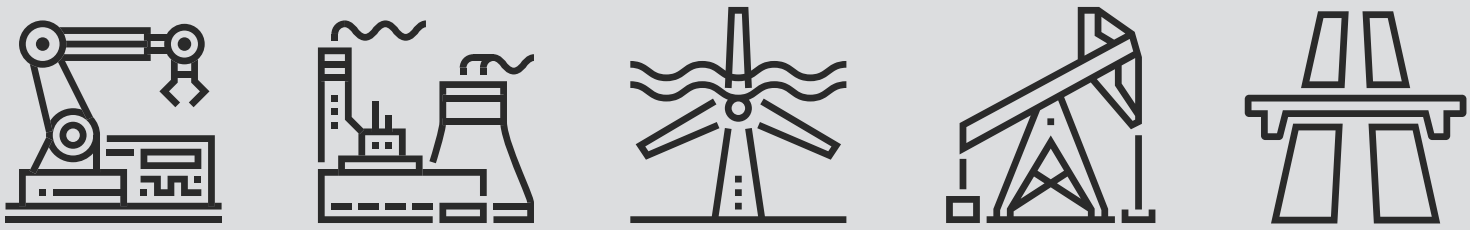

What's Hiding in your SCADA Network?

GREYCORTEX
All-Seeing Network Security

GREYCORTEX MENDEL uses advanced artificial intelligence, machine learning, and data analysis to find risks to your SCADA network safety, reliability, and productivity.

Advanced attacks against industrial control systems are **common**, **dangerous**, and have **serious consequences**. Many existing security tools don't work with these industrial systems, and many SCADA security tools don't detect risks from connected non-SCADA devices.

GREYCORTEX MENDEL identifies risks to your SCADA network, including attacks against the network, but also careless technicians, poor segmentation, etc.

SCADA is an industrial control system architecture that uses computers, networked data communications, etc. found in process plants or machinery.

SCADA Controls:

- Factories
- Electrical generation, transmission, and distribution
- Oil and gas refining/pipelines
- Airports, shipping, space stations

GREYCORTEX MENDEL analyzes the SCADA networks:

- Machine learning anomaly detection on all SCADA protocols
- Signatures for known threats
- Visibility into communications between SCADA devices
- Change discovery visibility
- On layers L3-L7
- Detailed visualization of IEC 60870-5-104, IEEE-1815-2012 DNP3, Modbus, ENIP/CIP

GREYCORTEX is constantly improving its SCADA capabilities. We plan the following additional features:

- IEC 61850 GOOSE, SV, ISO 9506 MMS protocols, and more
- Advanced network behavioral analysis on L2-L7
- Working on substations traffic analysis
- Extending parsing of more protocols related to substations
- Improving visualization down to the end-point level in SCADA networks
- Advanced visualization of app data

GREYCORTEX

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 216, info@greycortex.com, www.greycortex.com