THREAT INTELLIGENCE TUSHUNCHASI

Tashmatova Shaxnoza Sabirovna
TDTU Katta oqituvchi
Erkinov Shohjahon Sherali o'g'li
Xayriddinov Shaxboz Shavkatovich
Ravshanov Amirshox Inoyatovich
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Ushbu maqolada Threat Intelligence (tahdidlar razvedkasi) tushunchasi, uning mazmuni, turlari va axborot xavfsizligi tizimidagi ahamiyati tahlil qilinadi. Threat Intelligence – bu kiberxavfsizlik tahdidlarini aniqlash, tahlil qilish va oldini olishga qaratilgan ma'lumotlarni yig'ish hamda qayta ishlash jarayonidir. Maqolada strategik, operativ va taktik darajadagi razvedka turlari, shuningdek, tahdid indikatorlari (IOC – Indicators of Compromise) tushunchasi yoritiladi. Tahdidlar haqidagi ma'lumotlar zararli dasturlar, fishing hujumlari, APT (Advanced Persistent Threat) kampaniyalari va boshqa kiberxavf manbalarini aniqlashda muhim rol o'ynaydi.*

Kalt so'zlar: *Threat Intelligence, kiberxavfsizlik, tahdid indikatorlari (IOC), APT, fishing hujumlari, zararli dastur, SOC, xavfsizlik monitoringi, risk tahlili, proaktiv himoya.*

Threat Intelligence (TI) — bu axborot tizimlari va tarmoqlarga tahdid soluvchi xavf-xatarlar haqidagi ma'lumotlarni yig'ish, qayta ishlash, tahlil qilish va amaliy xavfsizlik choralariga aylantirish jarayonidir.

TI ning asosiy vazifasi — tashkilotni kiberhujumlardan oldindan himoya qilish va xavfsizlik qarorlarini aniq ma'lumotlarga asoslanib qabul qilishdir. Threat Intelligence jarayoni oddiy monitoringdan farqli ravishda proaktiv himoya tamoyiliga asoslanadi.

Threat Intelligence turlari

Threat Intelligence to'rt asosiy darajaga bo'linadi.

1.1-jadval. Threat Intelligence turlari jadvali

Daraja	Tavsifi	Kimlar uchun	Misol
Strategic	Umumiy strategik tahdidlar tahlili	Rahbariyat	Global ransomware tendensiyasi
Tactical	Hujum usullari va metodlari (TTP)	Xavfsizlik mutaxassislari	MITRE ATT&CK bosqichlari
Operational	Aniq hujum kampaniyasi haqida ma'lumot	SOC jamoasi	Ma'lum APT guruhi faoliyati
Technical	Texnik indikatorlar (IOC)	Tizim administratorlari	IP, hash, domen nomi

Threat Intelligence (tahdidlar razvedkasi) zamonaviy kiberxavfsizlik tizimining muhim tarkibiy qismi hisoblanadi. U axborot tizimlari va tarmoqlarga tahdid soluvchi xavf-xatarlar, tahdid aktorlari, ularning maqsadlari, imkoniyatlari hamda qo'llaydigan usullari to'g'risidagi ma'lumotlarni tizimli ravishda yig'ish, qayta ishlash, tahlil qilish va amaliy himoya choralariga aylantirish jarayonini anglatadi. Ilmiy nuqtai nazardan Threat Intelligence risklarni boshqarish mexanizmining ajralmas qismi bo'lib, u qaror qabul qilish jarayonini analitik ma'lumotlar bilan ta'minlaydi. Oddiy monitoring tizimlaridan farqli ravishda, Threat Intelligence faqat hodisani qayd etish bilan cheklanmaydi, balki tahdidning kelib chiqish sabablari, rivojlanish bosqichlari va ehtimoliy oqibatlarini aniqlashga qaratiladi.

Threat Intelligence hayotiy sikli

Threat Intelligence doimiy sikl asosida ishlaydi. Threat Intelligence hayotiy sikli bosqichlari quyidagi 1.2- jadvalda keltirilgan.

Bosqich	Tavsifi	Natija
Planning	Maqsad va ehtiyojlarni aniqlash	Tahlil yo'nalishi belgilanadi
Collection	Ma'lumot yig'ish	Xom ma'lumot
Processing	Ma'lumotni tozalash va saralash	Tahlilga tayyor ma'lumot
Analysis	Tahdidni chuqur o'rganish	Xavf baholash
Dissemination	Hisobot va tavsiyalar berish	Qaror qabul qilish
Feedback	Jarayonni takomillashtirish	Yaxshilangan tizim

Threat Intelligence konseptual jihatdan tahdid aktori, tahdid vositasi va tahdid maqsadi kabi asosiy elementlarga tayanadi. Tahdid aktori deganda hujumni amalga oshiruvchi shaxs, guruh yoki tashkilot tushuniladi. Ularning motivatsiyasi turlicha bo'lishi mumkin: moliyaviy foyda olish, siyosiy bosim o'tkazish, sanoat josusligi yoki shunchaki zarar yetkazish. Tahdid vositalari esa zararli dasturlar, eksploitlar, botnetlar yoki boshqa texnik usullarni o'z ichiga oladi. Tahdid maqsadi esa ma'lumotlarni o'g'irlash, tizimni ishdan chiqarish yoki maxfiy axborotni qo'lga kiritishdan iborat bo'lishi mumkin. Ushbu uch element o'zaro bog'liq holda tahdid modelini shakllantiradi.

Threat Intelligence axborot xavfsizligi risklarini boshqarish jarayonida muhim o'rin tutadi. Risk odatda tahdid, zaiflik va ta'sir ko'paytmasi sifatida ifodalanadi. Threat Intelligence tahdid ehtimolini aniqlash, mavjud zaifliklardan foydalanish imkoniyatini baholash va potensial zarar darajasini prognoz qilish orqali riskni aniqroq hisoblash imkonini beradi. Natijada tashkilot o'z xavfsizlik siyosatini real ma'lumotlarga asoslanib shakllantiradi hamda resurslarni samarali taqsimlaydi.

Threat Intelligence doimiy sikl asosida ishlaydi. Dastlab rejalashtirish bosqichida razvedka maqsadlari va ehtiyojlari belgilanadi. Keyingi bosqichda turli manbalardan ma'lumotlar yig'iladi. Bu manbalar ochiq axborot resurslari, tijorat tahdid oqimlari, ichki log fayllar, SIEM tizimlari, shuningdek, yopiq forumlar yoki dark web platformalar bo'lishi mumkin. Yig'ilgan ma'lumotlar qayta ishlanadi, tozalanadi va strukturallashtiriladi. So'ngra tahlil bosqichida tahdidning kelib chiqish

sabablari, qo‘llanilgan usullar va ehtimoliy oqibatlari aniqlanadi. Tahlil natijalari tegishli bo‘limlarga yetkaziladi va fikr-mulohaza asosida jarayon takomillashtiriladi. Bu jarayon doimiy ravishda takrorlanib, tizimni yanada samarali qiladi.

Threat Intelligence turli darajalarda amalga oshiriladi. Strategik darajada u global yoki mintaqaviy kiberxavfsizlik tendensiyalarini o‘rganishga qaratiladi va asosan yuqori rahbariyat uchun mo‘ljallangan bo‘ladi. Taktik darajada hujumchilarning taktika va texnikalari, ya’ni TTP (Tactics, Techniques, Procedures) tahlil qilinadi. Operatsion darajada esa aniq hujum kampaniyalari va faol tahdidlar o‘rganiladi. Texnik darajada esa zararli IP manzillar, domenlar, fayl hash qiymatlari kabi indikatorlar aniqlanadi. Ushbu indikatorlar “Indicators of Compromise” deb ataladi va xavfsizlik tizimlariga integratsiya qilinadi.

Threat Intelligence ko‘pincha MITRE ATT&CK modeli bilan bog‘liq holda qo‘llaniladi. Ushbu model hujumchilarning harakat bosqichlarini tizimli ravishda tasniflaydi. Masalan, razvedka bosqichida hujumchi tizim haqida ma’lumot to‘playdi, dastlabki kirish bosqichida fishing yoki eksploitlardan foydalanadi, keyinchalik tizimda saqlanib qolish va huquqlarni oshirishga harakat qiladi. Oxirgi bosqichda esa ma’lumotlarni o‘g‘irlash yoki tizimga zarar yetkazish amalga oshiriladi. Threat Intelligence mazkur bosqichlarning har birini aniqlash va erta ogohlantirish imkonini beradi.

Zamonaviy Threat Intelligence tizimlari sun’iy intellekt va mashinaviy o‘qitish texnologiyalari bilan integratsiya qilingan. Katta hajmdagi log va tarmoq trafigini qayta ishlash uchun Big Data texnologiyalaridan foydalaniladi. Mashinaviy o‘qitish algoritmlari noma’lum tahdidlarni aniqlash va anomaliyalarni topishda samarali hisoblanadi. Sun’iy intellekt yordamida tahdidlarni prognoz qilish, foydalanuvchi xatti-harakatlarini tahlil qilish va avtomatik javob choralarini qo‘llash imkoniyati yaratiladi. Bu esa inson omiliga bog‘liqlikni kamaytiradi va aniqlik darajasini oshiradi.

Threat Intelligence Security Operations Center (SOC) faoliyati bilan bevosita bog‘liqdir. TI ma’lumotlari SIEM, IDS/IPS, firewall va EDR tizimlariga integratsiya qilinadi. Natijada zararli IP manzillar avtomatik bloklanadi, shubhali faoliyat aniqlanadi va tezkor javob chorasi ko‘riladi. Bu esa hujumlarning kengayib ketishining oldini oladi va zarar miqdorini kamaytiradi.

Xulosa qilib aytganda, Threat Intelligence zamonaviy axborot xavfsizligi arxitekturasining muhim komponenti bo‘lib, tahdidlarni aniqlash, tahlil qilish, prognozlash va oldini olishga qaratilgan ilmiy asoslangan tizimdir.

U strategik boshqaruvdan tortib texnik himoya choralarigacha bo‘lgan barcha bosqichlarda qo‘llaniladi.

Proaktiv yondashuv, analitik tahlil va zamonaviy texnologiyalar bilan integratsiya Threat Intelligence ni kiberxavfsizlik sohasida muhim strategik instrumentga aylantiradi.

XULOSA

Xulosa qilib aytganda, Threat Intelligence zamonaviy kiberxavfsizlik tizimining ajralmas qismi hisoblanadi. U tashkilotlarga tahdidlarni oldindan aniqlash, xavf darajasini baholash va tezkor choralar ko‘rish imkonini beradi. Tahdidlar razvedkasi yordamida tashkilotlar reaktiv himoyadan proaktiv himoyaga o‘tadi, ya’ni hujum sodir bo‘lgandan keyin emas, balki undan oldin choralar ko‘rish imkoniyatiga ega bo‘ladi.

Threat Intelligence jarayoni ma’lumotlarni yig‘ish, tahlil qilish, kontekstual baholash va amaliy qarorlar qabul qilish bosqichlarini o‘z ichiga oladi. Bu esa axborot tizimlarining barqarorligi va xavfsizligini ta’minlashda muhim ahamiyat kasb etadi. Kelgusida sun’iy intellekt va avtomatlashtirilgan tahlil vositalarining qo‘llanilishi Threat Intelligence samaradorligini yanada oshiradi.

ADABIYOTLAR RO‘YXATI:

1. ENISA. Threat Intelligence – Collecting, Analysing and Disseminating Information on Cyber Threats.
2. NIST. Guide to Cyber Threat Information Sharing.
3. SANS Institute. Intelligence-Driven Incident Response.
4. MITRE Corporation. ATT&CK Framework Documentation.
5. IBM Security. X-Force Threat Intelligence Index Reports.