

SUN'IY INTELLEKT ELEMENTLARI ASOSIDA AXBOROT XAVFSIZLIGI RISKLARINI BAHOLASH YONDASHUVI

Maxmatqulov Tuychi Oqil o'g'li

“Mirzo Ulug‘bek” nomidagi O‘zbekiston Milliy Universiteti magistranti

tuychimaxmatqulov40@gmail.com

Muhammadiyev Abbos Namoz o'g'li

“Mirzo Ulug‘bek” nomidagi O‘zbekiston Milliy Universiteti magistranti

Annotatsiya. Ushbu tezisda axborot xavfsizligi risklarini baholashda ochiq kodli audit vositalaridan olingan topilmalarni sun'iy intellekt elementlari yordamida tahlil qilish yondashuvi bayon etiladi. Yondashuvda Nmap, Nuclei va Nikto kabi vositalar natijalari yagona finding modeliga keltiriladi, topilmalar xavfsizlik mazmuniga ko'ra semantik sinflarga ajratiladi va risk darajasi CVSS balli, tashkilot profili, topilma kategoriyasi hamda ehtimollik omillari asosida aniqlanadi. Sun'iy intellekt topilmalarni avtomatik guruhlash, takroriy ogohlantirishlarni kamaytirish, ehtimollik oralig'ini moslashtirish va risk natijalarini izohlash bosqichlarida qo'llanadi. Taklif etilgan yondashuv kiberxavfsizlik monitoringida topilmalarni ustuvorlashtirish va himoya choralarini asosli rejalashtirishga xizmat qiladi.

Kalit so'zlar: axborot xavfsizligi, risklarni baholash, sun'iy intellekt, mashinaviy o'rganish, CVSS, Nmap, Nuclei, Nikto, semantik sinflash, kiberxavfsizlik monitoringi.

KIRISH

Raqamli infratuzilma kengayib borayotgan hozirgi sharoitda tashkilotlar axborot tizimlarining xavfsizlik holatini doimiy kuzatib borishga majbur bo'lmoqda. Tarmoq xizmatlari, veb-ilovalar, ma'lumotlar bazalari, bulutli resurslar va ochiq API interfeyslar kundalik faoliyatning ajralmas qismiga aylangan. Shu bilan birga, ushbu resurslarning noto'g'ri sozlanishi yoki yetarli darajada himoyalanganligi kiberxavflarning ortishiga olib keladi. Natijada xavfsizlik auditori jarayonida topilmalarni aniqlash bilan cheklanib qolmasdan, ularni risk darajasiga ko'ra baholash va ustuvorlashtirish zarurati kuchaymoqda.

Amaliy kiberxavfsizlikda Nmap, Nuclei, Nikto, testssl.sh va OpenVAS kabi ochiq kodli audit vositalari keng qo'llanadi. Ular tarmoq portlari, xizmat versiyalari, veb-server konfiguratsiyasi, TLS sozlamalari, ochiq kataloglar, standart fayllar va noto'g'ri ochilgan interfeyslar haqida turli ko'rinishdagi ma'lumotlarni beradi. Biroq ushbu vositalarning natijalari bir xil tuzilishga ega emas: ayrimlari XML shaklida, boshqalari JSONL yoki oddiy matn shaklida hisobot beradi. Shu sababli natijalarni yagona tahliliy ko'rinishga keltirish axborot xavfsizligi boshqaruvida muhim vazifalardan biri hisoblanadi.

So'nggi yillarda kiberxavfsizlikda sun'iy intellektidan foydalanish kengaymoqda. Sun'iy intellekt tizimlari katta hajmdagi jurnallarni tahlil qilish, g'ayritabiiy xatti-harakatlarni aniqlash, zararli faoliyat belgilarini ajratish va xavfsizlik hodisalarini ustuvorlashtirishda qo'llanmoqda. Risklarni baholash sohasida ham sun'iy intellekt imkoniyatlaridan foydalanish dolzarbdir, chunki audit natijalari ko'p, takroriy va ayrim hollarda noaniq bo'ladi. Bunday sharoitda avtomatik sinflash, o'xshash topilmalarni birlashtirish va ehtimollikni moslashtirish xavfsizlik mutaxassisining ishini yengillashtiradi.

Mazkur tezisning asosiy g'oyasi shundan iboratki, audit vositalaridan olingan topilmalar oddiy texnik ro'yxat sifatida emas, balki sun'iy intellekt elementlari bilan boyitilgan yagona analitik model orqali baholanishi lozim. Bunda topilmaning texnik og'irligi, xavfsizlik mazmuni, tashkilot konteksti va ehtimollik noaniqligi birgalikda hisobga olinadi. Bunday yondashuv

xavfsizlik resurslarini eng muhim risklarni kamaytirishga yo'naltirish, qaror qabul qilishni soddalashtirish va monitoring jarayonini yanada samarali tashkil etish imkonini beradi.

Ishning maqsadi ochiq kodli audit vositalaridan olingan natijalarni yagona finding modeliga keltirish, topilmalarni sun'iy intellekt elementlari yordamida semantik sinflarga ajratish va risk darajasini ehtimollikka asoslangan kontekstli model yordamida baholash yondashuvini ishlab chiqishdan iborat. Ushbu maqsadga erishish uchun topilmalarni normallashtirish, semantik belgilarni ajratish, tashkilot profilini inobatga olish, Monte Carlo simulyatsiyasi orqali noaniqlikni hisobga olish va natijalarni amaliy talqin qilish vazifalari belgilandi.

MUAMMONING QO'YILISHI

Audit vositalari tomonidan shakllantiriladigan hisobotlarning asosiy muammosi ularning turlicha format va terminologiyada bo'lishidir. Masalan, Nmap tarmoq xizmatlari va portlar haqida ma'lumot beradi, Nuclei shablonlar orqali zaiflik yoki ekspozitsiya belgilarini aniqlaydi, Nikto esa veb-server konfiguratsiyasidagi kamchiliklarni ko'rsatadi. Har bir vosita foydali ma'lumot bersada, ularning natijalarini bir joyda solishtirish va umumiy risk ko'rsatkichiga aylantirish qo'lda bajarilganda ko'p vaqt talab qiladi.

Ikkinchi muammo topilmalar orasida takrorlanish va mazmuniy yaqinlikning mavjudligidir. Biror ochiq API hujjati bir vaqtning o'zida Nuclei tomonidan exposure sifatida, Nikto tomonidan veb-serverdagi ochiq resurs sifatida qayd etilishi mumkin. Agar bunday topilmalar birlashtirilmasa, hisobotda xavf sun'iy ravishda ko'payib ko'rinadi. Aksincha, o'xshash topilmalar semantik jihatdan bog'lansa, xavfsizlik mutaxassisi ularning umumiy sababini aniqlashi va bitta tuzatish chorasi orqali bir nechta ogohlantirishni bartaraf etishi mumkin.

Uchinchi muammo CVSS kabi texnik ballarning tashkilot kontekstini to'liq aks ettirmasligidir. Zaiflikning texnik og'irligi yuqori bo'lishi mumkin, lekin u ichki segmentda joylashgan va tashqi tarmoqqa ochiq bo'lmasa, amaliy risk nisbatan pastroq baholanishi mumkin. Yoki aksincha, texnik balli o'rtacha bo'lgan ochiq boshqaruv interfeysi bank yoki davlat tashkilotida katta xavf tug'dirishi mumkin. Shu sababli risk baholashda tashkilot profili va topilmaning real muhitdagi roli alohida inobatga olinishi zarur.

Sun'iy intellekt bu muammolarni to'liq avtomatik hal qiladigan vosita sifatida emas, balki tahlil jarayonini kuchaytiruvchi yordamchi mexanizm sifatida qaraladi. U topilma matnidan kalit belgilarni ajratish, o'xshash topilmalarni klasterlash, semantik kategoriyani taxmin qilish va avvalgi natijalar asosida ehtimollik oralig'ini moslashtirishda qo'llanishi mumkin. Bunday yondashuv inson ekspertining qarorini almashtirmaydi, balki unga ko'proq asoslangan va tezkor xulosa chiqarishga yordam beradi.

SUN'IY INTELLEKT BILAN BOG'LANGAN YONDASHUV

Taklif etilgan yondashuvda sun'iy intellekt uch bosqichda qo'llanadi. Birinchi bosqich - topilmalarni semantik tahlil qilish. Bu bosqichda skaner natijasidagi qisqa tavsif, xizmat nomi, URL manzili, shablon nomi, port raqami va konfiguratsiya belgilaridan foydalanib topilmaning xavfsizlik mazmuni aniqlanadi. Masalan, 'Swagger', 'ReDoc', 'OpenAPI', 'directory listing', 'default file' kabi belgilar exposure yoki directory_listing kategoriyasiga yaqinligini ko'rsatishi mumkin.

Ikkinchi bosqich - o'xshash topilmalarni guruhlash. Audit hisobotlarida bir xil manzilda yoki bir xil xizmatda bir-biriga yaqin ogohlantirishlar ko'p uchraydi. Sun'iy intellekt asosidagi klasterlash yondashuvi topilma nomi, tavsifi va obyekt belgilarining o'xshashligini hisobga olib, ularni bir guruhga jamlaydi. Bu false-positive yoki takroriy yozuvlar ta'sirini kamaytiradi hamda xavfsizlik bo'yicha qaror qabul qilishni soddalashtiradi.

Uchinchi bosqich - ehtimollik oralig'ini moslashtirish. Avvalgi audit natijalari, topilmaning takrorlanishi, tashqi tarmoqqa ochiqqligi, xizmatning ommaviyligi va kategoriya og'irligi asosida ehtimollik qiymati qat'iy son emas, balki interval sifatida baholanadi. Mashinaviy o'rganish elementlari mavjud tarixiy ma'lumotlar asosida ushbu intervalni toraytirishi yoki kengaytirishi mumkin. Masalan, uzoq vaqt davomida bartaraf etilmagan va tashqi tarmoqqa ochiq exposure topilmasi uchun ehtimollik yuqoriroq oraliqqa ko'tariladi.

Generativ sun'iy intellekt esa natijalarni izohlash bosqichida qo'llanishi mumkin. Risk hisoblanganidan so'ng tizim topilma nimani anglatishi, qanday xavf tug'dirishi va qanday umumiy tavsiya berilishi kerakligini tabiiy tilga yaqin shaklda tushuntiradi. Bunda generativ model xavfsizlik mutaxassisining ishini yengillashtiradi, lekin yakuniy qaror baribir inson ekspert tomonidan tasdiqlanishi lozim. Shu sababli yondashuvda 'AI yordam beradi, ekspert tasdiqlaydi' tamoyili muhim hisoblanadi.

TAKLIF ETILGAN MODEL

Modelda har bir topilma yagona finding obyekt sifatida qaraladi. Ushbu obyekt manba, topilma nomi, tavsif, obyekt manzili, kategoriya, texnik og'irlik, ehtimollik oralig'i va tashkilot profili kabi maydonlardan iborat bo'ladi. Bunday tuzilma turli audit vositalari natijalarini bitta hisoblash jarayoniga kiritish imkonini beradi. Topilmalarni yagona modelga keltirishdan keyin sun'iy intellekt yordamida semantik sinf tekshiriladi va kerak bo'lsa moslashtiriladi.

Risk qiymatini hisoblashda CVSS balli, ehtimollik, tashkilot profili va kategoriya og'irligi asosiy omillar sifatida olinadi. Sun'iy intellekt komponenti esa kategoriya aniqligini, ehtimollik oralig'ini va takroriy topilmalar ta'sirini sozlashda yordam beradi. Modelning umumiy ko'rinishi quyidagicha ifodalanadi:

$$R_i = CVSS_i \times P_i \times K_{org} \times K_{cat} \times K_{AI}$$

Bu yerda R_i - i-topilma uchun risk qiymati; $CVSS_i$ - texnik og'irlik balli; P_i - ehtimollik qiymati; K_{org} - tashkilot profili koeffitsiyenti; K_{cat} - topilma kategoriyasining nisbiy xavf og'irligi; K_{AI} - sun'iy intellekt yordamida aniqlangan ishonchlilik yoki kontekstni aniqlashtirish koeffitsiyentidir. K_{AI} qiymati topilmaning semantik aniqligi, takroriy tasdiqlanishi va tarixiy kuzatuvlardagi barqarorligiga qarab belgilanadi.

Masalan, topilma bir nechta vosita tomonidan mustaqil aniqlansa yoki avvalgi skanerlarda ham qayta-qayta uchrasa, K_{AI} qiymati riskni biroz oshirishi mumkin. Agar topilma tavsifi noaniq bo'lsa, faqat bitta vositada paydo bo'lsa yoki semantik model uni past ishonchlilik bilan tasniflasa, K_{AI} riskni ehtiyotkorlik bilan talqin qilishga yordam beradi. Bu yondashuv risk natijasini mutlaq hukm sifatida emas, balki dalillar darajasini hisobga olgan baho sifatida ko'rsatadi.

Topilmalar `open_port`, `service_version`, `weak_service`, `web_header`, `directory_listing`, `default_file`, `tls`, `exposure` va `generic` kabi sinflarga ajratiladi. `Exposure` va `weak_service` sinflari odatda yuqori xavf mazmuniga ega bo'ladi, chunki ular tashqi muhitga ortiqcha axborot berishi yoki zaif xizmatdan foydalanish ehtimolini oshirishi mumkin. `Web_header` yoki `open_port` sinfidagi topilmalar esa kontekstga qarab turlicha baholanadi. Shu sababli semantik sinflash riskni amaliy ma'noda tushunishga yordam beradi.

Noaniqlikni hisobga olish uchun Monte Carlo simulyatsiyasi qo'llanadi. Ehtimollik P_i bitta qat'iy qiymat sifatida emas, balki P_{min} va P_{max} oralig'i sifatida olinadi. Har bir iteratsiyada ushbu oraliqdan tasodifiy qiymat tanlanadi va risk qayta hisoblanadi. Natijada o'rtacha, minimal va maksimal risk qiymatlari shakllanadi. Sun'iy intellekt komponenti tarixiy ma'lumotlar asosida ushbu oraliqni moslashtirishi mumkin.

BAHOLASH OMILLARI

Quyidagi jadvalda sun'iy intellekt bilan bog'langan risk baholash jarayonida hisobga olinadigan asosiy omillar keltirilgan.

№	Omil	Mazmuni	Baholashdagi roli
1	CVSS balli	Topilmaning texnik og'irligini bildiradi	Risk hisoblashning bazaviy qiymatini beradi
2	Semantik kategoriya	Topilmaning xavfsizlik mazmunini ko'rsatadi	Riskni mazmuniy ustuvorlik bo'yicha farqlaydi
3	Tashkilot profili	Bank, davlat yoki xususiy sektor konteksti	Bir xil topilmani turlicha baholashga imkon beradi
4	Ehtimollik oralig'i	Topilmaning xavfga aylanish ehtimoli	Noaniqlikni Monte Carlo orqali modellashtiradi
5	Sun'iy intellekt koeffitsiyenti	Semantik ishonchlilik va takroriy tasdiqlanish darajasi	Topilma bahosini dalillar asosida aniqlashtiradi
6	Tarixiy monitoring	Topilmaning vaqt bo'yicha takrorlanishi	Davriy auditda risk dinamikasini ko'rsatadi

AMALIY TALQIN

Taklif etilgan yondashuv amaliy jihatdan topilmalarni oddiy ro'yxatdan ustuvorlashtirilgan risk ko'rsatkichlariga aylantiradi. Masalan, ochiq Swagger yoki ReDoc hujjati exposure kategoriyasiga kiritiladi. Agar u tashqi tarmoqqa ochiq bo'lsa va bir nechta vosita tomonidan aniqlansa, sun'iy intellekt komponenti buni yuqori ishonchlilikka ega topilma sifatida belgilashi mumkin. Natijada bunday holat bank profilida kritik yoki yuqori risk sifatida ko'rinadi.

Davlat tashkilotlari uchun riskni baholashda elektron xizmatlar uzluksizligi, fuqarolar ma'lumotlari va rasmiy portallarning ishonchliligi muhim ahamiyatga ega. Shu sababli exposure, weak_service va tls kategoriyalaridagi topilmalar yuqori e'tibor talab qiladi. Sun'iy intellekt yordamida topilmalar izohlanganda mas'ul xodim faqat texnik ogohlantirishni emas, balki uning xizmat uzluksizligi yoki ma'lumotlar ishonchliligiga qanday ta'sir qilishi mumkinligini ham tushunadi.

Xususiy sektorda risk bahosi tashkilot faoliyatiga bog'liq bo'ladi. Kichik ichki tizimdagi ochiq port pastroq baholanishi mumkin, lekin mijozlar bilan ishlaydigan internet-servisdagi xuddi shu topilma yuqori riskga ega bo'ladi. Sun'iy intellekt komponenti aktiv tavsifi, topilma kategoriyasi va avvalgi kuzatuvlar asosida ehtimollikni moslashtirishga yordam beradi. Bu xavfsizlik bo'yicha cheklangan resurslarni eng muhim yo'nalishlarga sarflashga xizmat qiladi.

Yana bir muhim jihat - generativ sun'iy intellekt yordamida risk natijalarini oddiy tilda izohlash imkoniyatidir. Masalan, 'OpenAPI hujjati ochiq' degan topilma rahbariyat uchun yetarli tushunarli bo'lmasligi mumkin. Izoh beruvchi modul esa bu holat tashqi foydalanuvchiga API tuzilmasi, endpointlar va ehtimoliy parametrlar haqida ma'lumot berishi, shuning uchun autentifikatsiya yoki IP cheklovi bilan yopilishi kerakligini tushuntiradi.

TOPILMALAR BO'YICHA NAMUNAVIY USTUVORLIK

Quyidagi jadvalda audit natijalarini sun'iy intellekt yordamida talqin qilish va ustuvorlikka ajratishning namunaviy ko'rinishi berilgan.

№	Manba	Kategoriya	Topilma mazmuni	AI talqini	Ustuvor chora
1	Nuclei	exposure	ReDoc yoki Swagger API hujjati ochiq	Tashqi razvedka uchun foydali axborot oshkor bo'lishi mumkin	Autentifikatsiya qo'yish yoki tashqi kirishni cheklash
2	Nikto	default_file	Standart fayl yoki katalog mavjud	Server konfiguratsiyasida ortiqcha resurs borligi ehtimoli yuqori	Keraksiz fayllarni o'chirish va sozlamani tekshirish
3	Nmap	service_version	Xizmat versiyasi aniqlangan	Versiya eskirgan bo'lsa ma'lum zaifliklar bilan bog'lanishi mumkin	Yangilash va firewall qoidalarini qayta ko'rish
4	Nikto	web_header	Xavfsizlik sarlavhasi yetishmaydi	Brauzer darajasidagi himoya mexanizmlari sust bo'lishi mumkin	HTTP xavfsizlik sarlavhalarini yoqish
5	Nuclei	tls	TLS konfiguratsiyasi bo'yicha ogohlantirish	Shifrlash sifati yoki protokol sozlamasi talabga mos emas	Sertifikat va TLS siyosatini yangilash

NATIJALAR VA MUHOKAMA

Taklif etilgan model asosida topilmalarni qayta ishlash natijasida ularning xavfsizlik mazmuni aniqroq ko'rinadi. Avval alohida vositalar tomonidan berilgan texnik ogohlantirishlar yagona finding modelida jamlanadi. Keyin sun'iy intellekt elementlari yordamida semantik kategoriya aniqlanadi, o'xshash topilmalar guruhlanadi va ehtimollik oralig'i moslashtiriladi. Shu tariqa yakuniy natija skaner hisobotidan farqli ravishda qaror qabul qilish uchun qulay risk ko'rsatkichiga aylanadi.

Modelning asosiy ustunligi kontekstga sezgirlikdir. Bir xil exposure topilmasi bank, davlat va xususiy sektor uchun bir xil darajada baholanmaydi. Bank sektorida moliyaviy operatsiyalar, mijozlar ma'lumotlari va reguliator talablari sababli risk ko'rsatkichi yuqoriroq chiqadi. Davlat tashkilotida xizmat uzluksizligi va fuqarolar ma'lumotlari birinchi o'ringa chiqadi. Xususiy sektorda esa xavf tashkilotning faoliyat yo'nalishi va axborot aktivlari qiymatiga bog'liq bo'ladi.

Sun'iy intellektdan foydalanish natijalarni yanada tushunarli qiladi. Klasterlash orqali bir xil muammoga oid takroriy ogohlantirishlar kamayadi. Semantik sinflash orqali topilma nima uchun xavfli ekanini aniqlash osonlashadi. Generativ izohlash orqali esa natijalar nafaqat texnik mutaxassislar, balki boshqaruv qarorlarini qabul qiluvchi shaxslar uchun ham tushunarli shaklga keladi. Bu kiberxavfsizlik auditining amaliy qiymatini oshiradi.

Biroq sun'iy intellekt natijalariga to'liq tayanish to'g'ri emas. Model noto'g'ri tasnif berishi, topilmani ortiqcha xavfli deb ko'rsatishi yoki ayrim muhim kontekstni hisobga olmasligi mumkin. Shuning uchun yakuniy qaror inson ekspert tomonidan tekshirilishi zarur. Ayniqsa kritik

infratuzilma, bank tizimlari yoki davlat axborot resurslarida avtomatik baholash faqat yordamchi vosita sifatida qaralishi kerak.

Modelning yana bir cheklovi sifatida ma'lumot sifati ko'rsatiladi. Agar skaner noto'g'ri natija bersa yoki ma'lumot yetarli bo'lmasa, sun'iy intellekt ham noto'g'ri xulosa chiqarishi mumkin. Shu sababli audit jarayonida manbalarni tekshirish, topilmalarni validatsiya qilish va xavfsizlik siyosatiga mos ravishda koeffitsiyentlarni sozlash talab etiladi. To'g'ri sozlangan holatda esa yondashuv xavfsizlik monitoringini ancha samarali qiladi.

Muhokama natijalari shuni ko'rsatadiki, risklarni baholashda sun'iy intellekt topilmalarni avtomatik tushunish, guruhlash va izohlash orqali muhim qo'shimcha imkoniyat yaratadi. Ammo modelning ilmiy-amaliy qiymati faqat AI mavjudligida emas, balki texnik ball, ehtimollik, tashkilot konteksti va semantik xavf mazmunini yagona hisoblash jarayonida birlashtirishidir.

Shuningdek, AI natijalarining izohlanishi ham alohida ahamiyatga ega. Risk balli nima sababdan oshgani, qaysi kategoriya tanlangani va qaysi dalil K_{AI} koeffitsiyentiga ta'sir qilgani ko'rsatilmasa, foydalanuvchi avtomatik bahoga ishonmasligi mumkin. Shu bois modelda har bir AI tavsiyasi bilan birga qisqa asos ham berilishi kerak. Bu yondashuv shaffoflikni oshiradi va ekspertga avtomatik bahoni tez tekshirish imkonini beradi.

Modelda ma'lumotlar maxfiylikni saqlash ham muhim masala hisoblanadi. Agar generativ sun'iy intellektidan foydalanilsa, ichki IP-manzillar, domenlar, foydalanuvchi nomlari yoki boshqa sezgir belgilar tashqi xizmatlarga yuborilmasligi kerak. Shu sababli amaliy qo'llashda lokal model, maskalash mexanizmi yoki faqat umumlashtirilgan matndan foydalanish tavsiya etiladi. Bu talab kiberxavfsizlik tizimlarida sun'iy intellektni mas'uliyatli qo'llashning muhim shartidir.

AI modulining yana bir vazifasi topilmalar bo'yicha izohlarni standartlashtirishdir. Masalan, bir xil mazmundagi topilma turli vositalarda turlicha nomlanishi mumkin. Sun'iy intellekt ularning umumiy ma'nosini ajratib, hisobotda yagona tushunarli izoh shakllantiradi. Bu, ayniqsa, rahbariyatga taqdim etiladigan qisqa hisobotlarda muhimdir, chunki texnik atamalar ko'p bo'lgan hisobotlar qaror qabul qilish jarayonini sekinlashtirishi mumkin.

Bunday arxitektura xavfsizlik nuqtai nazaridan ham qulaydir. Chunki sun'iy intellekt bevosita skanerlash yoki ekspluatatsiya bajaruvchi modulga aylantirilmaydi. U faqat mavjud hisobotlarni o'qiydi, matnli belgilarni ajratadi, o'xshash yozuvlarni aniqlaydi va risk formulasi uchun qo'shimcha koeffitsiyentlarni tavsiya qiladi. Shu orqali yondashuv etik audit tamoyillariga mos bo'lib, faqat ruxsat berilgan muhitda olingan natijalarni tahlil qilishga xizmat qiladi.

Sun'iy intellekt moduli umumiy risk baholash jarayonida mustaqil qaror chiqaruvchi blok sifatida emas, balki ma'lumotni boyituvchi va tahlilni aniqlashtiruvchi yordamchi qatlam sifatida joylashtiriladi. Dastlab parserlar skaner natijalarini o'qiydi va topilmalarni yagona maydonlarga ajratadi. Keyingi bosqichda AI moduli topilma tavsifi, URL, port, xizmat nomi va shablon nomi kabi belgilarni tahlil qilib, ularga semantik kategoriya taklif qiladi. Bu natija yakuniy hisoblashdan oldin qoidalar bazasi yoki ekspert nazorati bilan solishtiriladi.

XULOSA

Axborot xavfsizligi risklarini baholashda turli ochiq kodli audit vositalaridan olingan topilmalarni yagona modelga keltirish muhim ilmiy-amaliy masala hisoblanadi. Oddiy skaner hisobotlari ko'p hollarda topilmalar ro'yxatini beradi, lekin ular qaysi xavf birinchi navbatda bartaraf etilishi kerakligini yetarli darajada ko'rsatmaydi. Shu sababli topilmalarni risk darajasiga ko'ra ustuvorlashtirish zarur.

Tezida sun'iy intellekt elementlari bilan boyitilgan risk baholash yondashuvi taklif etildi. Ushbu yondashuvda topilmalar yagona finding modeliga keltiriladi, semantik sinflarga ajratiladi,

CVSS balli, ehtimollik, tashkilot profili, kategoriya og'irligi va AI ishonchlilik koeffitsiyenti asosida baholanadi. Monte Carlo simulyatsiyasi orqali noaniqlik hisobga olinib, riskning minimal, maksimal va o'rtacha ko'rsatkichlarini olish imkoniyati yaratiladi.

Sun'iy intellektning qo'llanishi topilmalarni avtomatik guruhlash, takroriy ogohlantirishlarni kamaytirish, ehtimollikni moslashtirish va natijalarni izohlash imkonini beradi. Shu bilan birga, AI yakuniy qarorni to'liq almashtirmaydi, balki inson ekspertining tahliliy imkoniyatini kuchaytiradi. Bunday yondashuv kiberxavfsizlik monitoringida tezkor, tushunarli va kontekstga mos risk bahosini shakllantirishga xizmat qiladi.

Kelgusida modelni tarixiy audit natijalari, aktivlarning biznes qiymati, ekspluatatsiya mavjudligi va real hodisalar statistikasi bilan boyitish mumkin. Bu risklarni baholashni yanada adaptiv, aniq va amaliy qaror qabul qilishga mos holga keltiradi.

FOYDALANILGAN ADABIYOTLAR

1. NIST SP 800-30 Rev.1. Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2012.
2. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - Guidance on managing information security risks.
3. FIRST. Common Vulnerability Scoring System v3.1: Specification Document, 2019.
4. OWASP. OWASP Risk Rating Methodology.
5. Nmap Project. Nmap Network Scanning Documentation.
6. ProjectDiscovery. Nuclei Documentation.
7. CIRT.net. Nikto Web Scanner Documentation.
8. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.
9. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. Pearson, 2021.