**SeaLog - Mesterséges intelligencia alkalmazása a digitális nyomelemzésben**

1. **A megoldás részletes, szakmai bemutatása**

A fejlesztés célja egy mesterséges intelligenciával támogatott szakértői rendszer kialakítása, amiben a felhasználó IT rendszereinek naplóbejegyzésit feltöltve olyan elemzés készül, mely automatikusan generált, objektív szakértői véleményeken keresztül segíti a vezetők tájékozódását, döntéshozatalát.

A kifejlesztett megoldás a COCO módszertanra épülve egy környezetfüggetlen, nem szabály alapú hasonlóságelemzést képes elvégezni. A hasonlóságelemzés egy fajta mesterséges intelligencia eljárás, egyszerre mesterséges neurális hálózat, szakértői rendszer, döntési fa, (n)LP-probléma, eset-alapú következtetés, vagyis egy fajta context free hibrid megoldás, mely egyesíteni igyekszik a rokon eljárások előnyeit. Újdonságtartalma:

* Több dimenziós numerikus és alfabetikus értéksor kezelés
* A hasonlóság matematikai megfogalmazódása.
* A beépített lépcsős függvények a döntési fák és a neurális hálók megoldások előnyeit ötvözi hátrányaik minimalizálása mellett:
* A lépcsős függvények context free módon, egymással konzisztens kapcsolatba hozható elemzési részeredményeket képesek kezelni.

1. **Gyártó bemutatása**

A Seacon Europe Informatikai Fejlesztő és Tanácsadó Kft, magyar magánszemélyek tulajdonában lévő vállalkozás. Széles szakmai kompetenciái, kialakított partnerkapcsolatai révén ügyfeleit a piacvezető szoftver technológiák alkalmazásával, az adott ügyfél belső IT szabványainak a betartásával képes kiszolgálni. Az egyedi fejlesztések mellett testre szabható típusrendszerekkel képes megrendelőit gyors, értékálló megoldásokhoz juttatni.

A cég munkatársai biztonsági szoftverek készítése területén megszerzett korábbi gyakorlatára, valamint konkrét, vevői igényekre alapozva- 2005-ben kezdett IT és információ biztonsági megoldásokkal, log elemző alkalmazásokkal foglalkozni, melynek keretében átfogóan kívánjuk kiszolgálni partnereinket. Kínálatunk a különböző termékektől a tanácsadáson keresztül az auditok támogatásáig terjed. Cégünk információbiztonsági megoldásai részben saját (SeaLog), részben képviselt termékekből, illetve az ezekre épülő megoldások szállításából, és a kapcsolódó konzultációs és bevezetési szolgáltatásokból áll.

1. **Innováció bemutatása**

A SeaLog rendszerben tárolt adatok rendszerek, alkalmazások, eszközök által gyűjtött logok, naplók, amelyekben valós személyek, vagy az IT infrastruktúra elemei által elvégzett tevékenységek digitális nyomai találhatók. Az adatok összegyűjtéséből hozzáadott érték keletkezik, ha ezeket az adatokat képesek vagyunk elemezni. A projekt célja egy egységes szakértői alkalmazás fejlesztése volt,

* egységes IT biztonsági lekérdező felületet létrehozása,
* a lekérdezések eredményei publikálhatók riportokban,
* objektív, hasonlóságelemzésen alapuló szakértői modul, amellyel az összegyűjtött digitális nyomokban nem csak az előre meghatározott szabályrendszer alapján tudunk összefüggéseket, anomáliákat keresni.

Termékünkben a COCO (Component Based Comparison for Objectivity) hasonlóság elemzési módszertan alapján dolgozó elemző modult helyeztünk el. A hasonlóságelemzés során objektumokat (pl. tranzakciókat) hasonlítunk össze bizonyos, általunk kiválasztott attribútumaik mentén. Az eljárás során meghatározható a „normális” objektum és megállapítható a többi objektum távolsága az ideálistól.

A projekt eredményekén több típusú elemzési feladat elvégzésére alkalmas a rendszer:

1. az attribútumok együttállásának összefüggéseit keressük, ilyenkor a „normális” működés és az attól való eltérés felfedezése, azaz gyanúgenerálás a cél. Az IT infrastruktúrában abnormális viselkedést keresünk, amik mentén visszaélési pontokat, hibás működést, rendellenes funkciókat tárhatunk fel.
2. az objektumok közül előre meghatározottan az ideálisak tekintett viselkedéshez képest szeretnénk értékelni a többit. Ilyenkor az ideális objektum attribútumai a határértékek és a többi objektum távolságát határozzuk meg ehhez képest. Ezzel tranzakció szintű visszaélések felderítésére, időszakos profiloktól eltérő viselkedések felderítésére nyílik lehetőség.

A módszer segítségével következtetések, „jóslások” is végezhetők egy újonnan megjelenő objektumra, azok attribútumainak ismeretében, vagyis elhelyezhető egy feltételezett objektum is és megállapítható a viszonya a létezőkkel.