FortiGate va pfSense/Suricata asosidagi ikki qatlamli gibrid himoya modelida tarmoq hujumlariga avtomatlashtirilgan javob berish

Komilov Abrorjon Maxamatsoli o‘g‘li
Vatan universiteti Raqamli texnologiyalar fakulteti,
Telekommunikatsiya injineringi mutaxasisligi magistranti
Kuvandikov J.T.
PhD., O‘ZMU Jizzax filiali
'Kompyuter ilmlari va dasturlashtirish" kafedrasi mudiri
https://doi.org/10.5281/zenodo.24446173

Annotatsiya. Mazkur maqolada zamonaviy kompyuter tarmoqlarida uchraydigan kiberhujumlarni aniqlash, ularning oldini olish va xavfsizlik hodisalariga avtomatlashtirilgan tarzda javob qaytarish masalalari yoritilgan. Tarmoq infratuzilmasini himoyalashda FortiGate hamda pfSense/Suricata texnologiyalarining o‘zaro integratsiyasiga asoslangan ikki qatlamli gibrid himoya modelini tashkil etish tamoyillari tahlil qilingan. Taklif etilayotgan modelda FortiGate birinchi himoya qatlami sifatida tarmoqlararo trafikni nazorat qilish, kirish va chiqish qoidalarini boshqarish hamda xavfli ulanishlarni cheklash vazifalarini bajaradi. pfSense/Suricata esa ikkinchi qatlamda tarmoq paketlarini chuqur tahlil qilish, hujum belgilarini aniqlash va xavfsizlik hodisalari to‘g‘risida ma’lumot shakllantirishga xizmat qiladi. Shuningdek, aniqlangan tahdidlarga avtomatik javob berish, zararli IP-manzillarni bloklash, shubhali qurilmalarni izolyatsiya qilish, hodisalarni jurnalga yozish va tizim faoliyatini monitoring qilish mexanizmlari ko‘rib chiqilgan.

Kalit so‘zlar: kiberxavfsizlik, FortiGate, pfSense, Suricata, tarmoq himoyasi, IDS, IPS, avtomatlashtirish, kiberhujum, monitoring, firewall, tahdidlarni aniqlash, IP-bloklash, gibrid himoya.

KIRISH

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida tashkilotlar, ta’lim muassasalari va korxonalarning faoliyati tobora ko‘proq kompyuter tarmoqlariga bog‘lanib bormoqda. Shu bilan birga, tarmoq infratuzilmalariga qaratilgan DDoS hujumlari, portlarni skanerlash, zararli trafik yuborish, ruxsatsiz kirish va boshqa kiberhujumlar soni ham ortmoqda. Bunday sharoitda an’anaviy tarmoqlararo ekranlardan foydalanishning o‘zi barcha tahdidlarni samarali bartaraf etish uchun yetarli bo‘lmay qolmoqda. Tarmoq xavfsizligini ta’minlashda bir nechta himoya texnologiyalarini o‘zaro integratsiyalash, hujumlarni aniqlash va ularga avtomatik javob qaytarish muhim ahamiyat kasb etadi. Shu nuqtayi nazardan, FortiGate hamda pfSense/Suricata vositalariga asoslangan ikki qatlamli gibrid himoya modelidan foydalanish istiqbolli yechimlardan biri hisoblanadi.

ASOSIY QISM

Ikki qatlamli gibrid himoya modeli tarmoq xavfsizligini bir-birini to‘ldiruvchi ikkita mustaqil, ammo o‘zaro integratsiyalashgan himoya vositasi yordamida ta’minlashga asoslanadi. Mazkur yondashuvning asosiy xususiyati shundaki, har bir himoya qatlami o‘ziga xos vazifalarni bajaradi va birinchi qatlamda aniqlanmagan yoki chuqur tahlil talab qiladigan tahdidlar ikkinchi

qatlam tomonidan aniqlanishi mumkin. Birinchi qatlamda FortiGate tarmoqlararo ekranidan foydalaniladi. Ushbu qurilma tashqi tarmoq va ichki lokal tarmoq o‘rtasidagi trafikni nazorat qiladi. U kiruvchi va chiquvchi ulanishlarni belgilangan xavfsizlik siyosati asosida tekshiradi, ruxsatsiz ulanishlarni cheklaydi, portlar va xizmatlar bo‘yicha filtrlashni amalga oshiradi. Shuningdek, FortiGate imkoniyatlaridan kelib chiqib, IPS, antivirus, veb-filtrlash va boshqa xavfsizlik funksiyalaridan foydalanish mumkin. Ikkinchi qatlam pfSense va uning tarkibida ishlaydigan Suricata tizimiga asoslanadi. pfSense tarmoq trafikini boshqarish, marshrutlash va xavfsizlik qoidalarini qo‘llash vazifalarini bajaradi. Suricata esa tarmoq paketlarini tahlil qilib, ma’lum hujum imzolari, shubhali trafik xususiyatlari va xavfli faoliyat belgilarini aniqlaydi. Suricata IDS rejimida hodisalarni qayd etishi, IPS rejimida esa mos ravishda sozlangan qoidalar asosida zararli trafikni bloklashi mumkin.

Mazkur arxitekturada tarmoq trafikining harakatlanishi oldindan belgilangan xavfsizlik siyosatiga muvofiq tashkil etiladi. FortiGate birlamchi filtrlashni amalga oshiradi, pfSense/Suricata esa ikkinchi darajali tahlil va aniqlash vazifasini bajaradi. Monitoring va avtomatlashtirish mexanizmi ikkala qatlamdan keladigan hodisalarni umumlashtirib, zarur javob choralarini ishga tushiradi. Bunda muhim jihat shuki, ikkala qurilmaning joylashuvi, marshrutlash qoidalari va trafikni yo‘naltirish tartibi to‘g‘ri loyihalashtirilishi kerak. Aks holda, ayrim trafik oqimlari himoya qatlamlarini chetlab o‘tishi yoki tarmoqda marshrutlash muammolari yuzaga kelishi mumkin.

FortiGate texnologiyasining birinchi himoya qatlami sifatidagi vazifalari. FortiGate zamonaviy tarmoqlarni himoyalashda qo‘llaniladigan ko‘p funksiyali xavfsizlik platformalaridan biridir. Uning asosiy vazifasi tarmoq chegarasidagi trafikni nazorat qilish va belgilangan xavfsizlik siyosatiga mos kelmaydigan ulanishlarning oldini olishdan iborat.

Birinchi himoya qatlamida quyidagi funksiyalardan foydalanish maqsadga muvofiq:

Tarmoqlararo ekran (Firewall). Ushbu funksiya IP-manzillar, portlar, protokollar va tarmoq interfeyslari asosida trafikni filtrlash imkonini beradi. Masalan, tashqi tarmoqdan ichki serverlarga faqat zarur xizmatlar orqali ulanishga ruxsat beriladi. Keraksiz portlar va xizmatlar esa bloklanadi.

Intrusion Prevention System (IPS). FortiGate tarkibidagi IPS funksiyasi ma’lum hujum usullariga xos belgilarni aniqlash va tegishli xavfsizlik siyosati asosida ularni bloklashga yordam beradi. Bu, ayniqsa, ekspluatatsiya urinishlari, zararli paketlar va ayrim tarmoq protokollaridagi hujumlarni aniqlashda muhimdir.

DoS himoyasi. Tarmoq resurslariga haddan tashqari ko‘p so‘rov yuborish orqali ularni ishdan chiqarishga qaratilgan hujumlarni cheklash uchun sessiyalar soni, trafik intensivligi va boshqa parametrlar asosida chegaralar o‘rnatiladi.

***IP-manzillarni boshqarish*.** Shubhali yoki zararli deb topilgan manzillarni bloklash, alohida manzillar guruhini yaratish va ularga nisbatan xavfsizlik siyosatini qo‘llash mumkin. FortiGate tizimining muhim imkoniyatlaridan yana biri Automation Stitches mexanizmidir. Ushbu mexanizm muayyan hodisa yoki shart yuzaga kelganda oldindan belgilangan avtomatik amallarni bajarishga mo‘ljallangan. Masalan, buzilgan qurilma yoki yuqori xavfli IP-manzil aniqlanganda, tegishli bloklash amali ishga tushirilishi mumkin. Shu tariqa FortiGate nafaqat trafikni filtrlovchi vosita, balki avtomatlashtirilgan himoya jarayonining muhim boshqaruv komponenti sifatida ham faoliyat yuritadi.

pfSense/Suricata yordamida tarmoq hujumlarini aniqlash. Ikkinchi himoya qatlamida pfSense va Suricata integratsiyasidan foydalanish tarmoq paketlarini chuqur tahlil qilish imkonini beradi. Bunda pfSense tarmoq infratuzilmasini boshqarish vazifasini bajarsa, Suricata hujumlarni aniqlash va oldini olish mexanizmini ta’minlaydi.

Suricata quyidagi asosiy faoliyat turlarini aniqlashda qo‘llanilishi mumkin:

– **Port scanning** – tarmoq qurilmalaridagi ochiq portlarni aniqlashga qaratilgan urinishlar.

– **DDoS** – server yoki tarmoq resurslariga katta hajmdagi so‘rovlar yuborish orqali xizmat faoliyatini izdan chiqarish.

– **Brute force** – parolni takroriy urinishlar orqali aniqlashga qaratilgan hujumlar.

– **Web-attack** – veb-ilovalarga nisbatan SQL injection, ayrim XSS va boshqa zararli so‘rovlar.

– **Malware communication** – zararli dasturlarning tashqi boshqaruv serverlari bilan aloqa o‘rnatish belgilari.

– **Suspicious traffic** – odatiy trafikdan farq qiluvchi, shubhali xususiyatlarga ega bo‘lgan paketlar va ulanishlar.

Suricata faoliyatida IDS va IPS rejimlari alohida ahamiyatga ega. IDS rejimida tizim tarmoq trafikini kuzatadi va aniqlangan hodisalarni qayd etadi, biroq trafikni mustaqil ravishda to‘xtatmaydi. IPS rejimida esa tizim trafik oqimiga bevosita ta’sir ko‘rsatib, mos qoidalar asosida zararli paketlarni bloklashi mumkin.

Suricata tizimining muhim xususiyatlaridan biri EVE JSON formatida hodisalar to‘g‘risidagi ma’lumotlarni shakllantirishidir. Ushbu ma’lumotlarda hodisaning turi, vaqt belgisi, manba va manzil IP-manzillari, portlar, protokol, aniqlangan qoida va xavflilik darajasi kabi parametrlar mavjud bo‘lishi mumkin. Masalan, tarmoqda noma’lum IP-manzildan serverning bir nechta portlariga ketma-ket ulanish urinishlari aniqlansa, Suricata tegishli ogohlantirishni shakllantiradi. Mazkur ogohlantirish keyingi bosqichda avtomatlashtirilgan tahlil tizimiga uzatiladi.

Tarmoq hujumlariga avtomatlashtirilgan javob berish mexanizmi. Ikki qatlamli gibrid himoya modelining eng muhim tarkibiy qismi aniqlangan hujumlarga avtomatlashtirilgan tarzda javob qaytarish mexanizmidir. An’anaviy xavfsizlik tizimlarida administrator hodisalarni kuzatib, ularni tahlil qiladi va zarur bloklash choralarini qo‘lda amalga oshiradi. Bunday yondashuv ko‘p sonli hodisalar yuzaga kelgan vaziyatlarda vaqt yo‘qotilishiga va inson omili bilan bog‘liq xatolarga sabab bo‘lishi mumkin. Taklif etilayotgan modelda esa Suricata tomonidan aniqlangan hodisalar maxsus avtomatlashtirish moduli orqali qayta ishlanadi. Ushbu modul Python dasturlash tili asosida ishlab chiqilishi mumkin. U Suricata jurnal fayllarini kuzatadi, yangi hodisalarni ajratib oladi, xavf darajasini baholaydi va tegishli himoya choralarini ishga tushiradi.

Avtomatlashtirilgan javob berish jarayoni quyidagi ketma-ketlikda amalga oshiriladi:

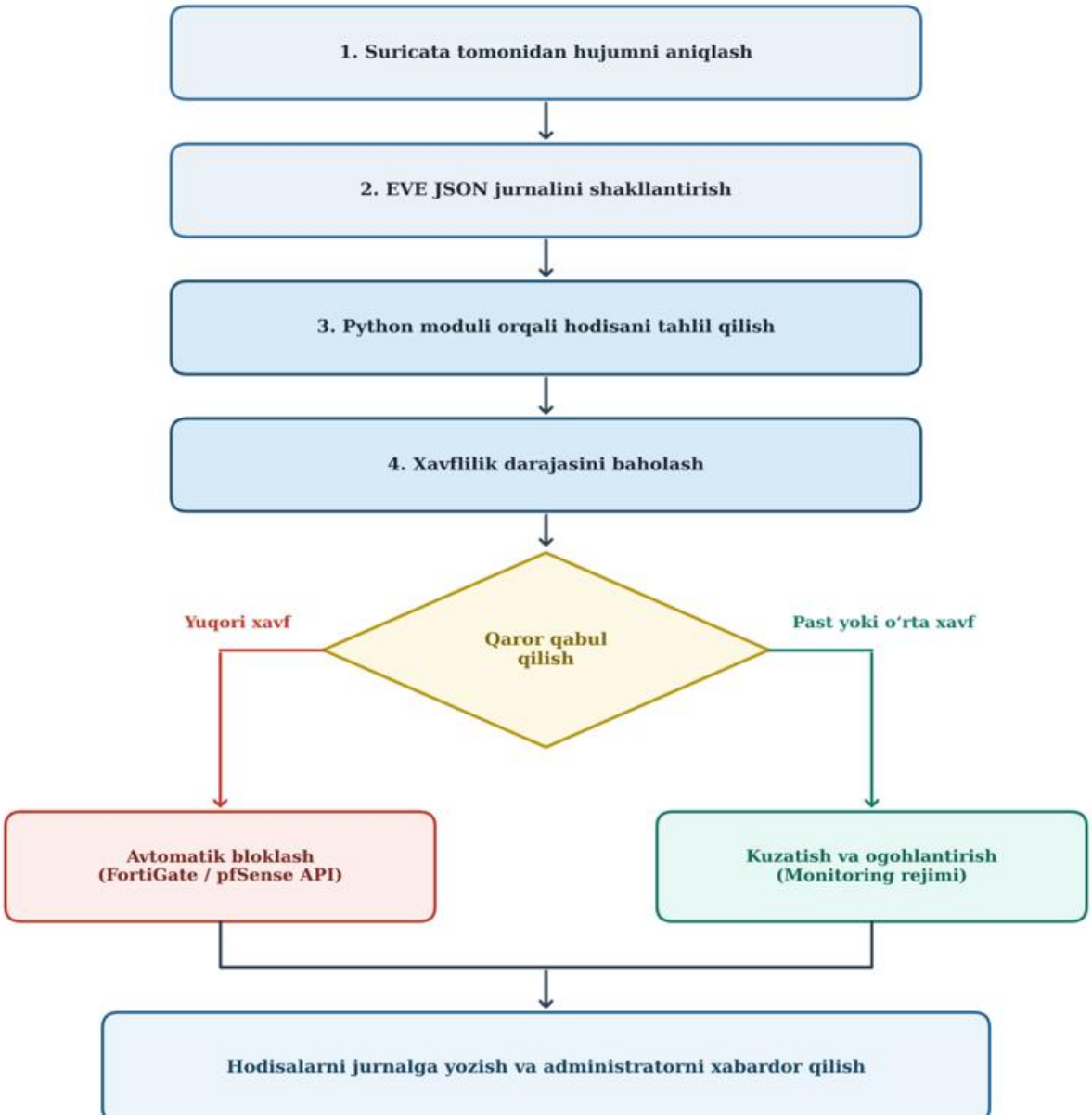
Birinchi bosqich – hodisani aniqlash. Suricata tarmoq trafikini kuzatish davomida shubhali yoki zararli faoliyatni aniqlaydi va tegishli ogohlantirishni EVE JSON jurnaliga yozadi.

Ikkinchi bosqich – hodisani tahlil qilish. Python asosidagi modul jurnal ma’lumotlarini o‘qiydi. Unda manba IP-manzili, hujum turi, hodisa vaqti, takrorlanish chastotasi va xavflilik darajasi aniqlanadi.

Uchinchi bosqich – xavfni baholash. Har bir aniqlangan hodisa belgilangan mezonlar asosida tasniflanadi. Masalan, bitta muvaffaqiyatsiz ulanish urinishiga nisbatan ko‘p sonli takroriy urinishlar yuqoriroq xavf sifatida baholanadi. Bunda oq ro‘yxatga kiritilgan ishonchli manzillar, ichki tarmoq qurilmalari va administrator IP-manzillari alohida hisobga olinadi.

To‘rtinchi bosqich – avtomatik javob choralarini bajarish. Xavf yuqori deb baholanganda, avtomatlashtirish moduli FortiGate yoki pfSense bilan API, webhook yoxud boshqa boshqaruv interfeysi orqali bog‘lanadi. Natijada zararli manba IP-manzili bloklanadi yoki shubhali qurilma alohida tarmoq segmentiga ajratiladi.

Beshinchi bosqich – hodisani qayd etish va xabardor qilish. Amalga oshirilgan harakatlar alohida jurnalga yoziladi. Administratorga elektron pochta yoki boshqa xabar almashish kanali orqali ogohlantirish yuboriladi.



1-rasm. Tarmoq hujumlariga avtomatlashtirilgan javob berish algoritmi.

Mazkur mexanizmda bloklash amali faqat ishonchli mezonlar asosida bajarilishi lozim. Chunki noto‘g‘ri aniqlangan hodisa sababli qonuniy foydalanuvchilarning IP-manzillari ham bloklanishi mumkin. Shu bois avtomatik javob berish tizimida oq ro‘yxat, vaqtinchalik bloklash, bloklash muddatini nazorat qilish va administrator tomonidan bekor qilish imkoniyatlari nazarda tutilishi kerak.

Avtomatlashtirilgan himoya algoritmining ishlash tamoyillari. Taklif etilayotgan gibrid modelda hujumlarni avtomatik aniqlash va bloklash jarayonini samarali tashkil etish uchun xavf darajasini baholash algoritmidan foydalanish mumkin. Bunda hujum belgilarini aniqlashda quyidagi parametrlar hisobga olinadi:

- N – muayyan vaqt oralig‘ida qayd etilgan shubhali so‘rovlar soni;
- T – kuzatuv vaqt oralig‘i;
- P – aniqlangan hodisaning xavflilik darajasi;
- R – takroriy hujumlar soni;

– S – xavfsizlik qoidalariga moslik darajasi.

Hodisaning umumiy xavf ko‘rsatkichini quyidagi shartli formula yordamida aniqlash mumkin:

$$K = \alpha N + \beta R + \gamma P$$

Bu yerda α, β va γ – parametrlarning ahamiyatini belgilovchi vazn koeffitsiyentlari. Ularning qiymatlari tarmoq infratuzilmasining xususiyatlari va xavfsizlik siyosatiga qarab belgilanadi. Masalan, bir IP-manzildan qisqa vaqt ichida ko‘plab portlarga ulanish urinishlari qayd etilsa, takroriylik va trafik intensivligi oshishi natijasida xavf ko‘rsatkichi ham ortadi. Agar aniqlangan hodisa ma’lum hujum imzosiga mos kelsa, uning xavflilik darajasi qo‘shimcha ravishda hisobga olinadi. Shartli qaror qabul qilish mexanizmi quyidagicha ifodalanadi:

$$K \geq K_{\text{yuqori}} \Rightarrow \text{IP bloklash}$$
$$K_{\text{quyi}} \leq K < K_{\text{yuqori}} \Rightarrow \text{Kuzatish va ogohlantirish}$$
$$K < K_{\text{quyi}} \Rightarrow \text{Oddiy monitoring}$$

Algoritmning asosiy ustunligi shundaki, u har bir hodisaga bir xil javob bermaydi, balki xavf darajasiga qarab turli himoya choralarini qo‘llaydi. Natijada kichik xavfli hodisalar uchun ortiqcha bloklashlarning oldi olinadi, yuqori xavfli hujumlarga esa tezkor javob qaytariladi.

Gibrid himoya modelining samaradorligi va amaliy qo‘llash imkoniyatlari. FortiGate va pfSense/Suricata asosidagi ikki qatlamli himoya modelidan foydalanish tashkilotlarning tarmoq infratuzilmasini kompleks himoyalash imkoniyatini yaratadi. Bunda ikki xil texnologiyaning o‘zaro to‘ldiruvchi funksiyalari xavfsizlikni ta’minlash jarayonini yanada samarali tashkil etishga xizmat qiladi.

Taklif etilayotgan modelning asosiy afzalligi shundaki, u tarmoq xavfsizligini ko‘p qatlamli himoya tamoyili asosida tashkil etib, FortiGate va pfSense/Suricata texnologiyalarining imkoniyatlarini o‘zaro uyg‘unlashtiradi. Bunda FortiGate yordamida tarmoq trafikini dastlabki filtrlash va ruxsatsiz ulanishlarni cheklash, Suricata orqali esa trafikni chuqur tahlil qilish hamda kiberhujumlarni aniqlash amalga oshiriladi. Avtomatlashtirish mexanizmining joriy etilishi aniqlangan tahdidlarga administratorning bevosita aralashuvisiz tezkor javob qaytarish, zararli IP-manzillarni bloklash va xavfsizlik hodisalarini qayd etish imkonini beradi. Shuningdek, turli himoya vositalaridan olingan ma’lumotlarni yagona monitoring tizimida jamlash tarmoqdagi xavfsizlik holatini kompleks baholashga xizmat qiladi. Modelning moslashuvchan arxitekturasi esa yangi tahdidlar paydo bo‘lganda xavfsizlik qoidalari va avtomatlashtirish algoritmlarini yangilash orqali himoya mexanizmlarini takomillashtirish imkonini yaratadi.

Modelning amaliy samaradorligini aniqlash uchun laboratoriya sharoitida tajriba-sinov ishlarini tashkil etish maqsadga muvofiq. Bunda portlarni skanerlash, brute force va DDoSga o‘xshash nazorat qilinadigan trafik ssenariylari yaratiladi. Har bir ssenariyda hujumni aniqlash vaqti, avtomatik javob berish vaqti, bloklash aniqligi, noto‘g‘ri bloklashlar soni hamda tizimning protsessor va operativ xotira resurslaridan foydalanishi baholanadi.

Samaradorlikni baholashda quyidagi ko‘rsatkichlardan foydalanish mumkin (1-jadval):

1-jadval. **Gibrid himoya modelining samaradorligini baholash ko‘rsatkichlari**

Ko‘rsatkich	Baholash mazmuni
Detection Rate	Hujumlarni aniqlash darajasi
False Positive Rate	Noto‘g‘ri ogohlantirishlar ulushi
Response Time	Hujumga javob berish vaqti

Ko‘rsatkich	Baholash mazmuni
Blocking Accuracy	Zararli trafikni to‘g‘ri bloklash darajasi
Resource Usage	Tizim resurslaridan foydalanish darajasi

Bunda aniqlash darajasi quyidagicha hisoblanadi:

$$DR = \frac{TP}{TP + FN} \times 100\%$$

Bu yerda TP – to‘g‘ri aniqlangan hujumlar, FN – aniqlanmay qolgan hujumlar soni.
Noto‘g‘ri ogohlantirishlar darajasi esa:

$$FPR = \frac{FP}{FP + TN} \times 100\%$$

Bu yerda FP – qonuniy trafikning hujum sifatida noto‘g‘ri aniqlanishi, TN – to‘g‘ri aniqlangan qonuniy trafik sonidir.

Javob berish vaqtini baholashda hujumning aniqlangan vaqti bilan bloklash amalining bajarilgan vaqti o‘rtasidagi farq hisobga olinadi. Ushbu ko‘rsatkichning kamayishi avtomatlashtirilgan himoya mexanizmining tezkorligini ifodalaydi. Shuni alohida ta’kidlash lozimki, yuqoridagi ko‘rsatkichlar modelni baholash metodologiyasini ifodalaydi. Ular bo‘yicha aniq sonli natijalar olish uchun laboratoriya sinovlari va real trafik sharoitidagi tajribalar talab etiladi. Mazkur modelni ta’lim muassasalari, bank va moliya tashkilotlari, davlat idoralari, korporativ tarmoqlar hamda server infratuzilmalarida qo‘llash mumkin. Ayniqsa, bir nechta lokal tarmoqqa ega tashkilotlarda turli xavfsizlik qatlamlarini birlashtirish va hodisalarga markazlashgan holda javob qaytarish muhim ahamiyat kasb etadi.

Modelni joriy etishdagi muammolar va ularni bartaraf etish yo‘llari. Ikki qatlamli gibrid himoya modelini amaliyotga joriy etishda ayrim texnik va tashkiliy muammolar yuzaga kelishi mumkin. Jumladan, FortiGate va pfSense o‘rtasidagi marshrutlash qoidalarini muvofiqlashtirish, trafikning ikki marta filtrlashdan o‘tishi natijasida kechikish yuzaga kelishi, xavfsizlik hodisalarining noto‘g‘ri tasniflanishi va avtomatik bloklash jarayonidagi xatolar shular jumlasidandir. Bunday muammolarni bartaraf etish uchun, avvalo, tarmoq topologiyasi puxta loyihalashtirilishi, har bir himoya qatlamining vazifalari aniq belgilanishi lozim. Shuningdek, xavfsizlik qoidalarining takrorlanishiga yo‘l qo‘ymaslik va trafik oqimini optimal tashkil etish zarur.

Avtomatlashtirilgan javob berish mexanizmida API orqali boshqaruv amalga oshirilganda autentifikatsiya, ruxsatlarni cheklash va ma’lumotlarni himoyalash talablariga qat’iy rioya qilinishi kerak. API kalitlari va maxfiy ma’lumotlar himoyalangan muhitda saqlanishi, avtomatik bloklash amallari esa qayd etib borilishi lozim. Yana bir muhim masala – noto‘g‘ri bloklashlarning oldini olishdir. Buning uchun ishonchli IP-manzillar ro‘yxatini shakllantirish, vaqtinchalik bloklash mexanizmini qo‘llash va zarur hollarda administrator tomonidan qarorni qayta ko‘rib chiqish imkoniyatini yaratish tavsiya etiladi. Natijada ikki qatlamli gibrid himoya modelining ishonchliligi, boshqaruvchanligi va amaliy samaradorligini oshirish mumkin.

XULOSA

FortiGate va pfSense/Suricata asosidagi ikki qatlamli gibrid himoya modeli tarmoq xavfsizligini kompleks tashkil etish va kiberhujumlarga avtomatlashtirilgan tarzda javob qaytarish imkoniyatini yaratadi. Birinchi qatlamda FortiGate orqali tarmoq trafikini filtrlash va xavfsizlik siyosatini boshqarish, ikkinchi qatlamda esa Suricata yordamida hujumlarni chuqur tahlil qilish

hamda aniqlash amalga oshiriladi. Tadqiqot doirasida taklif etilgan Python asosidagi avtomatlashtirish mexanizmi aniqlangan hodisalarni xavflilik darajasiga qarab tasniflash, zararli IP-manzillarni bloklash, administratorni xabardor qilish va xavfsizlik hodisalarini qayd etishga yo‘naltirilgan. Mazkur yondashuv inson omiliga bog‘liqlikni kamaytirish, javob berish tezligini oshirish va tarmoq infratuzilmasining himoyalanganlik darajasini yaxshilashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Ganiyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. – Toshkent: Fan va texnologiya, 2017. – 372 b.
2. Ganiyev S.K., Irgasheva D.Y., Xudoyqulov Z.T. Kiberxavfsizlik asoslari. Darslik. – 2022.
3. Nurmamatov M.Q., Hamidov M. Kiberxavfsizlik asoslari. Darslik. – Samarqand: SamDU, 2025. – 272 b.
4. Fortinet. FortiGate Administration Guide: Automation Stitches. Fortinet Documentation. – Elektron manba.
5. Fortinet. FortiOS Cookbook: Creating the Automation Stitches. – Fortinet Inc. – Elektron manba.
6. Open Information Security Foundation. Suricata User Guide: Intrusion Prevention System Mode. – Rasmiy texnik hujjat.
7. Open Information Security Foundation. Suricata Documentation. – Texnik qo‘llanma.