# GREYCORTEX Mendel 3.8.0

## HLAVNÍ FUNKCE

**Rozšířená klasifikace zařízení a jejich rolí (tagování)**

Dynamický přehled v síti získáte díky sledování aktivit nebo změn, které jsou důsledkem komunikace jednotlivých zařízení. Zcela nový mechanismus umožňuje manuální nebo automatizovaný způsob označování zařízení a podsítí prostřednictvím systému uživatelsky definovaných pravidel se snadno pochopitelnou syntaxí.

**Nová kategorizace zjištěných bezpečnostních událostí**

Mendel interpretuje všechny události zachycené ve vaší síti s větší přehledností prostřednictvím kategorizace do MITRE ATT&CK® taktik a technik, dále dle pravidel Proofpoint a taktéž i podle Greycortex přehledu nejrelevantnějších událostí (tzv. Top události).

**Analytický modul**

Hlubší a pokročilejší analýza dat díky přepracovanému modulu Analysis. Nově můžete definovat libovolný pohled (dotaz) nad zpracovanými a uloženými daty pomocí atributů, metrik a dalšími proměnnými.

**Podpora cloudu**

Partneři a zákazníci mají nově možnost nasadit Mendel do cloudového prostředí s využitím našeho předpřipraveného ISO souboru. S plnou podporou nasazení do AWS (kolektor i senzor mód) a omezeně i do Google Cloud a MS Azure (kolektor mód).

**Profilování systému pro rychlosti až 100 Gb**

Mendel nyní oficiálně podporuje 4×10Gbit na síťových kartách Intel X710, 10/25/40/100 Gbit na síťových kartách Napatech a experimentálně také síťové karty Nvidia Mellanox.

**Zjišťování podsítí**

Zjednodušení nasazení díky automatické identifikaci podsítí ve sledované infrastruktuře.

**Rozšířené nastavení dashboardů**

Přidána možnost importovat/exportovat, klonovat a přesouvat dashboardy do jiného rozložení. Přidáno textové pole s wysiwyg editorem a textová komponenta dashboardu.

**Zpracování protokolů BETA**

Možnost zpracovávat přijaté protokoly (logy) a generovat z nich bezpečnostní události (částečně pasivní přístup pro protokoly přijaté systémem Mendel na specifickém portu).

## FUNKCE OT/ICS/SCADA

Asset Discovery jako součást systému Mendel nebo jako samostatná aplikace BETA

Zobrazení CVE pro zranitelná OT aktiva BETA

Implementace OT/ICS parserů založených na protokolech Siemens S7 a OPC

Implementace detekce KNX a BACnet protokolů do nástroje Asset Discovery

Přidána detekce protokolů DICOM a KNX

Karta uživatelského rozhraní zobrazující data z průmyslových sítí přejmenována na OT metriky (dříve Scada)


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

GREYCORTEX

## DALŠÍ VYLEPŠENÍ

Optimalizováno zpracování dotazů do databáze pro lepší odezvu uživatelského rozhraní

Přidán popis detekovaných služeb v dialogovém okně s informacemi o službě

Přidáno rozhraní pro nastavení proměnných IDS pravidel v UI

Přidána možnost exportovat upozornění na události do samostatných e-mailů

Přidán zásuvný modul pro zasílání e-mailů o zjištěných požadavcích na odezvu

Přidána možnost generovat aplikační data v exportu IPFIX toků

Přidána možnost vložit podsíť pro více senzorů

Přidána signatura pro detekci požadavků v rámci SMB broadcastu

Přidána podpora nových parametrů v zásuvných modulech brány firewall

Přidána možnost importu souborů csv pro importování podsítí v UI

Přidána možnost sloučení více zdrojů síťových toků

Přidána možnost zpracovávat protokol IPv4 přes tunel IPv4

Přidána podpora pro zpracování protokolu GENEVE

Přidáno zobrazení nad aplikačními daty pro IDS události

Přidána možnost sloučit přenosy z více rozhraní pro oddělené zpracování RX a TX

Vylepšené ověřování a hlášení chyb pro nové IDS signatury

Vylepšená detekce lokálních služeb u chybných toků

Vylepšený zásuvný modul pro Checkpoint firewall

Vylepšený detektor skenování ARP protokolu

Vylepšené zpracování Netflow pro škálování na vyšší rychlosti

Vylepšené filtrování v uživatelském rozhraní (automatické dokončování, číslo portu pro nedefinované služby a další)

Vylepšená detekce opakovaných skenů (koreluje běžné antivirové skeny)

Vylepšené popisy detekovaných služeb

Vylepšené hlášení událostí do externích systémů při zpracování z více senzorů

Všechna dialogová okna jsou nyní přesouvatelná

## Oficiální podpora produktů Mendel

S vydáním verze 3.8.0 bude poskytována plná servisní podpora pro verze 3.8.x a 3.7.x. Podpora pro verzi 3.6.x bude s omezeními. Verze 3.5.x a starší již podporovány nejsou. Koncovým uživatelům s platnou podporou a údržbou nebo aktivním předplatným software doporučujeme přejít na podporovanou verzi (verze).

### Důležité upozornění

Upgrade na verzi 3.8.0 upravuje jádro systému (kernel) a povede k vynucenému restartu zařízení. Doporučujeme mít přímý nebo vzdálený přístup k zařízení, aby bylo možné jej v případě potřeby restartovat.

Pokud používáte samostatnou aplikaci „Greycortex Upgrade Proxy“ jako náhradu přístupu k aktualizačnímu serveru, je třeba nejprve aktualizovat toto proxy řešení na nejnovější verzi, aby byla dostupná řádná aktualizace produktu Mendel na poslední verzi (3.8.0).


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