
SOCURITY
WE PROTECT. YOUR DATA. YOUR USERS. YOUR BUSINESS.

# Alap 5/9 SOC

Biztonsági felügyelet ott és akkor, amikor az üzlet működik.

**RENDELKEZÉSRE ÁLLÁS**

**5/9**

Hétköznap, napi 8-10 órás szolgáltatási időszak.

**KINEK AJÁNLJUK?**

**Kis- és középvállalatok, valamint munkaidőben kritikus rendszerekkel működő szervezetek számára.**

**FŐ SZOLGÁLTATÁSI ELEMEK**

- SIEM rendszer felügyelete
- Biztonsági események elemzése és kezelése
- Incidenskezelés, eszkaláció és riportálás

**ÜZLETI ÉRTÉK**

Kedvező költségszint és gyors bevezetés - dedikált SOC kiépítése nélkül.

# Alap 5/9 SOC - működési részletek

Belépő szintű, kontrollált SOC-képesség a munkaidős kockázatok kezelésére.

## MŰKÖDÉSI FÓKUSZ

- A naplóforrások és biztonsági rendszerek eseményeinek napi szintű elemzése.
- Gyanús események osztályozása, kivizsgálása és dokumentálása meghatározott folyamat szerint.
- Incidens esetén a megfelelő ügyféloldali szereplő gyors, strukturált értesítése.

## ÜGYFÉL OLDALI EREDMÉNY

- Átláthatóbb biztonsági működés és ellenőrizhető incidenskezelés.
- A belső IT-csapat a jelentős eseményekre tud fókuszálni.
- Auditokhoz és megfelelőségi elvárásokhoz használható riportolási alap.

**EGYÜTTMŰKÖDÉSI KERET** Előre egyeztetett eszkalációs rend, kapcsolattartói kör és rendszeres szolgáltatási riport.

# SOC as a Service

Teljes körű, folyamatos védelmi képesség saját SOC nélkül.

**KINEK AJÁNLJUK?**

**Azoknak a szervezeteknek, amelyek 24/7 felügyeletet igényelnek, de nem tartanának fenn saját SOC infrastruktúrát.**

**RENDELKEZÉSRE ÁLLÁS**

**24/7**

SLA-alapú működés és dedikált kapcsolattartás.

**FŐ SZOLGÁLTATÁSI ELEMEK**

- Folyamatos monitorozás és incidensdetektálás
- Threat intelligence integráció
- Vezetői riportok és igény szerinti szakértői támogatás

**ÜZLETI ÉRTÉK**

Azonnal elérhető szakértői csapat, skálázható működés és kiszámítható költség.

# SOC as a Service - működési részletek

Külső SOC szervezet teljes technológiai és elemzői képességének igénybevétele szolgáltatásként.

## MŰKÖDÉSI FÓKUSZ

- 24/7 eseménykorreláció, riasztáskezelés és incidensdetektálás a szolgáltatási SLA szerint.
- Threat intelligence felhasználása a kockázatos aktivitások gyorsabb azonosításához.
- Rendszeres vezetői és operatív riportok a trendekről, incidensekről és teendőkről.

## ÜGYFÉL OLDALI EREDMÉNY

- Folyamatos védelmi lefedettség saját SOC-infrastruktúra és létszám felépítése nélkül.
- Kiszámítható szolgáltatási költség és rugalmasan bővíthető kapacitás.
- Gyors hozzáférés specialista tudáshoz összetett események esetén.

**EGYÜTTMŰKÖDÉSI KERET** SLA-k, incidenskezelési folyamatok, kijelölt kapcsolattartók és rendszeres szolgáltatásértékelés mentén.

# Dedikált belső SOC

A SOC-csapat az Ön környezetére és napi működésére összpontosít.

**KINEK AJÁNLJUK?**

**Nagyvállalatok, kritikus infrastruktúrák és magas biztonsági követelményű szervezetek számára.**

**MŰKÖDÉSI MODELL**

## Dedikált

Ügyfélkörnyezetre kizárólagosan fókuszáló szakértői csapat.

**FŐ SZOLGÁLTATÁSI ELEMEK**

- Folyamatos eseményelemzés és incidenskezelés
- Use case fejlesztés, SIEM hangolás és threat hunting
- Compliance- és audit-támogatás

**ÜZLETI ÉRTÉK**

Maximális dedikáltság, mély szervezeti ismeret és gyors reakcióidő.

# Dedikált belső SOC - működési részletek

Mélyen integrált SOC-működés, amely az ügyfél technológiájához, kockázataihoz és folyamataihoz igazodik.

**MŰKÖDÉSI FÓKUSZ**

- Dedikált elemzők folyamatosan fejlesztik a detektálási use case-eket és hangolják a SIEM-et.
- Threat hunting tevékenység az ismert riasztásokon túli, rejtett fenyegetések feltárására.
- Napi együttműködés az IT-, információbiztonsági és üzleti területekkel.

**ÜGYFÉL OLDALI EREDMÉNY**

- Rövidebb reakcióidő, mert a csapat ismeri az üzleti folyamatokat és a technológiai környezetet.
- Fejlettebb detektálási képesség és tartósan magasabb biztonsági érettség.
- Kiemelt támogatás compliance-, audit- és kritikus incidenshelyzetekben.

**EGYÜTTMŰKÖDÉSI KERET**

Az ügyfélszervezethez igazított szerepkörök, folyamatok, átadási pontok és rendszeres operatív egyeztetések.

# Belső SOC támogatás

Célzott tudás és kapacitás, amikor a meglévő SOC-nak szüksége van rá.

**IGÉNYBEVÉTEL**

## Rugalmas

Dedikált szakértő, órakeret vagy konzultációs támogatás.

**KINEK AJÁNLJUK?**

**Működő SOC szervezettel rendelkező vállalatok számára, ahol időszakos vagy speciális külső támogatás szükséges.**

**FŐ SZOLGÁLTATÁSI ELEMEK**

- SIEM optimalizálás és folyamatfejlesztés
- Threat hunting és incidensvizsgálati segítség
- Erőforrás-kölcsönzés, tudásmegosztás

**ÜZLETI ÉRTÉK**

Gyorsan bővíthető kapacitás a kritikus erőforráshiányok áthidalására.

# Belső SOC támogatás - működési részletek

A meglévő SOC képességeit kiegészítő, célzott szakértői beavatkozás a szükséges területeken.

| MŰKÖDÉSI FÓKUSZ | ÜGYFÉL OLDALI EREDMÉNY |
| --- | --- |
| • Dedikált szakértő vagy lehívható órakeret biztosítása pontosan definiált feladatra. | • A belső SOC működése nem lassul le átmeneti létszám- vagy kompetenciahiány miatt. |
| • SIEM- és detektálási optimalizálás, valamint folyamat- és use case-fejlesztés. | • A csapat tudása fejlődik a közös munka, mentorálás és átadott módszertan révén. |
| • Komplex incidens, threat hunting vagy átmeneti kapacitáshiány esetén azonnali támogatás. | • A támogatás az igényhez igazítható, ezért a költség és a kapacitás is kontrollálható. |

**EGYÜTTMŰKÖDÉSI KERET** Közösen definiált célok, feladatlista, rendelkezésre állási keret és tudásmegosztási terv alapján.

# 24/7 belső SOC kiegészítés

A belső SOC képességeire építve, a munkaidőn kívüli időszakok lefedésére.

**LEFEDETTSÉG**

**24/7**

Esti, éjszakai, hétvégi és ünnepnapi felügyelet.

**KINEK AJÁNLJUK?**

**Meglévő belső SOC-kal rendelkező szervezeteknek, ahol 24/7 lefedettségre van szükség.**

**FŐ SZOLGÁLTATÁSI ELEMEK**

- Távoli 24/7 monitorozás és elsődleges reagálás
- Incidens-eszkaláció és átadási folyamatok
- SOC as a Service vagy dedikált erőforrás alapú kiegészítés

**ÜZLETI ÉRTÉK**

Megőrzi a meglévő SOC értékeit, miközben költséghatékonyan teremti meg a teljes lefedettséget.

# 24/7 belső SOC kiegészítés - működési részletek

A belső SOC nappali működését kiegészítő modell a megszakítás nélküli és egységes védelemhez.

| MŰKÖDÉSI FÓKUSZ | ÜGYFÉL OLDALI EREDMÉNY |
| --- | --- |
| • Munkaidőn kívüli távoli felügyelet, riasztáskezelés és elsődleges reagálás. | • A szervezet megfelelhet a 24/7 működési, audit- vagy szabályozói elvárásoknak. |
| • Kritikus események meghatározott eszkalációs rend szerinti értesítése és dokumentálása. | • A belső SOC megőrzi saját szerepét és tudását, miközben a lefedettség teljessé válik. |
| • A következő munkanapra strukturált átadás a belső SOC számára, teljes kontextussal. | • Kedvezőbb modell, mint egy teljes saját, többműszakos SOC fenntartása. |

**EGYÜTTMŰKÖDÉSI KERET** Közös riasztási küszöbök, eszkalációs mátrix, átadási jegyzőkönyv és rendszeres közös felülvizsgálat.

# Az Ön SOC útja

A szolgáltatás a szervezeti érettséghez, a kockázatokhoz és a kívánt rendelkezésre álláshoz igazítható.




**A megfelelő modell a védelem, a költség és a szervezeti integráció egyensúlyát teremti meg.**

Induljon a jelenlegi igényeiből, és építse fel a következő képességet akkor, amikor az üzlet megkívánja.