GREYCORTEX
MENDEL

Cybersecurity Monitoring of OT Networks

Cybersecurity Visibility

Gain a comprehensive understanding of your network's complexity while enhancing threat detection and policy monitoring. With Mendel's detection capabilities through IDS, network behavior analysis, and full access to most OT protocol fields, you'll have the upper hand in safeguarding your critical assets.

Asset Inventory

OT cybersecurity begins with knowing your assets. Get a complete picture of your network and business applications through both active and passive asset discovery and advanced tagging. This empowers you to effectively manage and protect your valuable assets.

OT Metrics

Visualize your OT metrics, as you are used to in your current SCADA, alongside cybersecurity events. Our intuitive graphs allow you to monitor and analyze your operational technology performance seamlessly.

Easy to Integrate

Streamline implementation and operation, even for smaller teams with limited resources. Connect effortlessly with firewalls and third-party systems, such as SIEM, syslog and SNMP, or with our full API, ensuring a customized and efficient security setup.

On-premise Deployment

Take control of your data while it stays within your network. Rest assured that your information remains secure. For added flexibility or for companies without their own on-premise infrastructure, there is also the option of deploying our central event manager in the cloud.

GREYCORTEX Mendel protects

↓

ENERGY GENERATION AND DISTRIBUTION

MANUFACTURING

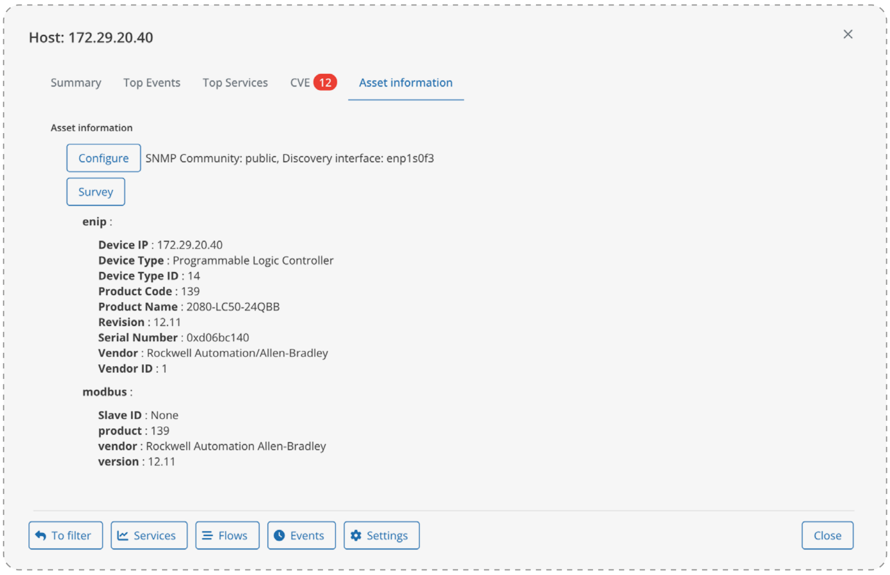
UTILIES

FACILITY MANAGEMENT

Easily View Complex Issues

Automated Asset Discovery

- Active discovery of the asset information of a device: vendor, manufacturing part numbers, hardware and software version, IT aspects like network information, etc.
- Mapping of known vulnerabilities (CVEs) to discovered assets
- Quickly detecting new devices, services, subnets, etc., in the network, or previously active devices or services that have ceased communication within the network.



Host: 172.29.20.40

Asset information

SNMP Community: public, Discovery interface: enp1s0f3

enip :

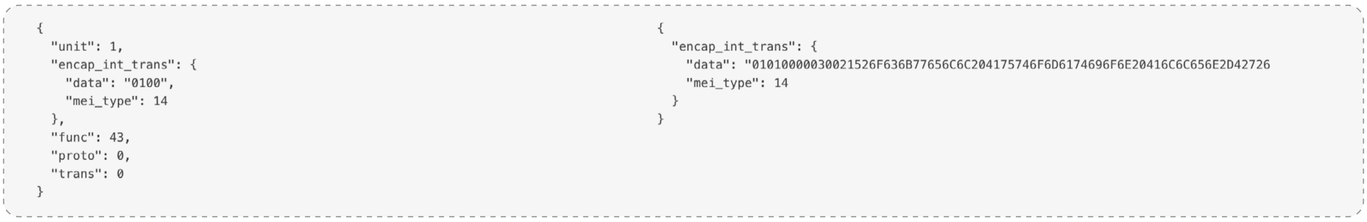
Device IP : 172.29.20.40
Device Type : Programmable Logic Controller
Device Type ID : 14
Product Code : 139
Product Name : 2080-LC50-24QBB
Revision : 12.11
Serial Number : 0xd06bc140
Vendor : Rockwell Automation/Allen-Bradley
Vendor ID : 1

modbus :

Slave ID : None
product : 139
vendor : Rockwell Automation Allen-Bradley
version : 12.11

Protocol Visibility

- Support for protocols from various vendors, including Siemens, ABB, Honeywell, Emerson, Schneider, GE, and more.
- The analysis and capture of full ICS and SCADA protocol content for supported protocols, such as 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.

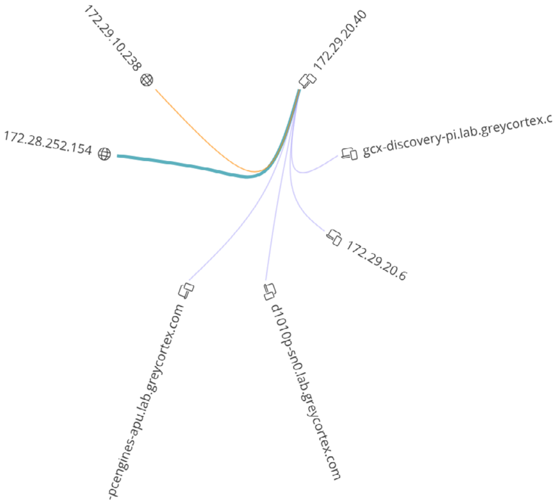


```
{
  "unit": 1,
  "encap_int_trans": {
    "data": "0100",
    "mei_type": 14
  },
  "func": 43,
  "proto": 0,
  "trans": 0
}
```

```
{
  "encap_int_trans": {
    "data": "01010000030021526F636B77656C6C204175746F6D6174696F6E20416C6C656E2D42726
    "mei_type": 14
  }
}
```

Quick Forensics and Troubleshooting

- Powerful network visualization from multiple perspectives.
- Detection of (un)authorized changes in asset software.
- Efficient filtering, sorting, searching and displaying of real-time data.
- Insights into security and operational events and incidents with full context.
- Performance of on-demand or event-based full packet capture for thorough analysis.


172.29.10.238
172.29.20.40
172.28.252.154
gcx-discovery-pi.lab.greycortex.c
172.29.20.6
-pcengines-apu.lab.greycortex.com
d1010p-sn0.lab.greycortex.com

Dynamic and Granular Network Visibility

- Full visibility into both IP and Ethernet traffic.
- Visualization of the network, its dependencies, assets and communications using flexible 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

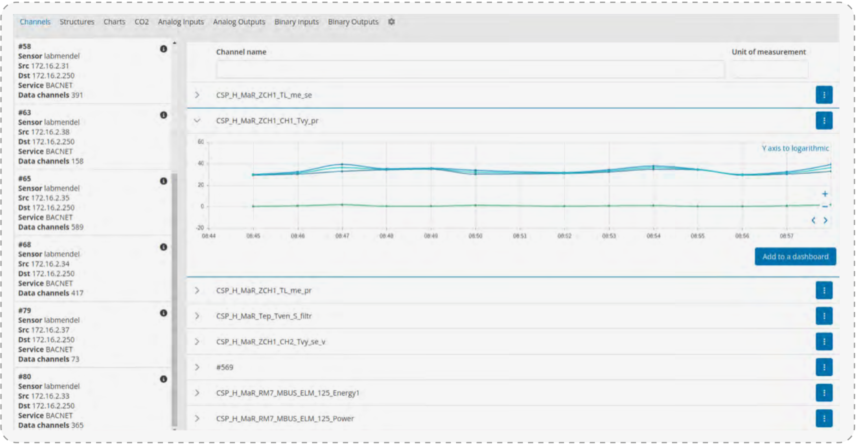
- Monitoring of defined communication matrix, specifying what device is allowed to communicate with one another, how, over what protocol, frequency, commands, values, and more.
- Validation of data at the application level, using framework to define dynamic rules with variables such as historian, EWS, HMI, PLC, and others.
- Detection of general changes in the network, including new communication vectors, new or changed services/ devices/subnets, and OT Perimeter bypassing.
- Monitoring of OT best practices.

Threat Detection

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

OT Metrics

- Passive extraction of protocol metrics from monitored traffic.
- Visual correlation of cybersecurity events with metric data commonly found in SCADA systems.
- Creation of customized dashboards for your specific needs.



#58
Sensor labmendel
Src 172.16.2.31
Dst 172.16.2.250
Service BACNET
Data channels 391

#63
Sensor labmendel
Src 172.16.2.38
Dst 172.16.2.250
Service BACNET
Data channels 158

#65
Sensor labmendel
Src 172.16.2.35
Dst 172.16.2.250
Service BACNET
Data channels 589

#68
Sensor labmendel
Src 172.16.2.34
Dst 172.16.2.250
Service BACNET
Data channels 417

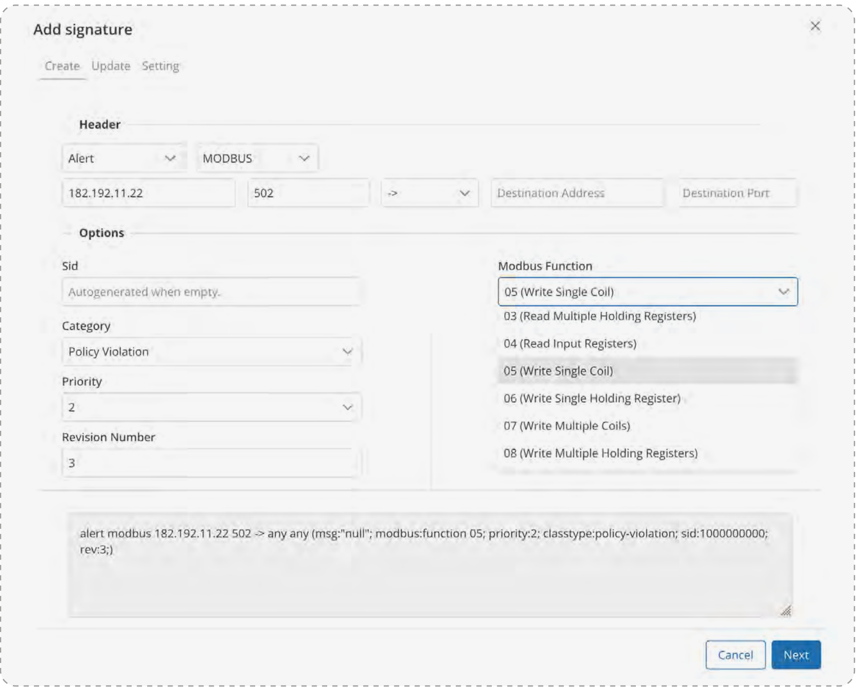
#79
Sensor labmendel
Src 172.16.2.37
Dst 172.16.2.250
Service BACNET
Data channels 73

#80
Sensor labmendel
Src 172.16.2.33
Dst 172.16.2.250
Service BACNET
Data channels 365

Channel name	Unit of measurement
CSP_H_MaR_ZCH1_TL_me_se	
CSP_H_MaR_ZCH1_CH1_Tvy_pr	
CSP_H_MaR_ZCH1_TL_me_pr	
CSP_H_MaR_Tep_Tven_S_filtr	
CSP_H_MaR_ZCH1_CH2_Tvy_se_v	
#569	
CSP_H_MaR_RM7_MBUS_ELM_125_Energy1	
CSP_H_MaR_RM7_MBUS_ELM_125_Power	

Custom Rule Creation

- Customization of detection rules to meet the unique requirements of your OT environment.
- Utilization of a user-friedly interface for creating custom rules.
- Syntax error prevention in complex detection rule creation.
- Building of a private library of customized detection rules tailored to your different applications.



Add signature

Header

Alert
MODBUS
182.192.11.22
502
->
Destination Address
Destination Port

Options

Sid: Autogenerated when empty.
Category: Policy Violation
Priority: 2
Revision Number: 3

Modbus Function: 05 (Write Single Coil)
03 (Read Multiple Holding Registers)
04 (Read Input Registers)
05 (Write Single Coil)
06 (Write Single Holding Register)
07 (Write Multiple Coils)
08 (Write Multiple Holding Registers)

```
alert modbus 182.192.11.22 502 -> any any (msg:"null"; modbus:function 05; priority:2; classtype:policy-violation; sid:1000000000;
rev:3;)
```

INPUTS

Network and Log Data

- Mirrored traffic (TAP, SPAN, RSPAN, ERSPAN, or other types of mirrored traffic, including firewalls)
- Support L2 to L7 layer of IP protocol, both 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 (including GREYCORTEX and ETPro)
- Third 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 and sorting

Reporting and Alerting

- Podmíněné hlášení (alarmy)
- Přizpůsobitelný výstupní formát
- Správa incidentů
- Lidsky čitelné formáty: (html), pdf, docx, csv, vlastní odkazy na grafické uživatelské rozhraní

Integration

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

SCALABILITY

Hardware or Virtual

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

All-in-one

- Single appliance containing a sensor and a collector
- 200 Mbps up to 10 Gbps monitored throughput
- Up to 12× 1GE and 4× 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

- 100 Mbps to 10 Gbps monitored throughput
- Up to 12× 1GE and 4× 10GE monitoring interfaces

Collector

- 50+ sensors per single collector
- Up to 200,000 monitored nodes per collector
- Up to three years of data history

Central Management Console

- Clustering of up to 50 collectors together

PROTECT YOUR INFRASTRUCTURE

↓

With GREYCORTEX Mendel, you are not just protecting your operational technology; you are also gaining valuable insights and control to protect your organization’s digital assets.

Start your cybersecurity journey with GREYCORTEX Mendel today.

Contact our sales representatives at info@greycortex.com.

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

www.greycortex.com