SeConical Automatizált Biztonsági Elemzés

Az incidenskezelés hatékony támogatása SeConical segítségével

Kótai Szabolcs
SeConical termékmenedzser
IT GRC szakértő

Agenda

- Elméleti bevezetés
- SeConical bemutatása
- Használati esetek
- SeConical működése
- Esettanulmány
- Jövőkép

Automatizált Biztonsági Elemzés

Miért van szükség az adatok feldolgozására?

Az adat nagy tömegben keletkezik.

Az adatot információvá kell alakítani.

Az információ felhasználási lehetőségei:

Lehetséges veszélyek felderítése	Kártékony felhasználói tevékenység felfedése	Trendelemzés	Üzleti folyamatok elemzése	Üzleti döntések előkészítése

Mi az „adat” és feldolgozása?

Minden informatikai rendszer és alkalmazás adatot generál a saját működéséről.

Az adat

- rendszerek, alkalmazások által generált,
- tartalma változó és igen bőséges,
- formátuma nem szabványos.

Adatból rendkívül nehéz számunkra hasznos információt kinyerni.

Célunk az adott rendszer

- biztonsági szintjének növelése,
- működésének folyamatos hatékonyabbá tétele.

Elemzési lehetőségek

	Manuális elemzés	Elemző alkalmazás
Kihívások	• Különleges szaktudás szükséges • Rendkívül lassú • Túl sok adat áll rendelkezésre • A fontos információk azonosítása	• Különleges szaktudás szükséges • Nagy erőforrás igényű • Nehézkes testreszabhatóság • Központi adattárház kell hozzá • Minden eszköz különböző módon állítja elő az adatot

Megoldás: SeConical

- Automatizáltan végzi az információk elemzését,
- Nem igényel speciális szakértelmet,
- Riport grafikonokkal, táblázatokkal, magyarázatokkal,
- Könnyedén testreszabható.
- Közvetlenül informálja:
  - Információbiztonsági vezető
  - Üzemeltetési vezető
  - Egyéb döntéshozók

Eredmény: egyszerű, gyors és olcsó megoldás

Használati esetek

- IT üzemeltetés támogatás
- Incidensek jelzése és kezelése
- Törvényi megfelelés támogatása
- Nemzetközi szabványok (NIST SP 800-53, COBIT 5, ISO/IEC 27001)
- Logelemzési szakértelem és erőforrások hiánya esetén is működő legelemzés és üzemeltetés támogatás
- Rendszerek bevezetése során problémák megoldása, finomhangolás támogatása

Verziók

- Fizikai appliance
- Virtuális appliance

Törvényi megfelelés

- ✓ Az Információbiztonsági törvényben a 3-as biztonsági osztály feletti rendszerekhez előírt naplóelemzési módszer.
- ✓ Az automatizált működés teljesíti a törvényi előírásokat:
  - ✓ 3.3.12.6.1.1. rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából;
  - ✓ 3.3.12.6.2. Folyamatba illesztés: Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes vagy tiltott tevékenységekre és történésekre reagál.
  - ✓ 3.3.12.7.1. Az elektronikus információs rendszer:

    3.3.12.7.1.1. lehetőséget biztosít naplócsökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő naplóáttekintési, naplóvizsgálati és jelentéskészítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait;

Biztonsági intézkedések

- Fejlesztés során saját szakértők által
- Kész terméket CCLab vizsgálta
  - Black-box
  - Grey-box
- Szerepkörök szerint szétválasztott jogosultságok
- Saját magát is elemzi és figyeli a rendszer

Architektúra

	Megnevezés	SeConical-Main modul	SeConical-External modul
Fizikai appliance	Eszközök elhelyezése	rack mount - 1U magas	rack mount - 1U magas
	Tápegységek száma	2 db	2 db
	Tápegységek teljesítménye	550W/550W	550W/550W
	Ethernet hálózat	1 x Gb RJ45 ethernet csatlakozó	1 x Gb RJ45 ethernet csatlakozó
Virtuális appliance	Processzor	4 mag (minimum 3 Ghz fizikai processzor)	4 mag (minimum 3 Ghz fizikai proc.)
	Memória	16 GB	48 GB
	HDD1	500 GB	100 GB
	HDD2	2000 GB	1000 GB
	Hálózat	4 db minimum 1 Gb hálózati adapter	4 db minimum 1 Gb hálózati adapter
	Operációs rendszer	Windows 2019 standard with Desktop Exp.	Ubuntu Server 20.04

Operációs rendszer	Verzió
Linux	Ubuntu 18.04-től
	Debian 10.0-tól
	Ubuntu 20.04-től
	Samba 4.11-től
	Zimbra collaboration suite 8.8.15-től
Windows	Windows server 2012-től

Automat Számosság alapú súlyozás

- Az értékes ir
  felhasználha
- Szabályok ke
  - intuitív, moc
  - automatiku
- Gyors feldolg

```
2022-03-13 12:34:12 Conn. from 1.2.3.4 to 3.4.5.6:3232 established.
2022-03-13 12:34:15 Conn. from 1.2.3.5 to 3.4.5.6:3232 established.
2022-03-13 12:34:19 Conn. from 1.2.3.6 to 3.4.5.6:3232 established.
2022-03-13 12:38:15 Conn. from 1.2.3.4 to 3.4.5.6:3232 closed.
2022-03-13 12:38:15 Conn. from 1.2.3.5 to 3.4.5.6:3232 closed.
2022-03-13 12:38:15 Conn. from 1.2.3.6 to 3.4.5.6:3232 closed.
```

date	minute	type	dest_ip	dest_port	count
2022-03-13	12:34	open	3.4.5.6	3232	3
2022-03-13	12:38	close	3.4.5.6	3232	3

```
2022-03-13 12
2022-03-13 12
```

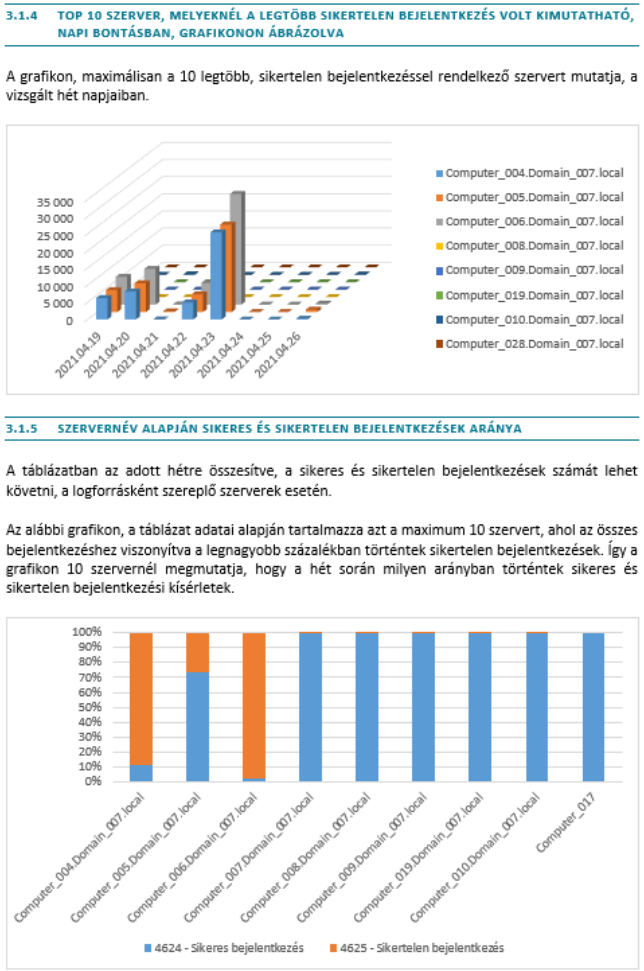
date					
2022-03-13					
2022-03-13	12:38:15	1.2.3.4	3.4.5.6	3232	close

Jelentések, következtetések

- ✓ Bejelentkezési események,
- ✓ Felhasználói fiókok kezelése,
- ✓ Jogosultságkezelési műveletek,
- ✓ Naplózással, rendszerdátummal kapcsolatos események,
- ✓ Rendszerleállás, újraindítás,
- ✓ Hardver és szoftver konfigurációváltozás
- ✓ Rendszerben fellépő hibák.

A grafikonok

- ✓ Megkönnyítik a keresést,
- ✓ Kényelmessé teszik a heti események értékelését,
- ✓ A kiugró viselkedést látványosan ábrázolják,
- ✓ Kiemelik a 10 legproblémásabb szervert vagy felhasználót.



Esettanulmány

Dátum	2022.06.09 (csütörtök)	2022.06.10 (péntek)	2022.06.11 (szombat)	2022.06.12 (vasárnap)
4733 - Egy tagot eltávolítottak egy helyi biztonsági csoportból			1	3
4732 - Egy tagot hozzáadtak egy helyi biztonsági csoporthoz			1	3
4738 - Felhasználói fiók módosítása	7	2	0	0
4722 - Felhasználói fiók engedélyezése	1			
4720 - Felhasználói fiók létrehozása	1			

Felhasználó neve	KemenyI	VargaR	NagyBe	RozsavizZ2	KicsiS	CserpesG
4723 - A megváltozott jelszó nem felel meg a jelszó házirendnek	1	1	1		1	1
4738 - Felhasználói fiók módosítása	1	1	1	3	1	1
4722 - Felhasználói fiók engedélyezése				1		
4724 - Az új jelszó nem felel meg a jelszó házirendnek				1		
4720 - Felhasználói fiók létrehozása				1		

datetime	second	computer	provider_name	event_id	channel	subject_user_name	subject_domain_name
2022.06.10 6:48	6	zeusz.rt.hu	Microsoft-Windows-Security-Auditing	5140	Security	RozsavizZ2	REN
2022.06.10 6:49	55	apollo.rt.hu	Microsoft-Windows-Security-Auditing	5140	Security	RozsavizZ2	REN
2022.06.10 6:48	6	apollo.rt.hu	Microsoft-Windows-Security-Auditing	5140	Security	RozsavizZ2	REN

Tesztelés alatt

Adattárolás, archiválás

- ✓ Időpecsét, Titkosított adatok
- ✓ Mély szintű nyomozás lehetősége
- ✓ Gyors keresés, szabályszerkesztő
- ✓ Nagy tárkapacitás, redundáns kialakítás

Intelligens monitorozás

- ✓ Valós idejű riasztások
- ✓ Machine talk, Mesterséges intelligencia
- ✓ Trendelemzés, Forecasting
- ✓ Proaktív beavatkozás a működésbe

Összegzés

A rendszerekben végbemenő biztonsági folyamatok, trendek bemutatása

Nincs szükség adatelemző szakértőkre

Automatikus heti és havi jelentés generálás

Bármely eszköz adattípusának feldolgozása

Az ügyfél igényeinek megfelelő finomhangolhatóság

Központi adattárház nélküli működés

Nem igényel üzemeltetési személyzetet

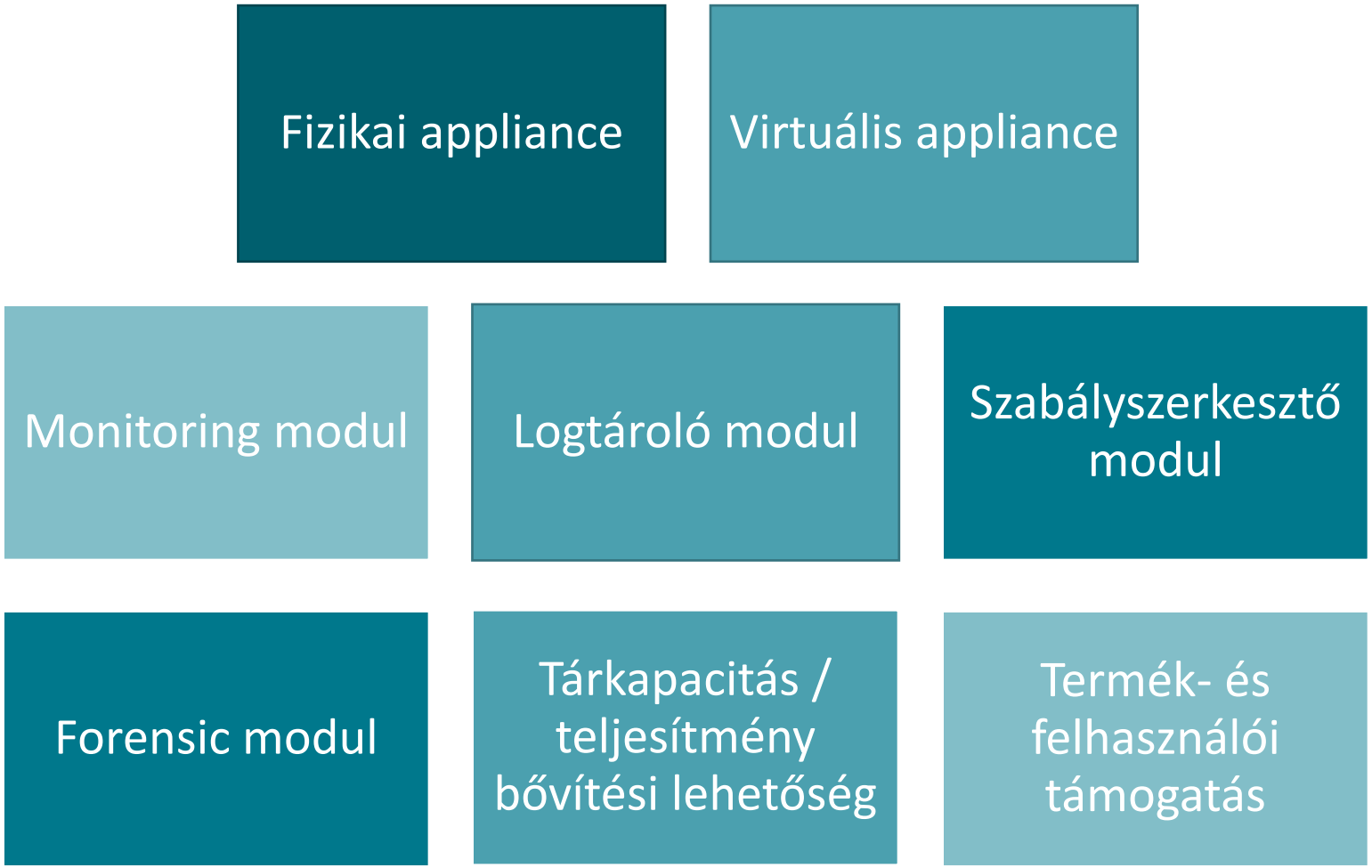
Biztonsági döntések alátámasztása

Titkosítva, időpecséttel ellátott tárolás

Trend- és folyamatelemzés

Forecasting és riasztások

Licencelés


Fizikai appliance
Virtuális appliance
Monitoring modul
Logtároló modul
Szabályszerkesztő modul
Forensic modul
Tárkapacitás / teljesítmény bővítési lehetőség
Termék- és felhasználói támogatás

SeConical

AUTOMATIZÁLT BIZTONSÁGI ELEMZÉS

MEGOLDÁS AZ
INFORMATIKAI BIZTONSÁGI ESEMÉNYEK
MEGFIGYELÉSÉRE ÉS AZ INCIDENSEK FELDERÍTÉSÉRE

Kótai Szabolcs
SeConical termékmenedzser
IT GRC szakértő

seconical@kurt.hu
www.seconical.hu