# MENEDZSELT BIZTONSÁGI SZOLGÁLTATÁSOK [MANAGED SECURITY SERVICES MSS]

# 1. ÁLTALÁNOS SZOLGÁLTATÁSLEÍRÁS

A Black Cell Magyarország Kft. (a továbbiakban egységesen, mint Black Cell) ügyfelei részére testreszabható Menedzselt Biztonsági Szolgáltatásokat [továbbiakban MSS] kínál.

## 1.1. IMPLEMENTÁCIÓ

A projekt méretétől és komplexitásától függően a Black Cell dedikált projektmenedzserrel biztosítja a zökkenőmentes implementációt.

Dedikált Projektmenedzser az alábbi feladatokat látja el:

- Forrástervezés
- Projektcsapat összeállítása és koordinálása
- Ütemtervezés
- Minőség és elégedettség biztosítása
- Problémák és kockázatok kezelése
- Nyomon követés
- Jelentések és projekt dokumentumok elkészítése

# 2. ALAPVETŐ KIBERBIZTONSÁGI SZOLGÁLTATÁSOK

A támogatás 8 óra / 5 nap [munkaszüneti napokat nem számítva], vagy 24 óra / 7 nap áll Ügyfeleink rendelkezésére. A szolgáltatás nyelve magyar és/vagy angol. A Black Cell MSS csapata a jelen dokumentumban leírt szolgáltatási szintű megállapodásokkal [SLA] összhangban reagál és megoldja a termék telepítésével, adminisztrálásával és működtetésével kapcsolatos problémákat és teljesíti az Ügyfelek által igényelt kéréseket/változtatásokat.

*Kommunikáció módja*

A Black Cell MSS csapata az alábbi kommunikációs csatornák egyikével, vagy kombinációjával fogadja és reagál az eseményekre/kérésekre:

- Jegykezelő rendszer [Black Cell Ügyfélportál - JIRA]
- E-mail
- Telefon

*Helyszíni támogatás*

Az Ügyfél, kritikus folyamatait érintő események kezelésére, igényelhetnek helyszíni hibaelhárítást, amennyiben a támogatás egyéb formái nem tudták megoldani az adott

problémát. A Black Cell munkatársai a probléma helyszíni kiértékelését követően elvégzik a hibaelhárítási folyamatot, annak érdekében, hogy megszüntessék a problémát, vagy mérsékeljék a súlyosságát.

## 2.1. TÁVOLI TANÁCSADÁS

A távoli tanácsadási megbízás keretében nyújtott szolgáltatások a következők:

- Proaktív állapotfelmérés [Health check] elvégzése
- Támogatás nyújtása az ügyféloldali hibaelhárítási folyamatok optimalizálásához
- Konfigurációs, üzemeltetési és alapvető hibaelhárítási legjobb gyakorlatok bemutatása
- Teljesítmény és szolgáltatás optimalizálási javaslatok

A távoli tanácsadási megbízás részét NEM képező elemek a következők:

- Új beállítás, vagy telepítés
- Új készülék telepítése
- Konfigurációs változtatások
- Egyéni szkriptek fejlesztése, módosítása
- Professzionális Kiberbiztonsági Szolgáltatások

Folyamat:

- Az Ügyfél a Black Cell JIRA ügyfélportálján keresztül feladja a tanácsadói szolgáltatás igénylését.
- A felhasznált tanácsadói órák az Ügyfél és Black Cell által közösen meghatározott órakeretből kerülnek levonásra, vagy a szerződésben foglalt óradíj ellenében kerülnek számlázásra [Pay as You Go].
- Az egyszerre minimálisan lehívható óraszám: 1 óra.
- A tanácsadói megbeszélés lemondására a tervezett kezdést megelőzően 24 órával van lehetőség.

## 2.2. HIBAELHÁRÍTÁS

A hibaelhárítás keretében nyújtott szolgáltatások a következők:

- Az Ügyfél által jelentett összes esemény a Black Cell eseménykezelő rendszerében egyedi azonosító alapján nyomon követhető és a szerződésben meghatározott súlyossági szintnek megfelelően priorizált.
- Az Ügyfél által jelentett összes esemény a Black Cell belső hibaelhárítási folyamatai mentén kerülnek kivizsgálásra és megoldásra.
- Az események súlyossági szintjüknek megfelelően kerülnek elosztásra a Black Cell MSS munkatársai között.

- A Black Cell MSS csapata folyamatosan monitorozza az összes Ügyfél által jelentett eseményt az időben történő, magas színvonalú kezelés és megoldás megkönnyítése érdekében.

### 2.2.1. TÁVOLI MŰSZAKI TÁMOGATÁS

A hibák diagnosztizálása és megoldása érdekében a Black Cell MSS csapata távoli hozzáférést igényelhet az Ügyfél rendszeréhez/informcióforrásaihoz [pl. naplófájlok]. Amennyiben a távoli hozzáférés nem biztosított, úgy a megoldáshoz szükséges idő [TTR] eltolódhat. A távoli hozzáférés csak az Ügyfél engedélyével és felügyeletével valósulhat meg. A Black Cell MSS csapata kizárólag az iparág által elismert eszközöket használja a távoli hozzáférés során folyamatos session recording mellett.

### 2.2.2. SÚLYOSSÁGI SZINTEK LEÍRÁSA

A hatékony hibaelhárítási folyamat érdekében a Black Cell MSS csapata az alábbi súlyossági szinteket ajánlja fel Ügyfelei részére:

P1 [Kritikus]: Az implementált termékkel kapcsolatos probléma, amely az Ügyfél üzleti stratégiája szempontjából kritikus folyamatokra gyakorol hatást, vagy okoz teljes leállást. Az azonosított probléma megszüntetésére megkerülő megoldás nem létezik.

P2 [Magas]: Az implementált termékkel kapcsolatos probléma, amely az Ügyfél üzleti folyamataira szignifikáns hatást gyakorol, viszont nem okoz teljes leállást. Az azonosított probléma megszüntetésére megkerülő megoldás nem létezik.

P3 [Közepes]: Az implementált termékkel kapcsolatos probléma, amely az Ügyfél üzleti folyamataira nem, vagy minimális hatást gyakorol. Az azonosított problémákra megkerülő megoldás létezik.

P4 [Alacsony]: Az implementált termékkel kapcsolatos probléma, amely az Ügyfél üzleti folyamatait nem érinti. A termék funkcionális kihasználhatóságát csökkentő hibák.

### 2.2.3. SÚLYOSSÁGI SZINTEK HOZZÁRENDELÉSE

Az Ügyfél által bejelentett hibákhoz a Black Cell MSS csapata a 2.2.2. fejezetben bemutatott-, vagy a szerződésben foglalt egyedi szolgáltatási szint megoldások alapján súlyossági szintet rendel. Abban az esetben, ha az Ügyfél nem adja meg a súlyossági szintet, akkor a Black Cell műszaki támogatást nyújtó csapata „közepes” súlyosságú incidenskezelési folyamat alapján végzi el a hibaelhárítást.

### 2.2.4. KOMPLEX HIBAELHÁRÍTÁS

Abban az esetben, ha az Ügyfél által bejelentett hiba több különálló problémából áll, akkor a Black Cell MSS csapata minden problémát önálló esetekre bont és az ilyen eseményeket a 2.2.2. fejezetben tárgyalt súlyossági szinteknek megfelelően osztályoz.

### 2.2.5. SÚLYOSSÁGI SZINTEK MÓDOSÍTÁSA

Abban az esetben, ha az Ügyfél olyan problémákkal találkozik, amelyek azonosak a korábban benyújtott és megoldott hibákkal, akkor új hibajegy benyújtása szükséges. A benyújtott hibajegyek időközbeni súlyosbodása, vagy enyhülése esetén a súlyossági szintek és a rájuk vonatkozó szolgáltatási szintű megállapodások módosulnak. Ismétlődő hibák esetén a Black Cell problémaelemzést indít annak érdekében, hogy azonosítsa a hibákat okozó gyökérproblémákat.

### 2.2.6. SZOLGÁLTATÁSI SZINTŰ MEGÁLLAPODÁSOK CÉLSZÁMAI

A Black Cell MSS csapat célja, hogy az Ügyfelek által benyújtott hibajegyeket a közösen elfogadott és szerződésben rögzített feltételeknek megfelelően kezelje (1. táblázat).

| Súlyossági szint | Reagálási idő | Ügyféltájékoztatás |
|---|---|---|
| Kritikus | 5 munkaórán belül* | Naponta |
| Magas | 8 munkaórán belül | Naponta |
| Közepes | 16 munkaórán belül | - |
| Alacsony | 24 munkaórán belül | - |

*Kritikus súlyosságú hiba esetén a hibabejelentő formanyomtatvány kitöltését követően telefonos megerősítés javasolt.

### 2.2.7. ESZKALÁCIÓS FOLYAMAT

A Black Cell célja, hogy minden hibát professzionálisan és gyorsan megoldjon. A Black Cell MSS csapata [Elemzők] a hibaelhárítási folyamat bármely pontján internál eszkalálhatja az adott esetet, amennyiben megállapítják, hogy speciális [pl. gyártói] segítségre van szükség a probléma megoldásához.

## 2.3. VÁLTOZÁS MENEDZSMENT ÉS OPTIMALIZÁLÁS

Az Ügyfél és a Black Cell által közösön elfogadott szabályrendszer kialakítását követően minden szabálykészlet és/vagy a telepített eszközre vonatkozó irányelvek fejlesztése, áttelepítése és felülvizsgálata a Black Cell változásmenedzsment folyamata szerint kerül végrehajtásra. Az Ügyfél az ügyfélportálon keresztül adhatja fel változtatási kérelmét, amelyet a Black Cell MSS csapata a szerződésben rögzített szolgáltatási szint megállapodással összhangban kiértékel, előkészít és végrehajt.

A változtatási kérelmek az ügyfélportálon keresztül kerülnek regisztrálásra és jóváhagyásra. A beküldött változtatási kérelmek egyedi azonosítót kapnak, amely megkönnyíti a kommunikációt

és lehetővé teszi a változtatás nyomon követését. A Black Cell MSS csapat 16 munkaórán belül áttekinti a kérelmeket és státuszt rendel hozzájuk.

### 2.3.1. VÁLTOZTATÁSI TÍPUSOK

Egyszerű változtatás

- Standard változtatás, amely magába foglalja a meglévő szabályok módosítását és/vagy létrehozását (<10 szabály) a telepített eszköz / szoftver szabálykészletében.
- Új kiszolgáló [host] létrehozása a korábban kialakított rendekben [policy]
- Forgalomelosztás a meglévő kiszolgálók [host] között
- Operációs rendszerbeállítások módosítása, kivéve IP címek módosítása.

Teljesítési idő: 2 munkanapon belül

Komplex változtatás

- Standard változtatás, amely magába foglalja a meglévő szabályok módosítását és/vagy létrehozását (>10 szabály) a telepített eszköz / szoftver szabálykészletében.
- Az implementált eszköz/szoftver IP cím módosítása
- Egyszerű architektúraváltoztatás (például DMZ vagy webszerver hozzáadása a tűzfal mögött).
- Szoftverfrissítések végrehajtása
- Új „site-to-site VPN” konfigurálása a telepített eszközön/szoftveren.

Teljesítési idő: Az Ügyfél és Black Cell által valamennyi komplex változtatásra vonatkozóan egyedileg, közösen kerül meghatározásra.

## 2.4. SZOLGÁLTATÁSMENEDZSMENT

A Black Cell által nyújtott szolgáltatásmenedzsment modulhoz tartozó feladatokat dedikált MSS mérnök és Szolgáltatásmenedzser látja el:

- A szolgáltatás teljesítményvizsgálatát havonként.
- Negyedéves Ügyfélvizsgálatot.
- Elemzi és megérti az Ügyfél üzleti- és biztonsági igényeit és maximalizálja a megoldások előnyeit.
- Egyedi kapcsolattartóként összeköti az ügyfelet a Black Cell csapatával és mindkét irányba biztosítja az információáramlást.
- Az Ügyfél és a Black Cell érdekeit egyaránt képviseli.
- Az implementációt követően ellátja a Projektmenedzseri feladatokat.

### 2.5. PROAKTÍV KOMMUNIKÁCIÓ ÉS FIGYELMEZTETÉS

Az Ügyfél proaktív módon történő tájékoztatása a termékfejlesztésekről, frissítésekről, javításokról és tanácsokról:

- VIP Hírlevelek
- Értesítések
- „Whitepaper”

### 2.6. TELJESÍTMÉNY ÉS SZOLGÁLTATÁS OPTIMALIZÁLÁS

A Black Cell szakértői által nyújtott tanácsadás, amely a vállalati (üzleti) igények alapján támogatja a kiszolgálók számának, a hardverkapacitásnak és a termékek architektúrájának meghatározását. A szolgáltatás célja a folyamatos szolgáltatásfejlesztés, valamint a biztonsági- és üzleti folyamatok összehangolása.

## 3. SPECIÁLIS KIBERBIZTONSÁGI SZOLGÁLTATÁSOK

A Black Cell alapvető Kiberbiztonsági Szolgáltatásain felül speciális szolgáltatásokat is kínál Ügyfelei részére. Az alábbi szolgáltatások, a Black Cell szakemberei által végzett részletesebb vizsgálaton alapúló jelentések révén, kifinomultabb és testreszabottabb megoldásokat jelentenek az Ügyfeleink részére.

### 3.1. MALWARE ELEMZÉS

Az Ügyfél által beküldött, gyanús fájlokat tartalmazó, minták részletes vizsgálaton esnek át. Az analízist követően a Black Cell szakértői átfogó jelentések formájában tájékoztatják Ügyfeleiket. A fájlok vizsgálata és tisztítása mellett a Black Cell lehetőséget biztosít Ügyfelei részére, hogy a gyanús „hash” és URL mintáit is kivizsgáltassa.

### 3.2. EGYEDI JELENTÉSKÉSZÍTÉS

Az Ügyfél által megvásárolt licensztől függően a Black Cell MSS csapata testreszabott jelentéseket készít az alábbi naplók alapján:

- Eszközön / szoftverben azonosított események.
- Ügyféloldali beavatkozást igénylő események.
- Eseménynapló egyszerűsített változata, amely bemutatja a felismert és blokkolt rosszindulatú programokat és a nem kívánt alkalmazásokat (Potentially Unwanted Applications, PUAs).
- Adatvesztés-megelőzés: minden olyan esemény bekerül a jelentésbe, amelyet adatvesztés-megelőzési szabályok hoznak létre.
- Átjáró (gateway) tevékenységekkel kapcsolatos események.

### 3.3. SIEM (SECURITY INCIDENT AND EVENT MANAGEMENT) ALAPÚ JELENTÉSEK ÉS MONITORING

A SIEM integrációval a Black Cell javítja az Ügyfél kiberfenyegetésekkel kapcsolatos észlelési- és reagálási képességeit.

- Testreszabott és részletes jelentések és naplómegőrzések
- Transzparens és centralizált reagálás
- Nehezen detektálható események észlelése
- Eseménykezelés hatékonyságának növelése
- A Black Cell Biztonsági Műveleti Központ képességei kiegészítik és összehangolják a biztonsági eszközöket / szoftvereket azáltal, hogy kihasználják az elemzés következő generációját.

### 3.4. SÉRÜLÉKENYSÉGVIZSGÁLAT

A Black Cell MSS csapata horizontális sérülékenységvizsgálati teszt elvégzésével azonosítja a célrendszer gyenge pontjait és sebezhetőségeit, amelyek megkönnyíthetik a támadó munkáját. A szolgáltatás a különböző sérülékenységvizsgálatok eredményeinek validálására fókuszál.

Vizsgálati típusok:

- Webhely/Web alkalmazás
- Hálózat [LAN, WIFI]
- Mobil alkalmazás
- Szoftver

Várható eredmények: Az Ügyfél átfogó képet kap a rendszerében rejlő biztonsági résekről és javaslatot tesz azok helyreállítására.