AZURE SENTINEL FELMÉRÉSI SZOLGÁLTATÁS

T · · Systems ·

Az Azure Sentinel felmérési szolgáltatás segítséget nyújt az Azure felhőben natív, biztonsági információs eseménykezelő (SIEM) és biztonsági szervezési automatizált válasz (SOAR) megoldás bevezetésének előkészítésében.
A felmérés eredményeként bevezetett Azure Sentinel szolgáltatás a felhőben működő vállalati biztonsági ökoszisztéma kialakítását teszi lehetővé.
Szolgáltatásunk igénybevétele kimagasló szintet eredményez az Azure Sentinel bevezetésének előkészítettségében, a naplóforrások menedzselhetőségében és az incidenskezelésben.

FOKOZZA IT-BIZTONSÁGI FELKÉSZÜLTSÉGÉT AZURE SENTINEL FELMÉRÉSI SZOLGÁLTATÁSUNKKAL!

A felmérési szolgáltatás segít pontosabban felmérni az Azure-ökoszisztéma meglévő naplóelemzési lehetőségeit, feltárja a kapcsolódó igényeket, illetve megtervezi, hogy milyen módon kerüljenek továbbításra a kiválasztott naplóforrások adatai, így erősödik a bevezetés előkészítettsége, annak folyamata és költségei tervezhetővé válnak.

SZOLGÁLTATÁSUNK ÜZLETI ELŐNYEI

A szolgáltatás segíthet az ügyfelek számára tisztázni a legfontosabb kérdéseket:

- Pontos ismeretet nyújtunk a bevonásra kerülő IT-rendszerekről és azok prioritásairól.
- Teljes ismeretet nyújtunk a naplózási, incidenskezelési rendszerekben alkalmazott rétegekről, úgymint a naplógyűjtési, naplófeldolgozási, naplótárolási, naplóelemzési, incidenskezelési és kiegészítő funkcionalitások rétegeiről és azok sajátosságairól.
- Megállapíthatóvá válnak a naplózási és incidenskezelési rendszerben alkalmazott szerepkörök.
- Azonosíthatóvá és kijelölhetővé válnak az Azure cloudban futó SIEM (Security Information and Event Management) rendszerbe köthető források.
- Felbecsülhetővé válik a SIEM bevezetésének átfutási ideje.
- Kontrollálhatóvá válnak a felkészülés pontos teljesítmény- és költségigényei.
- Láthatóvá válik az Azure cloud SIEM-migrációpotenciálja.
- Azonosításra kerülnek azok a szakmai kompetenciakövetelmények, amelyek a SIEM-alkalmazás üzemeltetéséhez és a naplóelemzéshez szükségesek.

A SZOLGÁLTATÁS TARTALMA

- Az on-premise és az Azure-infrastruktúra feltérképezése.
- A naplózási, incidenskezelési rendszerben alkalmazott naplógyűjtési, naplófeldolgozási, naplótárolási, naplóelemzési, incidenskezelési és a kiegészítő funkcionalitások rétegeinek és sajátosságainak feltérképezése.
- A naplózási és incidenskezelési rendszerben alkalmazott szerepkörök azonosítása.
- Az infrastruktúra felhőkészültségi szintjének megállapítása.
- Az implementációt követően várható Azure-költségek becslése.
- A naplózási adatok kiválasztása, típusainak és számosságának meghatározása.
- A naplótartalmak, a szabályrendszer, a lekérdezések, a dashboardok és a riportok azonosítása.
- Az incidenskezelési eljárások, playbookok azonosítása.
- A gépi tanulás és a viselkedésalapú funkcionalitásigények azonosítása.
- A tesztelési igények és a tervezett tesztesetek meghatározása.
- A dokumentációs és az oktatási igények felmérése.

A szolgáltatás lépései*

1. Felmérés

- Űrlapok kitöltése
- Konzultáció az ügyféllel

2. Kiértékelés

- A felmérés eredményeinek összegzése
- A szükséges következő lépések tisztázása

További információkért forduljon ügyfélmenedzseréhez, vagy írjon szakértőinknek a **cloudsolutions@t-systems.hu** e-mail-címre

* A felmérési szolgáltatás mintegy három hetet vesz igénybe.