GREYCORTEX MENDEL

Cyber Security Monitoring of ICS and SCADA Networks

The Best Foundation for Securing of ICS and SCADA networks

Deep visibility into ICS and SCADA networks, protocols, commands going to and coming from PLCs, other assets and related vulnerabilities combined with threat detection and policy monitoring are vital for the security of any organization.

Single Solution for IT and OT Monitoring

GREYCORTEX Mendel is a unique solution as it provides cyber security monitoring of OT, IT and IoT networks, on-premise and cloud environments, and combined environments too.

Small Footprint Monitoring of ICS and SCADA Networks

Mendel decreases the complexity of ICS and SCADA network security. It is easy to implement and operate and can even be handled by smaller teams with limited resources or in-depth knowledge and independently of their ICS and SCADA suppliers.

Bringing IT Security and OT Engineers Together

GREYCORTEX Mendel is a single tool that can be used by both IT and OT teams. It empowers IT operations and IT teams to collaborate on making ICS and SCADA networks both more secure and reliable.

More often than not, ICS and SCADA networks are composed of new and legacy devices from different manufacturers and these devices such as PLC's, RTU's, engineering workstations, human machine interfaces, historians and other field devices often lack even the most basic security features. This leaves ICS and SCADA networks vulnerable to both targeted and random cyberattacks. And even if these attacks are not always catastrophic, even the smallest malfunction can negatively impact regular business operations.

GREYCORTEX Mendel's ICS and SCADA module:

- is an **advanced industrial IDS** based on deep packet inspection (DPI) of ICS and SCADA traffic. Using traditional detection techniques as well as advanced artificial intelligence and machine learning, it detects both common and undocumented cyber attacks, behavioral anomalies, vulnerabilities and misconfigurations.
- **decreases the time and resources** necessary to make ICS & SCADA networks more secure and reliable.
- **integrates with common security technologies** like firewalls, gateways and SIEMs, and fills the gaps these technologies leave.
- **operates on Purdue level 3.5**. This enables it to monitor both SCADA/ICS networks and the IT-infrastructure surrounding them, without the possibility of jumping between both environments.

GREYCORTEX focuses on serving the needs of the following industries:

Energy

Utilities

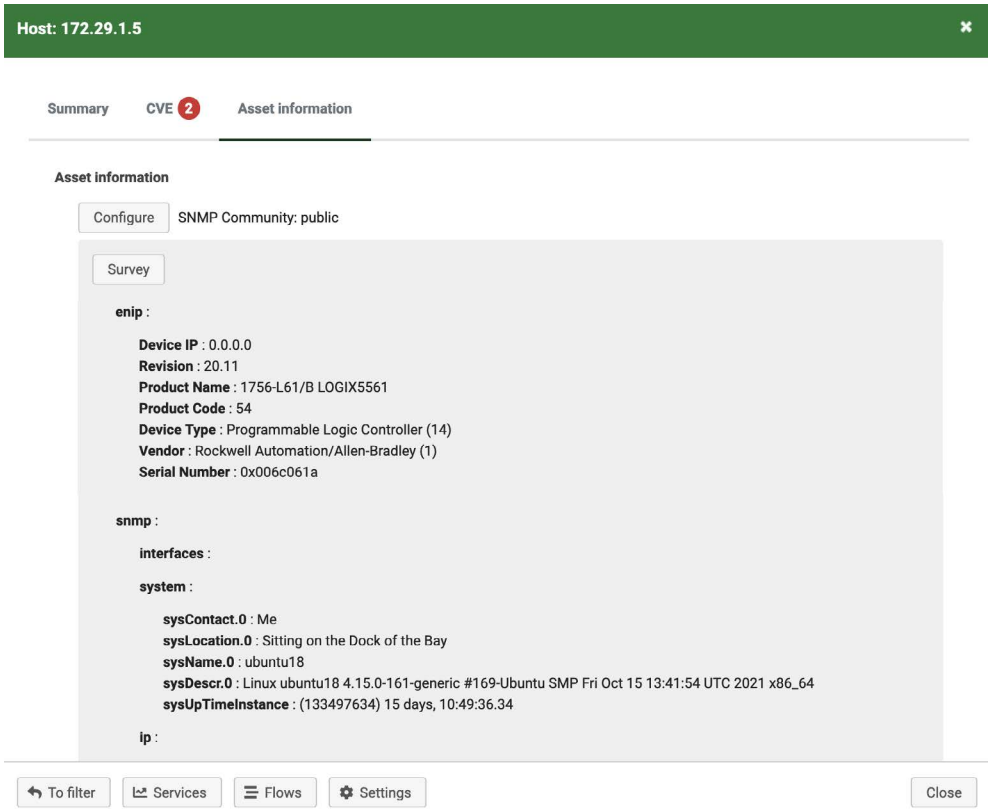
Industrial Manufacturing

Healthcare

Easily View Complex Issues

Automated Asset Discovery

- Active discovery of asset information of the device: vendor, manufacturing p/n, HW version, SW version, IT aspects like network information etc.
- Mapping of known vulnerabilities (CVEs) to discovered assets
- Quickly discover when new devices, services, subnets, etc. appear in the network, or previously active devices or services stop communicating

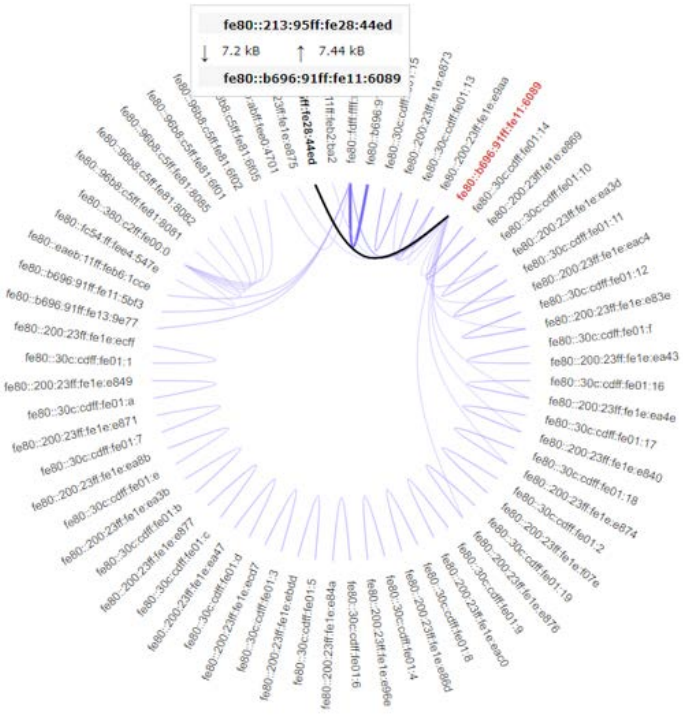


Protocol Visibility

- Support protocols from many vendors incl. Siemens, ABB, Honeywell, Emerson, Schneider, GE etc.
- Analyze and capture full ICS & SCADA protocol content for supported protocols including IEC 60870-5-104, IEC 61850 (GOOSE SV MMS), MODBUS, DLMS / COSEM, DNP3, Profinet, S7, SNMP, TELNET, CCLINK, ENIP/CIP, MQTT, COAP, OMRON FINS, LoRaWAN, BACnet & 30+ “office” protocols

Quick Forensics and Troubleshooting

- Powerful network visualization using many perspectives
- Detection of (un)authorized asset software changes
- Filter, sort, search and display any data in real time
- Security & operational events & incidents with full context
- On-demand or event-based full packet capture



Dynamic and Granular Network Visibility

- Full visibility into both IP and Ethernet traffic
- Visualize the network, its dependencies, its assets and communications using filtering parameters like subnetwork, protocol, vendor, and flow direction for any time period
- Detailed communication maps for auditing, hardening, or incident response

Policy Enforcement and Anomaly Detection

- Monitoring of defined communication matrix – what device is allowed to communicate with what device, how, over what protocol, frequency, commands, values, …
- Validating data on application level – framework for defining dynamic rules using variables such as historian, EWS, HMI, PLC…
- Detection of general changes in the network – new communication vectors, new or changed services / devices / subnets, OT Perimeter bypassing, …
- Monitoring of OT best practices

Threat Detection

- Simple threat and risk management through correlation of multiple advanced detection techniques like rule-based detection, supervised machine learning, and network behavior analysis
- Detection of known attacks, vulnerability exploits (CVEs), unauthorized control commands etc.
- Detection of signs of previously hidden malicious and unauthorized behavior and targeted, or “zero-day” attacks
- Supervised machine learning to detect anomalies in parameters like anomalous data transfer, number of communication partners or network services used, device response times etc.
- Monitoring of IT cyber security policies & best practices and network misconfigurations

Inputs

Network and Log Data

- Mirrored traffic (TAP, SPAN, RSPAN, ERSPAN or other types of mirrored traffic incl. firewalls)
  - upport L2 to L7 layer of IP protocol, IPv4 and IPv6
  - Ethernet traffic
  - Examples of supported protocols:
    IEC 60870-5-104, IEC 61850 (GOOSE SV MMS), MODBUS, DLMS / COSEM, DNP3, Profinet, S7, SNMP, TELNET, CCLINK, ENIP/CIP, MQTT, COAP, OMRON FINS, LoRaWAN, BACnet and 30+ "office" protocols
  - Custom protocols can be added upon request
- Netflow and IPFIX
- Device logs and application logs

Threat Intelligence

- Multi-source IDS signatures (incl. GREYCORTEX and ETPro)
- 3rd party threat intelligence and vulnerability databases
- Other databases (IP reputation, domain reputation, GEO IP, WHOIS, etc.)

Network, User and Asset Context

- Defining functional network zones and/or subnets for better clarity of control
- IP to hostname translation (using DNS and DHCP records)
- IP to domain-user translation (using domain controller event logs)
- Active polling for asset discovery and inventory details
- Integration with identity services including MS Active Directory and Cisco ISE and configuration databases

Outputs

Graphical User Interface

- Web user interface (IE, Firefox, Chrome, Opera, Safari, Edge, etc.)
- Completely granular access rights control
- Easily customizable dashboards and visualizations
- Unlimited data filtering & sorting

Reporting & Alerting

- Conditional reporting (alarms)
- Customizable output format
- Incident management
- Human-readable formats: email (html), pdf, docx, csv, custom links to GUI

Integration

- SIEM and SOC: based on syslog, CEF, LEEF and similar formats and API
- Flow export in IPFIX format with filtering possibility
- SOAR/orchestrators tools, firewalls, NACs, network switches and other infrastructure

Scalability

HW or Virtual

- Support for rack and DIN rail HW appliances from multiple vendors incl. Dell and HPE
- Support for virtual appliances VMware, KVM, Hyper-V and cloud environments (AWS, Google Cloud, …)

All-in-One

- Single appliance containing a sensor and a collector
- 200Mbps up to 10Gbps monitored throughput
- Up to 12x 1GE and 4x 10GE monitoring interfaces
- Up to 50 connected additional sensors per single
- All-in-One appliance
- Up to 100,000 monitored nodes per All-in-One appliance

Sensor

- 100Mbps to 10Gbps monitored throughput
- Up to 12x 1GE and 4x 10GE monitoring interfaces
- Collector
- 50+ sensors per single collector
- Up to 200,000 monitored nodes per collector
- Up to 3 years of data history

Central Management Console

- Clustering of up to 50 collectors together

Services

Network Asset Inventory Scan

Let GREYCORTEX assess your network with their offline Asset Discovery tool, providing you with a detailed overview of your network assets, their software versions and how they are interworking.

Device Assessments

Asset discovery when cross checking for vulnerabilities and issues with the supply chain for a wide range of protocols.

Security Audits

How devices communicate with each other, security policies (communication vectors, passwords, remote access), user behavior, security risks and asset discovery.

ICS/SCADA laboratory

The OT laboratory at GREYCORTEX's headquarters in Brno is open to its end users and partners for testing OT devices and software.

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

GREYCORTEX