GREYCORTEX Mendel 4.2

Hlavní funkcionality

Přehrávání PCAP a analýza

Rozšíření možností systému Mendel nejen o analýzu zrcadleného provozu v reálném čase, ale navíc o analýzu dříve zaznamenaných dat pomocí vestavěného záznamníku PCAP nebo dat zachycených jakýmkoliv jiným nástrojem. Přehrané PCAPy budou zpracovány a uloženy odděleně od ostatních dat v Mendelu, aby byl zajištěn co nejvyšší uživatelský komfort při zpětné analýze s maximálním důrazem na konzistenci a bezpečnost dat.

XSOAR Integrace

Integrační balíček pro platformu XSOAR zajistí přenos dat z produktu Mendel přímo do platformy XSOAR, která nabízí více možností pro orchestraci, automatizaci a případnou reakci na zjištěné kybernetické hrozby.

Průvodce pro vytváření IDS pravidel

S tímto novým nástrojem můžete krok za krokem přizpůsobovat pravidla s podstatně menšími znalostmi nebo je jako zkušený profesionál nastavit během okamžiku a efektivněji využít uspořený čas.

Nový reportovací modul

Přepracovaný způsob vytváření a vizuálního zpracování sestav ve formátu PDF. Pomocí nového a efektivnějšího enginu, využijete nové možnosti pro každou část reportu tak, aby byla přesně podle vašich představ. Samozřejmostí je použití libovolného předdefinovaného dashboardu a filtru, a dále například definování počtu řádků pro pohledy typu tabulka. Tento engine přichází jako základ pro jednotnou reportovací službu, která v budoucnu přinese efektivní proces tvorby komplexních reportů z jakýchkoliv dat dostupných v produktu Mendel.

Logování uživatelské aktivity

Auditujte každý krok uživatelů v grafickém rozhraní Mendelu nebo jejich dotazů prostřednictvím API tak, abyste vyhověli legislativním požadavkům nebo interním politikám.

Uživatelská kategorizace událostí pro IT a OT uživatele BETA

Zcela nová možnost konfigurace uživatelských účtů pro zajištění specifických potřeb IT nebo OT uživatelů. Rychlejší a efektivnější kategorizaci událostí s důrazem na rozdílné potřeby a zaměření IT a OT bezpečnostních a provozních specialistů. Obě skupiny uživatelů tak mohou spolupracovat prostřednictvím stejného produktu Mendel a zároveň se na data dívat dle vlastních potřeb.

OT Metriky pro BACnet EXPERIMENTAL

Vizualizace analyzovaných hodnot nebo metrik odvozených ze síťových toků v rámci zpracování OT protokolů v systému Mendel nabízí bezprecedentní pohled na chování průmyslových zařízení. Tato exkluzivní experimentální funkce přináší nový rozměr monitorování a porozumění.
Kontaktujte nás a prozkoumejte tuto zatím neveřejnou schopnost a získejte hlubší porozumění svým průmyslovým systémům.

GREYCORTEX Mendel 4.2

Další funkcionality

Změny uživatelského rozhraní pro lepší UX

- sloučené zobrazení pro systémová a uživatelská detekční pravidla + Threat Intelligence
- skupinové operace v nastavení detekce
- nastavení LACP prostřednictvím uživatelského rozhraní
- stránka MITRE jako upravitelný dashboard
- import jednotlivých podsítí včetně tagů

Rozšíření API pro zajištění podpory nad daty týkající se

- hostů (hosts)
- uživatelů (persons)
- reportů

Výpočet zpoždění a jitteru z časových VOIP metrik

Extrakce souborů z analyzovaného provozu pro externí analýzu v Sandboxu BETA

Zpracování AWS FlowLogs protokolu v modulu NetFlow EXPERIMENTAL

Vylepšení

Parsery pro záchyt ze sítě a další vylepšení

- Parsery (PostgreSQL, Bittorrent , IKE1/IKE2, QUIC and HTTP2)
- VOIP a Delay metriky, vylepšené ART/RTT
- Filtrování značek MPLS a VLAN ze zaznamenaných PCAPů

Parsery pro OT protokoly s detailnějším přehledem o průmyslových aplikacích

- BACnet
- OPC-UA
- S7

Vylepšení exportu NetFlow

- export pro verze 5/9
- aplikační data
- časové metriky

Rozšíření UnTE enginu o podporu pro korelaci událostí BETA

Oficiální podpora produktů Mendel

S vydáním verze 4.2.0 bude pro verze 4.2.x a 4.1.x poskytována plná servisní podpora. Pro předchozí verzi 4.0.x je již poskytována pouze omezená servisní podpora. Verze 3.9.x a starší již dále nejsou podporovány. Koncovým uživatelům s platnou podporou a údržbou nebo aktivním předplatným software se doporučuje upgradovat na podporované verze.

GREYCORTEX