AXBOROT KOMMUNIKATSIYA TARMOQLARIDA KIBERHUJUMLARNI ANIQLASH USUL VA VOSITALARI

Qurbonaliyeva Dilshoda Vali qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: *Maqolada zamonaviy kibertahdidlarning ortib borayotgan xavfi, ularning turlari (ransomware, phishing, DDoS, SQL ineksiya va boshqalar) va 2025-yilgi global statistik ma’lumotlar tahlil qilingan. Kiberhujumlarning asosiy maqsadlari (pul, moliyaviy ma’lumotlar, shaxsiy identifikatsiya ma’lumotlari) va ularning ishlab chiqarish, ta’lim va tibbiyot kabi sektorlarga ta’siri ko‘rib chiqilgan. Tarmoq xavfsizligini ta’minlashda NGFW, SIEM, XDR, ZTNA kabi zamonaviy himoya texnologiyalarining imkoniyatlari va ularning an’anaviy usullardan farqlari jadval shaklida taqqoslangan. Deception Technology (honeypotlar) orqali hujumchilarni aldash va ularning taktikalarini o‘rganish metodlari bayon etilgan. Maqolada foydalanuvchilarni xavfsizlik bo‘yicha o‘qitish, ko‘p faktorli autentifikatsiya va tizimli yangilanishlarni o‘tkazishning ahamiyati ta’kidlangan. Tadqiqot kibertahdidlarga qarshi kompleks yondashuv va proaktiv choralarni joriy etish zarurligini ko‘rsatadi.*

Kalit so‘zlar: *Kibertahdidlar, Ransomware, Phishing, DDoS hujumlari, SQL ineksiya, Tarmoq xavfsizligi, NGFW, SIEM, XDR, ZTNA, Deception Technology, Honeypot, Proaktiv himoya choralari, Kiberjinoyatlar statistikasi*

KIRISH

Kommunikatsiya tarmoqlari jadal rivojlanayotgan bugungi kunda axborot jarayonlari bilan bog‘liq munosabatlarda shaxsiy manfaatni ko‘zlagan holda o‘zganing kompyuteri, serveri yoki tarmog‘ini buzish orqali ma’lumotlarni o‘g‘irlash, tizimdan ruxsatsiz foydalanish yoki tizim egasiga foydalanishdagi noqulayliklarini keltirib chiqaradigan va firibgarlik orqali pul topish imkonini beradigan kiber hujumlarining soni ortib bormoqda [1].

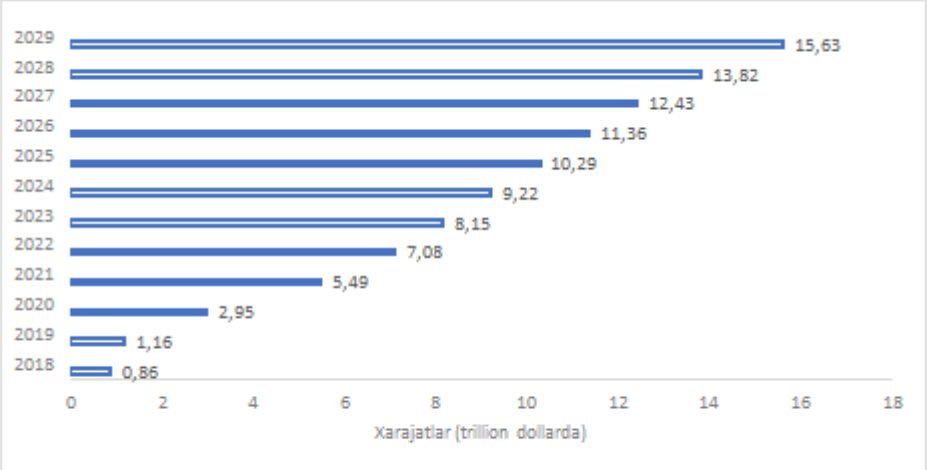
Kiberhujum tarmoqqa, kompyuter tizimiga yoki raqamli qurilmaga ruxsatsiz kirish orqali ma’lumotlar, ilovalar yoki boshqa aktivlarni o‘g‘irlash, fosh qilish, o‘zgartirish yoki yo‘q qilishga qaratilgan har qanday qasddan amalga oshirilgan harakatdir. Kiberhujumlarga asosan shaxsiy, jinoiy yoki siyosiy motivlar sabab bo‘ladi. Tizimga kirish va ma’lumotlardan foydalanish huquqiga ega insayderlar tomonidan amalga oshiriluvchi hujumlar odatda shaxsiy norozilik yoki moddiy manfaatlar evaziga sodir etiladi. Kiberjinoiyatchilar esa ruxsat etilmagan kirish orqali pul o‘g‘irlash, ma’lumotlarni o‘g‘irlash yoki biznesni buzish orqali moliyaviy foyda olishga intiladi [1].

Tahdidchilar odatda kompyuter tarmoqlari orqali tizimga kirishga urinishadi va ularning umumiy maqsadlarga quyidagilar kiradi [2]:

- Pul

- Korxona va tashkilotlarning moliyaviy ma’lumotlari
- Mijozlar ro‘yxati
- Mijoz ma’lumotlari, shu jumladan shaxsiy identifikatsiya qilinadigan ma’lumotlar yoki boshqa maxfiy shaxsiy ma’lumotlar
- Elektron pochta manzillari va kirish ma’lumotlari.
- Tijorat sirlari yoki mahsulot dizayni kabi intellektual mulk
- Axborot tizimlari yoki IT infratuzilmasini buzish.

2025- yil statistikalari shuni ko‘rsatadiki, dunyo bo‘ylab har kuni 2200 dan ortiq kiberhujumlar sodir bo‘lmoqda. Buning oqibatida global kiberhujumlar 30 foizga oshgan. Har haftada 1636 ta soha korxonalarii, 3341 ta ta’lim va tadqiqot obyektlari kiberhujumlarning eng yuqori xavfiga duch kelmoqda. Ishlab chiqarish sektorlarida Ransomware hujumlari eng katta talofat keltirib, hodisalarning taxminiy 29 foizini tashkil etmoqda. Quyida 2018-2029 yillarda butun dunyo bo‘ylab kiberjinoyatlarning taxminiy qiymati (trillion AQSH dollarida) statistikasi keltiriladi [3].



1-rasm. Kiberjinoyatlarning taxminiy qiymati.

Kibertahdidlarning turlari orasida to‘lov dasturi eng ko‘p aniqlangan bo‘lib, barcha hodisalarning taxminan 70 foizini tashkil qiladi. Ishlab chiqarish sanoati, so‘nggi ikki yilda xususan, eng ko‘p to‘lov dasturi hujumlariga duch kelgan va bu uni global miqyosdagi eng maqsadli sektorga aylantirgan. Buning sababi: ishlab chiqarish sektori jamiyat uchun zarur bo‘lgan turli sohalarni o‘z ichiga oladi. U iste’mol tovarlari, elektronika, avtomobilsozlik, energetika, farmatsevtika, oziq-ovqat va ichimliklar, og‘ir sanoat va neft va gaz kabi global iqtisodiyotlarga hissa qo‘shadi. Ishlab chiqarish ekotizimida ishlab chiqarish quvvatlari butun dunyo bo‘ylab tarqalgan va har bir ishlab chiqaruvchi ham iste’molchi yoki aksincha. Shuning uchun bitta kompaniyaga kiberhujum ekotizim bo‘ylab to‘lqinli ta’sir ko‘rsatishi mumkin va bu qimmat oqibatlarga olib kelishi mumkin. Natijada yuzaga keladigan xavflar tizimli, yuqumli va ko'pincha biron bir shaxs tushuna olmaydi yoki nazorat qila olmaydi. Bu nuqtai nazardan kiberhujumlarning turlari va asosiy kriteriyalarini o‘rganish, har bir tarmoq foydalanuvchisi uchun muhimdir.

1-jadval.

Kiberhujumlaming turlari bo‘yicha ma’lumotlar jadvali

Hujum Turi	Hujum Vektori	Asosiy Maqsad	Ko‘p Qo‘llaniladigan Usullar	Nishonlar	Aniqlash Qiyinligi	Oldini Olish Choralari
Phishing [4]	Email, SMS, soxta saytlar	Hisob ma'lumotlarini o‘g‘irlash	Ijtimoiy muhandislik, soxtalashtirish	Shaxslar, tashkilotlar	O‘rtacha	Foydalanuvchilarni o‘qitish, spam filtrlari, MFA
Ransomware [5]	Malware (email, yuklab olish)	Ma'lumotlarni shifrlash va fidye talab qilish	Zaifliklardan foydalanish	Tashkilotlar, infratuzilma	Yuqori (hujumdan keyin)	Zaxira nusxalar, yangilanishlar, EDR vositalari
DDoS [6]	Tarmoq trafigini haddan tashqari ko‘paytirish	Xizmatlarni to‘xtatish	Botnetlar, kuchaytirish hujumlari	Veb-saytlar, onlayn xizmatlar	Oson (trafik o‘sishi)	Trafik filtrlash, CDN xizmatlari
O‘rtada turgan odam hujumi [7]	Zaif tarmoq/dasturiy ta'minot	Kommunikatsiyalarni to‘xtatish yoki o‘zgartirish	Tinglovchi qurilmalar, SSL strip	Ochiq Wi-Fi foydalanuvchilari	Yuqori	Shifrlash (HTTPS, VPN), sertifikat tekshiruvi
SQL Ineksiya hujumi [8]	Veb-ilova kirish maydonlari	Ma'lumotlar bazasini buzish	Zararli SQL so‘rovlari	Veb-ilovalar, ma'lumotlar bazasi	O‘rtacha	Kirishni tekshirish, WAF (Veb-ilova to‘sig‘i)
Saytlararo script yaratish hujumi [9]	Veb-ilovalar	Sessiya ma'lumotlarini o‘g‘irlash	Zararli skriptlarni kiritish	Veb-sayt foydalanuvchilari	O‘rtacha	Ma'lumotlarni shifrlash, CSP sarlavhalari
Zero-Day Exploits hujumi [10]	Yangilanmagan dasturiy ta'minot	Ruxsatisiz kirish, ma'lumotlarni o‘g‘irlash	Noma'lum zaifliklardan foydalanish	Davlat, korporatsiyalar	Juda yuqori	Proaktiv yangilanishlar, xavf tahlili
Hisob ma’lumotlarini to‘ldirish hujumi [1]	Sizgan parollar ro‘yxati	Hisobni egallash	Avtomatlashtirilgan kirish urinishlari	Takroriy parol ishlatganlar	O‘rtacha	MFA, parolni almashtirish, CAPTCHA
Ijtimoiy Muhandislik[11]	Inson omili	Qurbonlarni aldash	Soxta talablar, "pulling evaziga" taklif	Xodimlar, rahbariyat	Yuqori	Xavfsizlik bo‘yicha mashg‘ulotlar, tekshiruv
Ichki Tahdidlar	Ruxsatlardan	Ma'lumotlarni buzish yoki	Imtiyozlarni suiiste'mol	Tashkilotlar,	Yuqori	Faollikni monitoring
[1]	suiiste'mol	o‘g‘irlash	qilish	intellektual mulk		qilish, ruxsatlarni cheklash

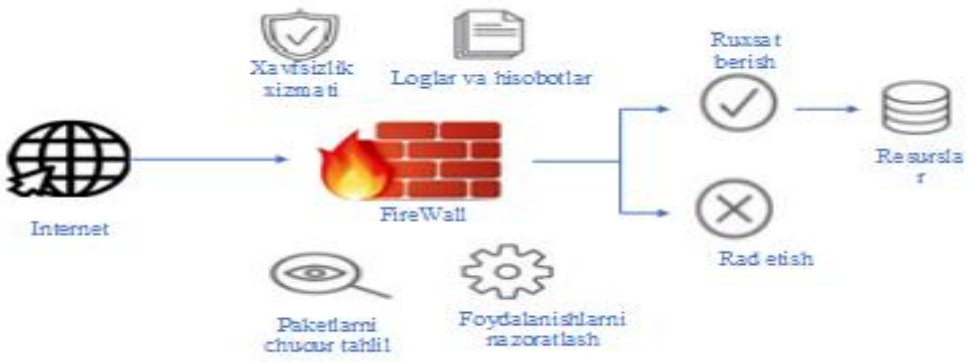
Asosiy tarmoqlarga to‘lov dasturlari hujumlari, murakkab fishing sxemalari hamda SQL Ineksiyaning ko‘payishi himoya choralarini tartibga solishning kuchaytirilishi va texnologiyalarni joriy etish zarurligini eslatib turadi.

ASOSIY QISMI

Tarmoq xavfsizligi bu tarmoqqa bo‘ladigan xujumlar va suqulib kirishlarni monitoringlash, bartaraf etish va javob qaytarish uchun mo‘ljallangan xavfsizlik siyosati, taktikasi va instrumentlarini tavsiflovchi soha hisoblanadi. Hozirgi kunda IT bozorida ko‘plab xavfsizlik yechimlari mavjud. Zamonaviy tarmoq himoya vositalari hujumlarning oldini olish, tarmoq xavfsizligini mustahkamlash va ma'lumotlarni himoya qilish uchun

ishlab chiqilgan. Quyida eng dolzarb va samarali tarmoq himoya vositalari o‘rganilan va tahlil qilingan.

NGFW (Next-Generation Firewall - Zamonaviy tarmoq xavfsizlik devori) – bu an’anaviy firewall (tarmoq devori) imkoniyatlarini kengaytirgan zamonaviy xavfsizlik yechimidir. U nafaqat trafikni filtrlash, balki chuqur paket tahlili (DPI), IDS/IPS (hujumlarni aniqlash va oldini olish), ilova darajasidagi xavfsizlik va foydalanuvchi autentifikatsiyasi kabi qo‘shimcha himoya funksiyalariga ham ega[12] . NGFW ilova darajasidagi xavfsizlikni amalga oshiradi. Oddiy firewall faqat IP manzillar va portlar bo‘yicha filtrlaydi. NGFW esa tarmoq trafigini chuqur tahlil qilib (DPI), ilovalar (masalan, Facebook, YouTube, Telegram) va ularning xatti-harakatlarini nazorat qiladi. Ma'lum bir ilovalarga kirishni bloklash yoki cheklash imkonini beradi. Ushbu texnologiya IPS(Intrusion Detection System) va IPS (Intrusion Prevention System) texnologiyalarni o‘z ichiga olgan holda hujumlarni oldindan aniqlaydi va oldini oladi. NGFW Active Directory (AD), LDAP va Radius kabi autentifikatsiya tizimlari bilan integratsiya qila oladi. Bu esa tarmoq resurslariga kim, qachon va qanday kirayotganini aniq nazorat qilish imkonini beradi.



2-rasm. Zamonaviy Firewall funksiyalari

Zamonaviy tahdidlar ko‘pincha SSL/TLS shifrlangan trafik orqali keladi. NGFW shifrlangan trafigini tekshirish va zararli ma’lumotlarni aniqlash imkoniyatiga ega.

2-jadval.

NGFW ning an’anaviy firewall bilan farqi

Xususiyat	An’anaviy Firewall	NGFW
Filtrlash	IP-manzillar va portlar bo‘yicha	Ilovalar, foydalanuvchilar va trafik tahliliga asoslangan
IDS/IPS	Yo‘q	Bor
SSL Trafik Tahlili	Yo‘q	Bor
Ilovalarni boshqarish	Yo‘q	Bor
Cloud va IoT qo‘llab-quvvatlashi	Cheklangan	To‘liq
Sandboxing	Yo‘q	Bor
Autentifikatsiya integratsiyasi	Yo‘q	Bor (Active Directory, LDAP va boshqalar)

SIEM (Security Information and Event Management - Xavfsizlik ma’lumotlari va hodisalarini boshqarish) – bu tarmoq va axborot xavfsizligi uchun ishlatiladigan ilg‘or tizim

bo‘lib, u xavfsizlik hodisalarini yig‘ish, tahlil qilish va avtomatik javob berish imkoniyatini taqdim etadi. SIEM turli log-fayllar, tarmoq hodisalari va hujum tahlillarini markazlashtiradi, ulardan foydalangan holda tahdidlarni erta aniqlaydi va hujumlarning oldini oladi [2]. Dastlabki bosqichda SIEM tizimi serverlar, tarmoqlar, firewalllar, antivirus dasturlar, IDS/IPS va boshqa xavfsizlik vositalaridan loglar va hodisalar haqidagi ma’lumotlarni avtomatik yig‘adi. Bunda tarmoq uskunalari (ruter, firewall, switch, IPS/IDS), dasturiy ta’minotlar (ERM, CRM, operatsion tizimlar, veb-serverlar), Bulut xizmatlari (AWS, Azure, Google Cloud) kabi manbaalardan foydalanadi. Ikkinchi bosqichda. SIEM big data texnologiyalaridan foydalangan holda ko‘plab manbalardan kelgan ma’lumotlarni bir joyga yig‘adi va ularni tahlil qiladi. Tahlil qilish algoritmlari – loglar va hodisalar orasidagi bog‘liqliklarni topib, g‘ayritabiiy xatti-harakatlarni aniqlaydi. Masalan, Agar xodim bitta IP manzildan tizimga kirsa, lekin keyin boshqa mamlakatdan kirishga urinayotgan bo‘lsa – SIEM ushbu xatti-harakatni potensial tahdid sifatida belgilaydi. Uchinchi bosqichda texnologiya hujumlarni oldindan aniqlab, avtomatik ravishda habardor qiladi yoki bloklaydi. Va so‘nggi bosqic hisobotlar va monitoringdan iborat bo‘ladi. Tarmoqning xavfsizlik holatini real vaqt rejimida ko‘rsatadigan vizual panellar (dashboards) va hisobotlar yaratiladi.

Quyidagilar dunyoning eng mashhur SIEM tizimlari:

Splunk Enterprise Security – Big Data va sun’iy intellekt asosida ishlaydi.

IBM QRadar SIEM – Katta tashkilotlar uchun kuchli xavfsizlik tizimi.

ArcSight (Micro Focus) – Katta hajmdagi log-fayllarni boshqarish uchun ideal.

Microsoft Sentinel (Azure SIEM) – Bulut infratuzilmasi bilan moslashgan SIEM.

LogRhythm SIEM – Kiberxavfsizlik tahdidlarini tezkor aniqlash imkoniyatiga ega.

Elastic SIEM – Ochiq kodli (open-source) SIEM yechimi.

XDR (Extended Detection and Response - Kengaytirilgan aniqlash va javob berish tizimi) – bu kiberxavfsizlik tizimlarining keyingi avlodi bo‘lib, u tarmoq, endpoint (foydalanuvchi qurilmalari), serverlar, bulut, e-pochta va boshqa IT infratuzilma manbalaridan tahdidlarni aniqlash va ularga avtomatik javob berish imkonini beradi. An’anaviy xavfsizlik tizimlari (EDR, SIEM, IDS/IPS) faqat bitta ma’lumot manbai yoki muhitga qaratilgan bo‘lsa, XDR barchasini birlashtirib, markazlashgan xavfsizlik himoyasini ta’minlaydi. Tarmoq, endpoint (kompyuter va mobil qurilmalar), bulut, e-pochta va boshqa xavfsizlik tizimlaridan ma’lumotlarni avtomatik ravishda yig‘adi. Sun’iy intellekt va Machine Learning asosida tahdidlarni aniqlaydi. EDR (Endpoint Detection and Response-Yakuniy nuqtani aniqlash va javob berish tizimi) faqat endpoint qurilmalarga qaratilgan bo‘lsa, XDR butun IT infratuzilmasiga tahdidlarni kuzatadi va avtomatik chora ko‘radi. Ohirgi bosqichda real vaqt rejimida tahdidlarni vizual panellar (dashboards) va hisobotlar orqali ko‘rsatadi. SIEM bilan integratsiya qilingan holda ishlaydi va xavfsizlik hodisalarini avtomatik tahlil qiladi. Bundan tashqari XDR forensik tahlil (hodisalar sababini aniqlash) va hujum yo‘nalishini tushunish uchun ham ishlatiladi.

3-rasm. Kengaytirilgan aniqlash va javob berish tizimining ishlash prinsipi

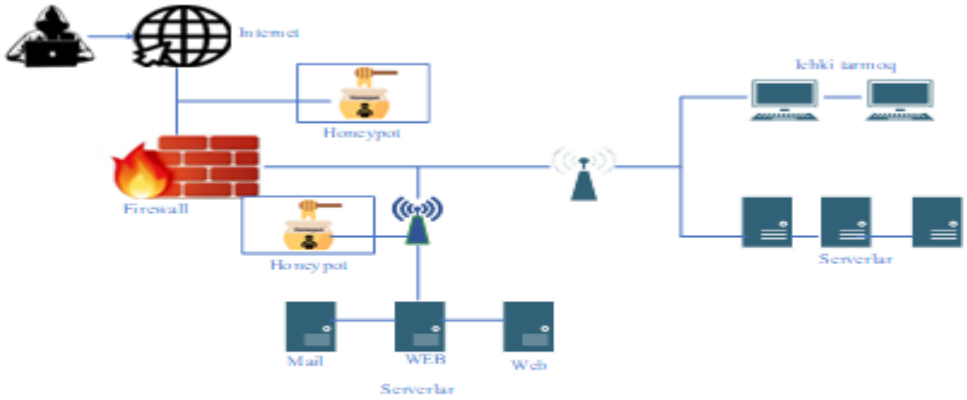
ZTNA (Zero Trust Network Access- Nol Ishonchga Asoslangan Tarmoqga Kirish) – bu tarmoq xavfsizligini ta’minlash uchun nol ishonch (Zero Trust) printsipiga asoslangan texnologiya bo‘lib, foydalanuvchilarga va qurilmalarga faqat minimal zarur ruxsat bilan kirish imkonini beradi.

Asosiy tamoyillar:

- "Ishonma, doim tekshir" (Never Trust, Always Verify) – Har qanday foydalanuvchi yoki qurilma avval autentifikatsiya qilinishi va tekshirilishi kerak.
- Minimal ruxsat (Least Privilege Access) – Foydalanuvchi va qurilmalarga faqat o‘z ishini bajarish uchun zarur bo‘lgan ruxsatlar beriladi.
- Davomiy monitoring (Continuous Authentication) – Kirish berilgandan keyin ham harakatlar doimiy ravishda nazorat qilinadi.
- Tarmoq perimetri o‘rniga identifikatsiya – Kirish imkoniyatlari nafaqat tarmoq joylashuvi, balki foydalanuvchi, qurilma va kontekst asosida belgilanadi.

ZTNA uch bosqichda ishlaydi. Dastlab, foydalanuvchi va qurilmani autentifikatsiya qilish jarayonidan o‘tiladi. Ushbu bosqichda foydalanuvchi va qurilma Multi-Factor Authentication (MFA) yordamida tekshiriladi. Qurilmaning xavfsizlik holati (device posture) aniqlanadi – masalan, antivirus o‘rnatilganmi, OS yangilanganmi? Foydalanuvchi roli va siyosatga muvofiq ravishda unga ruxsat beriladi yoki berilmaydi. Ikkinchi bosqichda minimal ruxsat asosida kirishni ta’minlash amalga oshiriladi. Foydalanuvchilar barcha tarmoqqa emas, balki faqat kerakli ilovalarga va ma’lumotlarga kirish huquqiga ega bo‘ladi. Ilovalar internet orqali to‘g‘ridan-to‘g‘ri ko‘rinmaydi, faqat ZTNA orqali kirish mumkin. Tizim har bir kirish so‘rovini kontekst (foydalanuvchi joylashuvi, qurilma holati, xatti-harakatlari) asosida baholaydi. So‘nggi bosqich monitoring va xavfsizlik tahlilidan iborat bo‘ladi.

Deception Technology (Honeypots & Trap Systems - Aldov texnologiyasi) – bu kiberxavfsizlik strategiyasi bo‘lib, tahdidlarni oldindan aniqlash va hujumchilarni aldash uchun soxta (fake) tizimlar, ma’lumotlar va xizmatlar yaratishdan iborat. Bu texnologiya xakerlarni haqiqiy tizimdan uzoqlashtirish, ularning harakatlarini kuzatish va mudofaa strategiyalarini yaxshilash uchun ishlatiladi [2].



4-rasm. Honeypotning tarmoqdagi arxitekturasi

Honeypotlar quyidagi ketma-ketlikda ishlaydi:

1. Soxta resurslar yaratish

- Honeypot (Tuzoqli serverlar) – Xavfsiz tizim kabi ko‘rinadigan, lekin haqiqatda hujumchilarni jalb qilish va kuzatish uchun ishlatiladigan serverlar.
- Honeynet – Bir nechta honeypot tizimlaridan iborat butun tarmoq simulyatsiyasi.
- Decoy Files (Tuzoqli hujjatlar) – Hujumchilarni jalb qilish uchun yaratilgan soxta hujjatlar. Agar kimdir ularni ochsa, tizim ogohlantiriladi

Trap Credentials (Soxta login ma’lumotlari) – Agar hujumchi ularni ishlatsa, xavfsizlik jamoasi darhol xabardor bo‘ladi.

2. Hujumchilarni aniqlash va kuzatish

- Honeypot yoki tuzoqli tizimlarga faqatgina ruxsatsiz shaxslar kiradi, shuning uchun bunday faoliyat avtomatik ravishda shubhali harakat sifatida qayd qilinadi.
- Tizim hujumchini to‘liq tahlil qiladi:

Qaysi usuldan foydalandi?

Qaysi ma’lumotlarga kirishga harakat qildi?

Qaysi buyruqlarni ishlatdi?

3. Xavfsizlik jamoasini ogohlantirish

- Hujum aniqlangandan keyin, tizim SIEM, XDR yoki SOAR xavfsizlik platformalariga ogohlantirish yuboradi.
- Tahlil natijasida, haqiqiy tarmoqqa tahdid soladigan ekspluatatsiya usullari aniqlanadi va ularni bloklash choralari ko‘riladi.

Yuqorida keltirilgan xavfsizlik vositalarini maqsadi, asosiy funksiyalari, afzalliklari va qo‘llanilish sohalarini bir biridan farqlash muhim hisoblaniladi.

3-jadval.

Kiberxavfsizlik vositalarining asosiy turlari va xususiyatlari jadvali

Texnologiya Nomi	Maqsadi	Asosiy Funksiyalari	Afzalliklari	Namunalar	Qo‘llanish Sohalari
NGFW	Tarmoq trafigini ilova darajasida filtrlash va hujumlarni oldini olish	Chuqur paket tahlili (DPI), IDS/IPS, SSL trafik tekshiruvi, ilovalarni boshqarish, autentifikatsiya integratsiyasi	An’anaviy firewallga nisbatan yuqori himoya, shifrlangan trafikni tahlil qilish	Palo Alto, Fortinet, Cisco Firepower	Korxonalarning tarmoq infratuzilmasi himoyasi, ilovalarga kirishni nazorat qilish
SIEM	Xavfsizlik hodisalarini markaziy monitoring va tahlil qilish	Loglarni yig‘ish, anomaliyalarni aniqlash, avtomatik ogohlantirish, hisobotlar	Ko‘p manbalardan ma’lumotlarni birlashtirish, sun’iy intellekt asosida tahlil	Splunk, IBM QRadar, Microsoft Sentinel	Tizimdagi shubhali faollikni aniqlash, qonuniy talablarga muvofiqlik (GDPR, PCI DSS)
XDR	Butun IT infratuzilmada tahdidlarni keng ko‘lamda aniqlash va javob berish	Endpoint, tarmoq, bulut ma’lumotlarini birlashtirish, AI/ML asosida tahlil, avtomatik javob	Har xil xavfsizlik tizimlarini integratsiyasi, hujum zanjirini to‘liq tahlil	CrowdStrike, Microsoft Defender XDR	Murakkab hujumlarni aniqlash (APT), forensik tahlil
ZTNA	"Nol ishonch" printsipi asosida minimal ruxsat bilan kirishni ta’minlash	Multi-Factor Authentication (MFA), qurilma holatini tekshirish, kontekst asosida kirish	Tarmoq perimetriga bog‘liq bo‘lmagan himoya, davomiy monitoring	Zscaler Private Access, Cisco Duo	Masofaviy ishchi xavfsizligi, maxfiy ma’lumotlarga kirishni himoya qilish
Deception Technology	Hujumchilarni soxta resurslar bilan aldash va ularni aniqlash	Honeypotlar, tuzoqli fayllar, hujumchilar harakatlarini kuzatish	Hujumlarni erta aniqlash, hujum usullarini o‘rganish	Attivo Networks, TrapX, Illusive Networks	Ichki tahdidlarni aniqlash, xakerlarning taktikalarini tahlil qilish

Jadval shuni ko‘rsatadiki, NGFW va ZTNA tizimlari orqali tarmoq kirishini qat’iy nazorat qilish, SIEM va XDR yordamida ko‘p qatlamli tahlil va avtomatik javob berish, Deception Tecnologyni hujumchilarni erta aniqlash va ularning taktikalarini o‘rganish maqsadlarida qo‘llash samarali hisoblaniladi. Ushbu texnologiyalarni qo‘llash bilan bir qatorda soha korxonalari yoki tashkilotlar quyidagilarga e’tibor qaratishi strategik himoyani ta’minlaydi:

1. Foydalanuvchi tarbiyasi Phishing va ijtimoiy muhandislik hujumlarining oldini olish uchun muhim.
2. Ko‘p faktorli autentifikatsiya (MFA) va parolni muntazam yangilash hisob ma’lumotlarini himoya qilish uchun zarur.

XULOSA

Zamonaviy dunyoda kibertahdidlar sonining ortishi xususan, ransomware, phishing, DDoS va SQL ineksiya kibi hujumlar orqali tashkilotlar, shaxslar va davlatlar uchun katta xavf tug‘dirmoqda. 2025-yil statistikasi shuni ko‘rsatadiki, har kuni 2200 dan ortiq kiberhujumlar sodir bo‘lib, global miqyosda zarar 30% ga oshgan. Ishlab chiqarish, ta’lim va tibbiyot sektorlari eng ko‘p zarar ko‘rgan sohalar hisoblanadi, ularning zaifliklari butun ekotizimga tizimli ta’sir ko‘rsatishi mumkin.

Bunga qarshi kurashishda NGFW, SIEM, XDR, ZTNA kabi zamonaviy himoya texnologiyalari muhim rol o‘ynaydi. NGFW ilova darajasidagi trafikni nazorat qilish, SIEM va XDR esa ko‘p qatlamli tahlil orqali tahdidlarni erta aniqlash imkonini beradi. Nol ishonch tamoyiliga asoslangan ZTNA tizimi foydalanuvchilarga minimal ruxsat asosida kirishni ta’minlab, xavfsizlikni tubdan mustahkamlaydi. Deception Technology (honeypotlar) esa hujumchilarni soxta tizimlarga jalb qilib, ularning taktikalarini o‘rganish va oldini olish uchun samarali vosita hisoblanadi.

Foydalanuvchilarni kiberxavfsizlik bo‘yicha tarbiyalash, ko‘p faktorli autentifikatsiya (MFA) ni joriy etish va tizimlarni vaqtida yangilab turish kabi oddiy, ammo muhim choralar ham jiddiy xavflarni kamaytirishga yordam beradi. Statistik ma’lumotlar va kuzatilgan tendensiyalar shuni ko‘rsatadiki, kibertahdidlarga qarshi muvaffaqiyat faqat texnologiya, tashkiliy choralar va inson omilini integratsiyalashgan holda samarali bo‘ladi. Kelajakda sun’iy intellekt va avtomatlashtirilgan himoya tizimlarining rivojlanishi kiberjinoyatchilikka qarshi kurashni yanada komplekslashtiradi, ammo tizimli tayyorgarlik va global hamkorlik zaruriy shart bo‘lib qolmoqda.

Asosiy tavsiya: Tashkilotlar o‘zlarining kiberxavfsizlik strategiyalarini proaktiv (oldingi) usulda shakllantirib, zamonaviy texnologiyalar, xodimlar tarbiyasi va qat’iy siyosatlarni uyg‘unlashtirish orqali xavflarni minimallashtirishi kerak.

FOYDALANILGAN ADABIYOTLAR RO‘YHATI:

1. N. Hoque, M.H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita, Network attacks: Taxonomy, tools and systems, 2014, Journal of Network and Computer Applications, p.307-324, doi: 10.1016/j.jnca.2013.08.001 ;
2. S Bozorov, N Akhmedova, D Qurbonaliyeva, K Gultekin, Survey on honeypot: Detection, countermeasures and future with MI. AIP Conference Proceedings, 2024. doi: 10.1063/5.0242098 ;
3. https://www.stationx.net/?s=cyber-security-breach-statistics%252025
4. Z. Alkhalil; Ch. Hewage; L. Nawaf; I. Khan, Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, in 2021 Editor's Pick: Computer Science, doi:10.3389/fcomp.2021.563060 ;
5. Meland PH, Bayoumy YFF, Sindre G. The ransomware-as-a-service economy within the darknet. Comput Secur. 2020; 92:101762. doi:10.1016/j.cose.2020.101762 ;

6. Y. Al-Dunainawi, B. R. Al-Kaseem and H. S. Al-Raweshidy, "Optimized artificial intelligence model for DDoS detection in SDN environment", IEEE Access, vol. 11, pp. 106733-106748, 2023.

7. J. Jiang, G. Han, F. Wang, L. Shu, M. Guizani, An efficient distributed trust model for wireless sensor networks, IEEE Trans. Parallel Distrib. Syst., 26 (5) (2014), pp. 1228-1237,

8. R.P. van Heerden, B. Irwin, I.D. Burke va L. Leenen, Description of a Network Attack Ontology Presented Formally, 2021, Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities, p 343–368, doi: 10.1007/978-3-030-72236-4_14 ;

9. M. Raunds, N. Pentgraft, Diversity in Network Attacker Motivation: A Literature Review, 2009, International Conference on Computational Science and Engineering, doi: 10.1109/CSE.2009.178.;

10. M. Agarwal, K. S. Gill, R. Chauhan, A. Kapruwan, D. Banerjee, 2024, 3rd International Conference for Innovation in Technology (INOCON), doi: 10.1109/INOCON60754.2024.10512250 ;

11. R. Ding, L. Sun, W. Zang, L. Dai, Z. Ding, B. Xu, Towards universal and transferable adversarial attacks against network traffic classification, 2024, Journal of Computer Networks, doi: 10.1016/j.comnet.2024.110790 ;

12. B. Dorsemaine, J.P. Gaulier, J.P Wary, N. Kheir, P. Urien, Internet of Things: A Definition and Taxonomy, In Proceedings of the 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9–11 September 2015. doi: 10.1109/NGMAST.2015.71 ;

13. Z. Doffman, Cyberattacks On IOT Devices Surge 300%, 2019, Measured in Billions.