GREYCORTEX Mendel 4.5

Hlavní funkce

Přepracovaná správa uživatelů a integrace identit

Kompletně přepracovaná práce s nastavením přístupu uživatelů a jejich oprávnění. Integrace s identitními službami v síťové infrastruktuře — například s Active Directory.

- Centralizované řízení přístupu uživatelů přes stávající poskytovatele identity
- Onboarding a offboarding s autentizací vůči identitním službám
- Granulární správa oprávnění v souladu s rolemi ve vaší organizaci
- Podpora jednotného přihlášení (SSO) a vícefaktorové autentizace (MFA)

Tyto změny zvyšují bezpečnost, zjednodušují administraci a zajišťují, že přidání nového uživatele je v plném souladu s vašimi procesy a infrastrukturou.

Předzpracovaná data pro dashboard

Na dashboard můžete definovat nové komponenty z předzpracovaných dat. Tím získáte ihned dostupné dashboardy založené na předzpracované síťové analýze, generované automaticky z uložených metadat — důležité informace tak máte okamžitě k dispozici.

Výhodou je rychlejší analýza incidentů díky okamžitému přístupu ke klíčovým vzorcům chování v síti a nižší zátěž systému díky předzpracovaným datům, které se použijí pro síťové analýzy.

Vysoká dostupnost (High Availability)

Plná ochrana a provozní kontinuita díky redundanci dat a vylepšenému nastavení vašich zařízení. Dva možné režimy dle komplexnosti sítě zajistí průběžnou synchronizaci konfigurace, detekčních pravidel a zachycených síťových dat na sekundární jednotku. V případě výpadku záložní systém plynule převezme provoz bez ztráty aktuálních a historických dat. Používání systému není přerušeno.

Detektor pro poprvé viděnou komunikaci

Nový detektor označí dosud neviděnou komunikaci mezi dvěma peery. Upozorní na první výskyt jakéhokoli příchozího či odchozího spojení. Je vhodné jej používat selektivně na částech systému, kde nová komunikace není primárně vítaná a může značit problém (např. řadiče domény, DNS servery, OT prostředí).

Další funkce

Rozšířené možnosti zálohování

- Hitachi HCP a AWS S3
- Místní záloha/obnovení nastavení na USB nebo na připojené síťové úložiště

Viditelnost do provozu Kubernetes — fáze 1

Monitoring a analýza vašich prostředí Kubernetes v cloudu i on-premise řešení. Získejte plnou viditelnost do east-west provozu mezi pody a službami. Detekujte anomálie napříč mikro službami a odhalte hrozby skryté uvnitř kontejnerizované infrastruktury.

Přepracovaná upozornění událostí v reálném čase

Vylepšený engine pro hlášení událostí v reálném čase je nově navržen pro vyšší rychlost, srozumitelnost a akce schopnost. Bezpečnostní události doručujeme v reálném čase s vylepšeným obsahem, chytrou kategorizací a prioritními upozorněními, aby váš tým mohl reagovat ve chvíli, kdy hrozba vznikne.

Ochrana proti obrovskému množství toků (DDoS a skenery)

Nově zabudovaná ochrana proti DDoS útokům nebo skenování udržuje Mendel rychlý i ve chvíli, kdy jedna IP adresa začne generovat či přijímat mimořádně velký počet toků. Systém automaticky agreguje nárazový provoz do souhrnných událostí, takže zůstává plná viditelnost bez ukládání milionů téměř totožných záznamů.

GREYCORTEX Mendel 4.5

Vylepšení

- Povoleno spojení Senzor–Kolektor přes systémová rozhraní
- Systémové rozhraní přijímá a odpovídá na ICMP (echo) pakety
- Prohazování směru toku na základě heuristik z modelu sítě
- Rozpoznání provozu podnikových zálohovacích řešení
- Detekujeme služby pro sdílení souborů jako aplikace
- BPF filtrování na úrovni rozhraní pro přesnější sběr dat
- Přidána podpora JA4
- Přesnější detekce verzí operačních systémů Windows
- Možnost ignorovat NTP server
- Zpracování ERSPAN verze 2, typ III
- Hostname jako výchozí volba pro False positive
- Signatury pro polský osobní identifikátor (PESEL)

Korelace událostí — migrace na UnTE

Původní korelační engine událostí byl odstraněn. Všechna jeho pravidla byla přepsána a přesunuta do vylepšeného UnTE enginu, který přináší lepší filtrování, seskupování a deduplikaci událostí — méně šumu a jasnější kontext.

Vylepšení UI & UX

Neustále zlepšujeme uživatelské rozhraní pro jeho lepší použitelnost tak, aby detekce hrozeb i jejich řešení byly rychlejší, přehlednější a intuitivnější. Novinky:

- Přepracovaná stránka Správce filtrů a předdefinované filtry
- Možnost povolit/zakázat podporu karet Napatech v UI
- Zobrazení rizika hosta v grafu topologie
- Přidány metriky do grafu peerů
- Zobrazení odpovídající OS ikony pro konkrétní OS systémy
- Import False positives
- Import IDS proměnných
- Export politik/podsítí/hostů v nastavení
- Přidání komentářů do reportů incidentů (PDF)
- Přidání komentářů do exportu incidentů
- Export podsítí do .csv kompatibilní s importem podsítí
- Vylepšená nápověda k pokročilým filtrům
- Aktualizovaný glosář pro vyhledávání v nastavení ME
- Možnost vypnout kontrolu podpisu pluginu
- Optimalizace prostoru v grafu peerů ve FullHD
- Drobná vylepšení v Manažerských a bezpečnostních reportech
- Ikony ve správě tagů
- Přesnější vyhledávání v nastavení

A další přepracování:

- Dialog zálohy Samba přepracován na dynamický dialog
- Refaktorované stránky: EM, FP, UNTE, NBA, IDS
- Dialog pro sdílený odkaz přepracován na dynamický dialog
- Dialog whois přepracován na dynamický dialog
- Dialog společnosti přepracován na dynamický dialog
- Dialog pluginu přepracován na dynamický dialog
- Dialog stažení systémových logů přepracován na dynamický dialog
- Lepší oddělení popisku ikony od tlačítka
- DataTable: přidán atribut „lazy“ pro odložené načítání dat
- Implementován dynamický dialog pro nahrání certifikátu

GREYCORTEX Mendel 4.5

OT

Rozšířené informace v inventáři hostů a zařízení

Zvýšení viditelnosti v síti díky doplnění externích provozních dat. Spojením bezpečnostních událostí v reálném čase s rozšířenými informacemi o zařízeních v síti získáte hlubší kontext pro každou situaci, rychlejší analýzu příčin, chytřejší prioritizaci a méně zbytečných upozornění. Máte možnost využít ručně či automaticky přidaných dat a tagů ke každému zařízení v síti a svá rozhodování podepřít o vylepšený monitoring událostí.

Přidána podpora nových OT protokolů

- DICOM – parser protokolu
- HL7 – parser protokolu
- Ether-S-Bus – parser protokolu
- PROFINET Realtime (PN-IO) – detekce

Vylepšení OT protokolů

- LLDP – rozšíření parseru o schopnosti MED (LLDP-MED)
- SIP – vylepšení protokolu
- ICCP – podpora uvnitř parseru MMS
- PROFINET – sjednocené pojmenování služeb
- PROFINET over DCE/RPC – vylepšení parseru
- PROFINET – alarmové zprávy služby PN-IO-RT
- PROFINET DCP – vylepšení parseru
- PROFINET – acyclic Real Time, rozšířená detekce PN-PTCP
- OPC/UA – vylepšení parseru protokolu pro funkce
- IEC-104 – vylepšená detekce a parsování
- IEC-104 – vylepšení OT metrik
- MODBUS – přepracované signatury

Oficiální podpora produktu GREYCORTEX Mendel

S vydáním verze 4.5.0 poskytujeme plný servisní support pro verze 4.5.x a 4.4.x.

Verze 4.3.x a starší již nejsou podporované. Koncovým uživatelům s platným supportem a údržbou nebo s aktivním softwarovým předplatným důrazně doporučujeme přejít na jednu z podporovaných verzí.