GREYCORTEX Mendel 4.6

Hlavní funkce

Historie názvů hostů (Hostname History)

Mendel zobrazuje přehled všech změn názvů hostů v jejich historii. Tyto názvy jsou shromažďovány z více zdrojů, jako jsou DNS, mDNS, NetBIOS, DHCP a TLS SNI, a soustředěny na jednom místě. Data jsou zobrazena v rámci časové osy hosta, díky čemuž mohou analytici sledovat vývoj názvu zařízení v čase, odhalovat změny identity a propojovat související aktivity i v případech, kdy se změní IP adresa nebo název daného zařízení.

Historické názvy hostů lze nyní vyhledávat, filtrovat a třídit, což díky přehlednému zobrazení umožňuje lepší porozumění chování hostů a jejich vztahů v síti.

Jak to funguje

- Mendel agreguje informace o názvech hostů z více zdrojů: DNS, DHCP, NetBIOS, mDNS a TLS SNI.
- Každý zjištěný název hosta je spolu s časovým údajem a informací o zdroji uložen do databáze hosta.
- Historické názvy hostů lze zobrazit, filtrovat a vyhledávat v přehledu v detailu hosta.
- Propojení v časové ose umožňuje analytikům sledovat změny identity hosta v průběhu času a lépe porozumět jeho aktivitám.

Vylepšený přehled o síti díky strukturovaným metadatům

Přehled o síťovém provozu je rozšířen systematickým zpracováním metadat aplikační vrstvy, která jsou dostupnější pro další analýzu. Klíčové informace o používaných protokolech jsou extrahovány a ukládány do samostatné struktury, což analytikům umožňuje rychleji a přesněji porozumět chování zařízení v síti.

Díky komunikačním vzorcům lze snáze rozlišit role jednotlivých zařízení, například tiskárny, DNS servery nebo uživatelské stanice. Rozpoznatelné vlastnosti zařízení urychlují jejich identifikaci, poskytují lepší kontext pro detekce a pomáhají lépe porozumět celkové síťové aktivitě.

Jak to funguje

- Metadata aplikační vrstvy jsou získávána z monitorovaného síťového provozu a ukládána do samostatné datové struktury.
- Dříve skryté informace z aplikační vrstvy jsou nyní dohledatelné, propojitelné s konkrétními hosty a využitelné při analýze.
- Důraz je kladen na identifikaci významných vlastností protokolů, které odhalují typ zařízení a jeho chování v síti.
- Data jsou získávána z IT i OT protokolů, například SNMP, SMB, DHCP, mDNS, HTTP nebo TLS.
- Na základě těchto metadat systém automaticky vytváří značky zařízení.
- Uživatelé si mohou nadefinovat svoje UnTE pravidla nad těmito metadaty pro vytváření svých vlastních značek.

Modul pro nahrávání a analýzu síťového provozu

Vylepšený modul pro nahrávání a analýzu síťového provozu sjednocuje dosavadní funkce sběru dat a analýzy PCAP souborů do jednoho přehledného místa. Uživatelé mají k dispozici záznamy provozu ze všech připojených senzorů, mohou je přímo přehrávat a analyzovat bez nutnosti přecházet mezi různými nástroji nebo provádět zbytečné kroky navíc.

Vylepšené ovládání, přehlednější uspořádání rozhraní a nové možnosti řízení přehrávání zvyšují komfort práce a zefektivňují analytické postupy. Modul zároveň vytváří základ pro další rozvoj pokročilé analýzy síťového provozu v prostředích IT i OT.

Jak to funguje

- Veškeré funkce související se záznamem a analýzou síťového provozu jsou nyní dostupné v jednom společném pracovním prostoru.
- Mendel se přímo připojuje k senzorům a získává z nich nahraná data.
- Uživatelé mohou provoz přehrávat přímo na senzoru nebo analyzovat již uložené záznamy podle potřeby.
- Nová funkce pro zastavení přehrávání umožňuje kdykoli ukončit probíhající zpracování dat.

Rozšíření podpory identity protokolů (SAML a SSO)

Mendel rozšiřuje podporu správy identity o protokol SAML, který doplňuje stávající možnosti ověřování pomocí LDAP, Kerberos a OAuth. Díky tomu lze Mendel snadno integrovat do podnikového prostředí s jednotným přihlašováním (SSO) a využít centrální správu uživatelských účtů.

Uživatelské rozhraní pro nastavení autentizace bylo přepracováno s důrazem na přehlednost a snadnější konfiguraci. Nové rozbalovací sekce, rozšířené volby a rychlé přihlášení pomocí OAuth2 zjednodušují práci správcům i koncovým uživatelům. Zároveň je možné upravovat nastavení autentizačních domén bez nutnosti znovu vytvářet celou konfiguraci. Podpora oprávnění založených na OAuth2 dále zvyšuje kompatibilitu, bezpečnost a použitelnost v podnikových identitních systémech.

Jak to funguje

- Podpora ověřování a autorizace pomocí protokolu SAML pro webový přístup.
- Možnost propojení s externími poskytovateli identity pro bezpečné jednotné přihlášení (SSO).
- Přepracované dialogy nastavení autentizace s rozbalovacími sekcemi a pokročilými volbami.
- Rychlé přihlášení pomocí OAuth2 pro zjednodušení přístupu přes federované identity.
- Možnost upravovat autentizační doménu bez nutnosti vytvářet novou konfiguraci.

Licenční podmínky a uživatelské role

Mendel nově vyžaduje, aby každý uživatel při prvním přihlášení samostatně potvrdil licenční podmínky (EULA). Souhlas je tak jednoznačně svázán s konkrétním uživatelským účtem, nikoli pouze s instalací systému. Tento přístup zvyšuje přehlednost, odpovědnost a splnění licenčních a interních požadavků.

Došlo k jasnému oddělení systémových rolí. Administrátorské a supportní účty slouží výhradně ke správě a údržbě systému, zatímco běžní uživatelé pracují se systémem pod svými osobními účty při každodenní analýze a práci. Pokud je administrátorský účet používán pro běžnou práci, systém na to upozorní a doporučí přepnutí na osobní účet. Tím se zlepšuje dohledatelnost činností, bezpečnost a oddělení odpovědností.

Jak to funguje

- Při instalaci nebo aktualizaci systému je vyžadováno potvrzení licenčních podmínek koncovým uživatelem.
- Administrátorské a supportní účty slouží pouze ke správě systému a nemohou licenční podmínky potvrzovat.
- Pro běžnou práci, jako je analýza nebo konfigurace, jsou určeny osobní uživatelské účty.
- Použití administrátorského účtu pro každodenní činnosti vyvolá upozornění s výzvou k přepnutí na osobní účet.
- Všechny kroky související s licenčními podmínkami jsou zaznamenány a dohledatelné pro účely auditu.

GREYCORTEX Mendel 4.6

Mechanismus pro sdílení statistik pro účely vylepšení Threat Intelligence

Mendel zavádí bezpečný mechanismus pro sdílení anonymizovaných provozních informací, který napomáhá zvyšovat kvalitu detekcí a rozvíjet Threat Intelligence. Agregovaná a anonymní data z reálných nasazení slouží k výzkumu, zpřesňování detekčních modelů a lepší ochraně proti novým typům hrozeb.

Přenos dat probíhá výhradně v zabezpečené podobě, je přísně omezený a aktivuje se pouze na základě výslovného souhlasu uživatele v rámci potvrzení licenčních podmínek. Celý proces je navržen s důrazem na ochranu soukromí, transparentnost a bezpečnost.

Jak to funguje

- Pravidelně dochází ke sdílení anonymizovaných statistik o detekcích a síťové komunikaci pro účely vylepšení Threat Intelligence.
- Přenos dat v strukturované podobě prostřednictvím zabezpečeného spojení.
- Bezpečné a škálovatelné zpracování dat v cloudovém úložišti.
- Interní analytické nástroje využívají agregovaná data ke zlepšení detekcí, pokrytí hrozeb a stability systému.
- Sdílení dat je dobrovolné a aktivuje se pouze po schválení uživatelem v rámci potvrzení licenčních podmínek.

Hardwarový bypass Napatechu se zachováním toků

Vysoce výkonné senzory vybavené adaptéry Napatech nyní mohou využít vylepšený hardwarový bypass, který zachovává informace o tocích a zároveň snižuje zátěž procesoru. Tato úprava cílí na rozsáhlá prostředí (např. linky nad 50 Gbit/s), kde dosavadní plný hardwarový bypass vedl k neúplným datům o tocích a omezené viditelnosti.

Nový režim umožňuje v případě nedostatku prostředků přeskočit hlubokou inspekci dat, aniž by došlo ke ztrátě klíčových informací o komunikaci. Zachována zůstává velikost toků, časování i důležitá metadata, což zajišťuje správný kontext detekce i při omezené hloubce analýzy.

Jak to funguje

- Přibývají dvě nové volby nastavení na úrovni senzoru:
  - **Hardware Stream Bypass** – vynechá payload, ale zachová vlastnosti toku (délku, objem dat, koncové body).
  - **Hardware TLS Bypass** – vynechá zpracovávání šifrovaného provozu při zachování TLS metadat.
- Nové nastavení umožňuje hardwarový bypass zcela vypnout pro testovací nebo záložní scénáře.
- Konfigurační rozhraní senzoru nyní obsahuje dvě nová zaškrtávací pole vedle stávající volby Stream Bypass.
- Změny se projeví po restartu senzoru nebo znovunačtení konfigurace.

Aktualizovaná integrace Zabbixu pro Asset informace

Integrace se systémem Zabbix byla aktualizována tak, aby využívala novou strukturu tagu pro Asset informace, představenou ve verzi 4.5. Díky tomu je správa hostů i jejich vizualizace přehlednější a jednotnější.

Data získaná ze Zabbixu – například výrobce, model, verze firmwaru nebo typ zařízení – se nyní přímo mapují na standardizované tagy v Mendel. To poskytuje jasnější a konzistentní pohled na síťová aktiva.

Integrace nadále funguje v režimu pouze pro zobrazení, podobně jako konektor SentinelOne. Získaná data se zobrazují v detailu hosta bez dalšího ukládání nebo filtrování. Výsledkem je lepší sladění externích inventářů s interní reprezentací aktiv v Mendelu a jednodušší základ pro další rozšiřování přehledu o IT i OT prostředí.

GREYCORTEX Mendel 4.6

Aktualizace frameworku OpenAppID

Mendel byl aktualizován tak, aby podporoval nejnovější verzi frameworku OpenAppID používanou v aktuálních detekčních signaturách. Díky tomu systém spolehlivě rozpoznává a klasifikuje aplikace i protokoly podle nejnovějších pravidel detekce.

Aktualizace rozšiřuje schopnost identifikovat nové vzorce chování aplikací a reagovat na změny v aplikační vrstvě sítě. Součástí jsou i nejnovější signatury, které zvyšují rozsah pokrytí a celkovou přesnost detekce.

Tím je zajištěna dlouhodobá kompatibilita s vyvíjejícími se znalostmi o hrozbách a analytici získávají lepší podklady pro včasnou a efektivní reakci na nové typy aplikačních útoků.

Vylepšení

Defaultní atributy pro export dat e-mailem

Exporty dat odesílané e-mailem nyní automaticky obsahují předdefinovanou sadu klíčových atributů. Součástí defaultního nastavení jsou důležité analytické a kontextové informace, jako je časový tag, identifikace zdroje a cíle, závažnost nebo kategorie MITRE. Díky tomu jsou exportovaná data vždy kompletní a připravená k dalšímu zpracování.

Zjednodušení nastavení a správy zdrojů toků

Proces přidávání nových zdrojů toků byl výrazně zjednodušen. Nastavení vstupů je nyní soustředěno výhradně na kolektory (nebo all-in-one zařízení), které jako jediné zpracovávají NetFlow data. Volby pro „Sensor“ byly odstraněna z uživatelského rozhraní i konfiguračních souborů a odpovídající nastavení v mshellu je deaktivováno.

Použití jednotné URL adresy v exportech

Exporty dat nyní správně využívají globálně nastavenou základní URL adresu při generování odkazů ke stažení. Dříve byly odkazy odvozeny od názvů jednotlivých senzorů, což mohlo vést k nejednotnostem v distribuovaných prostředích. Nové chování zajišťuje konzistentní a spolehlivé odkazy vhodné i pro integraci s externími nástroji a portály.

Zobrazení UUID v nastavení systému

Jedinečné identifikátory systému (UUID) jsou nově přímo viditelné v rozhraní Nastavení. UUID je zobrazen v části Nastavení → Přehled a také v Nastavení → Systém → Senzory a kolektory → [zařízení] → Licence. Tím se zjednodušuje diagnostika a odpadá nutnost zjišťovat UUID přes mshell.

Automatické předání IP adresy do služby IPVOID

Integrace se službou IPVOID byla upravena tak, aby při přesměrování automaticky předávala vybranou IP adresu. Místo obecné stránky s informacemi o vlastní IP adrese se nyní zobrazují údaje přímo k analyzované adrese z rozhraní Mendel. To urychluje práci analytiků a eliminuje nutnost ručního kopírování IP adres.

Vylepšení nápovědy a dokumentace pro Modbus

Nastavení Modbusu bylo upraveno s cílem usnadnit konfiguraci a import dat. Uživatelské rozhraní nyní nabízí jasnější pokyny a dokumentace byla rozšířena tak, aby pomohla správně definovat registry a předejít chybám v konfiguraci.

GREYCORTEX Mendel 4.6

Vylepšení uživatelského rozhraní

Návrat možnosti „vyloučit“ (exclude) u filtru tagů

Správa filtrů byla rozšířena o možnost „vyloučit“ (exclude) hosty nebo podsítě podle tagů. Analytici tak mohou přesněji cílit vyhledávání a lépe se soustředit na relevantní data při řešení incidentů. Funkce vrací operátor „vyloučit“ (exclude) pro filtry tagů a je optimalizována tak, aby neovlivňovala výkon systému.

Ikony výrobců podle MAC adres z databáze

Ikony výrobců MAC adres jsou nyní načítány přímo z databáze, nikoli ze souborového systému. Díky tomu vždy odpovídají aktuálním informacím o výrobci. Systém automaticky určí výrobce podle MAC adresy a zobrazí správnou ikonu, často používané ikony jsou navíc ukládány do mezipaměti pro rychlejší zobrazení.

Přepracovaná stránka Threat Intelligence

Stránka Threat Intelligence byla přehledně rozdělena do tří záložek pod jednou hlavní sekcí. Nové uspořádání přináší:

- dynamická okna pro přidávání a úpravy záznamů,
- pokročilé filtrování, vyhledávání a řazení,
- aktualizovaný slovník tagů pro jednotnou správu pojmů.

Přepracovaná sekce Detekce

Sekce Detekce byla sjednocena s designem ostatních částí systému. Nové uspořádání nabízí:

- filtry pro rychlý přístup k relevantním položkám,
- hromadné operace pro provádění akcí nad větším počtem záznamů,
- možnosti importu a exportu,
- přizpůsobitelné sloupce podle potřeb uživatele.

Vylepšený filtr kategorií u signatur

Filtr kategorií v nastavení signatur byl optimalizován pro rozsáhlá nasazení. Namísto načítání všech kategorií najednou, které mohlo zpomalovat rozhraní, je nyní použit našeptávač se skupinovými návrhy. To zajišťuje rychlejší odezvu a pohodlnější práci.

Další vylepšení

PowerShell skript pro export toků

Byl doplněn nový PowerShell skript umožňující export všech toků podle zadaného časového rozsahu. Skript přijímá počáteční a koncové datum a vytváří samostatný CSV soubor pro každý den v daném období. Skript je součástí dokumentace a slouží jako referenční příklad pro uživatele.

Oficiální podpora produktu GREYCORTEX Mendel

S vydáním verze 4.6.0 je plná produktová podpora poskytována verzím 4.6.x a 4.5.x. Základní podpora je nadále dostupná pro verzi 4.4.x.

Verze 4.3.x a starší již nejsou podporovány.

Zákazníkům s platnou podporou, údržbou nebo aktivním předplatným softwaru je důrazně doporučeno přejít na některou z podporovaných verzí.