# GREYCORTEX Mendel Datasheet

NDR

**Mendel od společnosti GREYCORTEX, NDR řešení pro firmy, státní správu a kritickou infrastrukturu nabízí hlubokou viditelnost v síti, pokročilou detekci a reakci na hrozby.**

## ZDROJE DAT

- Zrcadlený síťový provoz
- NetFlow/IPFIX
- Síťové a aplikační logy
- Zaznamenaný síťový provoz (PCAP)
- Síťový provoz z Kubernetes

## DETAILNÍ VIDITELNOST SÍTĚ

- Všechny podsítě, hosté, služby a toky obohacené o podrobné informace, včetně risk skóre pro každého interního hosta
- Metadata poskytují bohaté informace o chování sítě pro účely forenzního vyšetřování, zjištění souladu s předpisy atd.
- Tunelovaný provoz
- Dešifrování šifrované komunikace pomocí příslušného klíče
- Automatická identifikace kritických zařízení v síti, jako je Active Directory, e-mailový server, SMB server atd.
- Mapa toků zaměřená na hosta pro postupné vyšetřování komunikace v okolí vybraného hosta
- Historická data uložená po dobu měsíců jsou indexována a okamžitě dostupná
- Široké možnosti filtrování nad uloženými daty, přitom uživatelsky přívětivé

## VÝKONNÁ DETEKCE

založená na procesech strojového učení a matematických modelech, s pokročilou technologií pro odfiltrování falešně pozitivních detekcí.

### PREDIKTIVNÍ ANALÝZA

- Volumetrické anomálie
- DDoS útoky

Využívá pokročilé algoritmy umělé inteligence a strojového učení k předvídání a identifikaci potenciálních bezpečnostních hrozeb dříve, než se projeví jako plnohodnotný útok.

### ANALÝZA ZMĚN V SÍTI

- Nová zařízení, služby a komunikační vektory
- Nové administrátorské přístupy
- Zařízení, která přestala komunikovat (neaktivní a ztracení hosté)

Proces systematického zkoumání a mapování síťového prostředí s cílem identifikovat aktiva, zranitelná místa a potenciální místa kompromitace.

### ANALÝZA NA ZÁKLADĚ PRAVIDEL

- Detekce známého malwaru, exploitů a AI služeb v síťovém provozu
- Porušení bezpečnostních zásad

Metoda identifikace a vyhodnocování bezpečnostních hrozeb na základě předem definovaných pravidel nebo kritérií pro detekci a reakci v reálném čase.

### REPETITIVNÍ ANALÝZA

- Útoky Command & Control
- Útoky hrubou silou

Identifikace a analýza opakujících se vzorců nebo chování v síťovém provozu s cílem odhalit potenciální bezpečnostní hrozby nebo anomálie.

### ANALÝZA TOKŮ

- Skeny
- Útoky hrubou silou
- Enumerace

Investigace a interpretace toků síťového provozu s cílem zajistit přehled o komunikačních vzorcích, chování a potenciálních bezpečnostních hrozbách.

### ANALÝZA VÝKONU

- Problémy s výkonem sítě: vysoká doba odezvy, slow round trip time

Vyhodnocování a optimalizace provozní efektivity, spolehlivosti a škálovatelnosti bezpečnostních systémů a síťové infrastruktury prostřednictvím průběžného sledování výkonnostních ukazatelů.

### SÍŤOVÉ HONEYPOTY

- Lateral movement
- Zero-day exploity a průzkumné aktivity
- Pokusy o kradení přihlašovacích údajů

Emulace důvěryhodných zařízení a síťového provozu v interní síti pro okamžitou detekci podezřelé aktivity útočníka.

### ANALÝZA LOGŮ

- Nový firmware, noví uživatelé
- Změny v registrech a nastaveních

Shromažďování, parsing a analýza dat logů generovaných různými síťovými zařízeními, systémy a aplikacemi za účelem identifikace bezpečnostních incidentů, anomálií a provozních problémů.

## VYŠETŘOVÁNÍ A REAKCE

- Vysvětlení role interních hostů, reputace externích hostů a bezpečnostních událostí pomocí AI
- Centralizovaná platforma pro sledování, dokumentování a hlášení bezpečnostních incidentů
- Systém pluginů pro univerzální způsob interakce s firewally, NAC, ...
- Rozsáhlé možnosti exportu dat pro sdílení dat s jinými bezpečnostními nástroji

# KLÍČOVÉ SCHOPNOSTI

## Analýza chování sítě

Analýza síťového provozu založená na tocích prostřednictvím „unsupervised“ strojového učení a několika dalších detekčních metod (viz výše).

Detekční schopnosti:

- Aktivita malwaru – šíření, stahování, spamování atd.
- Aktivita útočníka – skenování, brute-force, exploitace atd.
- Aktivita C&C – RAT, APT, AVT, boti, červi, rootkity atd. – a exfiltrace date

## Hloubková kontrola packetů

- Monitoruje jakoukoli interakci s interní sítí nebo uvnitř ní
- Umožňuje kontrolovat provoz až do rychlosti 100 Gbit/s
- Detekční signatury pro malware, porušení politik, útoky a další závadné aktivity
- Detekce škodlivých souborů pomocí hashování
- Přehled komunikace s hosty na blacklistu
- Možnost přidávat uživatelské signatury s jednoduchou syntaxí za pomoci průvodce, včetně pravidel zohledňujících VLAN

## OT schopnosti

- Detekce, parsování a hlášení událostí včetně bohatých metadat pro průmyslové protokoly BACnet, CC-link, CoAP, DLMS/COSEM, DNP3, ENIP, EtherCAT, GE-STRP, IEC-104, IEC61850 (GOOSE, SV, MMS), MODBUS, MQTT, OMRON FINS, OPC UA, Profinet IO DCE/RPC, PROFINET-DCP, PROFINET Realtime (PN-IO), Siemens S7, SNMP, DICOM, HL7, Ether-S-Bus
- Specifické detekční OT signatury definované GREYCORTEX
- Metriky OT aplikací
- Detekce průmyslových zařízení (Asset discovery) s kontextovými vlastnostmi a rolemi
- Společná prezentace dat podle Purdue a MITRE ATT&CK

## Network Inventory

- Sloučení vrstev Viditelnost a Detekce do jednoho společného pohledu
- Zobrazení síťové infrastruktury z pohledu podsítí a zařízení, obohacená o risk skóre hosta (1–99), včetně historie rizika
- Mapa toků (Traffic Flow Map) zaměřená na hosta pro postupné vyšetřování komunikace vybraného hosta s jeho okolím.
- Data reprezentovaná formou řaditelné tabulky nebo škálovatelné grafické interpretace

## Historická metadata a forenzní analýza

Proprietární protokol Advanced Security Network Metrics (ASNM) je zaměřený na bezpečnost a výkon a slouží pro širší popis síťového provozu.

Zahrnuje:

- Obousměrný záznam toku (jeden tok obsahuje request i response)
- Metadata aplikačních protokolů pro FTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP/S, NTP, SMB, SNMP, LDAP, mDNS, NFS, MS-SQL, SIP, SSL/TLS, Kerberos atd.
- Retence dat v rozsahu měsíců až několika let (v závislosti na kapacitě úložiště)

## Monitorování výkonu

Analýza výkonu sítě a aplikací založená na tocích (NPM, APM):

- Povědomí o aplikacích
- Monitorování aktuální a průměrné šířky pásma
- Monitorování metrik výkonu jako jsou doba odezvy aplikace, round-trip, user-experience
- Detekce založená na pravidlech (například SLA)
- Automatická detekce založená na anomáliích

## Kategorizace zařízení

- Rozšířená klasifikace zařízení a jejich rolí s plnou historií tagů s jejich časovou referencí a zdrojem
- Dynamická viditelnost díky sledování nových aktivit nebo změn způsobených zařízeními komunikujícími ve vaší síti
- Ruční nebo automatizovaný způsob označování hostitelů nebo podsítí podle pravidel vytvořených uživatelem pomocí snadno pochopitelného průvodce

## Záznam a přehrávání provozu

- Zachycení paketů na vyžádání nebo na základě pravidel podle zdrojové a cílové IP, MAC, protokolu, portu atd.
- Možnost přehrávat a analyzovat PCAPy zaznamenané samotným nástrojem Mendel nebo zpracovat přenosy zachycené jinými nástroji

## AI asistent pro vyšetřování

- Vysvětlení interních IP adres – pravděpodobná role zařízení odvozená z kontextu hosta (L7 metadata, názvy hostů, tagy, MAC adresy, pozorované služby)
- Vysvětlení externích IP adres – vyhodnocení reputace (škodlivá, podezřelá, průzkumná, neškodná, pravděpodobně neškodná, neznámá)
- Vysvětlení bezpečnostní události – co se stalo, proč je to důležité, kontext MITRE ATT&CK a doporučené následné kroky
- Výstup v angličtině, češtině, němčině a polštině, nezávisle na jazyce uživatelského rozhraní
- Globálně zapnuto nebo vypnuto administrátorem; výslovné potvrzení uživatelem před prvním použitím

Funkce založená na cloudu. Vybraná síťová metadata jsou zpracovávána externí AI službou hostovanou v infrastruktuře EU. Vyžaduje odchozí připojení; není k dispozici v air-gapped nasazeních.

# VSTUPY

Komplexní přístup k analytickému zpracování dat z mnoha různých zdrojů pro zajištění síťové bezpečnosti, a to včetně různých vrstev modelu OSI, využití znalostní báze hrozeb, funkcí dohledu chování jednotlivých sítí a jejich uživatelů pro účinné prosazování nastavených interních politik a zmírňování či eliminaci hrozeb.

### Síťová data

- Zrcadlený provoz (TAP, SPAN, RSPAN, ERSPAN nebo jiný typ zrcadleného provozu)
- Podpora linkové vrstvy
- Podpora síťové vrstvy včetně protokolů IPv6
- Dekapsulace tunelovaného provozu
- Podpora transportní vrstvy
- Podpora aplikační vrstvy
- Protokoly založené na Flow (NetFlow family, IPFIX, sFLOW, JFlow, NetStream a protokoly toku VPC)
- Z jiných zařízení Mendel (senzor, mikrosenzor nebo kolektor)

### Znalostní báze hrozeb

- Soubor detekčních pravidel Proofpoint Emerging Threats a interní výzkum GREYCORTEX
- Další databáze informací o hrozbách IP adres, doménových reputací a škodlivých souborů
- Možnost integrace vlastních informačních kanálů TI (včetně národních platforem MISP)
- Definice události podle MITRE ATT&CK Enterprise a Mitre ATT&CK ICS

### Znalost sítě

- Definice politik podle segmentů/podsítí, které sdílejí stejné vzorce chování, například management, obchod, servery, WiFi, VoIP, tiskárny, DMZ atd.
- Spojení IP s doménou (pomocí DNS záznamů)

### Znalost uživatelů

- Spojení IP s názvem hosta (prostřednictvím logů z doménových řadičů, AD, LDAP, CISCO ISE, Microsoft Entra ID (korelace přihlášení/odhlášení; vyžaduje konfiguraci na straně Entra ID) a všechny poskytnuté protokoly s těmito informacemi v rámci sledované sítě od různých služeb)

# VÝSTUPY

Systém poskytuje komplexní sadu výstupů a integrací pro efektivní monitorování a správu zabezpečení sítě a zajišťuje účinné monitorování, analýzu a reakci na bezpečnostní incidenty.

### Grafické uživatelské rozhraní (GUI)

- Webové uživatelské rozhraní (Firefox, Chrome, Opera, Edge)
- Hlavní interaktivní pohled založený na znalostech GREYCORTEX a frameworku MITRE ATT&CK®
- Rozsáhlé snadno přizpůsobitelné dashboardy s možností předzpracování dat
- Manažerské a bezpečnostní dashboardy pro zjednodušený přehled
- Operativní a široké možnosti filtrování
- Průvodce tvorbou vlastních IDS pravidel
- Dva motivy designu (světlý a tmavý)
- Kontextová nápověda a obsáhlá uživatelská dokumentace

### Reporty a notifikace

- Reporty generované na základě definovaných podmínek
- Bohatý a přizpůsobitelný výstupní formát s možností přidání přímého odkazu do GUI
- Formáty vhodné pro koncového uživatele: e-mail (HTML) a PDF

### Integrace

- SIEM – dávkový reporting nebo reporting v reálném čase na základě CEF, LEEF, Syslog nebo API
- SOAR – přizpůsobitelná integrace založená na exportu událostí a API s integračním balíčkem pro Palo Alto XSOAR
- XDR – přizpůsobitelná integrace s platformami EDR na základě rozhraní API nebo podle specifik dodavatele
- IPFIX – export toků ve formátu IPFIX
- IDENTITA – Active Directory, Cisco ISE a běžné externí protokoly pro doplnění identity uživatele
- FIREWALL/NAC – MikroTik, Juniper, FortiGate, Palo Alto, Checkpoint atd.
- OUTPUT – přizpůsobitelné datové výstupy
- API – obecné rozhraní RESTful API pro integraci s další infrastrukturou
- BACKUP – data a konfigurace napříč SMB, HCP, objektovým úložištěm kompatibilním s S3 (AWS S3 a on-premises) nebo lokálně připojeným úložištěm USB

# NASAZENÍ

Škálovatelnost nasazení a vysoká dostupnost se liší podle konkrétních podmínek a kombinací v dané infrastruktuře. Interoperabilita s identitními službami pro správnou správu uživatelů a jejich oprávnění prostřednictvím řízení přístupu na základě rolí (RBAC), včetně kompatibility s SSO/MFA.

### Senzor

- Monitorování sítě s propustností až 100 Gbps
- Až 20 monitorovacích rozhraní na každém HW zařízení s libovolnou kombinací 1GbE, 10GbE, 25GbE nebo s HW akcelerovanými kartami FPGA až 8× 25/10GbE nebo 4×100/40GbE
- V režimu virtualizace nebo Cloud nasazení zpracování až 10 Gbps
- Volitelně malý HW mikrosenzor s monitorovacími porty až 3× 1GbE

### Kolektor

- Až 100 senzorů pod jedním kolektorem (na základě celkové zpracovávané kapacity)
- Až 150 000 monitorovaných síťových uzlů na jeden kolektor
- Uchovávání historických dat je omezeno pouze velikostí dostupného (navrženého) datového úložiště
- Nasazení ve virtualizovaném prostředí (včetně Cloudu) se zpracováním až 20 připojených senzorů
- Úložiště s více diskovými oddíly s podporou rychlých disků (NVMe, SSD, SAS)
- Možnost online a offline aktualizace samotného systému nebo připojených senzorů

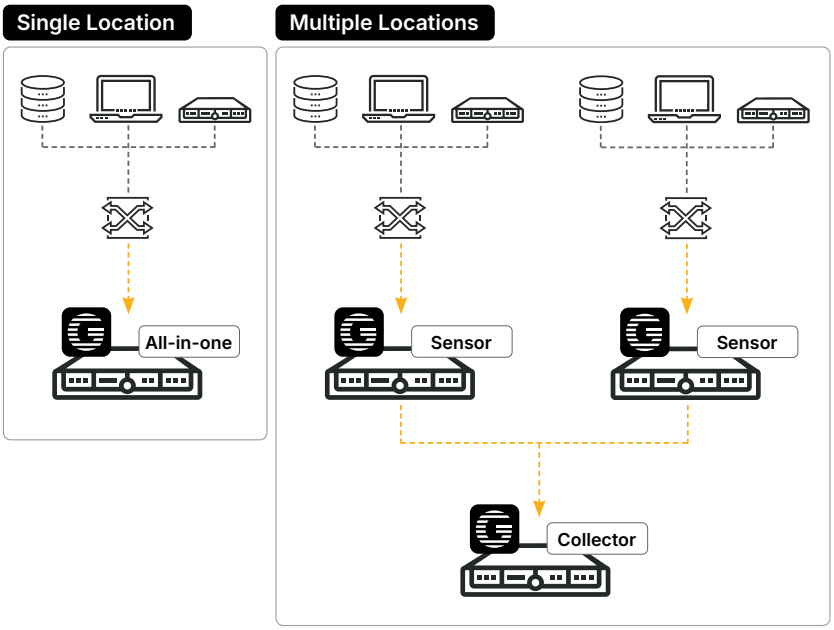
### All-in-One

- Jedno zařízení obsahující zároveň senzor i kolektor
- Monitorování sítě s propustností až 50 Gbps
- Až 20 monitorovacích rozhraní na každém HW zařízení s libovolnou kombinací 1GbE, 10GbE, 25GbE nebo s HW akcelerovanými kartami FPGA až 8× 25/10GbE nebo 4×100/40GbE
- Až 20 připojených dalších senzorů na jedno All-in-One zařízení
- Až 50 000 monitorovaných uzlů na jedno All-in-One zařízení
- Úložiště s více diskovými oddíly s podporou rychlých disků (NVMe, SSD, SAS)
- Možnost online a offline aktualizace samotného systému nebo připojených senzorů

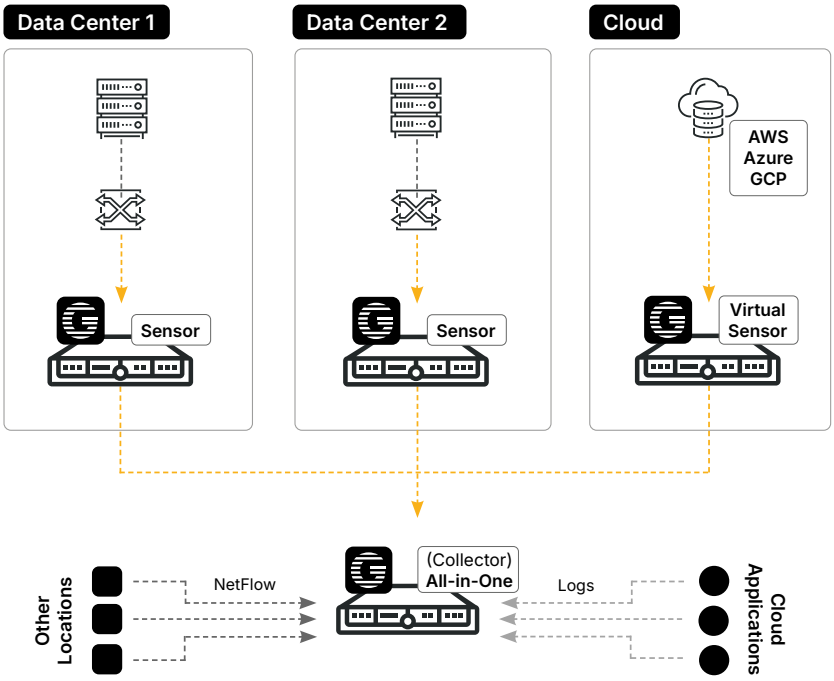
### Centrální správa událostí

- Spojení až 20 kolektorů do jednoho centrálního místa
- Přehled a správa všech událostí na jednom místě z celé připojené infrastrukturyinfrastructure

## Deployment




## Hybrid Cloud Deployment




## Vyzkoušejte GREYCORTEX Mendel

**Proof of Concept (PoC)**
Pro vyzkoušení GREYCORTEX Mendel vám nabízíme měsíční bezpečnostní audit sítě.


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

www.greycortex.com