RELEASE 5.0 | SRPEN 2026

GREYCORTEX Mendel 5.0

HLAVNÍ FUNKCE

01 Mapa toků (Traffic Flow Map)

Mapa toků využívá vizualizaci zaměřenou na hosta (**host-centric**) a umožňuje rychlé prošetření **síťové komunikace jednoho interního hosta**. Pomáhá analytikům rychle pochopit, s jakými protistranami host komunikuje, v jakém směru a v jakém rozsahu.

Mapa vychází z jednoho interního hosta a zobrazuje jeho nejvýznamnější protistrany ve zvoleném časovém okně. Ve výchozím nastavení je výběr protistran a zvýraznění v grafu založeno na počtu toků, analytik však může podle kontextu vyšetřování přepnout metriku na pakety, objem dat, retransmise nebo nezodpovězené toky. Z libovolného vybraného uzlu lze zobrazení rozšířit a procházet komunikační cesty krok za krokem.

Detaily o hostovi a komunikaci jsou viditelné přímo v mapě. Najetím na uzel se zobrazí informace o IP adrese, najetím na hranu detaily komunikace mezi propojenými hosty. Kliknutím na hranu se otevře další okno s podrobnostmi o komunikaci pro bližší prozkoumání.

KLÍČOVÉ MOŽNOSTI

- Přehled komunikace zaměřený na jednoho hosta
- Automaticky zvolený nebo uživatelem zadaný vstupní host (entry host)
- Postupné rozšiřování z vybraných uzlů
- Komunikace prioritizovaná a zvýrazněná podle zvolené metriky
- Podporované metriky: toky, pakety, data, retransmise, procento nezodpovězených toků a absolutní počet nezodpovězených toků
- Výchozí zobrazení podle počtu toků
- Směrové hrany a rozlišení neúplných toků
- Najetí na uzel zobrazí detaily IP adresy
- Najetí na hranu zobrazí detaily komunikace
- Kliknutí na hranu otevře podrobné informace o komunikaci
- Podpora přiblížení, posunu a filtrů

02 AI asistent (AI Assistant)

AI asistent poskytuje vysvětlení generovaná umělou inteligencí pro interní IP adresy, externí IP adresy a bezpečnostní události, a pomáhá tak analytikům **interpretovat role zařízení**, **reputaci IP adres** a kontext události ve strukturovaném, srozumitelném jazyce. U bezpečnostních událostí pracuje asistent na dvou úrovních: **Vysvětlit událost** (*Explain event*) poskytuje kontext k samotné události, zatímco **Vyšetřit událost** (*Investigate this event*) analyzuje konkrétní komunikaci v kontextu konkrétního hosta a vrací strukturované posouzení. Obě akce jsou dostupné u detekcí Network Behavior Analysis, IDS, Log Processing a UnTE; nejsou dostupné u událostí System Monitoring.

Analýza interních IP adres identifikuje pravděpodobnou roli zařízení na základě dostupného kontextu hosta, jako jsou metadata vrstvy 7 (*Layer 7*), názvy hostů, tagy, MAC adresy a pozorované služby. **Analýza externích IP adres** vyhodnocuje reputaci a klasifikuje adresy jako škodlivé, podezřelé, související s průzkumem (*reconnaissance*), neškodné, pravděpodobně neškodné nebo neznámé. **Vysvětlení události** shrnuje, co se stalo, proč je to důležité, jaký je relevantní kontext MITRE ATT&CK a jaké jsou doporučené následné provozní kroky, a obsahuje také postup, jak ověřit, zda nejde o falešně pozitivní hlášení.

Vyšetřit událost (*Investigate this event*) provádí hlubší analýzu jedné konkrétní komunikace v kontextu daného hosta. Kromě vysvětlení poskytuje posouzení: verdikt, relevanci a míru jistoty detekce a odhadovanou pravděpodobnost falešně pozitivního hlášení, vždy s uvedením odůvodnění. Odděluje pozorovaná fakta od možných interpretací, uvádí, co dostupná data nedokazují, vypisuje doporučené kroky vyšetřování v pořadí podle priority a tam, kde je to vhodné, navrhuje úzce vymezenou výjimku omezenou na konkrétní signaturu, zdroj, cíl a směr komunikace.

Jazyk výstupu AI lze nastavit nezávisle na jazyce uživatelského rozhraní a asistent podporuje angličtinu, češtinu, němčinu a polštinu. Funkci lze globálně zapnout nebo vypnout. Obsahuje upozornění při prvním použití týkající se zpracování externí AI službou a umožňuje zpětnou vazbu palcem nahoru/dolů pro sledování kvality. Tato nastavení platí pro AI asistenta jako celek, bez ohledu na to, která funkce výstup generuje.

KLÍČOVÉ MOŽNOSTI

- Identifikace role zařízení u interních IP adres
- Vyhodnocení reputace externích IP adres
- Vysvětlení bezpečnostní události a doporučené následné kroky
- Dvě úrovně analýzy události: Vysvětlit událost (*Explain event*) pro kontext, Vyšetřit událost (*Investigate this event*) pro posouzení v kontextu hosta
- Dostupné u detekcí Network Behavior Analysis, IDS, Log Processing a UnTE; nedostupné u událostí System Monitoring
- Postup pro ověření, zda jde o falešně pozitivní hlášení
- Verdikt události s relevancí detekce, mírou jistoty detekce a posouzením reálnosti v daném prostředí
- Odhadovaná pravděpodobnost falešně pozitivního hlášení včetně odůvodnění
- Jasné oddělení pozorovaných faktů od možných interpretací
- Doporučené kroky vyšetřování v pořadí podle priority
- Návrh úzce vymezené výjimky omezené na signaturu, zdroj, cíl a směr komunikace
- Provozní doporučení pro následnou úpravu konfigurace nebo omezení komunikace
- Využití kontextu hosta, metadat vrstvy 7, tagů, MAC adres a informací o službách
- Kategorie reputace pro externí IP adresy: škodlivá, podezřelá, průzkumná (*reconnaissance*), neškodná, pravděpodobně neškodná a neznámá
- Vysvětlení běžným jazykem, co se stalo a proč je to důležité
- Vysvětlení kontextu MITRE ATT&CK tam, kde je to relevantní
- Zvýraznění klíčových technických indikátorů
- Vícejazyčný výstup AI: angličtina, čeština, němčina a polština
- Nastavení jazyka AI nezávislé na jazyce uživatelského rozhraní
- Globální nastavení zapnutí/vypnutí AI asistenta
- Upozornění při prvním použití týkající se zpracování externí AI službou
- Označení výstupu vygenerovaného AI
- Zpětná vazba k užitečnosti palcem nahoru/dolů

03 Nové risk skóre a jeho vizualizace (Risk Score)

Přepracovaný model hodnocení rizika založený na hostech pomáhá analytikům rychleji **identifikovat nejrizikovější hosty**. Nové skóre nahrazuje předchozí výpočet jednotným, normalizovaným modelem založeným na bezpečnostních událostech souvisejících s hostem a přináší konzistentní vizualizaci rizika napříč celým uživatelským rozhraním.

Riziko se počítá z událostí souvisejících s hostem, z jedinečnosti v rámci podsítě a z aktuálnosti závažné aktivity. Starší signály se v čase oslabují díky historickému doznívání (*historical fading*), zatímco nedávné a relevantní problematické chování riziko zvyšuje. **Skóre se ukládá v čase**, což analytikům umožňuje sledovat trendy a chápat, jak se riziko hostů vyvíjí.

Risk skóre (*Risk Score)* je oddělené od závažnosti události a používá vlastní vizuální indikátor s číselným skóre a rizikovými pásmy. Informace o riziku se zobrazují na dashboardech, v přehledu Hosty podle rizika (*Hosts by Risk)*, v Dialogu hosta (*Host Dialog*) a na stránce hosta (*Host page*), včetně trendů, souvisejících událostí

a souvisejícího kontextu.

KLÍČOVÉ MOŽNOSTI

- Nové normalizované risk skóre na úrovni hosta
- Výpočet rizika na základě událostí
- Zohlednění jedinečnosti v rámci podsítě a aktuálnosti závažné aktivity
- Historické doznívání starších rizikových signálů
- Vlastní vizuální indikátor odlišný od závažnosti události
- Riziková pásma od Bez rizika (*No Risk*) po Kritické riziko (*Critical Risk*)
- Historie rizika a vizualizace trendu
- Tabulka Hosty podle rizika (*Hosts by Risk*) a dashboardy Hlavní, Přehled, Rizika a další
- Detaily rizika v dialogu hosta (*Host Dialog*) a na stránce hosta (*Host page*)
- Filtrování podle rozsahu skóre nebo rizikového pásma

ROZSAH RISKOVÉHO SKÓRE

Skóre	Pásmo
1–19	Bez rizika (No Risk)
20–49	Nízké riziko (Low Risk)
50–69	Střední riziko (Medium Risk)
70–89	Vysoké riziko (High Risk)
90–99	Kritické riziko (Critical Risk)

04 Přepracovaný dialog hosta (Host Dialog)

Dialog hosta byl přepracován tak, aby uživatelům poskytoval přehlednější pohled na interní i externí hosty, více zaměřený na vyšetřování. Stránka Summary nyní přehledněji zobrazuje identitu hosta, podsíť, senzor, název hosta, MAC adresu, čas objevení, riziko, tagy a související kontext.

U interních hostů dialog obsahuje nové zobrazení rizikového skóre a vylepšenou reprezentaci tagů včetně časového kontextu. U externích hostů se rozvržení zaměřuje na identitu IP adresy, název hosta, reputaci, vlastnictví sítě a relevantní akce pro vyšetřování.

Přeorganizovány byly také běžné akce. Analytici mohou využít vylepšené možnosti Filtrovat hosta (*Filter host*) pro IP adresu, podsíť a název hosta s logikou set, OR a NOT. Výběr senzoru nyní podporuje vyhledávání a zobrazuje objem pozorovaného provozu, což analytikům pomáhá pochopit, který senzor hosta detekoval a kolik provozu zaznamenal.

KLÍČOVÉ MOŽNOSTI

- Přepracovaný Dialog hosta (*Host Dialog*) pro interní i externí hosty
- Reorganizovaná stránka Shrnutí (*Summary*) s přehlednějším kontextem hosta
- Nové zobrazení rizikového skóre u interních hostů
- Vylepšená reprezentace tagů s časovým kontextem
- Vyhledávatelný výběr senzoru s informací o objemu provozu
- Reorganizovaná tlačítka akcí
- Vylepšené možnosti Filter host pro IP adresu, podsíť a název hosta
- Podpora filtrovací logiky set, OR a NOT
- Aktualizovaný vizuální design

05 Historie tagů a časová reference (Tag History)

Práce s tagy byla přepracována tak, aby podporovala historické sledování přiřazení tagů. Tagy již nejsou chápány pouze jako aktuální atribut hosta – Mendel nyní ukládá, kdy byly tagy přiřazeny, aktualizovány nebo odebrány, včetně jejich zdroje, je-li dostupný.

Analytici si mohou prohlédnout historii tagů pro hosty a identity, filtrovat pomocí tagů platných ve zvoleném časovém intervalu a rozlišovat zdroje tagů, jako jsou uživatelské akce, detekční logika, pravidla UnTE, shody s pravidly modulu pro zachytávání síťového provozu nebo externí importy.

Zpracování tagů na backendu bylo rovněž sjednoceno a refaktorováno pro zlepšení spolehlivosti, práce s API a dlouhodobé udržovatelnosti.

KLÍČOVÉ MOŽNOSTI

- Historické sledování přiřazení tagů
- Čas přiřazení, aktualizace a odebrání tagů
- Viditelnost zdroje tagu
- Historie tagů pro hosty a identity
- Filtrování tagů podle času
- Jednotný model ukládání tagů
- Vylepšené zpracování na úrovni API a backendu
- Lepší podpora auditu, řešení problémů a reportingu

06 Detekce neaktivních a ztracených hostů (Inactive and Lost Host Detection)

Detekce neaktivních hostů zavádí nový mezistav v životním cyklu hosta, který hlásí, že host přestal komunikovat. Analytici tak získají čas na prošetření dříve, než je host trvale odstraněn.

Zůstane-li host neaktivní po nastavenou dobu nečinnosti, systém vygeneruje událost **Neaktivní host** (*Inactive Host*) a zároveň zachová všechny informace o hostovi. Pokud se host neobjeví znovu před vypršením nastavené lhůty (*lease time*) pro **Ztraceného hosta** (*Lost Host*), stávající politika vygeneruje událost Ztracený host a hosta i související informace trvale odstraní.

Dočasná ztráta komunikace je nyní oddělená od trvalého odstranění hosta, což poskytuje dřívější přehled o mizejících hostech při zachování automatického úklidu životního cyklu hostů.

KLÍČOVÉ MOŽNOSTI

- Nová detekce neaktivních hostů (*Inactive Host Detection*)
- Konfigurovatelná doba pro detekci nečinnosti
- Včasné upozornění, když se host stane neaktivním
- Stávající politika Ztracený host (*Lost Host*) pro trvalé odstranění hosta
- Konfigurovatelná lhůta (*lease time*) pro Ztracený host
- Automatický úklid po delší nečinnosti
- Jasné oddělení stavů neaktivní a ztracený host
- Chování politiky Ztracený host ve variantách Allowed / Not allowed
- Vylepšené vysvětlení životního cyklu hosta v uživatelském rozhraní

DŮLEŽITÉ TECHNICKÉ ZMĚNY

Upgrade a modernizace platformy

Mendel nyní běží na upgradované platformě operačního systému s novějším jádrem a aktualizovanými základními komponentami, což zlepšuje celkovou bezpečnost, stabilitu a dlouhodobou udržovatelnost.

- Upgradovaná platforma operačního systému
- Novější linuxové jádro založené na CentOS Stream 9
- Bezpečnostní aktualizace a opravy zranitelností
- Vyšší stabilita a spolehlivost systému
- Moderní základ platformy pro budoucí rozšíření

Upgrade IDS enginu

IDS engine byl upgradován na nejnovější generaci, což zlepšuje výkon detekce, rozšiřuje pokrytí protokolů a poskytuje moderní základ pro budoucí rozšíření.

- Upgradovaný IDS engine
- Vyšší výkon detekce
- Rozšířená podpora protokolů, včetně LDAP, mDNS, SIP/SDP, ENIP a FTP
- Rozšířené možnosti pravidlového enginu (podpora VLAN)
- Lepší udržovatelnost a dlouhodobá podpora platformy

Vylepšení Status Monitoru

Subsystém Status Monitor byl výrazně vylepšen, aby poskytoval spolehlivější monitorování služeb a konzistentnější hlášení stavu systému.

- Spolehlivější monitorování stavu služeb
- Konzistentnější detekce a hlášení výpadků
- Vyšší stabilita systému
- Snazší diagnostika a řešení problémů
- Snížení technického dluhu
- Moderní základ pro budoucí vylepšení platformy

Vylepšený administrátorský přístup

Administrátorská oprávnění jsou nyní spravována prostřednictvím role Admin, což snižuje závislost na výchozím administrátorském účtu a zvyšuje celkovou bezpečnost.

- Role Admin pro administrátorské úkony
- Nižší závislost na výchozím administrátorském účtu
- Povinná změna hesla po nasazení
- Vyšší bezpečnost při předávání zákazníkovi
- Lepší správa přístupu na základě rolí

Detekce AI služeb

Mendel nyní detekuje a klasifikuje AI služby v síťovém provozu, což poskytuje lepší přehled o využívání AI aplikací v monitorovaných prostředích.

- Detekce síťového provozu souvisejícího s AI
- Klasifikace AI služeb v síťových tocích
- Lepší přehled o využívání AI aplikací
- Podpora bezpečnostních politik organizace
- Rozšiřitelný rámec pro nově vznikající AI služby

Vylepšená detekce operačních systémů

Fingerprinting operačních systémů byl zpřesněn, aby zlepšil přesnost identifikace zařízení a spolehlivost klasifikace hostů.

- Přesnější detekce verzí systému Windows
- Vylepšená identifikace zařízení s Androidem
- Méně falešně pozitivních výsledků
- Spolehlivější klasifikace hostů
- Vylepšený fingerprinting operačních systémů

Korelace identit z Entra ID

Mendel nyní koreluje události přihlášení a odhlášení z Microsoft Entra ID s monitorovanými hosty, což poskytuje dodatečný kontext identity pro bezpečnostní vyšetřování.

- Automatická korelace přihlášení a odhlášení v Entra ID
- Propojení uživatele se zařízením
- Lepší kontext pro vyšetřování
- Rozšířené možnosti auditu
- Lepší přehled o identitách v síti

Viditelnost rozhraní v NetFlow

Záznamy NetFlow mohou nyní obsahovat logické názvy vstupních a výstupních rozhraní hlášené síťovými zařízeními, což poskytuje dodatečný kontext pro analýzu provozu.

- Logické názvy vstupních a výstupních rozhraní ukládané spolu s toky
- Metadata o rozhraních dostupná při analýze
- Lepší přehled o provozu
- Rozšířené možnosti vyšetřování v NetFlow
- Ověřeno v produkčním provozu se zařízeními KB

Zálohovací úložiště kompatibilní s S3

Zálohovací úložiště nyní podporuje objektová úložiště kompatibilní s S3, což přináší větší flexibilitu nad rámec nasazení s Amazon S3.

- Podpora objektových úložišť kompatibilních s S3
- Kompatibilita se standardními implementacemi S3 API
- Větší flexibilita nasazení
- Podpora on-premises objektových úložišť
- Zjednodušená konfigurace záloh

DALŠÍ VYLEPŠENÍ

Různá vylepšení každodenního provozu, použitelnosti platformy a celkové uživatelské zkušenosti.

- Nové UnTE tagy pro vrstvu 7 (Layer 7)
- Informace o kompatibilitě pluginů
- Aktualizované pojmenování profilů
- Vylepšení uživatelského rozhraní a použitelnosti
- Různá vylepšení stability a výkonu

OFICIÁLNÍ PODPORA PRODUKTU GREYCORTEX MENDEL

S vydáním verze 5.0.0 je **plná podpora poskytována pro verze 5.0.x a 4.6.x** a základní podpora pro verzi 4.5.x.

Verze 4.4.x a starší již nejsou podporovány.

Koncovým uživatelům s platnou podporou a údržbou nebo s aktivním softwarovým předplatným důrazně doporučujeme upgrade na některou z podporovaných verzí.