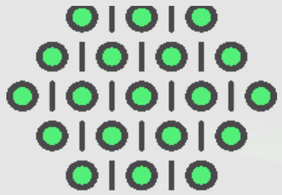
ENERGY LOGSERVER

SIEM PLAN

BY THE POWER OF
YOUR DATA

ENERGY PORTFOLIO

ENERGY LOGSERVER



LOG MANAGEMENT

- Event centralization
- Document collection
- Data Analysis
- Malfunction diagnosing
- Troubleshooting
- Reporting

SIEM

- Alerting
- Security analytics
- Incident management
- Vulnerability detection
- File integrity monitoring
-Compliance regulations
- Advanced data visualization
- Playbook

NETWORK PROBE

- Detect suspicious behaviors
- Recognize zero-day attacks
- Identify the source of the problem
- Visualization
- Categorizations

ENERGY SOAR

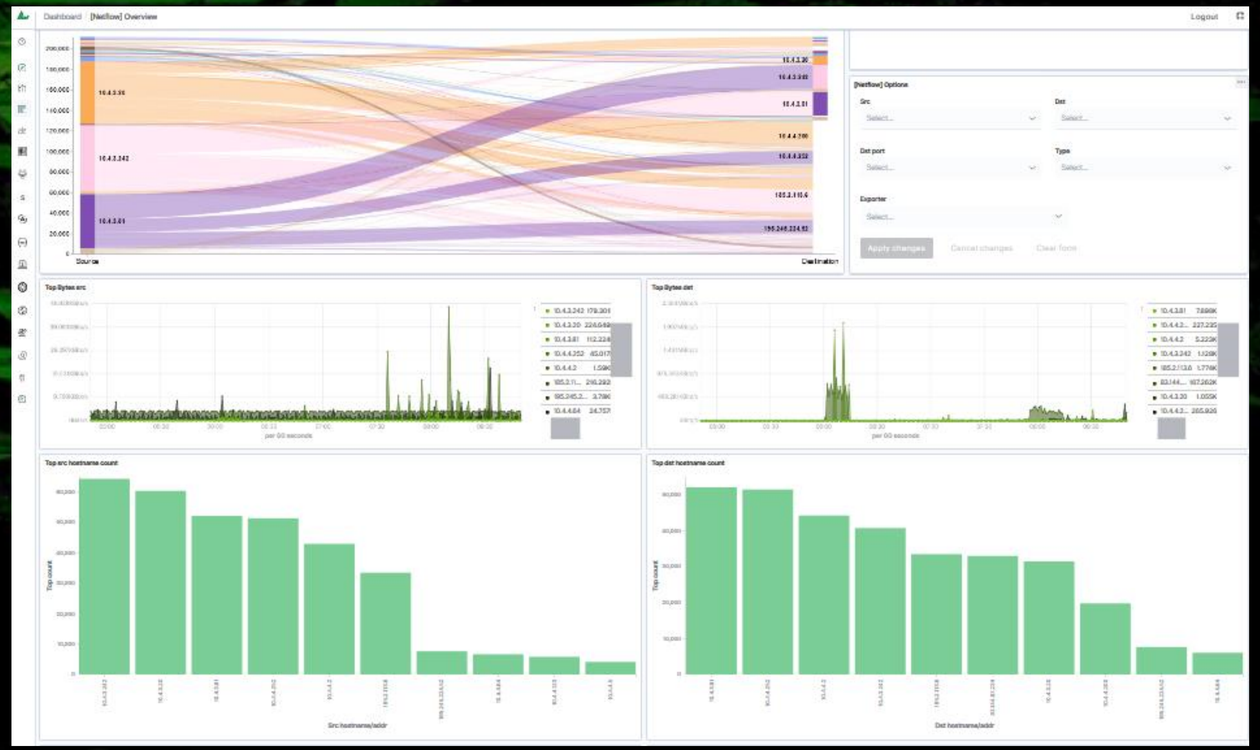
SOAR

- Automation
- Manage Incidents
- Active response
- Easy integration
- Playbooks
- MISP connected (Threat Intelligence Platform)

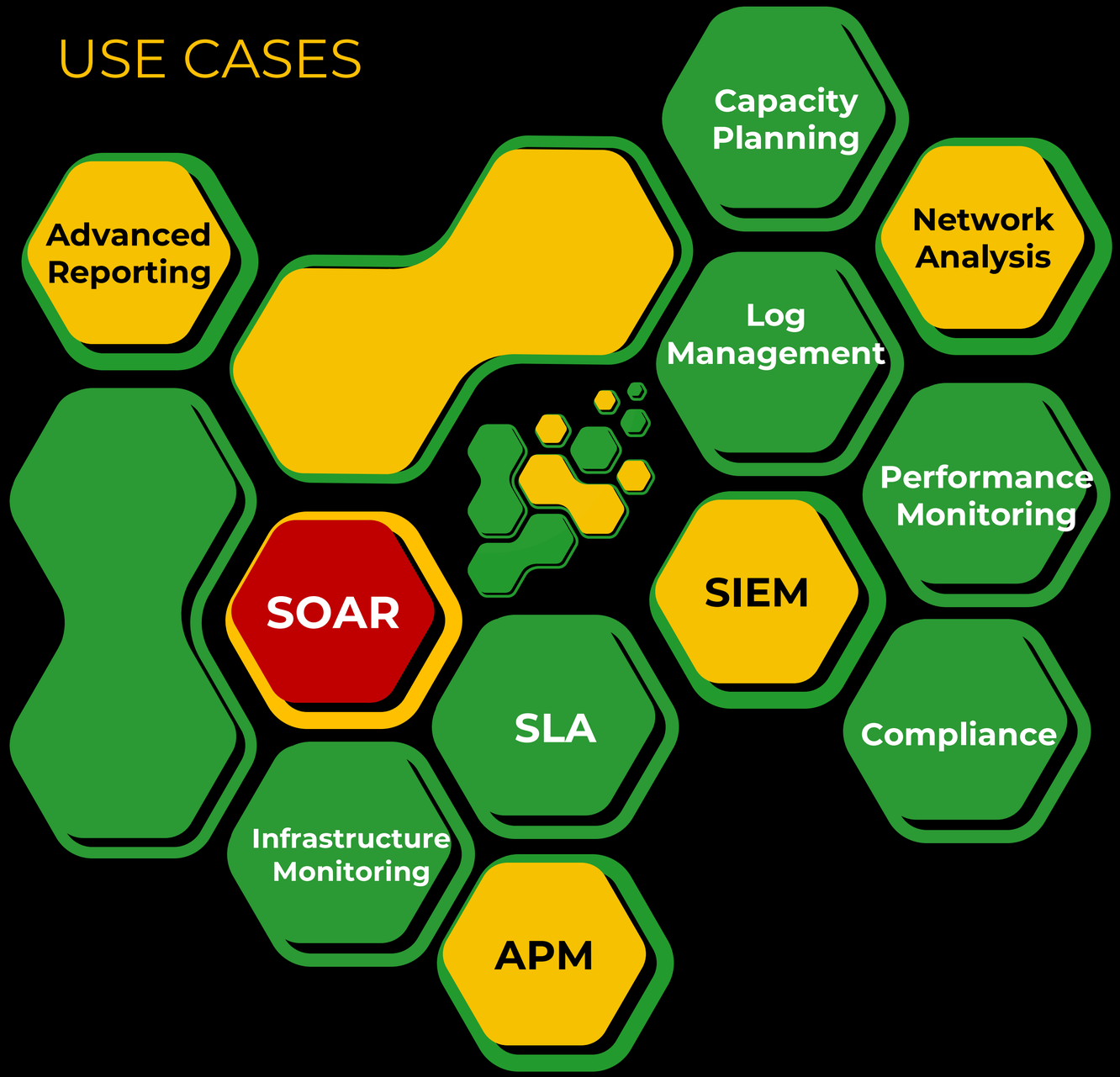
IT DATA INPUT

ANY TEXT DATA

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



USE CASES



ENERGY LOGSERVER

- Powerful Log Management
- Innovative SIEM
- Network Analysis
- Infrastructure monitoring
- Application performance monitoring
- METRIC Server
- TRENDS forecast machine
- AWS/Azure inventory and billing
- Long term Data Archiving
- Compliance

LOG MANAGEMENT PLAN

- User management with precise permissions system
- Integration with LDAP, AD, Radius, SSO
- Scalable architecture
- Predefined parser for dozens of sources
- Fast search engine
- Reporting
- Archive management
- Internal audit
- Build-in dashboards

SIEM PLAN

- Alerting module with more than 700 detection rules
- Risk Management
- Incident Management
- Detect security incidents and suspicious behaviour from logs
- Alerting Rules scan data every minute
- IOC integrations
- Bad IP, URL database, TOR sites
- MISP Integration
- MITRE ATT&CK
- Compliance: GDPR, NIST, CIS, PCI DSS, HIPAA etc.
- File Integrity Monitoring
- Vulnerability Scanner
- Endpoint Detection & Response
- Suspicious logins, multiple logins

NETWORK PROBE

- Probe for network traffic analysis
- High performance data collection up to 10 Gbps
- More than 100 000 Flows per second
- Netflow analysis (v5, v9, IPFIX, sflow
- Network Traffic Analysis on layers L2-L7
- Correlation of network data with Logs
- Network bad IP Reputation
- IoC bases integration: IP adresses, malware file hashs, domains, URL
- Zero-day attack identification
- Behavioral analysis of network user activity in network
- Application performance & errors monitoring
- SRT, RTT, Delay, Jitter, Retransmission monitoring