ai automotive summit

Beyond the AI Hype: What AI Can Actually Do for Your Product Security

2026. 09. 07. 15:40 | Future Lab | HUN · 20 perc

Pentz Tamás
Senior Threat Intelligence Analyst · PCA Cyber Security

Pentz Tamás, a PCA Cyber Security vezető fenyegetés-információs elemzője, a termékbiztonság fejlődő területéről és a mesterséges intelligencia kritikus szerepéről beszél a sebezhetőségek azonosításában és enyhítésében.

MIRŐL VOLT SZÓ

A prezentáció a fizikai termékek átfogó biztonságát vizsgálja, lefedve a teljes életciklust a gyártás előtti fázistól a piac utáni bevezetésig. Pentz Tamás kifejti, hogy a modern járművek összetett ökoszisztémák, amelyek motorvezérlőket, mobilkapcsolatot és Android alapú fejegységeket tartalmaznak, és ezek mind összekapcsolódnak, valamint sebezhetőek a kiberfenyegetésekkel szemben. Például a jövőbeli technológiák, mint a V2X kommunikáció, tovább növelik a támadási felületet, lehetővé téve a járművek egymás közötti és az infrastruktúrával való kommunikációját.

A vita jelentős része arra összpontosít, hogy az mesterséges intelligencia csökkenti a támadók belépési korlátját a sebezhetőségek automatizált felfedezésével és kihasználásával. Pentz Tamás kiemeli, hogy a támadók az AI-t használják a mikrokód elemzésére és a kiaknázások tesztelésére, míg a védekezők hasonló eszközöket használhatnak a hatalmas mennyiségű adat szűrésére és a magas kockázatú problémák kiemelésére. Például a Google megfigyelte, hogy az APT 45 csoport az AI-t használta a régebbi mikrokód sebezhetőségek keresésére. Ezek a fejlemények azt jelentik, hogy a biztonsági szakembereknek AI-alapú eszközöket kell alkalmazniuk a fenyegetések hatalmas mennyiségének hatékony kezelésére.

KIEMELT MEGÁLLAPÍTÁSOK

- AI jelentősen csökkenti a komplex kiberfenyegetések végrehajtásához szükséges készségeket.
- A védekezők mesterséges intelligenciát használhatnak a szoftver-összetételi lista (SBOM) és a hardver-összetételi lista (HBOM) gyűjtésének és elemzésének automatizálására.
- A sebezhetőség kockázatát inkább az elérhetőségének és potenciális hatásának mértéke, mint a elméleti súlyossági pontszám határozza meg.

ÜZLETI HATÁS

Az AI biztonsági folyamatokba való integrálása lehetővé teszi a szervezetek számára, hogy olyan nagy mennyiségű adatot kezeljenek, amelyek egyébként túlterhelnék az emberi elemzőket. A helyi AI modellek használatával a bizalmas összetevők elemzése és a bűnözői fórumok figyelése révén a vállalatok hatékonyabban azonosíthatják a beszállítói lánc kockázatait és a konkrét verziók sebezhetőségét. Ez a megközelítés optimalizálja a költséges emberi szakértelem használatát, biztosítva, hogy a hardver tesztelő csapatok csak a legkritikusabb, validált fenyegetésekre összpontosítsanak.

KÖVETKEZTETÉS

Pentz Tamás azzal zárja, hogy hangsúlyozza: mivel az támadók már használják az AI-t, a védekezőknek is lépést kell tartaniuk azzal, hogy ugyanezt a technológiai eszköztárat alkalmazzák. Ajánlás, hogy az AI-t asszisztensként használják a hamis pozitívok csökkentésére és az alacsonyabb szintű elemzések kezelésére, miközben az emberi felügyeletet fenntartják a végső döntéshozatalhoz. A végső cél az, hogy ezeket a modelleket emberi intuícióval képezzék ki, hogy biztosítsák a robusztus védelmet az egyre kifinomultabb automatizált fenyegetésekkel szemben.

ai automotive summit

Beyond the AI Hype: What AI Can Actually Do for Your Product Security

2026. 09. 07. 15:40 | Future Lab | HUN · 20 perc

Pentz Tamás
Senior Threat Intelligence Analyst · PCA Cyber Security

Pentz Tamás, a Senior Threat Intelligence Analyst at PCA Cyber Security, establishes a framework for product protection that encompasses the entire lifecycle of physical products, from pre-production to post-manufacturing security.

WHAT WAS DISCUSSED

Pentz Tamás explains that modern product security must account for a vast ecosystem of interconnected components, including engine controllers, mobile networks, Android head units, and V2X communication systems. The scope of protection extends beyond the physical hardware to include cloud-based updates and mobile applications connected to the product's backend. For example, a vehicle's security is now tied to its ability to communicate with other cars and infrastructure in a connected environment.

The presentation highlights how artificial intelligence lowers the barrier to entry for attackers by automating vulnerability discovery and code analysis. Pentz Tamás notes that attackers use AI to scan legacy microcode for flaws, while defenders use it to filter massive amounts of data into manageable tasks for human analysts. For example, Google observed threat actors using AI to identify and test vulnerabilities in older codebases. These elements mean that AI acts as a force multiplier that necessitates a shift toward automated, high-speed defensive screening.

KEY TAKEAWAYS

- Attackers use AI to bypass traditional security barriers and rapidly identify exploitable flaws in legacy systems.
- Defenders can utilize AI to automate the collection and analysis of Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM).
- Human intuition remains essential in the security loop to validate AI-generated results and handle high-level decision-making.

BUSINESS IMPACT

The integration of AI into threat intelligence allows companies to manage the overwhelming volume of daily vulnerabilities more efficiently. By using local AI models to analyze firmware dumps and open-source components, organizations can achieve an 80% confidence level in identifying risks before involving expensive hardware testing teams. This approach optimizes resource allocation, ensures that human experts focus on the most critical threats, and protects against massive financial losses, such as the billions of dollars potentially at risk in compromised cryptocurrency hardware.

CONCLUSION

Pentz Tamás concludes by emphasizing that because attackers are already utilizing these advanced tools, organizations must adopt similar AI-driven methodologies to keep pace. The recommendation is to use AI as an assistant to reduce false positives and streamline data processing while maintaining a human-in-the-loop system to ensure accuracy and security.