	emcagltprod	12	System running out of memory. Availability of the system is in risk.

**Rules [HIGH]**

Description	Level	Count
System running out of memory. Availability of the system is in risk.	12	34
Agent event queue is flooded. Check the agent configuration.	12	2
Windows: Administrators Group Changed	12	2
Multiple authentication failures followed by a success.	12	1

**Agents pie chart [HIGH]**

**Alerts level 9-10 [MEDIUM]**

1-50 of 1,329

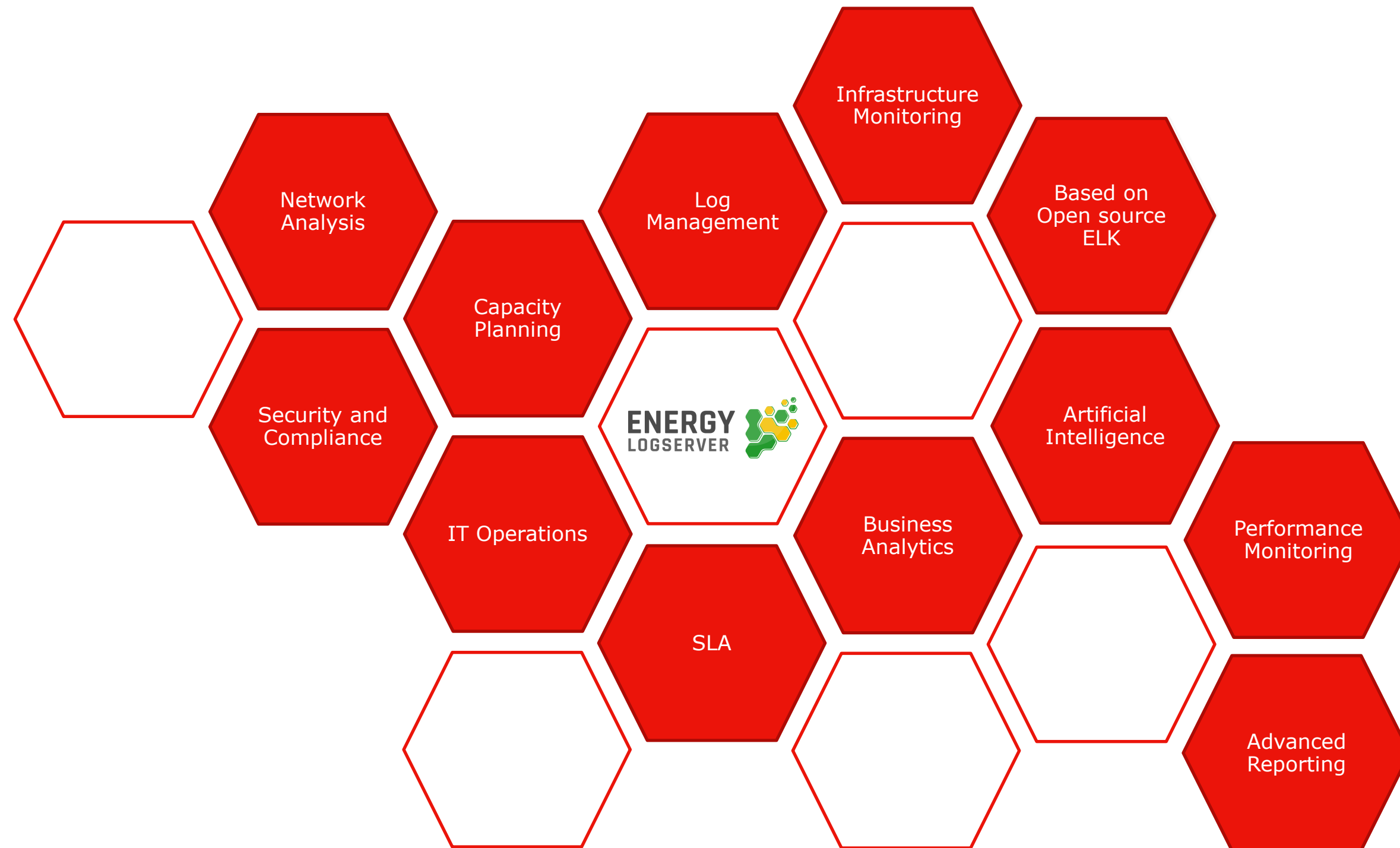
Time	agent.name	rule.level	rule.description
> Feb 26, 2020 @ 05:12:49.735	emPRD-srv-www	10	Multiple web server 503 error code (Service unavailable).
> Feb 26, 2020 @ 08:25:38.352	emPRD-srv-www	10	syslog: User missed the password more than one time.

**Rules [MEDIUM]**

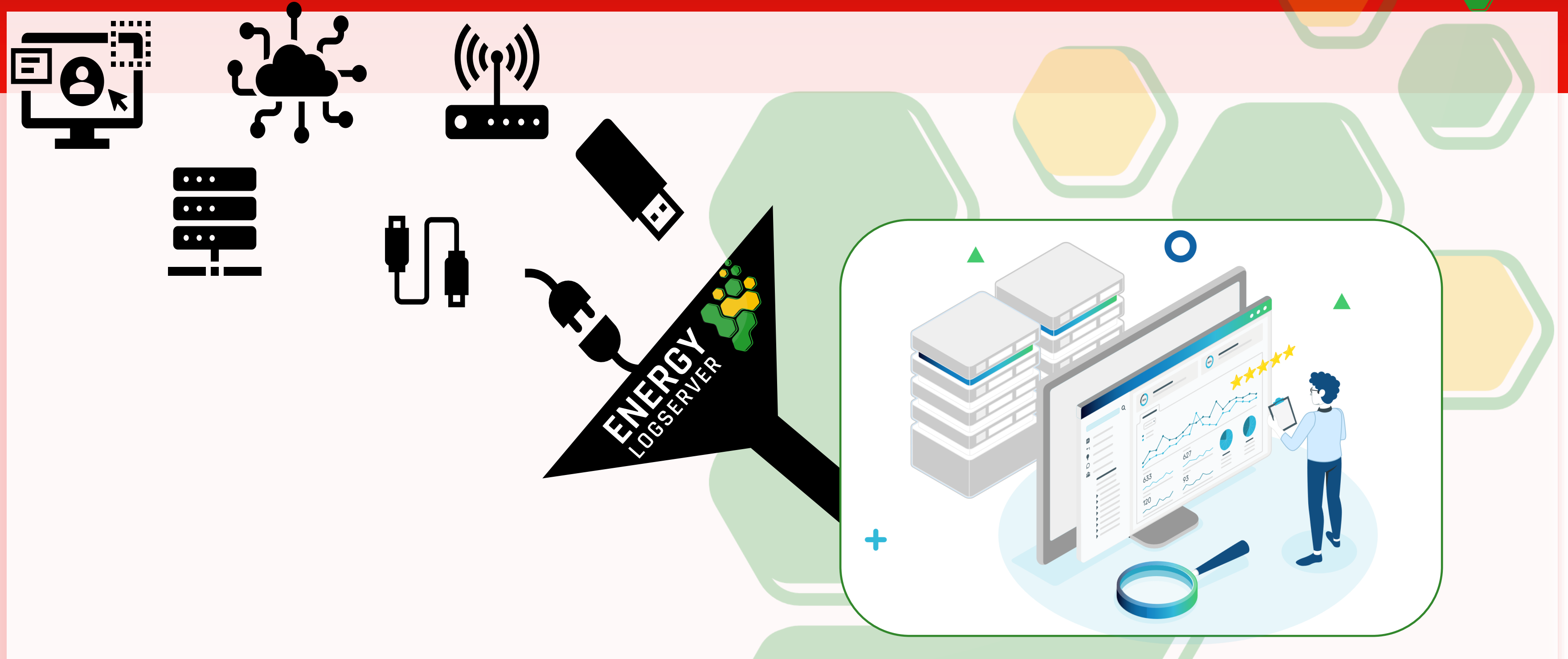
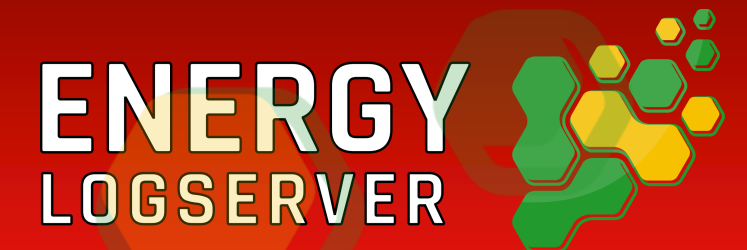
Description	Level	Count
Windows Application error event	9	391
Multiple System error events	10	373
Multiple Windows error events.	10	306
Auditd: device enables promiscuous mode	10	100
Multiple Windows Logon Failures.	10	32

**Agents pie chart [MEDIUM]**

# Zakaj Energy LogServer?



# Zakaj Energy LogServer?



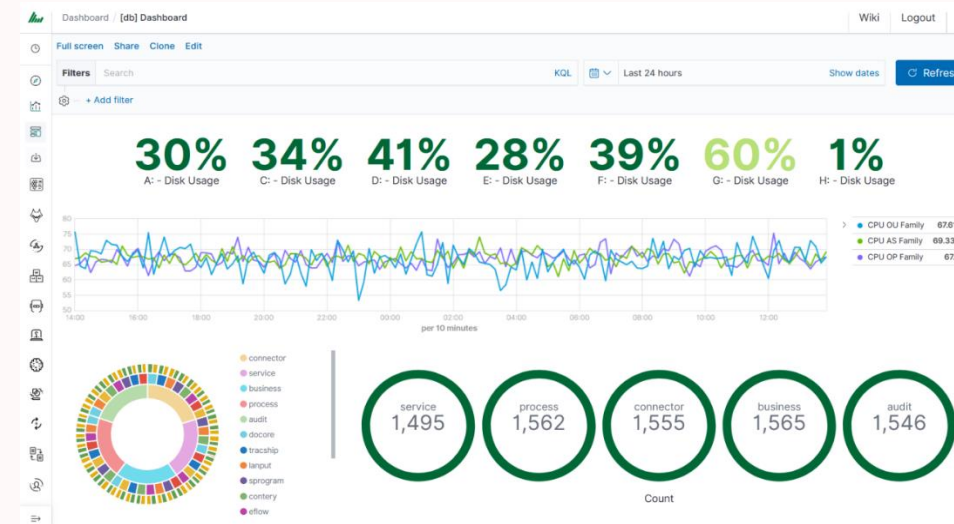
# Zakaj Energy LogServer?



## 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

**IoT**

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

# Zakaj Energy LogServer?



- Energy LogServer **SIEM LITE**



**A1**

**ENERGY  
LOGSERVER**



**Thank  
you**

A1 ICT Distribucija

E [ict-partners@A1.si](mailto:ict-partners@A1.si)  
M 040 440 373