

KIBERXAVFSIZLIK SOHASIDA SUN'IY INTELLEKT

Dildor Arifovna Sabirova

Xalqaro Nordik universiteti "Sanoatni boshqarish va raqamli texnologiyalar" kafedrası
Dotsent

Annotatsiya:

Ushbu maqolada sun'iy intellekt (SI)ning kiberxavfsizlik sohasidagi roli va qo'llanilishi tahlil qilinadi. Maqolada SI agentlarining tahdidlarga javob berish, xatti-harakatlarni tahlil qilish, firibgarlik va zararli faoliyatni aniqlash, shuningdek, real vaqt rejimida tizimlarni monitoring qilish imkoniyatlari ko'rib chiqilgan. SI asosidagi texnologiyalar orqali Security Operations Center (SOC) va korporativ IT tizimlarining samaradorligi oshirilishi, shuningdek, xavfsizlik tahdidlarini oldindan aniqlash va oldini olish mumkinligi ta'kidlangan. Shu bilan birga, maqolada SI qo'llanishidagi muammolar, "qora quti" effekti, noto'g'ri ma'lumotlar va kiberjinoyatchilar tomonidan yuzaga kelishi mumkin bo'lgan xatarlar ham muhokama qilingan.

Kalit so'zlar: sun'iy intellekt, kiberxavfsizlik, axborot xavfsizligi, xaker, kiberhujum, SI agentlari, tahdidlarni aniqlash, fishing xabarlar, firibgarlikni aniqlash, spam, Security Operations Center (SOC), "Qora quti" effekti.

Bugungi kunda kimda – mobil vosita, ijtimoiy tarmoqlarda akkaunt yoki bank ilovalari mavjud bo'lsa, allaqachon raqamli xavf ostida hisoblanadi. Xakerlar tobora ijodkorroq bo'lib, hujumlar murakkablashmoqda, ma'lumotlar esa tobora qimmatliroq bo'lmoqda. Shu sababli kiberxavfsizlik himoyasi statik bo'la olmaydi: u doimiy ravishda o'rganishi, moslashishi va tahdidlarga oldindan javob bera olishi zarur.

Sun'iy intellekt bu borada nafaqat zamonaviy texnologik vosita, balki kiberhujumlarga qarshi samarali strategiya hisoblanadi. U inson tomonidan aniqlanishi qiyin bo'lgan zaifliklarni aniqlashga yordam beradi va xavfli vaziyatlarga insonning qo'l bilan javob bera oladigan tezligidan ancha yuqori tezlikda reaksiya ko'rsatadi. Ushbu maqolada sun'iy intellektning axborot xavfsizligida qo'llanish istiqbollari tahlil qilinadi.

Sun'iy intellekt tizimlari real vaqt rejimida katta hajmdagi tarmoq trafigi, loglar (ish faoliyati yozuvlari) hamda foydalanuvchi va ilova faoliyatini tahlil qiladi. Ular odatiy xatti-harakatlardan chetga chiqishlarni aniqlaydi, bu esa kiberhujum, ma'lumotlar oqishi yoki zararli faoliyatni ko'rsatishi mumkin.

Tizimlar quyidagi holatlarni aniqlay oladi:

- Odatiy bo'lmagan vaqtda yoki boshqa mintaqadan hisobga kirish urinishlari;
- Potentsial ma'lumotlar oqishi bilan bog'liq chiqish trafigining keskin oshishi;
- Portlarni skanerlash, shubhali kirish urinishlari yoki korporativ tarmoq ichidagi hujumlar.

Zamonaviy modellar faqat oldindan ma'lum zararli faoliyat belgilarini emas, balki foydalanuvchi va tizim xatti-harakatlarini ham tahlil qiladi, bu esa ularning o'zgaruvchan muhitda ayniqsa samarali ishlashini ta'minlaydi.

Sun'iy intellekt fayllar, jarayonlar va dastur kodini avtomatik tahlil qilish uchun qo'llaniladi. U quyidagi imkoniyatlarga ega:

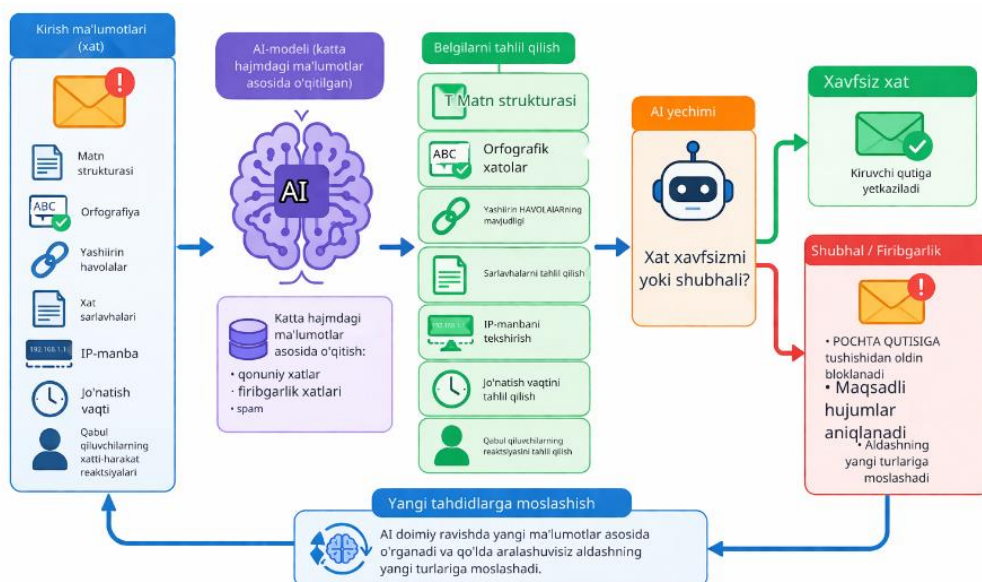
- shifrlash yoki kodni murakkablashtirish (obfuskatsiya) qo'llangan holatlarda ham xavfsiz dasturlarni zararli dasturlardan farqlay oladi;
- troyanlar, keyloggerlar, rootkitlar va boshqa tahdidlarga xos bo'lgan xatti-harakatlarni aniqlaydi;

- signatura bazasini yangilamasdan turib, ma'lum zararli dasturlarning yangi yoki o'zgartirilgan variantlarini aniqlay oladi.

Algoritmlar fayllarni shunchaki skanerlash bilan cheklanmaydi, balki ularning xatti-harakatlarini izolyatsiyalangan muhitda modellashtiradi. Natijada tizim sozlamalarini o'zgartirish, tarmoq resurslariga murojaat qilish yoki boshqa jarayonlarga kirib borish kabi urinishlar aniqlanadi.

Sun'iy intellekt katta hajmdagi ma'lumotlar asosida o'qitilib, qonuniy elektron xatlarni shubhali xatlardan turli belgilar orqali ajrata oladi. Bunda matn tuzilishi, imlo xususiyatlari, yashirin havolalar, xat sarlavhalari, IP-manba, yuborilgan vaqt hamda hatto qabul qiluvchilarning hatti-harakat reaksiyalari tahlil qilinadi. Shu tufayli u quyidagi imkoniyatlarni ta'minlaydi:

- Ommaviy fishing xabarlarini foydalanuvchining elektron pochta qutisiga yetishidan oldin bloklaydi;
- ichki yozishmalar ko'rinishida niqoblangan maqsadli hujumlarni aniqlaydi;
- yangi turdagi firibgarliklarga o'zini avtomatik moslaydi.



1-chizma. Fishing (firibgarlik) va spamni SI orqali aniqlash jarayoni

SI tahdidni aniqlash bilan cheklanmaydi, balki darhol quyidagi harakatlarni amalga oshira oladi: shubhali hisobni bloklash, zararlangan qurilmani izolyatsiya qilish, zaif resursga kirishni to'sish yoki SOC (Security Operations Center)ga avtomatik xabar yuborish. Bu javob berish vaqtini soatlardan soniyalarga qisqartiradi va potentsial zararlarni kamaytiradi. Shuningdek, SI hisobotlar tayyorlaydi, hodisalarni xavf darajasiga ko'ra ustuvorlashtiradi va javob berish ssenariylarini taklif qiladi, bu esa tahlilchilar ishini yengillashtiradi va qaror qabul qilishni tezlashtiradi.

Zamonaviy korporativ IT-sistemalar har kuni terabaytlar hajmidagi loglar (ish faoliyati yozuvlari) va xavfsizlik hodisalarini generatsiya qiladi. Bunday hajmdagi ma'lumotlarni qo'lda yoki oddiy skriptlar yordamida qayta ishlash mumkin emas. SI tizimlari real vaqt rejimida tahlil olib boradi va tahdidlarni erta bosqichda aniqlaydi.

An'anaviy xavfsizlik tizimlarining asosiy muammosi — tahlilchilarni noto'g'ri signal bilan ortiqcha yuklashdir. SI esa noto'g'ri pozitiv va noto'g'ri negativ hodisalarni sezilarli darajada kamaytiradi, aniqlikni oshiradi.

SI konfiguratsiyalar, kod, tarmoq sozlamalari va foydalanuvchi xatti-harakatlarini tahlil qilib, zaiflik yoki xavfsizlik xatolarini hujumlardan oldin aniqlaydi. Neyron tarmoqlar hodisalar, xavf darajasi, standartlarga moslik va boshqa xavfsizlik aspektlari bo'yicha hisobotlarni avtomatik shakllantiradi, bu esa mutaxassislar ishini sezilarli darajada tejaydi. Shu bilan birga SI yangi turdagi hujumlarni, imzo mavjud bo'lmagan zero-day zaifliklar, APT-guruhlarining yashirin mavjudligi yoki ma'lumotlarga odatiy bo'lmagan yo'llar orqali kirishni aniqlashda samaralidir.

SI faqat hujumlarni aniqlash bilan cheklanmay, ularni oldindan prognoz qiladi. U hujumchilar va tashqi tahdidlar xatti-harakatlarini o'rganib, xavf yuzaga kelishidan oldin aniqlaydi.

SI-texnologiyalari va tizimlari:

- **NGFW (Next-Generation Firewall):** Oddiy qoidalar orqali IP, port va protokollarni bloklashdan tashqari, foydalanuvchi xatti-harakatlari, paket mazmuni va tarixini tahlil qiladi. Shifrlangan trafikda ham anomaliyalarni aniqlash imkoniyatiga ega;
- **EDR/EDP:** Qurilmalar va ilovalarning xatti-harakatlarini monitoring qiladi, shubhali vaziyatlarda qurilmani izolyatsiya qiladi va jarayonlarni to'xtatadi;
- **IDS/IPS:** Kirish va hujumlarni oldini olish vositalari sun'iy intellekt (SI) tufayli aqlilashmoqda. An'anaviy tizimlar faqat imzo (signature)larga tayanadigan bo'lsa, SI-asosidagi yechimlar xatti-harakatlardagi noodatiy holatlarni aniqlaydi: noodatiy kirish yo'llari, tarmoq tartiblaridagi kutilmagan o'zgarishlar, infratuzilmani skanerlash urinishlari va hokazo. Agar noma'lum foydalanuvchi standart bo'lmagan port orqali ma'lumotlarni ma'lumotlar bazasi serveridan so'rasa, SI vaziyatni darhol tahlil qiladi va tahdid tasdiqlanishini kutmasdan ulanishni bloklashi mumkin;
- **Bulut xavfsizligi:** Multi-cloud muhitlarda foydalanuvchi va servis interaktsiyalarini tahlil qilib, shubhali ma'lumotlar harakatini aniqlaydi;
- **IoT xavfsizligi:** Har bir IoT qurilmaning xatti-harakatini tahlil qilib, g'ayrioddiy faoliyatda tahdidlarni bloklaydi;
- **XDR va SIEM:** Millionlab hodisalarni birlashtirib, ularni kontekstli va tahliliy tarzda ko'rsatadi, yashirin bog'liqliklarni aniqlaydi.

Kiberxavfsizlikdagi sun'iy intellekt (SI) agentlari: ogohlantirishlarni qayta ishlash, noto'g'ri signallarni filtrlash, shubhali tizimlarni izolyatsiya qilish va hisobotlar tayyorlash kabi bugungi kunda takrorlanuvchi va oddiy ishlarning katta qismini avtomatik bajara oladi. Shu bilan mutaxassislar hodisalarni tergov qilish, tizimdagi zaifliklarni tahlil qilish, himoya arxitekturasini yaratish va oldini olish choralarini joriy etish kabi muhim vazifalarga e'tibor qaratishi mumkin. Natijada jamoaning samaradorligi oshadi va butun axborot xavfsizligi tizimi barqarorroq bo'ladi.

Sun'iy intellektning kiberxavfsizlikka ta'siri axborot xavfsizligi (AXB) va SI-modellar bilan ishlash sohasida ikki tomonlama malakaga ega mutaxassislarga talabni oshirmoqda. Shu bilan birga, yangi lavozimlar shakllanmoqda, masalan, **“SI asosidagi kiberxavfsizlik mutaxassisi”** yoki **“shaxsiy SI-assistentlarni boshqaruvchi kordinator”**.

Zamonaviy Security Operations Center (SOC) markazlari intellektual qaror qabul qilish markazlariga aylanishmoqda. SI yordamida ular faqat reaksiya berishdan oldini olishga o'tadi — ya'ni threat hunting bilan shug'ullanadi: an'anaviy vositalar bilan aniqlanmagan tahdidlarni faol qidiradi.

SI katta hajmdagi ma'lumotlarni tezkor tahlil qilish, xatti-harakat profillarini tuzish, hujum zanjirlarini aniqlash va hatto javob choralarining senariylarini taklif qilish imkonini beradi. Shu

nuqtai nazardan, SI faqat yordamchi emas, balki mudofaa jarayonida to'liq ishtirok etuvchi muhim vosita hisoblanadi.

Kiberxavfsizlik tobora jismoniy xavfsizlik bilan chambarchas bog'lanib bormoqda. Zamonaviy videokuzatuv, kirishni nazorat qilish va obyektlarni monitoring qilish tizimlari aqllilashmoqda — ularda SI shubhali xatti-harakatlarni aniqlaydi, ruxsatsiz kirish urinishlarini qayd etadi va perimetr bo'ylab noodatiy holatlarni aniqlaydi.

Firibgarlikni aniqlash tizimlari (fraud detection) o'rganishga qodir SI-modellar tufayli tobora aniqroq bo'lmoqda. Ular foydalanuvchilarning xatti-harakatlarini, vaqt bo'yicha o'zgarishlarni, geografik joylashuvni, qurilma turini, odatlarni va noodatiy harakatlarni tahlil qiladi. Shubhali operatsiyaga oddiy reaksiya berish o'rniga, SI firibgarlik sodir bo'lishidan oldin uni oldindan aniqlash va faoliyatni minimal noto'g'ri bloklash bilan to'xtatish imkoniga ega.

Ammo shuni ta'kidlash kerakki, kiberxavfsizlikda sun'iy intellektni qo'llash osonlik bilan amalga oshmaydi. Bu texnologiyalar himoyani kuchaytirishi mumkin bo'lsa-da, o'z navbatida zaifliklar va xatoliklarga sabab bo'lishi ham mumkin. Masalan, SI-modellar real ma'lumotlar asosida o'qitiladi: loglar (ish faoliyati yozuvlari), tarmoq trafiki, telemetriya va foydalanuvchi xatti-harakatlari. Agar bu ma'lumotlar yetarli bo'lmasa, noto'g'ri yoki eskirgan bo'lsa, algoritm noto'g'ri xulosalar chiqaradi: haqiqiy tahdidlarni o'tkazib yuborishi yoki hech qanday asos bo'lmagan joylarda ogohlantirish berishi mumkin.

Ko'plab sun'iy intellekt modellar, ayniqsa neyron tarmoqlar, qaror qabul qilish jarayonidagi ichki tamoyillarni ochmaydi. Shu holat **“qora quti”** effekti sifatida tanilgan.

Kiberxavfsizlik sohasida bu jiddiy muammo hisoblanadi: tizim kirishni bloklaganda, tahdidni aniqlaganda yoki javob choralarini ishga tushirganda, qaror qanday asosda qabul qilinganini tushunish muhimdir. Bundan tashqari, amaldagi tartib va qonunlarga muvofiq kompaniya himoya tizimining xatti-harakatlarini tushuntira olishga majburdir.

SI nafaqat himoyachi, balki nishon ham bo'lishi mumkin. Jinoyatchilar zararli ma'lumotlarni qo'llab, algoritmlarni chalg'itishi mumkin. Natijada neyron tarmoq haqiqiy tahdidlarni e'tiborsiz qoldirishi yoki aksincha, hech qanday xavf tug'dirmaydigan hodisalarga javob berishi mumkin.

Kiberjinoyatchilar generativ SI-modellarni ishga solib, ishontiruvchi fishing xatlari, deepfake audio, hujumlarni avtomatlashtirish va himoyani chetlab o'tish kabi vositalar yaratadi. Masalan, hujumchi SI yordamida ma'lum bir kompaniyaning ish xatlarining uslubini taqlid qilib, yuqori darajada ishonchli maqsadli hujumni amalga oshirishi mumkin.

Xulosa. Sun'iy intellekt kiberxavfsizlikda tahdidlarga tezkor, aniq va keng qamrovli javob berish imkoniyatini yaratadi. U tahdidlarga nafaqat javob beradi, balki ularni oldindan aniqlash va oldini olishga yordam beradi. Biroq shuni tushunish muhimki: SI sehrli vosita emas, balki uning samaradorligi ma'lumotlar, tizim infratuzilmasi va undan foydalanuvchi mutaxassislariga bog'liq. Axborot xavfsizligida SI kelajagi, texnologiya va mutaxassislik tajribasi birgalikda ishlaydigan uyg'unlik yondashuvlaridadir. Shu hamkorlikni samarali qo'llay oladiganlar raqamli dunyoda haqiqiy ustunlikka ega bo'ladi.

Foydalanilgan adabiyotlar

1. Okdem, S., & Okdem, S. (2024). *Artificial Intelligence in Cybersecurity: A Review and a Case Study*. Applied Sciences.
2. Jalolov, T. S. (2024). *Sun'iy intellektni kiberxavfsizlik tizimlarida qo'llash: tahdidlarni erta aniqlash usullari*. Modern Digital Technologies in Education: Problems and Prospects.

3. Хакимов А.А. (2023). Роль искусственного интеллекта в кибербезопасности. *Universum: технические науки*. — Анализ применения ИИ в автоматизации обнаружения и реагирования на кибератаки.

4. Бердимуродов М.А., Вахобов С.М. (2026). Кибербезопасность в искусственном интеллекте. Лучшие интеллектуальные исследования. — Роль ИИ в защите и новые векторы атак.