LOGNESS

elasticsearch

LOGNESS

Monster at your service

LOGNESS International Kft., 1145 Budapest, Törökőr u. 22.

Tel.: +36 1 789 9323 E-mail: info@logness.us Web: www.logness.us

LOGNESS SIEM

– új generáció, fenntartott egyszerűség

Az elmúlt évek sikerprojektjeinek tapasztalatait és eredményeit LOGNESS SIEM termékünkbe integrálva, tovább tágítottuk annak határait. Tettük mindezt a termékcsaládtól megszokott „könnyű bevezethetőség, egyszerű használat, átlátható licenc politika és funkciógazdag tartalom" alapelveket követve. Új, nagy tömegű adatfeldolgozásra optimalizált adatbázis, dedikált, szabadszavas keresőmotor, megújult felhasználói felület, új agent komponensek. Pár példa a generációváltáshoz kapcsolódó újítások közül.

További információért keresse fel weboldalunkat a **www.logness.hu** címen.

LOGNESS Windsender

- Naplóüzenetek titkosított, biztonságos (TLS) továbbítása
- Szabványos syslog protokollok, fájlból történő naplózás támogatása
- Plugin-ekkel szabadon bővíthető felépítés (IIS, MS SQL, log-file, TMG, DHCP, stb.)
- Naplóállományok valós idejű normalizációja és adatbázisba szervezése
- Heartbeat funkció a forrás rendszerek leszakadásának ellenőrzésére
- Nagyvállalati infrastruktúra támogatása – policy alapú telepítés, konfiguráció és frissítés

LOGNESS Collector

- Naplóállományok fogadása, szűrése és központi menedzselése
- Nyers naplóállományok tárolása adatbázisban vagy fájlstruktúrában
- Hiteles, digitálisan aláírt és időpecsételt tárolás, mentés és archiválás
- Naplóállományok előszűrése, tárhely kapacitások ideális kihasználása
- Engedélyezett forrás-csoportok definiálhatósága, új források figyelése
- Kiesett források figyelése, naplóállományok „agent" és „agentless" alapú gyűjtése

LOGNESS Parser

- Naplóállományok valós idejű normalizációja és adatbázisba szervezése
- Elasticsearch open source, noSQL adatbázis alkalmazása
- Elosztott, sávosan bővíthető feldolgozási infrastruktúra
- 500+ előre definiált szűrési szabály a legelterjedtebb hoszt rendszerek out-of-box integrálására
- Valós idejű riasztás és korreláció-analízis, felhasználóbarát szabály-varázsló
- Többdimenziós anomália analízis, viselkedési minták elemzése

LOGNESS Intelligence

- Felhasználóbarát, magyar nyelvű felhasználói felület
- Strukturált értékelés, előre definiált napi, heti és havi naplóelemzési riportok
- Esemény alapú, hosszú távú statisztikai trendelemzés és riasztás
- Intelligens, szabadszavas keresőmotor a forensic elemzések hatékony támogatására
- Incidensek, riasztások és akciók nyomon követésének integrált támogatása