GREYCORTEX MENDEL

# Kyberbezpečnostní dohled průmyslových sítí

## Kompletní přehled o kybernetické bezpečnosti

Získáte komplexní viditelnost a hluboký vhled do vaší sítě. GREYCORTEX Mendel monitoruje dodržování nastavených pravidel a detekuje hrozby prostřednictvím IDS, analýzy chování sítě a plného přístupu k OT protokolům. To vám dává jistotu a plnou kontrolu nad všemi kritickými aktivy.

## Správa aktiv

Kybernetická bezpečnost operačních technologií začíná znalostí toho, co máte ve své síti. Získáte perfektní přehled o své síti a podnikových aplikacích díky aktivnímu i pasivnímu zjišťování aktiv a jejich pokročilému tagování. Tím je budete schopni efektivně spravovat a chránit.

## OT metriky

Své OT metriky zobrazíte stejným způsobem jako jste zvyklí ve svém stávajícím SCADA systému, navíc v souvislosti bezpečnostními událostmi. Intuitivní grafy vám umožní monitorovat a analyzovat výkonnost vašich operačních technologií.

## Snadná integrace

Implementaci a provoz GREYCORTEX Mendel zvládnou i menší týmy s omezenými zdroji. Prostřednictvím našeho plnohodnotného API jej snadno propojíte s firewally i systémy jako SIEM, syslog nebo SNMP, což zajistí účinné nastavení přizpůsobené vašim potřebám.

## Lokální nasazení

Lokální nasazení umožňuje plnou kontrolu nad vašimi daty bez jejich odesílání mimo vaši síť. Nabízíme také nasazení v cloudu pro organizace bez vlastní lokální infrastruktury.

**GREYCORTEX Mendel chrání**

**VÝROBA A DISTRIBUCE ENERGIÍ**

**PRŮMYSLOVÁ VÝROBA**

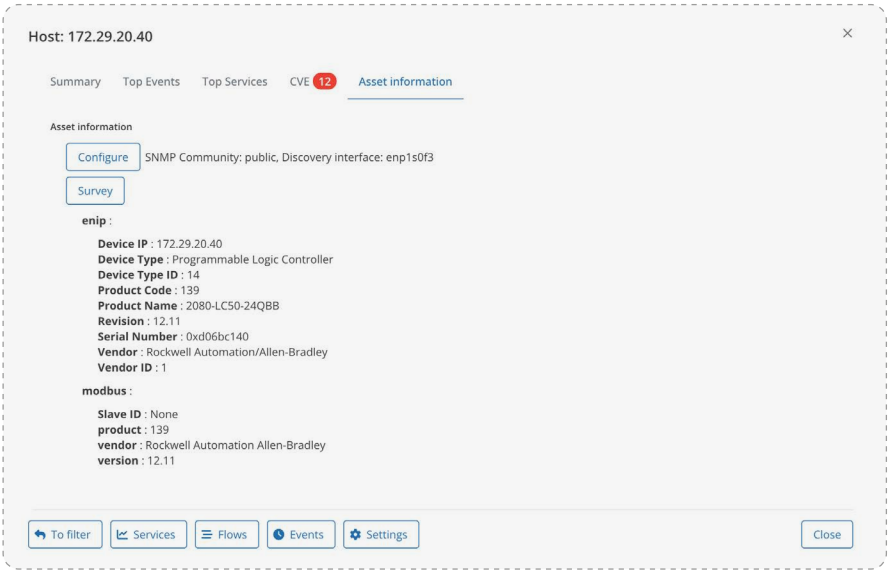
**KRITICKÁ INFRASTRUKTURA**

**SPRÁVA BUDOV**

# Jednoduchý vhled do složitých problémů

## Automatizovaná identifikace zařízení

- Aktivní zjišťování informací o zařízeních a jejich detailech: výrobce, výrobní číslo, verze HW, verze SW, IT aspekty, jako jsou informace o síti a další
- Mapování známých zranitelností (CVE) na identifikovaných zařízení
- Rychlá detekce nových zařízení, služeb a podsítí v síti, včetně stavu, kdy dříve aktivní zařízení či služby přestanou komunikovat




## Viditelnost protokolů

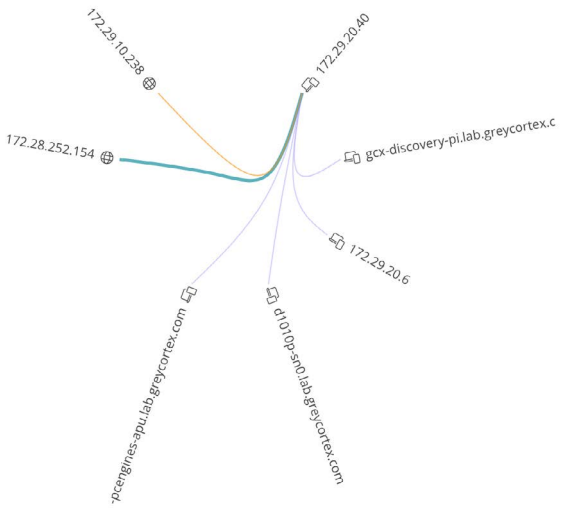
- Podpora průmyslových protokolů mnoha dodavatelů včetně Siemens, ABB, Honeywell, Emerson, Schneider, GE a dalších
- Analýza a zachycení úplného obsahu OT protokolů pro podporované protokoly včetně IEC 60870-5-104, IEC 61850 (GOOSE SV MMS), MODBUS, DLMS / COSEM, DNP3, Profinet, S7, SNMP, TELNET, CCLINK, ENIP/CIP, MQTT, COAP, OMRON FINS, LoRaWAN, BACnet a více než 30 „kancelářských“ protokolů


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

```
{
  "encap_int_trans": {
    "data": "0101000003002152 6F636B77656C6C204175746F6D6174696F6E20416C6C656E2D42726",
    "mei_type": 14
  }
}
```


## Rychlá forenzní analýza a řešení problémů

- Robustní vizualizace sítě s využitím mnoha pohledů
- Detekce (ne)autorizovaných změn softwaru aktiv
- Filtrování, třídění, vyhledávání a zobrazení libovolných dat v reálném čase
- Bezpečnostní a provozní události a incidenty prezentované v širokém kontextu
- Nahrávání plného provozu (pcap) na základě detekovaných událostí



## Dynamický a granulární přehled o síti

- Úplný přehled o IP i ethernetovém provozu
- Vizualizace sítě, jejích závislostí, zařízení a komunikace a filtrování pomocí parametrů, jako je podsíť, protokol, výrobce a směr komunikace, a to za libovolné časové období
- Podrobné zmapování komunikace pro audit, bezpečnostní testování nebo reakční plány po incidentech

## Kontrola bezpečnostních politik a detekce anomálií

- Monitorování vymezené komunikační matice – jaké zařízení smí komunikovat s jakým zařízením, jakým způsobem, přes jaký protokol, s jakou frekvencí, s jakými příkazy, hodnotami, ...
- Ověřování dat na aplikační úrovni – struktura pro definování dynamických pravidel pomocí proměnných, jako je například historian, EWS, HMI, PLC a další
- Detekce změn v síti – nové komunikační vektory, nové a pozměněné služby, zařízení nebo podsítě, obcházení OT perimetru a další
- Monitorování osvědčených postupů v OT

## Detekce hrozeb

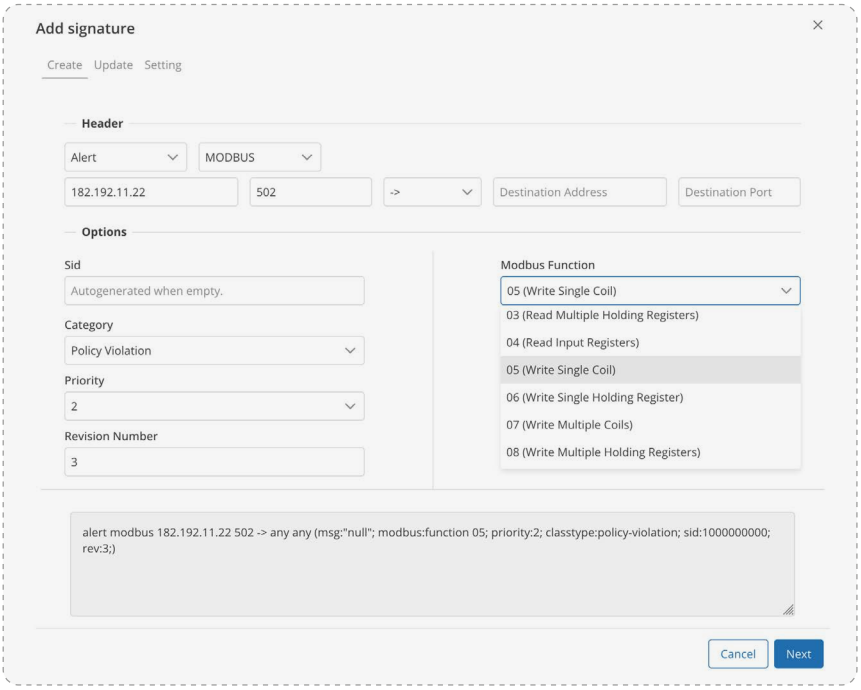
- Jednoduchá správa hrozeb a rizik prostřednictvím korelace několika pokročilých detekčních technik, jako je detekce založená na pravidlech, asistované strojové učení a analýza chování sítě
- Detekce známých útoků, zneužití zranitelností (CVE), neoprávněných řídicích příkazů a dalších
- Detekce příznaků dříve skrytého a neautorizovaného chování a cílených nebo „zero-day“ útoků
- Asistované strojové učení pro detekci anomálií v parametrech, jako je anomální přenos dat, počet komunikačních partnerů nebo používaných síťových služeb, doba odezvy zařízení a další
- Monitorování zásad a osvědčených postupů kybernetické bezpečnosti IT a chybné konfigurace sítě

## OT metriky

- Pasivní extrakce metrik protokolu ze sledovaného provozu
- Vizuální korelace událostí kybernetické bezpečnosti s metrickými údaji, které se běžně vyskytují v systémech SCADA
- Dashboardy nastavitelné přímo pro vaše specifické potřeby


## Vytváření uživatelských pravidel

- Přizpůsobení pravidel detekce tak, aby splňovala jedinečné požadavky vašeho OT prostředí
- Uživatelsky jednoduché rozhraní pro vytváření vlastních pravidel
- Prevence syntaktických chyb při vytváření složitých detekčních pravidel
- Soukromá knihovna vlastních detekčních pravidel přizpůsobených různým aplikacím



# VSTUPY

## Síťová data a logy

- Zrcadlený síťový provoz (TAP, SPAN, RSPAN, ERSPAN nebo jiné typy zrcadleného provozu včetně firewallů)
- Podpora vrstev L2 až L7 protokolů IPv4 i IPv6
- Ethernetový provoz
- Příklady podporovaných protokolů: 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 a více než 30 „kancelářských“ protokolů
- Na vyžádání lze přidat vlastní protokoly
- Netflow a IPFIX- Logy zařízení a aplikací

## Databáze hrozeb a zranitelností

- Signatury známých hrozeb z více zdrojů (včetně GREYCORTEX a ETPro)
- Zpravodajské databáze hrozeb a zranitelností třetích stran
- Další databáze (reputace IP, reputace domény, GEO IP, WHOIS atd.)

## Kontext sítě, uživatelů a zařízení

- Definování funkčních zón sítě a/nebo podsítí pro vyšší přesnost dohledu
- Překlad IP na hostitelské jméno (pomocí záznamů DNS a DHCP)
- Překlad IP na uživatele domény
- Aktivní dotazování pro zjišťování aktiv a podrobností o inventáři
- Integrace se službami MS Active Directory, Cisco ISE a konfiguračními databázemi

# VÝSTUPY

## Grafické uživatelské rozhraní

- Webové uživatelské rozhraní (IE, Firefox, Chrome, Opera, Safari, Edge atd.)
- Detailní řízení přístupových práv
- Snadno přizpůsobitelné ovládací panely a vizualizace
- Neomezené filtrování a třídění dat

## Reportování a upozornění

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

## Integrace

- SIEM a SOC: na základě syslogu, CEF, LEEF a podobných formátů a API
- Export toků ve formátu IPFIX s možností jejich filtrování
- Nástroje SOAR/orchestrátory, firewally, NAC, síťové přepínače a další infrastruktura

# ARCHITEKTURA

## HW nebo virtuální

- Podpora pro HW zařízení do racku a na lištu DIN od různých dodavatelů, včetně společností Dell a HPE
- Podpora virtuálních zařízení VMware, KVM, Hyper-V a cloudových prostředí (AWS, Google Cloud, ...)

## All-in-one

- Jedno zařízení obsahující senzor a kolektor
- Monitorovaná propustnost 200 Mb/s až 10 Gb/s
- Až 12× 1GE a 4× 10GE monitorovacích rozhrani
- Až 50 připojených dalších senzorů na jedno zařízení All-in-One
- Až 100 000 monitorovaných zařízení

## Senzor

- Monitorovaná propustnost 100 Mb/s až 10 Gb/s
- Až 12× 1GE a 4× 10GE monitorovacích rozhrani

## Kolektor

- Více než 50 senzorů na jeden kolektor
- Až 200 000 monitorovaných zařízení na jeden kolektor
- Až 3 roky historie uložených síťových metadat

## Centrální konzole pro správu

- Seskupení až 50 kolektorů dohromady

**CHRAŇTE SVOU INFRASTRUKTURU**

S GREYCORTEX Mendel chráníte své provozní technologie a získáváte cenné informace a kontrolu nad ochranou digitálních aktiv vaší organizace.

**Začněte chránit svou infrastrukturu ještě dnes.**

Kontaktujte naše obchodní zástupce na adrese cs@greycortex.com.


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