Microsoft Security

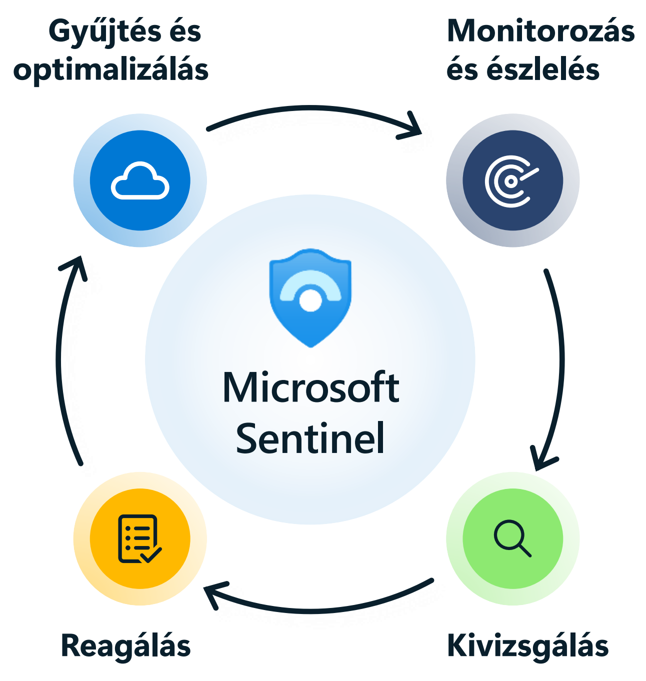
Microsoft Sentinel

AI-alapú SIEM a modern biztonság jegyében

Napjaink összetett kiberfenyegetési környezetében a biztonsági műveleti központok (SOC-k) jelentős kihívásokkal néznek szembe. A kibertámadások száma és fejlettsége fokozatosan nő, túlterhelik az elemzőket, akik így könnyebben elmulasztják a valódi támadásokat. A biztonsági csapatokat a nem egységes eszközök, az átláthatóság hiánya és a régi SIEM-megoldásokból hiányzó kulcsfontosságú funkciók is akadályozzák, így sebezhetővé válnak az újonnan megjelenő fenyegetésekkel szemben.

E kihívások leküzdéséhez megbízható SIEM szükséges, amely megóvja a többfelhős, többplatformos környezetet, amely vezető AI-eszközökre, automatizálásra és fenyegetésintelligenciára épül.

Alakítsa át biztonsági tevékenységeit a Microsoft Sentinellel!



Modernizálja vállalata biztonsági tevékenységeit a Microsoft Sentinellel, egy mesterséges intelligenciával működő, felhőnatív SIEM-megoldással, amely páratlan hatékonysággal és intelligenciával nyújt védelmet a fejlődő kiberfenyegetések ellen.

- **Egyszerűen skálázható védekezés** a felhő rugalmasságával és költséghatékonyságával a vállalat magabiztos bővítéséhez
- **Átfogó fenyegetésmenedzsment** és proaktív védelem AI, SOAR, UEBA és TIP segítségével
- **Az új fenyegetések azonosítása** AI-alapú, valós idejű észleléssel és gépi tanulással
- **Az incidensreagálás automatizálása** a válaszidők és a munkaterhelés csökkentése érdekében
- **A megfelelőség támogatása** ágazatspecifikus biztonsági szabványokkal és szabályozói keretrendszerekkel

Ha a Microsoft Sentinel mellett dönt, egy olyan SIEM-megoldásba ruház be, amelyet a jövőre terveztek, így elláthatja a biztonsági csapatait azokkal az eszközökkel, amelyekkel megvédhetik a vállalatát a folyamatosan változó fenyegetési környezetben.

Biztonsági eredmények elérése egy innovatív SIEM-mel

Teljes körű védelem egy átfogó SIEM-megoldással

Páratlan láthatóság és védelem a nagyvállalat minden részén a Microsoft Sentinel iparágvezető SIEM-képességeinek köszönhetően

Gyorsabb reagálás az új fenyegetésekre

A Microsoft Sentinel fejlett AI-jának és páratlan fenyegetésintelligenciájának köszönhetően egy lépéssel a támadók és az új fenyegetések előtt jár

Skálázható biztonsági megoldás a felhő rugalmasságával

A Microsoft Sentinel felhőnatív architektúrájával a vállalata növekedésének megfelelően bővítheti a biztonságot, és mindig a megfelelő összetettségű megoldásokat vezetheti be

Tíz fontos Microsoft Sentinel-képesség a biztonsági központ jövője érdekében

Napjaink összetett biztonsági környezetében olyan SIEM-platformra van szükség, amely egyetlen egységes felületen integrálja a különféle kulcsfontosságú funkciókat. Egy egységes platformmal a biztonsági csapatok egyszerűsíthetik az üzemeltetést, hatékonyabban észlelhetik a fenyegetéseket és gyorsabban reagálhatnak az incidensekre, így átfogó védelmet alakíthatnak ki a vállalatnak.

1. Felhőnatív architektúra

A Microsoft Sentinel felhőnatív architektúrája hatékony skálázást tesz lehetővé a biztonsági csapatoknak, akik így páratlan rugalmassággal működhetnek, a vállalat pedig megszabadul a felesleges infrastruktúra költségétől és komplexitásától.

2. Generatív AI-alapú fenyegetésészlelés

A generatív AI-val működő Biztonsági Copilot fenyegetésészlelési és -kezelési képességeinek köszönhetően akár már három hónap alatt 30%-kal csökkenthető az átlagos megoldási idő (MTTR), ami jelentősen javítja a vállalat biztonsági helyzetét.

3. Széles körű adatgyűjtés

A Microsoft Sentinel több mint 350 adatösszekötőt tartalmaz, és számos különféle környezetet támogat, például többfelhős szolgáltatásokat és helyi rendszereket is, így táfogó átláthatóságot biztosít a teljes digitális ökoszisztéma felett.

4. Rugalmas adatkezelés

A Microsoft Sentinel rugalmas adatszintezést és -kezelést kínál, amelynek köszönhetően Ön szabadon összegyűjtheti, tárolhatja és elemezheti az összes biztonsági adatot, és közben a költségeket is optimalizálhatja.

5. Gépi tanulás és automatizálás

A Microsoft Sentinel beépített SOAR- és UEBA-képességei orkesztrációt, automatizálást és fejlett viselkedésanalitikát biztosítanak, így Ön egyszerűsítheti az észlelést és a reagálást, proaktívan azonosíthatja a fenyegetéseket és hatékonyan kezelheti az incidenseket.

6. Fejlett fenyegetéskorreláció

A Microsoft Sentinel fúziós technológiája összeveti a különböző forrásokból származó adatokat, így azokat az összetett, többfázisú támadásokat is észleli, amelyeket a hagyományos eszközök általában nem, így Ön teljes képet kaphat az aktív fenyegetésekről.

7. Integrált veszélyforrás-felderítés

A Microsoft Sentinel felhasználja a Microsoft hatalmas globális hálózatából és a biztonsági közösségből származó fenyegetésinformációkat, így az Ön csapata hatékonyabban és gyorsabban észlelheti, elemezheti és kezelheti a veszélyforrásokat.

8. Proaktív veszélyforrás-vadászat

A fejlett veszélyforrás-keresési képességeknek köszönhetően a biztonsági csapatok proaktív módon megkereshetik és felszámolhatják a potenciális fenyegetéseket, mielőtt azok kárt okoznának.

9. A biztonsági központ optimalizálása

A naponta generált egyedi javaslatok segítségével növelheti az adatai értékét, kézben tarthatja a költségeket és 17%-kal bővítheti a biztonsági lefedettséget.

10. Testreszabható irányítópultok és vizualizációk

A Microsoft Sentinel testreszabható irányítópultja egyedi, valós idejű, az aktuális követelményeknek megfelelően formázott elemzéseket nyújt a biztonsági csapatoknak, így támogatja a gyorsabb döntéshozatalt és a fenyegetések hatékonyabb elhárítását.

Bizonyított SIEM-vezető

Az ügyfelek világszerte bíznak a Microsoft Sentinelben, amely átfogó képességeinek, széles körű lefedettségének és erős innovációinak köszönhetően hathatós védelmet nyújt a vállalatoknak a jelenlegi és a jövőbeni fenyegetésekkel szemben.

SIEM-vezető[1]
a Gartner® Magic Quadrant™ for Security Information & Event Management felmérésben

Több min 25 ezer
vállalat bízza magát világszerte a Microsoft Sentinelre

Átfogó
SIEM-képességek: AI, SOAR, UEBA, TIP

Több mint 350 adatösszekötő
az átfogó adatgyűjtéshez

A Microsoft Sentinel működés közben: hat módszer a csapat hatékonyságának növelésére

A Microsoft Sentinel AI és automatizálás segítségével továbbfejleszti a SIEM-élmény minden aspektusát, a zökkenőmentes implementációtól kezdve a fejlett fenyegetésészlelésen át a biztonsági elemzők támogatásáig. Ismerjen meg hat hatékony módszert, amellyel ezek az innovációk növelhetik a csapat hatását és az általános biztonsági teljesítményt!

1. A megvalósítás felgyorsítása automatizált migrálással

A biztonsági mérnökök számos hatékony migrációs eszközt használhatnak, amelyek megkönnyítik a meglévő SIEM-megoldások lecserélését, és gondoskodnak a zökkenőmentes adatintegrációról, megőrzik a biztonsági konfigurációkat, és a lehető legkisebb mértékben akadályozzák az üzleti tevékenységet.

2. A védelem kiterjesztése több eszközre

A biztonsági mérnökök egyszerűen kibővíthetik a biztonsági adatok gyűjtését és elemzését a különböző identitásokra, e-mail-fiókokra, hálózatokra, felhőalkalmazásokra és -szolgáltatásokra, valamint végpontokra a használatra kész összekötőkkel.

3. Gyorsabb fenyegetésészlelés és reagálás

A korrelációs motor gyorsabban alakítja át incidensekké a riasztásokat. A Security Copilot incidens-összefoglalókat, hatáselemzéseket és helyreállítási javaslatokat jelenít meg az elemzőknek, így lerövidíti a válaszidőt.

4. Bármilyen területen alkalmazható

A biztonsági csapatok testreszabható megoldások gazdag tárából válogathatnak, amiben több mint 21 ezer GitHub-kódkontribúció, több mint 200 Microsoft által fejlesztett szabály és több mint 280 közösségi erőforrás érhető el az észleléshez, valamint az irányítópultokhoz és az útmutatókhoz.

5. Átfogóbb vizsgálatok

A Security Copilot egyszerűbbé teszi az összetett incidenseket, mivel összegzi és korrelálja a különböző rendszerekből származó adatokat, így az elemzők gyorsan megérthetik a fenyegetések kiterjedését, hatását és okait, ezzel 85%-kal csökken a vizsgálatokhoz szükséges idő.

6. A rutinfeladatok automatizálása

A Biztonsági Copilot automatizálja az olyan rutinfeladatokat, mint a naplóelemzés, a riasztások osztályozása, a szkriptek áttekintése és az adatok korrelálása, így az elemzők a nagyobb értékű stratégiai tevékenységekre összpontosíthatnak.

Bizonyított üzleti hatás

A SIEM megtérülése

A Microsoft Sentinel felhőnatív eszköz, így nincs szükség hozzá a költséges infrastruktúrára, így segít csökkenteni a tőke- és üzemeltetési kiadásokat. A vállalatok igény szerint skálázhatják a biztonsági tevékenységeiket így magasabb megtérüléshez juthatnak.

44%-kal
alacsonyabb összköltség a hagyományos SIEM-szolgáltatókhoz képest[2]

234%-os
megtérülés három év alatt[2]

A biztonsági elemzők hatékonysága

A Microsoft Sentinel AI-val és automatizálással fokozza a biztonsági központ hatékonyságát, és csökkenti a fenyegetések észleléséhez és elhárításához szükséges időt. Automatizálja a gyakori feladatokat és rangsorolt incidensekbe egyesíti az értesítéseket, így a biztonsági csapatok a legkritikusabb problémákra összpontosíthatnak.

85%-os
csökkenés a fejlett vizsgálatokhoz szükséges munkaidőben[2]

79%-os
csökkenés a téves riasztások számában[2]

A kockázati profil láthatósága

A felhő egyszerű skálázhatóságának és felhőszolgáltatásokhoz és más adatforrásokhoz való azonnal használható összekötőknek köszönhetően jelentősen javíthatja a kockázati profil átláthatóságát.

35%-os
csökkenés a biztonságsértések kockázatában[2]

93%-os
csökkenés az új kapcsolat konfigurálásához szükséges időben[2]

Első lépések

Ha szeretné Ön is megtapasztalni a Microsoft Sentinel előnyeit, indítson ingyenes próbaidőszakot, és fedezze fel a további erőforrásokat és bemutatókat! A Microsoft Sentinel optimális választás azoknak a vállalatoknak, amelyek szeretnék javítani a biztonsági tevékenységeiket, csökkenteni a költségeiket és javítani a hatékonyságukat.

További információ →   **Díjszabás →**   **Ügyféltörténetek →**

---

1. **Gartner, Magic Quadrant for Security Information and Event Management, szerzők: Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 2024. május 8.** A Gartner nem támogatja a tanulmányaiban szereplő vállalatokat, termékeket és szolgáltatásokat, és nem javasolja a felhasználóknak, hogy csak a legjobb minősítést kiérdemlő vagy más módon kiemelt gyártókat válasszák. A Gartner kutatási jelentései a Gartner kutatási és tanácsadói részlegének véleményét tartalmazzák, és nem tekintendők ténymegállapításoknak. A Gartner nem vállal semmilyen kifejezett vagy vélelmezett jótállást a jelen kutatásra vonatkozóan, beleértve az eladhatóságra és az adott célra való alkalmasságra vonatkozó jótállást is. A GARTNER név a Gartner, Inc. és/vagy társvállalatainak bejegyzett védjegye és szolgáltatási védjegye az Egyesült Államokban és nemzetközi szinten; a Magic Quadrant pedig a Gartner, Inc. és/vagy társvállalatainak bejegyzett védjegye; a jelen kiadványban ezeket engedéllyel használjuk. Minden jog fenntartva.
2. **Forrester Total Economic Impact™ of Microsoft Sentinel** The Total Economic Impact(TM) Of Microsoft Sentinel, a Forrester Consulting által megbízásból készített tanulmány, 2024. március. Az eredmények a megkérdezett ügyfelek alapján összeállított, átlagos vállalkozáson alapulnak.

Microsoft Security