

KIBERXAVFSIZLIKNI AVTOMATLASHTIRISHDA SUN'IY INTELLEKT ROLI

Botirova Nigoraxon Shuxratjon qizi
Toshkent amaliy fanlar universiteti, Axborot texnologiyalari fakulteti,
Kompyuter injiniringi kafedrası o'qituvchisi

Annotatsiya

Ushbu maqolada kiberxavfsizlikni avtomatlashtirish jarayonida Sun'iy intellekt texnologiyalarining o'rni keng va chuqur yoritilgan. Zamonaviy axborot tizimlarida xavfsizlikni ta'minlashda avtomatlashtirilgan yondashuvlarning ahamiyati, tahdidlarni aniqlash, tahlil qilish va ularga tezkor javob berishda Machine Learning algoritmlarining roli batafsil tahlil qilingan. Shuningdek, Security Operations Center faoliyatida sun'iy intellektdan foydalanishning amaliy jihatlari, afzalliklari, muammolari va istiqbollari keng ko'rib chiqilgan.

Kalit so'zlar: kiberxavfsizlik, sun'iy intellekt, mashinaviy o'rganish, avtomatlashtirish, tahdidlarni aniqlash, SOC, axborot xavfsizligi, raqamli himoya, kiberhujumlar, anomaliya tahlili

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi natijasida jamiyat hayotining barcha sohalari raqamlashtirilmoqda. Bank tizimlari, davlat boshqaruvi, elektron tijorat, ta'lim va sog'liqni saqlash kabi sohalarda axborot tizimlaridan keng foydalanilmoqda. Bu esa ma'lumotlar xavfsizligini ta'minlash masalasini yanada dolzarb qilib qo'ymoqda. Kiberhujumlar sonining ortishi, ularning murakkablashuvi va avtomatlashtirilgan shaklga o'tishi zamonaviy kiberxavfsizlik tizimlarini takomillashtirishni talab etmoqda.

An'anaviy kiberxavfsizlik tizimlari ko'pincha qo'lda boshqariladigan va reaktiv xarakterga ega. Ya'ni, ular hujum sodir bo'lgandan keyin choralar ko'radi. Bunday yondashuv esa zamonaviy tahdidlarga qarshi yetarli emas. Shu sababli, proaktiv va avtomatlashtirilgan xavfsizlik tizimlariga ehtiyoj ortmoqda. Aynan shu nuqtada sun'iy intellekt asosidagi yechimlar muhim ahamiyat kasb etadi.

Kiberxavfsizlikni avtomatlashtirish bu xavfsizlik jarayonlarini minimal inson aralashuvi bilan amalga oshirishni anglatadi. Bu jarayonda tahdidlarni aniqlash, monitoring qilish, hodisalarga javob berish va tizimlarni himoyalash kabi vazifalar avtomatik tarzda bajariladi. Sun'iy intellekt esa ushbu jarayonlarning markaziy elementi hisoblanadi.

Sun'iy intellekt tizimlari katta hajmdagi ma'lumotlarni qayta ishlash va tahlil qilish imkoniyatiga ega. Masalan, tarmoq trafiklari, foydalanuvchi faoliyati va tizim loglari doimiy ravishda monitoring qilinadi. AI ushbu ma'lumotlar asosida normal va noodatiy faoliyatni ajrata oladi. Bu esa anomaliya aniqlash imkonini beradi. Anomaliyalarni aniqlash esa kiberhujumlarni erta bosqichda aniqlashda juda muhim hisoblanadi.

Mashinaviy o'rganish algoritmlari yordamida tizimlar vaqt o'tishi bilan o'z faoliyatini yaxshilab boradi. Ya'ni ular yangi tahdidlarni aniqlashni o'rganadi va moslashadi. Bu esa kiberxavfsizlikni yanada samarali qiladi. Masalan, phishing hujumlari yoki zararli dasturlar har safar yangi shaklda paydo bo'ladi. AI esa ularning umumiy xususiyatlarini aniqlab, yangi variantlarini ham tanib olish imkoniyatiga ega bo'ladi.

Kiberxavfsizlikni avtomatlashtirishda yana bir muhim yo'nalish bu hodisalarga javob berish tizimidir. AI asosidagi tizimlar hujum aniqlangandan so'ng avtomatik tarzda choralar ko'radi. Masalan, zararli IP manzillar bloklanadi, zararlangan tizim izolyatsiya qilinadi yoki foydalanuvchi faoliyati vaqtincha cheklanadi. Bu esa hujumning kengayishining oldini oladi va zarar miqdorini kamaytiradi.

Zamonaviy tashkilotlarda Security Operations Center muhim rol o'ynaydi. Ushbu markazlarda kiberxavfsizlik bilan bog'liq barcha jarayonlar boshqariladi. Biroq SOC tizimlarida juda katta hajmdagi ma'lumotlar oqimi mavjud bo'lib, ularni qo'lda tahlil qilish murakkab va samarasiz hisoblanadi. Sun'iy intellekt yordamida ushbu muammo hal etiladi. AI ogohlantirishlarni avtomatik saralaydi, muhimlarini ajratadi va tahlil qiladi. Bu esa mutaxassislar ishini yengillashtiradi va samaradorlikni oshiradi.

Sun'iy intellekt asosidagi avtomatlashtirishning asosiy afzalliklaridan biri bu tezlikdir. AI tizimlari insondan bir necha barobar tez ishlaydi va katta hajmdagi ma'lumotlarni qisqa vaqt ichida qayta ishlaydi. Bundan tashqari, ular 24 soat davomida uzluksiz ishlash imkoniyatiga ega. Bu esa doimiy monitoringni ta'minlaydi.



1-rasm. Kiberxavfsizlikni avtomatlashtirishda sun'iy intellekt ro'li

Ushbu rasmda Kiberxavfsizlikni avtomatlashtirishda sun'iy intellekt ro'li mavzusini to'liq qamrab olgan sxema berilgan va yoritilgan.

Yana bir muhim afzallik bu aniqlikdir. AI tizimlari inson xatolarini kamaytiradi va tahdidlarni aniqlash aniqligini oshiradi. Shu bilan birga, avtomatlashtirish xarajatlarni kamaytirish va resurslardan samarali foydalanish imkonini beradi.

Biroq, sun'iy intellekt texnologiyalarining ayrim cheklovlari ham mavjud. Eng katta muammolardan biri bu noto'g'ri aniqlashlar hisoblanadi. Ba'zi hollarda tizim oddiy faoliyatni ham tahdid sifatida qabul qilishi mumkin. Bu esa ortiqcha resurs sarfiga olib keladi.

Bundan tashqari, AI tizimlari katta hajmdagi sifatli ma'lumotlarga muhtoj. Agar ma'lumotlar yetarli yoki to'g'ri bo'lmasa, tizim noto'g'ri qarorlar qabul qilishi mumkin. Shuningdek, sun'iy intellektni joriy etish yuqori texnik bilim va moliyaviy resurslarni talab qiladi.

Yana bir muhim jihat shundaki, kiberjinoyatchilar ham sun'iy intellektidan foydalanmoqda. Ular AI yordamida murakkab hujumlarni ishlab chiqmoqda va xavfsizlik tizimlarini aldashga harakat qilmoqda. Bu esa kiberxavfsizlik sohasidagi kurashni yanada murakkablashtirmoqda.

Shu sababli, eng samarali yondashuv bu sun'iy intellekt va inson hamkorligidir. AI tizimlari tezkor tahlil va avtomatlashtirishni ta'minlaydi, inson esa strategik qarorlar qabul qiladi va tizimni nazorat qiladi. Bu kombinatsiya yuqori darajadagi xavfsizlikni ta'minlaydi.

Kelajakda kiberxavfsizlik sohasida sun'iy intellektning roli yanada ortishi kutilmoqda. Avtonom xavfsizlik tizimlari, o'z-o'zini himoya qiluvchi platformalar va real vaqt rejimida ishlovchi tizimlar keng tarqaladi. Shuningdek, nol ishonch konsepsiyasiga asoslangan xavfsizlik arxitekturalari rivojlanadi.

qoridagi tahlillar shuni ko'rsatadiki, kiberxavfsizlikni avtomatlashtirishda Sun'iy intellekt texnologiyalari zamonaviy axborot tizimlarining ajralmas qismiga aylanib bormoqda. Raqamli transformatsiya jarayonining kengayishi bilan birga kiberxavflarning soni va murakkabligi ortib borayotgan bir sharoitda an'anaviy himoya usullari yetarli darajada samarali bo'la olmayapti. Shu bois avtomatlashtirilgan va aqlli xavfsizlik tizimlarini joriy etish zaruratga aylanmoqda.

Sun'iy intellekt asosidagi tizimlar kiberxavfsizlikni yangi bosqichga olib chiqib, tahdidlarni real vaqt rejimida aniqlash, tahlil qilish va ularga tezkor javob berish imkonini yaratadi. Ayniqsa, Machine Learning algoritmlari yordamida tizimlar o'z-o'zini o'rganish va yangi tahdid turlariga moslashish qobiliyatiga ega bo'lmoqda. Bu esa proaktiv himoya modelini shakllantirishda muhim omil hisoblanadi.

Shuningdek, Security Operations Center faoliyatida sun'iy intellektni qo'llash orqali xavfsizlik jarayonlarini sezilarli darajada optimallashtirish mumkin. AI yordamida ogohlantirishlarni saralash, ustuvorliklarni aniqlash va avtomatik javob berish jarayonlari tezlashadi. Natijada mutaxassislar yuklamasi kamayadi va ular murakkab strategik masalalarga e'tibor qaratish imkoniyatiga ega bo'ladi.

Biroq, sun'iy intellekt texnologiyalarining joriy etilishi bilan bir qatorda ayrim muammolar ham yuzaga kelmoqda. Jumladan, noto'g'ri aniqlashlar, ma'lumot sifati bilan bog'liq muammolar va avtomatlashtirish darajasining ortishi natijasida inson nazoratining kamayishi xavfi mavjud. Bundan tashqari, kiberjinoyatchilar ham sun'iy intellektidan foydalanib, yanada murakkab va yashirin hujumlarni amalga oshirmoqda.

Foydalanilgan adabiyotlar

1. IBM Security. Cost of a Data Breach Report 2023. IBM Corporation, 2023.
2. ENISA. ENISA Threat Landscape 2022. European Union Agency for Cybersecurity, 2022.
3. Cisco. Cybersecurity Report Series 2021–2024. Cisco Systems, 2024.
4. Microsoft. Digital Defense Report 2023. Microsoft Security, 2023.
5. World Economic Forum. Global Cybersecurity Outlook 2024. WEF, 2024.
6. NIST. AI Risk Management Framework 1.0. National Institute of Standards and Technology, 2023.
7. Gartner. Top Trends in Cybersecurity 2022–2024. Gartner Research, 2024.
8. Sarker, I. H. Machine Learning for Cybersecurity: A Comprehensive Review. Journal of Cybersecurity and Privacy, 2021.
9. Goodfellow, I., McDaniel, P., Papernot, N. Making Machine Learning Robust Against Adversarial Inputs. Communications of the ACM, 2020.
10. Shokri, R., et al. Privacy Risks in Machine Learning Systems. IEEE Security & Privacy, 2021.