GREYCORTEX Mendel 4.1.0

HLAVNÍ FUNKCIONALITY

Nový vzhled

Nové uživatelské rozhraní (UI) s přepracovaným vzhledem. Bylo vytvořeno s cílem snížit vizuální složitost, poskytnout snadný přístup k nejdůležitějším údajům, a to vše se zachováním možnosti se dále podle potřeby postupně zanořovat k získání komplexních informací. #light #dark

Pokročilé integrace (nejen) pro XDR schopnosti

EDR integration / stage 1

Generické, na pluginech založené řešení, určené ke spolupráci s různými dodavateli koncových klientů (via API). Aktuální pokrytí v rámci první etapy je zaměřeno na získávání dat z koncových bodů pro zajištění vyšší míry bezpečnosti a slouží k obohacení dat v Mendelu.

Využití dat:

- Rozšířené informace o zařízení/koncovém bodu přímo v uživatelském rozhraní Mendel
- Události z EDR viditelné v uživatelském rozhraní produktu Mendel včetně hypertextových odkazů do EDR konzole
- Schopnost odezvy (manuálně/automaticky) iniciovaná Mendelem a prováděná klientem EDR

CISCO ACI/APIC integration

Rozšířená viditelnost prostřednictvím aplikace politik ze softwarově definované infrastruktury/sítě. Například aplikace tagů na zařízení či podsítě odpovídající informacím získaným z ESG/EPG. #APIC

API version 2

Druhá verze pro ještě větší integrační potenciál propojení produktu Mendel s externími informačními zdroji nebo poskytnutí zpracovaných dat příjemcům k dalšímu zpracování. #restfulAPI #v2

Aktuální pokrytí:

- Události
- Signatury IDS a Zpracování logů, IDS proměnné
- Externí vizualizace nebo analýza před zpracovaných dat (síťová data uložená v databázi ME)
- Záznam provozu (vytvoření a uložení pcap záznamu na základě externího požadavku)
- Správa “False positives”
- UnTE signatury (4.1.0)
- Toky (4.1.0)
- Integrace se zdroji Threat Intelligence a s nástroji třetích strany
- Blacklisty založené na IP adresách (včetně MISP)
- Blacklisty založené na škodlivých souborech
- Škodlivé domény

Důležité: S novou verzí 4.1.0 využívá produkt (Mendel) vyšší verzi API = v2. Tato verze přichází s jednotným jazykem a novou sadou klíčových slov.

Pokročilé filtrování

Ovládněte datové výstupy pomocí dotazů založených na bohaté syntaxi s novým pokročilým fulltextovým filtrem. Síťový modul byl přepracován pro vysoký výkon a je schopen poskytovat široké možnosti vyhledávání.

Hlavní schopnosti:

- Bohatá syntaxe
- Našeptávač skladby dotazu
- Zvýraznění hledaného stringu

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

OSTATNÍ FUNKCIONALITY

Nové OT parsery pro BACnet a Profinet na DCE/RPC

LACP bonding na síťových rozhraních Mendel

Ověření IoC v historii pomocí API

Vylepšené zpracování ERSPAN komunikace (dekapsulace na síťových rozhraní Mendel)

VYLEPŠENÍ

Systémové profily mohou nyní konfigurovat i uživatelé s rolí administrátor

Upgradované ovladače Napatech pro širší kompatibilitu

Nově objevené podsítě jsou nyní hlášeny v událostech

Optimalizace záložky hostitelů/služeb

Přidáno rozhraní do konfigurace „Asset Discovery“

Sdružená stránka „Zdroje identit“ pro nastavení AD + ISE + Identity logs

Oficiální podpora produktů Mendel

S vydáním verze 4.1.0 bude pro verze 4.1.x a 4.0.x poskytována plná servisní podpora. Pro předchozí verzi 3.9.x je poskytována omezená servisní podpora. Verze 3.8.x a starší již nejsou podporovány. Koncovým uživatelům s platnou podporou a údržbou nebo aktivním předplatným SW se doporučuje upgradovat na podporované verze.

Dodatečné informace

Pro zrychlení a vylepšení aktualizací systému a aktualizací dat připravujeme nový aktualizační/upgrade server. Abyste byli připraveni k budoucímu použití nového serveru, povolte prosím na svém firewallu IP adresu 46.28.107.158. Rovněž je třeba zachovat aktuální IP 89.221.218.75 (update.greycortex.com).

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

GREYCORTEX