Security Information and Event Management (SIEM)

SMP SOLUTIONS
Services · Motivation · Partnership



MI AZ A SIEM?

- Központilag gyűjti, elemzi és korrelálja a különböző rendszerekből származó naplókat és biztonsági eseményeket.
- Támogatja a kibertámadások gyors felismerését, a fenyegetések azonosítását és a biztonsági incidensekre adott hatékony reagálást.

HOGYAN MŰKÖDIK EGY SIEM ÜZEMELTETÉSI TÁMOGATÁSI SZOLGÁLTATÁS?

ÜZEMELTETÉS, FELÜGYELET, HIBAKEZELÉS ÉS FOLYAMATOS FEJLESZTÉS



KOMPLEX FENYEGETÉSEK, GYORSABB FELISMERÉS

- A növekvő és egyre összetettebb kiberfenyegetések gyors eseményfelismerést és elemzést igényelnek.
- A rendszerekből, alkalmazásokból és infrastruktúraelemekből származó nagy mennyiségű naplóadat hagyományos módszerekkel nehezen kezelhető.
- A központi eseménykezelés támogatja a fenyegetések azonosítását, az incidenskezelést és a megfelelőségi elvárásokat (NIS2, DORA, ISO 27001).

MI A MEGOLDÁSUNK A FENTI PROBLÉMÁRA?

- **Rendszerfelügyelet és rendelkezésre állás** – A SIEM komponenseinek, szolgáltatásainak és működési állapotának folyamatos ellenőrzése.
- **Hibaelhárítás és eszkaláció** – A felmerülő hibák kivizsgálása és elhárítása, szükség esetén gyártói támogatás bevonásával.
- **Konfiguráció és szabálykezelés** – A SIEM-beállítások, korrelációs szabályok és kapcsolódó konfigurációk karbantartása.
- **Logforrások és collectorok támogatása** – A naplóforrások, collectorok és adatfolyamok működésének felügyelete, valamint a felmerülő hibák kezelése.
- **Kapacitás és teljesítmény** – A rendszer erőforrásainak, terhelésének és teljesítményének folyamatos nyomon követése és optimalizálása.
- **Finomhangolás és módosítások** – A rendszer működésének, detekcióinak és beállításainak folyamatos optimalizálása az aktuális igényeknek megfelelően.

MIÉRT AZ SMP?

- Átfogó kiberbiztonsági szakértelem a biztonsági események felismerésében, elemzésében és kezelésében.
- Nem csupán technológiai platformot biztosítunk: szakértői támogatást nyújtunk a biztonsági felügyelethez, incidenskezeléshez és a detektálási képességek finomhangolásához.
- Megoldásainkat az ügyfél informatikai környezetéhez igazítjuk, támogatva a NIS2, DORA és ISO 27001 megfelelőséget.

VENDOR PORTFOLIÓ

Microsoft
IBM
FORTINET
splunk>

Bodnár Péter
IT Security Account Manager

+ 36 20 386 3245 | peter.bodnar@smp.hu | www.smp.hu
SMP SOLUTIONS ZRT. | 1138 Budapest, Madarász Viktor u. 47-49. 2. ép. 3. em.