AI CYBERSECURITY SUMMIT

Kiberbiztonság az AI-ban vagy AI a kiberbiztonságban?

2026. 09. 08. 12:35 | Innovation Hall | HUN · 20 perc

Balogh Péter
Territory Manager · Google Cloud, Hungary

Balogh Péter, a Google Cloud Magyarország területi vezetője keretrendszert hoz létre az AI-rendszerek fejlődő kiberfenyegetésekkel szembeni védelmére, miközben lehetővé teszi a biztonságos üzleti bevezetést.

MIRŐL VOLT SZÓ

A prezentáció kiemeli, hogy az AI felgyorsítja a kibertámadásokat, lehetővé téve a szereplők számára, hogy kifinomult fenyegetéseket generáljanak gyorsabban, mint ahogy a hagyományos beszerzési folyamatok képesek védekezni ellenük. Példák közé tartozik a Fraud GPT és a Worm GPT használata a rosszindulatú tevékenységek automatizálására, valamint a polimorf támadások megjelenése, ahol az AI gyorsan módosítja a forráskódot a felismerés elkerülése érdekében. Balogh Péter megjegyzi, hogy még az egyszerű feladatok, mint például egy meggyőző adathalász oldal létrehozása, most már csak 18 percet vesz igénybe a hónapok helyett.

Ezen kockázatok ellensúlyozására a felszólaló egy proaktív védelmi stratégia mellett érvel, amely az AI-t használja fenyegetés-információkhoz és automatizált válaszhoz. Ez magában foglalja a teljes kódbázisok elemzésére szolgáló Gemini használatát, a specifikus fenyegetési szereplők, például az APT 29 azonosítását, valamint a belső biztonsági szabályok automatikus generálását. Ezek az elemek együttesen azt jelentik, hogy a szervezeteknek át kell térniük a manuális, Excel-alapú biztonságról az AI-kiegészített rendszerekre, hogy lépést tartsanak az automatizált ellenségekkel.

KIEMELT MEGÁLLAPÍTÁSOK

- AI lehetővé teszi a támadók számára, hogy kifinomult adathalász webhelyeket és rosszindulatú kódokat percek alatt hozzanak létre, nem pedig hónapok alatt.
- A Shadow AI jelentős kockázatot jelent, ha a munkavállalók felügyelet nélkül töltik fel a vállalati érzékeny adatokat nyilvános modellekbe.
- A többrétegű védelem olyan integrált rendszereket igényel, amelyek egymással kommunikálnak, nem pedig egymástól elszigetelt biztonsági eszközöket.

ÜZLETI HATÁS

A gyakorlati alkalmazás során a Chrome Enterprise Core telepítésével blokkolhatók a jogosulatlan AI-oldalak, a Gemini Enterprise használatával pedig biztosítható, hogy az adatok biztonságos DMZ-n belül maradjanak. Ezeknek a keretrendszereknek a bevezetésével a vállalatok áttérhetnek az eseti manuális védekezésről az automatizált folyamatokra, és végül egyensúlyt érhetnek el az AI-innováció üzleti igénye és az ügyféladatok, valamint a szellemi tulajdon védelmének szükségessége között.

KÖVETKEZTETÉS

Balogh Péter négy lépésből álló folyamatot javasol: a kézi védelemről az AI-val kiegészített biztonságra való áttérés, a böngésző szintű vezérlők használata, a Mandianthez hasonló etikus hackerekkel történő rendszeres ellenőrzés, és végül a teljesen automatizált rendszer elérése. A cél egy olyan biztonságos környezet létrehozása, ahol a vállalat szabadon használhatja az AI-t anélkül, hogy veszélyeztetné a szervezeti biztonságot.

AI CYBERSECURITY SUMMIT

Cybersecurity in AI or AI in Cybersecurity?

2026. 09. 08. 12:35 | Innovation Hall | HUN · 20 perc

Péter Balogh
Territory Manager · Google Cloud, Hungary

Péter Balogh, Territory Manager at Google Cloud, Hungary, establishes a framework for securing AI systems against evolving cyber threats while enabling safe business adoption.

WHAT WAS DISCUSSED

Péter Balogh explains how attackers use AI to accelerate threats, such as generating polymorphic code that changes rapidly to evade detection. He highlights that tools like Fraud GPT and Worm GPT allow low-skilled actors to launch sophisticated attacks faster than a company can procure security software, for example, by creating perfect clones of corporate websites in just 18 minutes.

The presentation covers internal risks like Shadow AI, where employees upload sensitive data to public models, and the danger of indirect prompt injections hidden in files. Balogh advocates for a proactive defense using AI agents to automate the triage of thousands of daily alerts and the generation of security rules. These elements mean that organizations must move from manual, reactive security to an automated, AI-augmented pipeline to keep pace with modern adversaries.

KEY TAKEAWAYS

- Attackers can now use AI to generate sophisticated phishing calls and clone websites in minutes rather than months.
- Shadow AI poses a significant risk when employees bypass firewalls by using mobile hotspots to access unauthorized AI tools.
- A multi-layered defense strategy must include automated triage, browser-level controls, and continuous validation by ethical hackers.

BUSINESS IMPACT

Implementing these strategies allows businesses to adopt AI safely without compromising data integrity or falling victim to automated fraud. By using Gemini Enterprise, companies ensure that data remains within a secure DMZ and is not used to train public models. Furthermore, utilizing Chrome Enterprise Core helps prevent the accidental leakage of internal API keys and sensitive corporate information.

CONCLUSION

Péter Balogh concludes by recommending a four-step evolution from manual defense to fully automated systems. He urges the audience to adopt public frameworks, utilize browser-level protections, and engage with professional validation services like Mandiant to ensure a robust security posture.