Új funkciókkal április 1-jén érkezik a Microsoft Copilot for Security

Az elmúlt két évben riasztó mértékben, másodperceként 579-ről több mint 4000-re emelkedett a Microsoft rendszerein belül regisztrált jelszótámadások száma. Mindeközben a kiberbűnözés okozta kár globálisan a 2015. évi 3 billió dollárról, előrejelzések szerint 2025-re, mintegy 10,5 billió dollárra nő. Annak ellenére, hogy a szervezetek átlagosan mintegy 80-féle kiberbiztonsági szoftvert használnak, még mindig nehezen tudnak megbirkózni a túlterheléses támadásokkal, a hamis riasztások miatti kifáradással és a biztonsági megoldások átláthatatlanságával.

A Microsoft mai bejelentése szerint a Microsoft Copilot for Security április 1-jén válik elérhetővé világszerte. Ez lesz az iparág első generatív mesterséges intelligenciával megtámogatott megoldása, amely a kiberbiztonságért felelős szakembereknek és rendszergazdáknak fog segíteni abban, hogy felfedjék azokat a támadásokat is, amelyek jelenleg rejtve maradnak. Felgyorsíthatják munkafolyamataikat, és javíthatják a védekező műveletek hatékonyságát. A Copilot hatalmas mennyiségű adatot és azokból kivonható információt képes átlátni: a Microsoft több mint 78 billió biztonsági incidensre figyelmeztető jelet dolgoz fel ennek segítségével minden egyes nap. Ezt egészíti ki a nagy nyelvi modellekre épülő információgyűjtés, amely az adott helyzetre érvényes javaslatokat és cselekvési tervet kínál. A Copilot támogatásával a vállalatok és szervezetek gépi sebességgel, és csak a mesterséges intelligenciára jellemző kiterjedtséggel képesek megvédeni a rendszereiket, miközben a biztonsági folyamataik is teljesen átalakulnak. A Copilot for Security világszerte április 1-jén válik elérhetővé, nyolc nyelven lesz képes megérteni a beszéltnyelvi utasításokat (prompt) és válaszokat adni rájuk, a felhasználó felületének feliratait pedig 25 nyelvre fordították le.

> „A második alkalommal elvégzett Copilot for Security felmérésünk megerősítette azt, amit mi magunk is megtapasztaltunk a szoftver használata közben: még a tapasztalt biztonsági szakemberek munkája is **22%-kal lesz gyorsabb a Copilottal**, miközben a **feladatvégrehajtás pontossága 7%-kal javul.** A felmérésünkbe bevont szakemberek **97%-a válaszolta azt, hogy szeretné tovább használni a Copilotot** a mindennapi munkájában. – mondta el Renate Strazdina, a Microsoft Közép-Európáért felelős műszaki igazgatója. „A Microsoft Copilot for Security képessé teszi a szakembereket arra, hogy jobban kihasználják a tudásukat, hogy még gördülékenyebben működjenek együtt egymással, hogy több információra tegyenek szert, és hogy időben válaszolhassanak a biztonsági incidensekre. Az új eszköz használatával teljesen átalakul a kiberbiztonsági munka, éppen ezért tölt el bennünket nagy izgalommal és örömmel, hogy végre mindenkivel megoszthatjuk a világon.

Használatarányos előfizetési modell

A Microsoft célja az, hogy a nagyobb biztonságot mindenki számára elérhetővé tegye. Éppen ezért, a piacon egyedülálló módon, a Microsoft egy „pay-as-you-go” licencmegoldással a lehető legtöbb szervezet számára teszi hozzáférhetővé a Copilot for Security-t. Ez egy rendkívül rugalmas, használatarányos előfizetést jelent, amely lehetővé teszi, hogy a vállalatok azonnal megkezdhessék az új eszköz használatát. Elég ezt követően, a tényleges használatnak megfelelően és a költségek ismertében dönteni a továbbhasználatról.

A Copilot for Security újdonságai

A Microsoft Copilot for Security abban segít a kiberbiztonsági és IT szakembereknek, hogy még hatékonyabban tudják felhasználni a tudásukat és működhessenek együtt a kollégáikkal, hogy még több mindenre lássanak rá az általuk felügyelt rendszereken belül, és hogy gyorsabban tudjanak reagálni az incidensekre. A Copilot for Security az alábbi új képességeket kínálja:

- **Az egyéni prompt-lista funkció** arra szolgál, hogy a felhasználók a saját korábbi beszéltnyelvi utasításaikat elmentve kiberbiztonsági munkafolyamatokat és feladatokat hozzanak létre.
- **A tudásbázis-integráció funkció**, amely egyelőre előzetesként érhető el, lehetővé teszi a Copilot for Security integrálását a vállalatirányítási rendszerbe, valamint olyan feladatok végrehajtását, amely az adott vállalat saját cselekvési tervét követi.
- **A felhasználó összekötheti a saját, Defender EASM-ben, a külső támadások elhárítására létrehozott felületét a Copilottal**, hogy azonosíthassa és kielemezhesse a legfrissebb, külső támadások kockázataira vonatkozó információkat.
- **A Microsoft Entra audit és diagnosztikai logok** további információkkal szolgálnak a biztonsági fenyegetések azonosításához, vagy az egyes felhasználókhoz vagy incidensekhez köthető informatikai problémák elemzéséhez. Mindezekről szöveges összefoglalókat készít.
- **A felhasználási jelentés** áttekintést nyújt arról, hogy a csapatok hogyan használják a Copilotot. Ez lehetőséget ad újabb pontok azonosítására a munkafolyamaton belül, ahol tovább lehet optimalizálni a működést.

Mesterséges intelligenciával megtámogatott biztonság mindenkinek

A Copilot for Security megalapozhat egy önállóan is működőképes, átfogó biztonsági rendszert, de beépülhet egy már meglévő biztonsági rendszerbe is. A Microsoft egyéb biztonsági rendszereivel való könnyű integrálhatóságát az IT és biztonsági szakemberek fogják nagyra értékelni, akik megtapasztalhatják azt a sebesség- és hatékonyság növekedést, amit a Microsoft idézett felmérése feltárt.

Itt az idő az MI felfedezésére!

Egyre több, az üzleti működés minden területét érintő, generatív MI-alapú szolgáltatás jelenik meg a piacon, amelyek azt bizonyítják, hogy az új technológia számtalan lehetőséget kínál, ugyanakkor új kihívásokat és kockázatokat is hordoz magában. A Microsoft, mindezeket figyelembe véve, nagyobb átláthatóságot, védelmet és kontrollt kínál az MI-applikációk vonatkozásában, függetlenül attól, hogy az illető szervezet Microsoft Copilot-ot vagy más, harmadik féltől származó generatív mesterséges intelligencia alapú szoftvert használ-e. A Microsoft azt szeretné elérni, hogy minden szervezet magabiztosan és biztonságos körülmények között kezdhesse meg a mesterséges intelligencia alkalmazását.

Annak érdekében, hogy a szervezetek védett és ellenőrzött módon használhassák a mesterséges intelligenciát, a Microsoft az alábbi szolgáltatásokkal bővítette meglévő termékeit:

- **Az MI használatából fakadó kockázatok felderítése**: a kiberbiztonságért felelős csapatok feltárhatják az MI használatából adódó potenciális veszélyforrásokat, mint amilyen például a szenzitív adatok kiszivárgása, vagy az, hogy a felhasználók nagy kockázati besorolású applikációkhoz férhetnek hozzá.

- **Az MI-alapú applikációk és az adatok védelme**: a biztonságért felelős szakemberek és rendszergazdák védőernyőt vonhatnak a használatba vett MI-alapú applikációk és az általuk gyűjtött és előállított szenzitív adatok fölé, ideértve a promptokat és a válaszokat is.
- **Ellenőrzött használat**: a biztonságért felelős szakemberek irányíthatják az MI-alapú applikációk használatát az interakciók korlátozásával és loggolásával, így tárva fel az ezen applikációk használata közben előforduló bármilyen illegális tevékenységet vagy a vállalati szabályok megsértését, illetve kivizsgálhatják az így felmerülő incidenseket.

Biztonság a mesterséges intelligencia korszakában

A Copilot for Security alkalmazásával a szervezetek többféle oldalról is képesek megvédeni a munkakörnyezeteiket, legyen szó a kiberbiztonságról, a törvényi megfelelőségről, az adatvédelemről, a perifériák kezeléséről vagy a személyes adatok védelméről. A mesterséges intelligencia korszakában, minden eddiginél fontosabbá válik az egységes megoldások alkalmazása, amelyek betömik a védelmi rendszer réseit.

Sajtókapcsolat:

- Karolina Krizenecka, PR vezető
- kkrizenecka@microsoft.com

Eredeti tartalom: Microsoft

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/12247/uj-funkciokkal-aprilis-1-jen-erkezik-a-microsoft-copilot-for-security/