BIZTONSÁGI INCIDENSEK HATÉKONY KEZELÉSE

Simon János, simon.janos@synergon.hu
Synergon Informatika Rt.

Az informatika világában egyre nagyobb jelentőséggel bírnak a különböző biztonsági kérdések. Különösen igaz ez az oktatásban, ahol nagy számú, sokszor nem felügyelt gépről bejelentkező felhasználóval számolhatunk. A biztonsági megoldásokkal kapcsolatban a védelmi/megelőző megoldások állnak a fókuszban, és kevés szó esik ezen berendezések hatékony üzemeltetéséről, a biztonsági események korrelálásáról; noha a jelzések kiértékelése nélkül a biztonsági rendszer használhatósága jelentősen visszaesik.

Az előadásban egy olyan terméket mutatunk be, amely a hálózati topológia ismeretében képes a beérkező naplóadatok és egyéb jelzések kiértékelésére, korrelálására, valamint a támadást meghiúsítandó, a hálózati eszközök biztonsági beállításainak módosítására. Emellett az eszköz képes a különböző incidensek hibajegyeinek kezelésére is.