AI CYBERSECURITY SUMMIT

Hogyan használható az AI a security incidensek detektálása során?

2026. 09. 08. 12:15 | Innovation Hall | HUN · 20 perc

Gerner Viktor
Információbiztonsági szakértő · ONE Magyarország Zrt.

Gerner Viktor, az ONE Magyarország Zrt. információbiztonsági szakértője, bemutatja a Security and Operation Center (SOC) fejlesztésének és működtetésének kihívásait, valamint a mesterséges intelligencia biztonsági elemzésbe való integrálását.

MIRŐL VOLT SZÓ

A prezentáció a SOC-ot olyan hibrid rendszerként írja le, amely gépvezérelt adatfeldolgozást és emberi elemzést ötvöz a tényleges biztonsági incidensek és a téves riasztások megkülönböztetésére. Gerner Viktor elmagyarázza, hogy a szolgáltatás szigorú IT-biztonsági határokat és a adatok bizalmas kezelését igényli ahhoz, hogy hatékonyan támogassa a klienseket a fenyegetések, például kártevők vagy titkosító kulcsok azonosításában és kezelésében.

A megbeszélés a SOC-szolgáltatás fenntartásának nehézségeit tárgyalja, beleértve a nagy adatmennyiséget, a kiberfenyegetések dinamikus jellegét és az elemzői munka ismétlődő jellegét, amely magas fluktuációhoz vezet. Gerner Viktor kiemeli az új termékről a fejlett piaci igények felé történő átmenetet, ahol a hangsúly az eredeti fejlesztésről a hosszú távú karbantartásra és a komplex, fejlődő problémák megoldására helyeződik. Ezek az elemek azt mutatják, hogy egy sikeres SOC megköveteli a technológiai innováció és a fenntartható emberi műveletek közötti egyensúlyt.

KIEMELT MEGÁLLAPÍTÁSOK

- A SOC szolgáltatást kilenc éve nyújtják, és ehhez egyedi architektúra szükséges a különböző ügyfelek közötti szigorú elszigeteltség biztosításához.
- A kutatási és fejlesztési program feltárta, hogy a meglévő adatbázisok kezdetben nem voltak alkalmasak mesterséges intelligencia modellek képzésére, és hat hónap intenzív képzésre és adatszimplifikációra volt szükség.
- Az AI modell 87%-os pontossággal azonosította az eseményeket közvetlenül a naplókból, ami megegyezik az emberi elemzők eredményeivel.

ÜZLETI HATÁS

Az AI integrációjának célja a naplók szabályalapú feldolgozásának optimalizálása és a biztonsági riasztások minőségének javítása. Az riasztási szintű elemzésről a közvetlen naplóelemzésre való áttéréssel a rendszer pontosabban kategorizálhatja az eseményeket, például megkülönböztetve a hamis riasztásokat azoktól, amelyeknek nincs azonnali hatása, de hosszú távon jelentősek lehetnek. Ez a megközelítés javítja a szolgáltatás képességét, hogy régióspecifikus biztonságot nyújtson a magas szintű ügyfelek számára, miközben biztosítja a DORA szabványoknak való megfelelést.

KÖVETKEZTETÉS

Gerner Viktor azzal zárja, hogy hangsúlyozza: a végső döntés a kliens felé történő eskalálásról mindig egy emberi elemzőnél marad. A végső cél egy csúszó ablak karbantartási rendszer bevezetése, amely folyamatosan tanul az új adatokból, hogy a legfrissebb fenyegetés-információkat szolgáltassa. A beszélő arra ösztönzi a közönséget, hogy fontolja meg, hogyan javíthatják ezek a fejlesztések az általános szolgáltatási minőséget és a válaszidőket az új fenyegetésekre.

AI CYBERSECURITY SUMMIT

How Can AI Be Used to Detect Security Incidents?

2026. 09. 08. 12:15 | Innovation Hall | HUN · 20 perc

Viktor Gerner
Information Security Expert · ONE Magyarország Zrt.

Viktor Gerner, an Information Security Expert at ONE Magyarország Zrt., discusses the development and operational challenges of implementing artificial intelligence within a Security Operations Center (SOC).

WHAT WAS DISCUSSED

Viktor Gerner explains that a SOC combines machine components for data processing with human analysts who make critical decisions based on those inputs. The service, which has been active for nine years, requires strict IT security boundaries and high confidentiality to manage diverse client data. For example, the system processes logs from firewalls into a SIEM, where rules generate alerts for human escalation.

The presentation highlights the difficulties of maintaining a service where human analysts face repetitive work and high turnover. Viktor Gerner describes the struggle to develop custom AI solutions because many vendors offer cloud-based products that do not meet the specific requirement of local data storage in Hungary. These challenges led to an internal research and development program to create a static proof of concept. Taken together, these elements demonstrate the transition from manual alert monitoring to automated incident detection.

KEY TAKEAWAYS

- The AI model achieved an 87% accuracy rate in identifying incidents directly from logs, matching the performance of human analysts.
- A significant hurdle in AI development is the need for high-quality, normalized training data, as raw operational logs are often unsuitable for machine learning.
- The final decision to escalate an incident remains a human responsibility to ensure compliance with security standards like DORA.

BUSINESS IMPACT

The implementation of AI aims to improve service quality by enabling faster reactions to new threats and providing region-specific security. By using anonymized data from a broad client base to train models, the organization can identify patterns that protect all customers simultaneously. This approach positions the company to offer more sophisticated, proactive security services that move beyond generalities to address specific, evolving cyber threats.

CONCLUSION

Viktor Gerner concludes by emphasizing that the ultimate goal is a sliding-window maintenance model where the AI continuously learns from new data. He recommends that any future development must prioritize traceability and explainability over "black box" systems. The speaker encourages the audience to view AI as a tool to optimize the rule-based process and enhance the overall quality of security operations.