TAHDID RAZVEDKASI YORDAMIDA INSIDENTLARNI ANIQLASH

Usmanbayev Doniyorbek Shuxratovich
Muhammad al-Xorazmiy nomidagi TATU katta o'qituvchisi
Ortiqov Azamat Jo'ramirza o'g'li
Muhammad al-Xorazmiy nomidagi TATU "Axborot xavfsizligi" yo'nalishi magistranti

Razvedkaga asoslangan hodisalarga javob berish (IDIR) - bu kiberxavfsizlik hodisalarini boshqarishga yondashuv bo'lib, u hodisalarga javob berish faoliyatining samaradorligi va samaradorligini oshirish uchun tahdidlar haqida ma'lumotni o'z ichiga oladi. Bu xavfsizlik hodisalarini proaktiv ravishda aniqlash, ularga javob berish va yumshatish uchun ichki va tashqi tahdidlar haqida ma'lumotdan foydalanishni o'z ichiga oladi. IDIR tashkilotlarga tahdidlar haqida ma'lumot to'plash, tahlil qilish va hodisalarga javob berish jarayonlariga qo'llashga yordam beradigan turli xil vositalar va texnologiyalar tomonidan qo'llab-quvvatlanadi.

Razvedkaga asoslangan hodisalarga javob berish strategiyalari

Tahdidlar haqida razvedka ma'lumotlarini to'plash: Tashkilotlar xavfsizlik yetkazib beruvchilari, ochiq kodli manbalar, sanoat hisobotlari va o'zlarining tarixiy ma'lumotlari kabi turli manbalardan tahdidlar haqida razvedka ma'lumotlarini to'playdi va tahlil qiladi. Ushbu razvedka ma'lumotlariga ma'lum hujum naqshlari, murosaga kelish ko'rsatkichlari (IoC), tahdid ishtirokchilari tomonidan qo'llaniladigan taktikalar, texnikalar va protseduralar (TTP) haqidagi ma'lumotlar kiradi.

Tahdidlarni aniqlash va oldini olish: Xavfsizlik vositalari va tizimlariga tahdidlar haqida ma'lumot kiritish orqali tashkilotlar potentsial xavfsizlik tahdidlarini yaxshiroq aniqlashlari va oldini olishlari mumkin. Bu aniqlangan tahdidlar haqida ma'lumotga asoslangan holda buzg'unchiliklarni aniqlash va oldini olish tizimlari (IDPS), xavfsizlik devori qoidalari va elektron pochta filtrlari uchun maxsus qoidalar va imzolarni yaratishni o'z ichiga olishi mumkin.

Proaktiv monitoring: Tarmoq va tizim faoliyatini doimiy ravishda kuzatib borish potentsial tahdidlarni erta aniqlash imkonini beradi. Tahdidlarni aniqlash xavfsizlik guruhlariga ma'lum hujumlar naqshlariga mos keladigan shubhali faoliyatlarni aniqlashga yordam beradi va bu ularga to'liq hodisa sodir bo'lishidan oldin javob berish imkonini beradi.

Hodisalarga javob berishni rejalashtirish : Tahdidlar haqida ma'lumot tashkilotlarga turli tahdidlarning potentsial ta'sirini va tegishli javob choralarini tushunishga yordam berish orqali hodisalarga javob berishni rejalashtirishga yordam beradi. Bunga ma'lum bir tahdid aniqlanganda amalga oshiriladigan aniq choralarni aniqlash kirishi mumkin.

Hodisani tekshirish: Xavfsizlik hodisasi yuz berganda, tahdidlar haqidagi ma'lumotlar hujumning mohiyatini, qo'llanilgan taktikalarni va hujum ortidagi potentsial sabablarni tushunishga yordam beradi. Ushbu ma'lumot tergov bosqichida tezkor xodimlarga xabardor qarorlar qabul qilishga yordam beradi.

Tahdidni aniqlash: Ba'zi hollarda, tahdidlar haqida ma'lumot hujum uchun mas'ul bo'lgan tahdid ishtirokchilarini aniqlashga yordam beradi. Ushbu ma'lumot tashkilotlar uchun raqiblarining niyatlari, usullari va kelajakdagi potentsial maqsadlarini tushunish uchun qimmatli bo'lishi mumkin.

Yengillashtirish va tiklash: Razvedkaga asoslangan hodisalarga javob berish tashkilotlarga tahdidlar haqida razvedka ma'lumotlaridan to'plangan ma'lumotlar asosida samarali yumshatish va tiklash strategiyalarini ishlab chiqishga yordam beradi. Bu hodisani cheklash uchun vaqtinchalik choralarni amalga oshirish, tahdidni bartaraf etish va keyin tizimlarni normal holatiga to'liq tiklashni o'z ichiga olishi mumkin.

Doimiy takomillashtirish: Hodisa hal qilingandan so'ng, tashkilotlar o'zlarining javob choralarini tahlil qilishlari va ularni mavjud tahdidlar haqida ma'lumot bilan taqqoslashlari mumkin. Ushbu tahlil javob berish jarayonidagi kamchiliklarni va takomillashtirish kerak bo'lgan sohalarni aniqlashga yordam beradi.

Kiber tahdidlar razvedkasi platformalari: Ushbu platformalar turli manbalardan olingan tahdidlar razvedkasi ma'lumotlarini to'playdi va tahlil qiladi, mavjud tahdidlar va tahdid ishtirokchilari haqida amaliy ma'lumotlarni taqdim etadi.

DNS filtrlash va veb-xavfsizlik yechimlari: Ushbu vositalar potentsial zararli saytlarni aniqlash va tasniflash uchun tahdidlar haqida ma'lumot olish ma'lumotlaridan foydalanish orqali zararli veb-saytlar va domenlarga kirishni bloklashi mumkin.

Elektron pochta xavfsizligi yechimlari: Elektron pochta xavfsizligi vositalari fishing elektron pochtalari va zararli qo'shimchalarni aniqlash va filtrlash uchun tahdidlarni aniqlash ma'lumotlaridan foydalanishi mumkin.

Endpoint Protection Platforms (EPP): EPP yechimlari antivirus, zararli dasturlarga qarshi va boshqa xavfsizlik xususiyatlarini birlashtiradi.

Tahdidlarni aniqlashni integratsiyalash ularning paydo bo'layotgan tahdidlarni aniqlash va ularga javob berish qobiliyatini oshiradi.

XULOSA

Razvedkaga asoslangan hodisalarga javob berish yondashuvi tashkilotlarning kiberxavfsizlik darajasini oshirishda muhim ahamiyatga ega.

Tahdidlar haqida razvedka ma'lumotlarini xavfsizlik tizimlariga integratsiya qilish orqali potentsial hujumlarni erta aniqlash, ularga tezkor javob berish va zararlarni kamaytirish mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. Usmanbayev D. Improving and evaluating methods network attack anomaly detection //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – С. 1-5.

2. Bozorov, Suhrobjon, and Doniyor Usmanbayev. Balanced ANN and majority based voting approach for building IDS. AIP Conference Proceedings. Vol. 3377. No. 1. AIP Publishing LLC, 2025.

3. Usmanbayev D. S. Kiberxavfsizlik: IT Infratuzilmasini Himoya Qilishning Zamonaviy Usullari //Green Economy and Development. – Т. 3. – №. 5. – С. 665738.

4. Mirpulatovich, K. M., Zakirovna, T. N., Gulnora, K., & Ismoilovna, U. D. S. (2019). Methodology for Developing a Mandatory Security Policy Based on Two Value Chains. Methodology, 6(11).