

# SeaLog



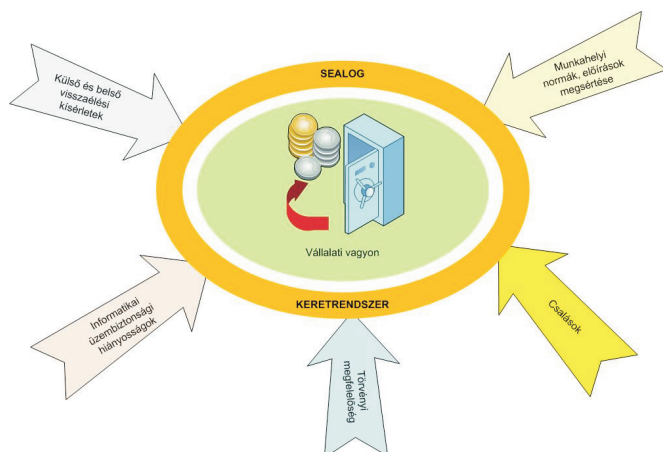
*„A rendszer feladata a vállalat kritikus folyamatai mentén keletkező, az informatikai rendszerek által rögzített **digitális nyomok** összegyűjtésével, feldolgozásával a rendellenességek feltárása, fenyegetések felderítése, előrejelzések készítése. Végeredményében a működési kockázat csökkentése”*

A vállalatok/szervezetek üzleti folyamatait, bonyolításuk során a résztvevő külső és/vagy belső szereplők munkáját a folyamatok minden egyes lépésében már túlnyomó részben informatikai rendszerek támogatják, vagy ilyen rendszerekkel felügyelik. A végrehajtás mentén, a vállalati rendszerek által létrehozott digitális nyomok egyre szélesebb körben állnak rendelkezésre. Ebből megfelelő feldolgozással és elemzéssel hatékonyan állíthatók elő előrejelzések/figyelmeztetések/riasztások amelyek a működési folyamatokban található kockázatokra többféle szempontból rámutathatnak, úgymint:

- IT üzembiztonsági hiányosságok,
- munkahelyi normák előírások megsértése,
- törvényi megfelelőségek hiánya,
- külső és belső visszaélési kísérletek.

A SeaLog feladata a cég működése szempontjából kritikus folyamatok kockázatainak csökkentése a következőkkel:

- Informatikai rendszerek használatának felügyelete és ellenőrzése
- Kritikus események automatikus figyelése
- Megfelelőségi auditok támogatása
- Veszteségek csökkentése
- HR kockázati szintek mérése
- IT kockázatok minimalizálása
- Visszaélések, csalások felderítése
- Működési anomáliák előrejelzése
- A cég működésének, a munkatársak tevékenységének az áttekinthetőbbé tétele



A **SeaLog** rendszer rugalmasságánál fogva egyaránt alkalmas biztonsági célú, valamint üzemeltetést támogató események figyelésre. Használatával javítani tudjuk egy cég verseny-képességét, biztonságát és jó hírét.



## A DIGITÁLIS NYOM

A SeaLog tervezésekor egy olyan szemléletet követtünk, amely szerint a különböző – akár nem informatikai jellegű – rendszerek releváns eseményeit egy közös eseménytérben képezzük le, amelyet aztán automatikus, informatikai és mesterséges intelligencia módszerekkel újra értelmezünk. A kapott eredményeket a felhasználók által értelmezhető és tovább feldolgozható formában megjelenítjük.

Ennek érdekében az informatikai rendszerekben keletkező naplókat és minden egyéb adatot is figyelembe veszünk, amelyekből egy adott folyamat összes lépése megbízhatóan visszakövethető, rekonstruálható. Ez a digitális nyom. A digitális nyomok keresését az üzletileg kritikus folyamatok mentén érdemes végezni, ezért a rendszer kiépítését célszerűen kockázatelemzéssel kell kezdeni, melynek során meghatározzuk a biztonsági és/vagy üzleti szempontból legérzékenyebb rendszereket és folyamatokat, és az ezek mentén gyűjtendő naplóadatok/operatív adatok körét, melyeket első körben javasolt bekötni az elemző rendszerbe.

## A RENDSZER SZOLGÁLTATÁSAI

Az alkalmazás alapvetően a kockázat kezeléssel foglalkozó szakértők/auditorok/belső ellenőrök támogató rendszere. Fő feladata kockázatkezelés szempontjából fontos, időben elhúzódó folyamatok összetett vizsgálatának biztosítása. Néhány fontos szolgáltatása:

- digitális nyomok összegyűjtése, feldolgozása
- megfelelőségi előírások/szabály menedzsment
- eseményfigyelés, incidenskezelés
- jelentések, megfelelőségi riportok generálása
- kapcsolati háló felderítés
- adatelemzés, adatbányászat
- új szabályok/visszasságok automatikus felderítése
- tényadatok alapján előrejelzések készítése.

## A RENDSZER FELÉPÍTÉSE

A rendszer adattárházi/adatpiaci alapokon egymásra épülő funkcionális szintekből áll. Ezek a funkciószintek a Gyűjtés, a Feldolgozás, az Elemzés, és a Mesterséges Intelligencia. Működése során nem csak a különböző rendszerekből átvett adatokat tisztítja, rendszerezi, hanem speciális üzleti logika alkalmazásával a gyanút adó adatkombinációk esetén automatikus riasztást is küld a biztonsági menedzserek felé. Nemcsak előzetes ismeretek, dokumentációk alapján lehet a figyelendő eseményeket meghatározni, hanem támogatást nyújt ahhoz is, hogy a felhasználók - akik akár az informatika azon területén nem is jártasak - maguk is felfedezzenek gyanús, vagy rendellenes tevékenységeket.

A SeaLog rendszer gyorsan bevezethető, mert:

- moduláris keretrendszer,
- előre felkészített interfészekkel rendelkezik.

Könnyen üzemeltethető, mert:

- széleskörű rendszergazdai/felügyeleti funkciók,
- professzionális támogatással rendelkezik.

Biztonságos, mert:

- hiteles adatokkal dolgozik,
- használatának lépései naplózásra kerülnek.

Seacon europe

8000 Székesfehérvár  
Kertalja út 11.

Telefon: (06) 22 / 501-632

Fax: (06) 22 / 501-633

<http://www.seacon.hu>

[seacon@seacon.hu](mailto:seacon@seacon.hu)