SeConical

Appliance megoldás az informatikai biztonsági események megfigyelésére és az incidensek felderítésére

SeConical
SECURITY ANALYTICS

A SeConical általános leírása

A **SeConical** logelemző appliance, naplóbejegyzések gyűjtését és feldolgozását végző szoftverrendszer, mely a naplóbejegyzések feldolgozása után hetente, automatikus elemzést követően, riportot készít az elmúlt hét biztonsági eseményeiről. A riportok átvizsgálása során fény derülhet az informatikai rendszerben történt incidensekre, valamint olyan folyamatokra, melyek jelenleg még nem okoznak, de a jövőben problémát okozhatnak. Incidens esetén a szakértők további manuális logelemzést is végezhetnek az appliance-ben, az okok és problémák mélyebb felderítése céljából.
A heti jelentéseken kívül, a vezetők számára havonta készül egy átfogó riport az elmúlt hónap eseményeiről. Ez kumulálva és trendelemzésre alkalmas módon szemlélteti a szervezet informatikai infrastruktúrájában végbemenő biztonsági folyamatok változásait.
A szervezet naplózási rendszere a SeConical segítségével átláthatóvá, könnyen kezelhetővé válik, mert a felhasználók igényei alapján lett kialakítva.

A SeConical felépítése

A **SeConical** appliance egy webes workflow vezérelt alkalmazásrendszer, amely main és external szerverekből áll. A main szerveren található a **Felügyeleti** modul, mely az automatikus vezérlésen felül a felhasználók kényelmes kiszolgálásáért felel. Az external szerver, a rendszer lelke, melyen a **Logelemző** alkalmazás fut.
A **Felügyeleti** modul lehetővé teszi, hogy valós időben lehessen nyomon követni az appliance üzemállapotát. Segítségével módosíthatók a beállítások, illetve elérhetők a különböző logelemzési riportok, valamint ez a modul felelős a két szerver összehangolt működéséért.
A L**ogelemző** modul a naplóbejegyzések gyűjtését és feldolgozását végző szoftverrendszer – előbbit **Flume**, utóbbit **LogDrill** nevű alegység végzi –, mely a naplóbejegyzések feldolgozása után hetente, automatikusan egy elemzési riportot készít az elmúlt hét eseményeiről. A riportok rugalmasan alakíthatók az ügyfél igényeinek megfelelően és a riportok alapján további személyes átvizsgálása során fény derülhet az informatikai rendszerben történt incidensek mélyebb okaira, melyek részletes kivizsgálása és korrigálása gyorsabbá és egyszerűbbé válik.
Az appliance nagy előnye, hogy nem igényel üzemeltetési személyzetet és logelemző szakértőket. A bevezetés után automatikusan működik, készíti a heti és havi jelentéseket, melyek értelmezéséhez nincs szükség speciális szaktudásra. Biztonsági incidens gyanúja esetén, eseti jelleggel szükséges csak logelemző vagy forensic szakértőhöz fordulni, aki egy külön (opcionálisan) illeszthető **Forensic modul** segítségével az összegyűjtött logokban manuális logelemzéssel az okok és problémák felderítése céljából mélyre tud hatolni.

Olyan szervezeteknek ajánljuk, ahol elvárás

- az IBTV által előírt tevékenységekről készült naplóállományok elemzéséről rendszeres riportok előállítása az adott elektronikus információs rendszer (EIR) besorolásának megfelelően,
- a nemzetközi szabványokban (NIST SP 800-53, COBIT 5, ISO/IEC 27001) megfogalmazott hatékony, biztonságos és automatizált logelemzési folyamat megvalósítása,
- hogy a loggyűjtés, logelemzés és jelentés készítés ne terhelje a szervezet humán erőforrásait, hanem azokat az illetékesek automatikusan, mindig határidőre kézhez kapják,
- hogy az informatikai rendszerek üzemeltetését támogató logelemzési jelentések készüljenek rendszeresen.

Saját fejlesztésű **SeCube** alkalmazásunk opcionális modulként illeszthető a SeConical rendszerhez. A SeCube IT GRC szoftver egy egységes keretrendszerben modulárisan összeilleszthető szoftver-komponensekből álló, workflow vezérelt, elemzési, tervezési és folyamatos karbantartási tevékenységeket támogató webes rendszer, mellyel a szervezet információbiztonsági irányítási rendszere (IBIR) megteremthetővé, átláthatóvá és kézben tarthatóvá válik. A két rendszer összekapcsolásának nagy előnye az, hogy a SeConical riportokból kiolvasható fenyegetettségek rögtön beilleszthetők a SeCube kockázatmenedzsment folyamatába, ahol a felhasználók megkapják a kockázatkezelési terveket is.

A SeConical fő jellemzői

- rack szekrénybe szerelhető appliance
- moduláris felépítésű, testre szabható rendszer
- könnyen telepíthető, egyszerűen üzemeltethető
- rugalmasan illeszthető a már meglévő loggyűjtő megoldásokhoz
- egy rendszerben megvalósított adatgyűjtés, tárolás, feldolgozás és elemzés
- informatikai rendszerek felügyeletének ellátása
- hierarchikus (jogosultság-függő) dashboard felületen kezelhető
- nemzetközi szabványokban (NIST SP 800-53, COBIT 5, ISO/IEC 27001) megfogalmazott hatékony, biztonságos és automatizált logelemzési folyamat megvalósítása

A SeConical részletes funkcionalitása

Központi loggyűjtés: A központi loggyűjtéssel a szervezet logforrásai által naplózott információk egy helyre, strukturáltan kerülnek összegyűjtésre, majd mentésre kiajánlásra, ezzel elősegítve az automatikus logelemzést és az esetleges manuális nyomozati vizsgálatokat is.

Automatizált logelemzés és riportkészítés: A logelemzés során a logállományok automatikus és ütemezett feldolgozása lehetővé teszi az IT rendszerek állapotának figyelemmel kísérését és riportokba foglalását, esetenként azok viselkedésének, problémáinak előrejelzését. A SeConical logelemző modulja nagy, különböző formátumú, struktúrájú és forrású adattömegek villámgyors elemzésére is képes. A logelemzés eredményeiből automatikus készül heti és havi jelentés, valamint egy kattintással készíthetők ad-hoc jelentések, melyek a rendszerbe feltöltött információk alapján generálódnak.

Logtovábbítás: A logtovábbítás lehetővé teszi, hogy az adatokat más rendszerek is feldolgozhassák. A logtovábbítás szolgáltatás által a logforrásból nyert adatok a SeConical rendszeren keresztül jutnak el a Megrendelő által meghatározott helyekre.

Felügyelet: A felügyeleti modulban nyomon követhető a SeConical valós idejű állapota és loggyűjtő agentek állapota, elvégezhetők különböző beállítások és parancsok, illetve kezelhető és létrehozható többféle logelemzési riport, majd ezek megnézhetők itt.

Manuális logelemzés: A Forensic modul segítségével lehetőség van az összegyűjtött logokban manuális logelemzésre annak érdekében, hogy incidens esetén az okok és problémák felderítése céljából mélyre tudjanak fúrni a szakértők.

SeCube: Egy moduláris felépítésű IT GRC alkalmazás, melynek segítségével egy szervezet információbiztonsági irányítási rendszere, átláthatóvá és kézben tarthatóvá válik. Részletesen: https://www.secube.hu/