GREYCORTEX Mendel 4.0.0

HLAVNÍ FUNKCIONALITY

Network Inventory

Viditelnost a Detekce v jednom společném pohledu. Zobrazí vaší síťovou infrastrukturu z pohledu podsítí a zařízení doplněnou o rizika a další bezpečnostní pohledy. Data jsou přehledně interpretována formou tabulek a grafických přehledů.

API / fáze 3

Ještě větší integrační potenciál s novými možnostmi propojit Mendela s externími zdroji informací (Threat Intelligence) nebo poskytovat zpracovaná data k dalšímu využití (SIEM, atd.). #restfulAPI

Aktuální pokrytí API:

- Události (4.0.0)
- Signatury IDS a Zpracování logů, IDS proměnné (4.0.0)
- 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“
- Integrace se zdroji Threat Intelligence a s nástroji třetích stran
  - Blacklisty založené na IP adresách (včetně MISP)
  - Blacklisty založené na škodlivých souborech
  - Škodlivé domény (4.0.0)

Integrace

- s platformou poskytující informace o hrozbách. #MISP
- Zpracování logů doplněno o využití identity přihlášených uživatelů získané z logů a její spárování s konkrétními hosty. #Radius
- **Community ID Flow Hashing**: přidává do svých toků průmyslový standard „Community ID“, který umožňuje vzájemně korelovat data z různých monitorovacích nástrojů, jako jsou: Arkime, Elasticsearch, **GREYCORTEX Mendel (v4.0+)**, Security Onion, VAST, Wireshark, Zeek a mnoho dalších.

DALŠÍ VYLEPŠENÍ

Modul **NetfFow** byl přepracován pro vyšší výkon a doplněn o nové funkce:

- až 50 Gbitů původního provozu,
- až 1000 externích zdrojů (přepínačů),
- ukládá pole HTTP, TLS a DNS z IPFix,
- extrahuje výkonové metriky,
- extrahuje parametry (například příchozí rozhraní/port),
- detekuje blacklistované IP adresy,
- podporuje výkonnostní profily pro optimalizaci nasazení a zpracování,
- příjem a zpracování NetFlow na více síťových rozhraních jednoho stroje.

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

GREYCORTEX

Vylepšená detekce pro rozpoznání zdroje datových anomálií na „**outliers**“ s možností definovat false positives a omezit falešnou detekci

Vlastní pravidla definovaná (přidaná nebo importovaná) uživatelem pro **zpracování logů** = zpracování logů je nyní v plně produkční verzi včetně uživatelské správy z UI

„**Failsafe**“ režim s vylepšeným výkonem k odstranění problémů s nestabilním připojením (sensor–kolektor)

Podpora řetězce identifikátoru toku pro rychlou a jednoduchou reprezentaci daného toku sítě. **#Community ID**

Vylepšení uživatelského rozhraní pro lepší UX:

- top události a služby v (malém) dialogovém okně,
- tlačítko „Kopírovat“ pro IP a MAC v dialogovém okně,
- podrobné informace o službách detekovaných v tocích,
- převedení uživatele pod jiného „Supervisora“,
- uživatelem definovaná doba uchovávání dat.

Vylepšené network capture (signatury jsou schopny pokrýt TCP flagy v tocích)

GE-SRTP OT parser

Podpora nejnovějších ovladačů síťových karet

Oficiální podpora produktů Mendel

S vydáním verze 4.0.0 bude pro verze 4.0.x a 3.9.x poskytována plná servisní podpora. Pro předchozí verzi 3.8.x je poskytována omezená servisní podpora. Verze 3.7.x a starší již nejsou podporovány. Koncovým uživatelům s platnou podporou a údržbou nebo aktivním předplatným SW se doporučuje upgradovat na podporované verze.

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