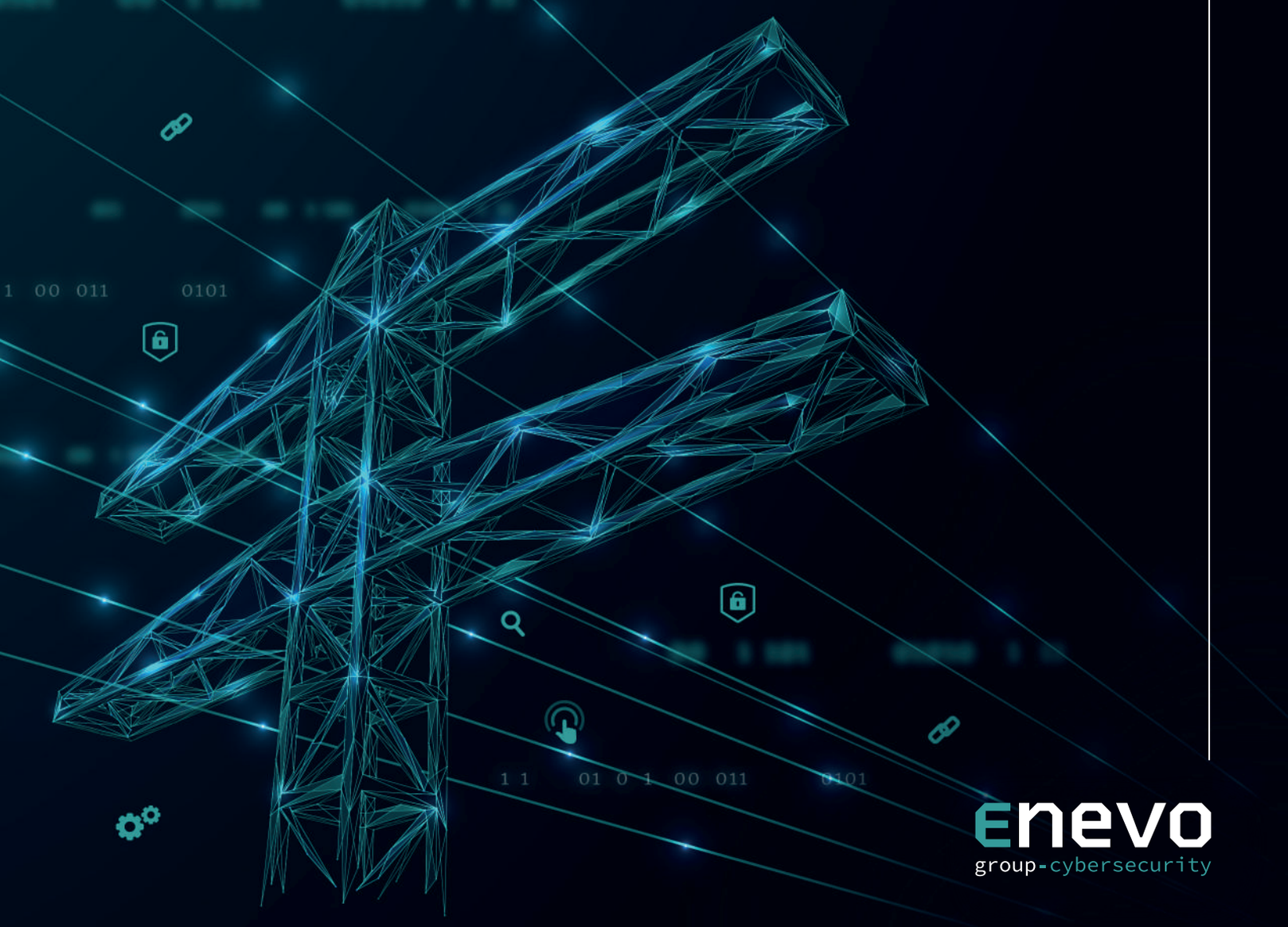
www.enevocyber.com

subSIEM

Substation Security Event Management Solution



Enevo
group-cybersecurity

subSIEM

The complexity of modern cyber-attacks on industrial infrastructure requires an integrated approach to securing our Electrical Grid. subSIEM allows you to locally collect all the information needed by an Incident Response Team, while building an up-to-date asset inventory and an accurate topology of your Substation Network.

We believe this increased visibility is useful not only for providing real-time alerts on malicious activity inside your network, but by integrating subSIEM with your local control systems, it will provide timely information to process operators to maneuver the process in a more defensive position, reducing potential impact.

BENEFITS AND CONSIDERATIONS FOR USING subSIEM

Strengthen Security Posture

Provides a comprehensive and centralized view of the security posture within the infrastructure.

Asset inventory

Build an up-to-date asset inventory together with a data-flow diagram.

Increased visibility

Centralized system to collect and aggregate log data from the entire infrastructure, identifies, categorized, and analyze incidents and events (past events included).

Facilitates incident response

Reduce downtime and speed up recovery.

Helps prioritize hardening activities

Industrial equipment's & networking firmware patching, servers & workstations updates.

Regulatory and compliance requirements

Tracks compliance according to Industry Security controls.

subSIEM ARCHITECTURE

subSIEM

Integrations

SCADA application (local or central) via IEC-104 protocol for main security alerts Third Party Applications or other SOCs via syslog or custom API

SubSOC

SubSIEM

DISPATCH LEVEL

HISTORIAN SERVER | SCADA SERVER | APPLICATIONS SERVER | DISPATCH HMI's | ENG WS's

DISPATCH NETWORK

FIREWALL

SubSIEM

SUBSTATION LEVEL

HISTORIAN SERVER | SCADA SERVER | SCADA HMI | ENG WS's | RTU

SUBSTATION NETWORK

PROTECTION RELAYS

SubSIEM
Substation Cyber Security Enabler

- Substation Security Posture Dashboard
- Local SIEM
- Security Events mapped to MITRE ICS framework
- Black-box for Security Events and Network Traffic (over 1 year)
- Substation Asset Inventory (hardware and software)
- Detecs configuration / firmware changes for protection relays
- Builds Network Topology and Network Flows
- Forwards Network Traffic to SubSOC for detailed analysis

Collects all Substation and Central Dispatch Centre Security Relevant Information

- Network device logs from firewall, routers and switches
- OS logs from workstations (Engineering, Operator) and servers (SCADA/DCS, Historian, Domain Controller)
- Application logs from SCADA/DCS
- Engineering Specific Applications Logs
- Deep packet inspection on IEC61850, IEC104, DNP and Modbus protocols
- Industrial Device logs
- Tailored Extraction of Security Events (using Industrial Control Protocols)
- Antivirus / EDR alerts

subSIEM OVERVIEW

Security teams must address the expansion of the attack surface from industrial networks caused by remote workforces and interconnection of OT industrial network with IT network. The challenges that subSIEM solves are:

1. Industrial visibility: effective security measures are viable only after we know what needs to be protected. We collect logging from: network devices (firewalls, routers and switches), OS logs (workstations: Engineering, Operator, and servers: SCADA/DCS, Historian, Domain Controller) and application logs (SCADA/DCS, Engineering Specific Application logs). We offer custom traffic scanning capabilities, protocols identification, parsing, enrichment, reporting, threat-hunting, customized point-in-time traffic analysis and traffic graph capabilities that allows OT security teams to have a centralized inventory of all assets and processes.

2. Deep packet inspection on Industrial Protocols: We collect and translate industrial protocols traffic flows (ex: IEC 61850, IEC 104, MODBUS, DNP3) in readable format that allows security teams to have comprehensive industrial visibility and control, understand processes and connections.

3. Operation tracking: identify and alert abnormal industrial operations applied to assets within the inventory. Detect configuration and firmware updated for protection relays. Code commands inventory for the industrial assets will be updated after firmware updates and process control review.

4. Incident and threat detection: once the visibility and asset management are in place we understand the profiles of all assets, communication flows and processes within the network and we can identify, categorized and alert incidents or abnormal events to security teams in real-time. False positives events can be customized to better filter and tune the events capabilities, alerts are prioritized based on criticality to allow security teams to respond more effectively and efficiently.

5. Root Cause analysis: events from multiple assets can be corelated into a dashboard that is design to allow a centralized view of a chain of events that is design to improve reaction time, mitigation and isolation of assets.

6. Incident management: enables security teams in real-time to detect, investigate, and respond to industrial cybersecurity incidents. The capabilities that are offered by our solution allow us to improve the current security posture for a highly secure environment that will provide visibility of: unauthorized or abnormal activities (asset access and configuration), user access (monitor live sessions), mapping of security events to Mitre ICS framework.

7. Seamless integration with existing OT infrastructure and 3rd party SIEM: the solution that we offer does not cause any operational disruption or traffic flow rerouting. The integration and monitoring of 3rd party SIEM solutions, combined with the direct monitoring via typical SCADA solutions using IEC-104 protocol makes subSIEM a highly customized and easy to integrate solution.

HARDWARE DETAILS

subSIEM is based on hardware designed for use in electrical substations: a Power Automation Server TUV certified according to IEC 61850-3 and IEEE 1613, that provides high reliability and stability for Centralized Substation Protection and Control Systems in HV/MV Substations.

TUV
IEC 61850-3
CERTIFIED

TUV
IEEE 1613
CERTIFIED

HARDWARE DETAILS

GENERAL

Certification:
CE,
FCC,
IEC-61850-3,
IEEE-1613

Power Requirements:
Redundant Power Supply,
800W 100-240VAC/DC

Dimensions (W x D x H):
440 x 460 x 88 mm

Enclosure:
SECC and aluminium

Weight:
10.0 Kg

Mounting:
2U Rackmount

Cooling:
4 x hot swap high speed fan

SYSTEM HARDWARE

CPU:
Compatible with Intel® Xeon® Processor Scalable Family

Chipset:
Intel® C621 chipset

Memory:
Up to 12 x 2400/2666MHz DDR4 ECC Standard ECC RDIMM/LRDIMM Max. capacity per channel: 768GB

Storage:
4 x 2.5" hot-swap SATA HDD (RAID0/1/5/10)
1 x M.2 2280 SATA SSD

Display:
1 x VGA, 2 x DVI-D (Resolution: 2K/60p)

Watchdog Timer:
Programmable 256 levels time interval, from 1 to 255 seconds for each tier

System Management:
IPMI Aspeed AST2500 BMC

COMMUNICATION

LAN:
4 x 10/100/1000 Base-T RJ45 ports
(expandable with 4 x FO SFP)

USB:
3 x USB 3.0

Expansion:
2 x standard PCIe x16 Slot Gen3 low profile
1 x standard PCIe x8 Slot Gen3 low profile
1 x standard PCIe x4 Slot Gen3 low profile
1 x Mini PCIe
1 x PCIe + PCI interface for ECUP card extension

ENVIRONMENT

Operating Temperature:
-20 ~ up to 60 °C

Operating Humidity:
5 ~ 95% RH (non-condensing)

Storage Humidity:
5 ~ 95% RH (non-condensing)

DEVELOPMENT

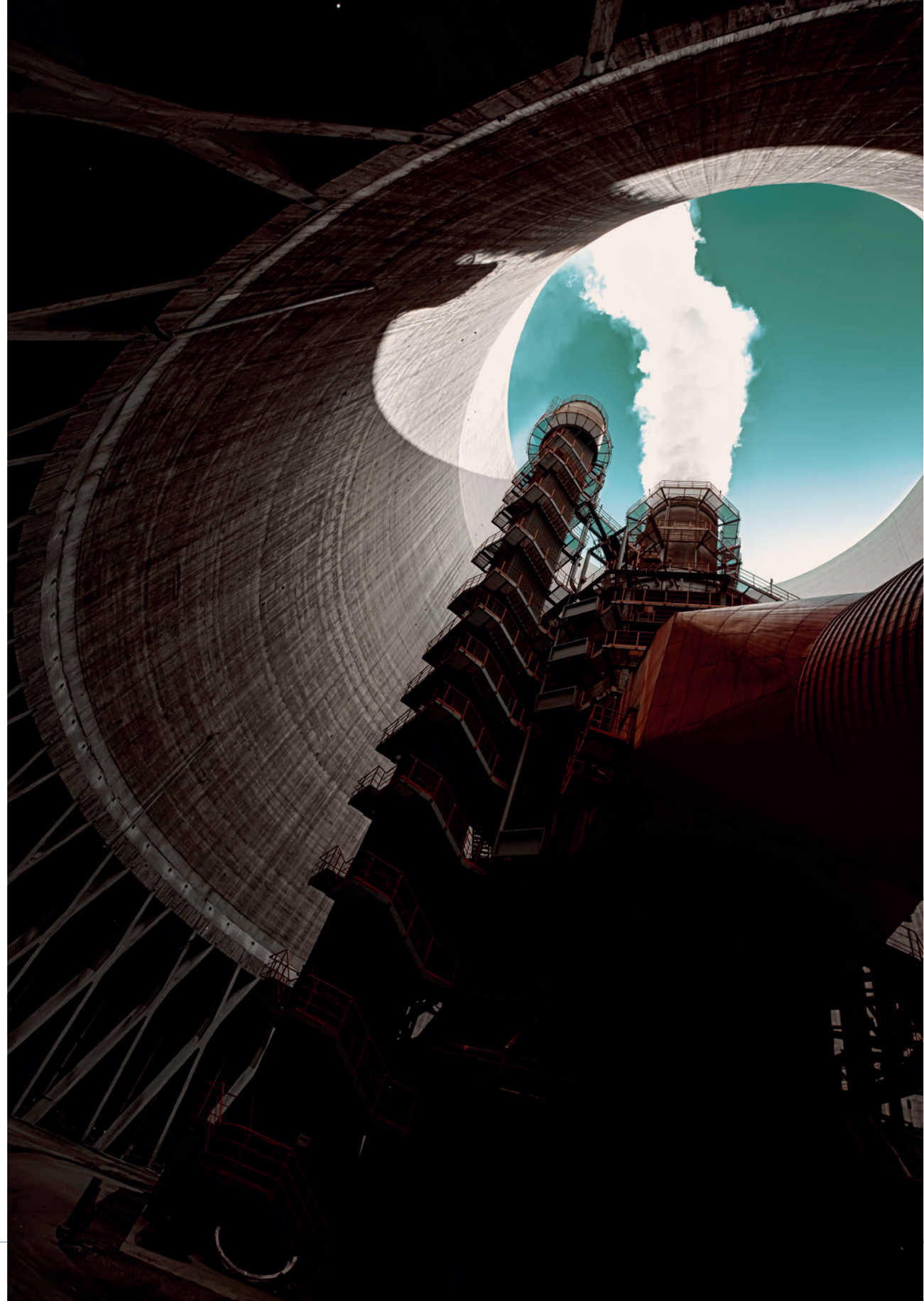
subSIEM was performed by an interdisciplinary team of Cyber Security experts, Automations engineers, IT specialists, DevOps, Read Team and Blue Team, with extensive experience in Industrial Environments.

The team has battle proven background in:

- **Infrastructure assessments:** Evaluate the security of a system by performing penetration testing (black box and gray box scenarios). Test the security measures already installed;
- **Technical audits:** Build asset inventory, network diagram/data flow diagram, compromised assessments;
- **Process Consolidation:** Prepare a hardening plan based on the assessments results;
- **Operation control hardening:** Process mapping and recheck after firmware upgrades;
- **Digitalization initiative:** the new era of convergence of both IT/OT networks demands for new measures of protection against external threats, we rely on our experience to provide technical solutions for both sides of IT/OT networks from network segmentation, infrastructure visibility and management to equipment replacement and process review;
- **Awareness & Training:** On- and Off-site knowledge exchange programs, OT testing infrastructure, staff augmentation.

subSIEM

Substation Security Event Management Solution



enevo
group-cybersecurity

ROMANIA

BUCHAREST

Address:
AFI Lakeview - Barbu Vacarescu Street, nr. 301-311, 11th Floor, 020276, Bucharest, Romania

Phone: +40 371 017 242
Fax: +40 372 258 353
Email: office@enevogroup.com

SIBIU

Address:
Automecanica Industrial Park, Aurel Vlaicu Street nr. 41, Medias, 551041, Sibiu, Romania

Phone: +40 371 017 242
Fax: +40 372 258 353
Email: office@enevogroup.com

GERMANY

MÜNCHEN

Address:
15 Dingolfinger Straße, 81673, München, Germany

Phone: +40 371 017 242
Fax: +40 372 258 353
Email: office@enevogroup.com

KINGDOM OF SAUDI ARABIA

AL KHOBAR

Address:
Eastern Cement Tower, King Fahad Road, 7th Floor, Al Khobar, 34227, Kingdom of Saudi Arabia

Phone: +966 013 857 1113
Fax: +966 013 857 1113
Email: ksa@enevogroup.com