

Siemens S7

EtherNet/IP

OPC UA

IEC 61850

PROFINET

Modbus

BACnet

IEC 60870-5-104

DNP3

Jedno řešení pro monitorování a ochranu IT i OT sítí

ČESKÉ NDR ŘEŠENÍ

Přehled o IT i OT aktivech

Všechna zařízení uvidíte v jednom přehledu.
U každého si zobrazíte jeho typ, výrobce,
verzi HW i SW a risk skóre včetně vývoje v čase.

Bez dopadu na provoz

Monitorujte síťový provoz pasivně pomocí toků a paketů,
bez zásahů do zařízení a bez dopadu na jejich výkon.

Detekce hrozeb dřív, než naruší provoz

Odhalte známé kybernetické útoky, neoprávněné změny
i neobvyklé aktivity v IT i OT sítích.

Soulad s předpisy

Mějte k dispozici průběžné monitorování, auditní záznamy
a reporty pro splnění požadavků zákona o kybernetické
bezpečnosti a normy IEC 62443.

Lokální nasazení i v izolovaných sítích

Celé řešení běží ve vaší vlastní infrastruktuře – od jedné lokality
až po distribuované či fyzicky oddělené sítě.

**GREYCORTEX Mendel
chrání**



VÝROBA A DISTRIBUCE ENERGIE



**VODÁRENSTVÍ
A DALŠÍ VEŘEJNÉ SLUŽBY**



VÝROBNÍ A ZPRACOVATELSKÝ PRŮMYSL



FARMACEUTICKÁ VÝROBA



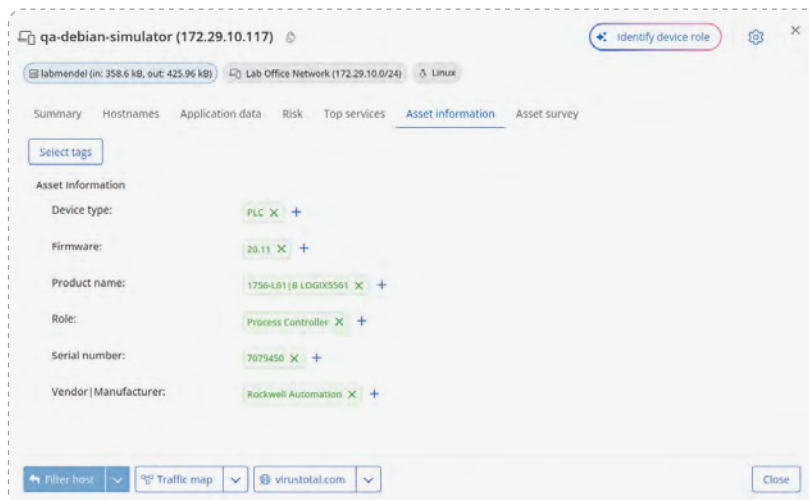
SPRÁVA BUDOV

Jeden pohled na IT i OT

Identifikace zařízení

Všechna zařízení, jejich detaily a známé zranitelnosti

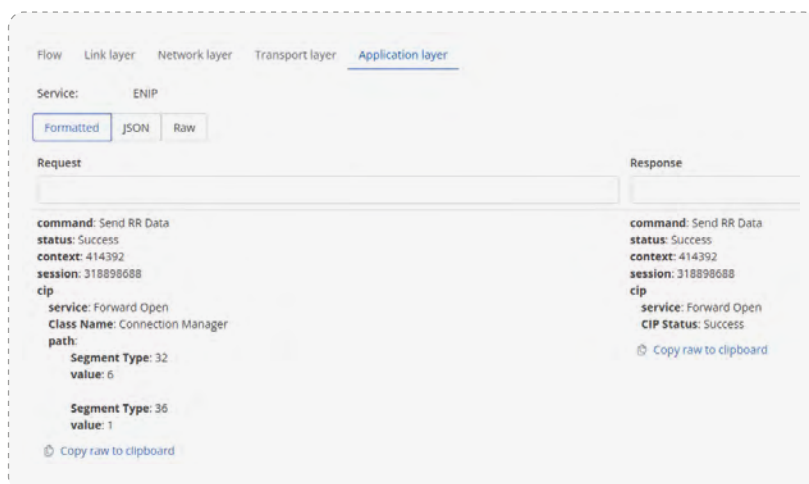
- Pasivní zjišťování informací o zařízeních ze síťového provozu, včetně výrobce, verze HW a SW, operačního systému a síťových údajů.
- Mapování známých zranitelností (CVE) na identifikovaná zařízení.
- Detekce nových zařízení, služeb a podsítí.
- Detekce neaktivních a ztracených zařízení. Zařízení, které přestane komunikovat, se nejprve označí jako neaktivní. Analytik tak má čas zařízení prověřit, než ho systém trvale odstraní.
- Automatické i ruční tagování zařízení.



Viditelnost protokolů

Podrobný vhled do průmyslových protokolů

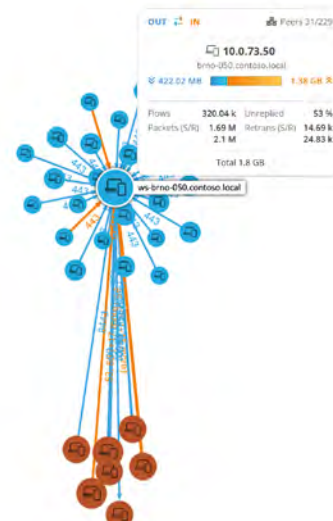
- Podpora nejpoužívanějších průmyslových protokolů od řady výrobců, včetně Siemens, ABB, Honeywell, Emerson, Schneider a GE.
- Hloubková analýza a extrakce metadat z podporovaných ICS a SCADA protokolů, včetně BACnet, CC-Link, CoAP, DLMS/COSEM, DNP3, EtherNet/IP, EtherCAT, Ether-S-Bus, GE-SRTP, IEC 60870-5-104, IEC 61850 (GOOSE, SV, MMS), Modbus, MQTT, OMRON FINS, OPC UA, PROFINET (IO DCE/RPC, DCP, Realtime PN-IO), MELSEC-E4, Siemens S7, SNMP, HART-IP, M-Bus, DICOM, HL7 a více než 30 „kancelářských“ protokolů.



Viditelnost síťového provozu

Veškerá komunikace mezi IT, OT a vnějšími sítěmi

- Úplný přehled o IP i ethernetovém provozu.
- Vizualizace sítě, jejich závislostí, zařízení a komunikace s filtrováním podle podsítě, protokolu, výrobce a směru komunikace, a to za libovolné časové období.
- Přehled komunikace mezi zařízeními i s vnějšími sítěmi s možností filtrovat interní a externí provoz.
- Dohled nad vzdálenými a dodavatelskými přístupy, včetně VPN.
- Mapa toků (Traffic Flow Map) zobrazuje nejvýznamnější protistrany zařízení, směr a objem komunikace.



Detekce hrozeb

Známé útoky, anomálie a neoprávněná aktivita

- Detekce známých útoků, malwaru a zneužití zranitelností (CVE).
- Detekce neoprávněných řídicích příkazů pomocí detekčních signatur specifických pro OT.
- Detekce komunikace Command & Control (C&C), skenování, útoků hrubou silou a exfiltrace dat.
- Skryté, cílené a zero-day útoky odhalené pomocí analýzy chování sítě a strojového učení.
- Zařazení detekovaných událostí do MITRE ATT&CK.

Vyšetřování a threat hunting

Vysvětlení pomocí AI, risk skóre a prohledatelná historie

- Risk skóre pomáhá určit, kterým hostům věnovat pozornost. Zohledňuje bezpečnostní události, jejich relevanci v rámci podsítě a aktuálnost.
- Historie a trend risk skóre u každého zařízení.
- AI asistent určí pravděpodobnou roli zařízení, vyhodnotí reputaci externích IP adres, vysvětlí bezpečnostní událost v kontextu MITRE ATT&CK a doporučí další kroky.
- Funkce **Vyšetřit událost** posoudí konkrétní komunikaci v kontextu hosta a nabídne zhodnocení, odhadovanou pravděpodobnost falešně pozitivního hlášení a doporučené kroky vyšetřování seřazené podle priority.
- Threat hunting v historických datech, která jsou indexovaná a okamžitě dostupná.

AI Assistant: Explain **EARLY ACCESS**

Event Summary:

Signature ID: 900005006

Name: Blacklist: Spamhaus DROP blacklist

MITRE ATT&CK: Information/Blacklist

Description: This event is generated when there is a communication with a host present in low reputation databases. This host is then blacklisted and tagged as untrusted. An IP address earns a negative reputation when a suspicious activity, like spam or viruses originating from that address is detected and reported to blacklist sources.

1. What this event means

This alert indicates that traffic was observed involving an IP address listed on the Spamhaus DROP (Don't Route Or Peer) blacklist. DROP-listed IPs are typically associated with serious abuse (spam, malware, botnets, or other malicious activity) and are recommended to be completely blocked at the network edge.

The rule logic (`!srcip:src, spamhaus_drop, > 10`) shows that the **source IP** has a high-risk reputation score in the Spamhaus DROP list, above the defined threshold.

2. Typical risk and impact

- Potential connection to known malicious or heavily abused infrastructure.
- Risk of:
 - Malware delivery or command-and-control (C2) communication
 - Spam or phishing campaigns
 - Scanning, brute-force, or other preparatory attacks
- If the blacklisted IP is **internal** (NATed or misclassified), it may indicate a compromised host in your environment.

3. How to verify if this is a false positive

1. Confirm the blacklisting status

- Identify the source IP from the event in your SIEM/NDR logs.
- Check it directly against Spamhaus:
 - Use Spamhaus lookup tools (e.g., web lookup for DROP/EDROP).
 - Verify that the IP is currently listed and not an outdated entry.

2. Determine if the IP is internal or external

- If it is an **internal IP** (RFC1918 or your assigned ranges):
 - Check if your IP reputation feed is misconfigured (e.g., applying to internal ranges).
 - Investigate the internal host for compromise (see section 4).
- If it is an **external IP**:
 - Check whether this IP belongs to a legitimate partner, vendor, or customer.
 - Contact the owner only if you have an established relationship and business need.

3. Review the context of the connection

- Direction: Was the connection **outbound** (internal → internet) or **inbound** (internet → internal)?
- Ports and protocols: HTTP/HTTPS, SMTP, SSH, RDP, custom ports, etc.
- Volume and pattern: Single connection vs. repeated/automated attempts.
- Associated alerts: Any malware, C2, or intrusion alerts involving the same IP or host.

4. Check for business justification

- Verify with application owners or system owners if there is any legitimate reason to communicate with this IP or its network.
- If there is no clear business need, treat the event as suspicious by default.

4. Immediate operational actions

1. Block or restrict traffic

- At perimeter firewalls, IPS, or routers, block traffic to/from the specific IP or its broader netblock if aligned with your policy.
- Ensure your edge devices are already enforcing Spamhaus DROP recommendations where appropriate.

2. Investigate the internal host involved

- Identify the internal source/destination host (depending on direction) using:
 - Firewall logs
 - NetFlow/Flow
 - DHCP logs (for main IP → hostname/owner)

This analysis is produced by an AI system. Decisions should not be based solely on this output without appropriate validation.

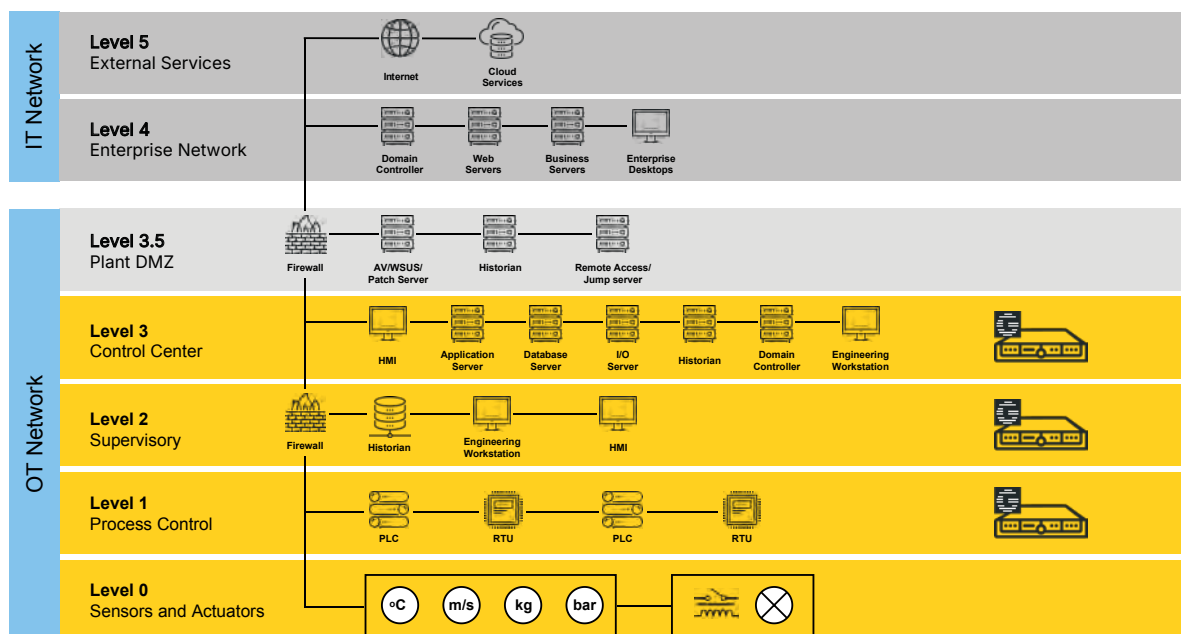
Is this information helpful?  

Soulad s předpisy a audit

Podklady pro auditory i pro plnění zákona o kybernetické bezpečnosti

- Ověřování segmentace sítě s upozorněním, pokud zařízení komunikuje do internetu nebo mezi segmenty v rozporu s nastavenými pravidly.
- Průběžné monitorování a auditní záznamy pro požadavky zákona o kybernetické bezpečnosti a normy IEC 62443.
- Uchovávání událostí a metadat po dobu měsíců až let pro potřeby auditu.
- Historie tagů u každého zařízení: kdy a z jakého zdroje byly tagy přiřazeny, změněny nebo odebrány. Slouží jako podklad pro audit.
- Detekce a klasifikace AI služeb v síťovém provozu.
- Reporty ve formátech pro snadné sdílení, včetně e-mailu a PDF.
- Export dat ve formátech CSV a IPFIX.

Nasazení nástroje Mendel v Purdue modelu



VSTUPY

Síťový provoz, telemetrie a logy

- Zrcadlený provoz (TAP, SPAN, RSPAN, ERSPAN nebo jiný typ zrcadleného provozu, včetně provozu firewallů)
- NetFlow, IPFIX, sFlow, JFlow, NetStream a VPC Flow Logs
- Dekapsulace tunelovaného provozu
- Podpora protokolů ve vrstvách L2 až L7 pro IPv4 i IPv6
- Ethernetový provoz
- Zaznamenaný síťový provoz (PCAP)
- Logy zařízení a aplikací

Úplná metadata ICS protokolů

- BACnet, CC-Link, CoAP, DLMS/COSEM, DNP3, EtherNet/IP, EtherCAT, Ether-S-Bus, GE-SRTP, IEC 60870-5-104, IEC 61850 (GOOSE, SV, MMS), Modbus, MQTT, OMRON FINS, OPC UA, PROFINET (IO DCE/RPC, DCP, Realtime PN-IO), MELSEC-E4, Siemens S7, SNMP, HART-IP, M-Bus, DCOM, HL7 a více než 30 „kancelářských“ protokolů
- Další i vlastní protokoly lze přidat na vyžádání

Zjišťování aktiv a kontext sítě

- Pasivní zjišťování aktiv ze síťového provozu
- Integrace s identitními službami, NAC a adresářovými službami prostřednictvím logů nebo RESTful API

VÝSTUPY

Reportování a upozornění

- Podmíněná hlášení (alarmy)
- Přizpůsobitelný výstupní formát
- Správa incidentů
- Lidsky čitelné formáty

Integrace

- SIEM na základě Syslogu, CEF, LEEF a API
- SOAR a XDR přes API
- Export toků do formátu IPFIX s možností filtrování
- Identita: Active Directory, Microsoft Entra ID, Cisco ISE a externí logy
- Firewally a NAC
- RESTful API

NASAZENÍ

HW nebo virtuální

- HW zařízení do racku a na lištu DIN od různých dodavatelů, včetně společností Dell a HPE
- Virtuální a cloudová zařízení (VMware, KVM, Hyper-V, AWS, Google Cloud, Microsoft Azure a další)
- Volitelně malý HW mikrosenzor s monitorovacími porty až 3× 1GbE

Senzor

- Monitorování sítě s propustností až 100 Gbps
- Až 20 monitorovacích rozhraní (1/10/25GbE nebo karty FPGA až 8× 25/10GbE či 4× 100/40GbE)
- Ve virtuálním nebo cloudovém nasazení až 10 Gbps

Kolektor

- Až 100 senzorů pod jedním kolektorem
- Až 250 000 monitorovaných síťových uzlů na jeden kolektor
- Uchovávání historických dat omezené pouze kapacitou úložiště

All-in-One

- Jedno zařízení obsahující senzor i kolektor
- Monitorování sítě s propustností až 50 Gbps
- Až 20 dalších připojených senzorů
- Až 80 000 monitorovaných síťových uzlů

**CHRAŇTE SVOU
INFRASTRUKTURU**

GREYCORTX Mendel je české řešení pro viditelnost síťového provozu a detekci kybernetických hrozeb v IT i OT sítích.

Kontaktujte nás na cs@greycortex.com.