XAVFSIZLIK VOSITALARINI BOSHQARISH ARXITEKTURASI

Po’latov Doston Normurod o’g’li
Yoqubova Madinabonu Abdushukur qizi
Torebaeva Naziyra
Shonazarov Sarvarbek Maqsud o‘g‘li

Annotatsiya: *Xavfsizlik vositalarini boshqarish arxitekturasi, tashkilotning xavfsizlik vositalarini bir-biriga integratsiya qilish va ulardan olingan ma'lumotlarni to'plash, tahlil qilish va monitoring qilish imkonini beradi. Bu arxitektura xavfsizlik tizimini boshqarishni osonlashtiradi, xavfsizlik hodisalariga tez reaksiya berishni ta'minlayadi va xavfsizlik risklarini minimalga tushirishga yordam beradi.*

Kalit so’zlar: *Xavfsizlik vositalari, Boshqarish arxitekturasi, Integratsiya,Ma'lumot to'plash, Tahlil qilish, Monitoring, Xavfsizlik tizimi,Xavfsizlik hodisalari, Tez reaksiya, Xavfsizlik risklari Minimalga tushirish.*

Abstract: *The security management architecture allows for the integration of the organization's security tools and the collection, analysis and monitoring of information obtained from them. This architecture facilitates the management of the security system, provides a quick reaction to security incidents and helps minimize security risks.*

Keywords: *Security tools, Management architecture, Integration, Data collection, Analysis, Monitoring, Security system, Security incidents, Rapid response, Minimizing security risks.*

KIRISH

Xavfsizlik vositalarini boshqarish arxitekturasi, bir tashkilotning xavfsizlik operatsiyalarini tartibga solish va xavfsizlik vositalarini effektiv tarzda boshqarish uchun qurilgan tuzilma va jarayonlardan iborat bo'ladi. Ushbu arxitektura, xavfsizlikning yuqori darajada ta'minlanishi, hujumlarga tez reaksiya berish, muammo va kamchiliklarni aniqlash va bartaraf qilish imkoniyatlarini beradi. Quyidagi kalit so'zlar, xavfsizlik vositalarini boshqarish arxitekturasining muhim komponentlari va jarayonlarini aks ettiradigan misollar hisoblanadi:

1. Xavfsizlik informatsiyasi yo'llash (Security Information and Event Management, SIEM): Xavfsizlik hodisalari va tizimdagi tashqi va ichki voqealar bilan bog'liq ma'lumotlarni to'plab, to'plangan ma'lumotlarni analiz qilish, hujumlarni va anomaliyalarni aniqlash, va hujumlarga tez reaksiya berish imkonini beradi.

2. Intrusion Detection System (IDS) va Intrusion Prevention System (IPS): Tarmoqdagi hujum yo'nalishlarini aniqlash, zararli faoliyatni identifikatsiya qilish va hujumlarga tez reaksiya berish imkonini beradi.

3. Vulnerability Management: Tarmoqdagi ochiq bo'shliqlarni topish, ularga qarshi qonuniy imkoniyatlarni ta'minlash, yamalarni va to'ldirishlarni boshqarish va monitoring qilish imkonini beradi.

4. Access Control Systems: Foydalanuvchilar hisoblariga kirishni nazorat qilish, ta'minotli foydalanuvchilar va ro'yhatdan o'tish jarayonlarini boshqarish va taqdim etish imkonini beradi.

5. Firewalls: Tarmoqni hujumlardan himoya qilish uchun trafikni filtratsiya qilish, xavfsizlik sozlovchilari tomonidan sozlangan qoidalar bo'yicha yo'l yo'riqnoma berish imkonini beradi.

6. Secure Socket Layer (SSL) va Virtual Private Network (VPN): Ma'lumotlar uchun shifrlanishni ta'minlash va maxfiy tarmoqlarda o'zaro ulanishni ta'minlash imkonini beradi.

7. Endpoint Security: Tarmoqdagi qurilmalarni (komp'yuterlar, smartfonlar, planshetlar) himoya qilish va zararli dasturlarni, hujumlar va kompyuter viruslarini aniqlash va bartaraf qilish imkonini beradi.

8. Identity and Access Management (IAM): Foydalanuvchilar va ularga beriladigan ruxsat beradi.

9. Encryption: Ma'lumotlarni shifrlash va shifrdan o'tkazish jarayonlarini boshqarish va ma'lumotlar ustidan muxlislarni taqdim etish imkonini beradi.

10. Security Incident Response: Xavfsizlik hodisalariga tezlik bilan reaksiya qilish, hujumlarni aniqlash va bartaraf qilish, ma'lumotlarni tiklash va normal holatga qaytarish jarayonlarini o'rganish va boshqarish imkonini beradi.

11. Network Segmentation: Tarmoqdagi tizimlar va qurilmalarni segmentlarga bo'lish, hujum va hujumlarining tarqalishini cheklash va tarqalishni cheklash imkonini beradi.

12. Security Information Sharing: Xavfsizlik hodisalarini va ma'lumotlarni boshqa tashkilotlar bilan o'zaro almashish va ma'lumot almashish sharoitlarini taqdim etish imkonini beradi.

13. Security Policy Management: Xavfsizlik siyosat va qoidalarini belgilash, ularga rioya qilish, o'zgartirishlarni boshqarish va xavfsizlik standartlariga muvofiqligini nazorat qilish imkonini beradi.

14. Log Management: Tarmoqdagi hodisalar, tashqi va ichki voqealar, foydalanuvchi faoliyatlari va monitoring ma'lumotlarini to'plab, saqlash, tahlil qilish va xavfsizlik tahlili va diagnozini amalga oshirish imkonini beradi.

15. Patch Management: Tarmoqdagi o'rnatilgan dasturlar va tizimlar uchun yangi to'ldirishlarni qabul qilish, ularga tezlik bilan o'rnatish va yangilanishlarni monitoring qilish imkonini beradi.

Bu kalit so'zlar, xavfsizlik vositalarini boshqarish arxitekturasining muhim qismlarini va jarayonlarini ifodalaydi. Bu arxitektura tashkilotlar uchun yaxshi tashkil etilgan bo'lsa, xavfsizlikni ta'minlash, muammo va kamchiliklarni aniqlash va hujumlarga tez reaksiya berish imkonini oshiradi.

Xavfsizlik vositalarini boshqarish arxitekturasi avzalliklar va kamchiliklarga ega bo'lishi mumkin. Quyidagi avzalliklar va kamchiliklar ko'rish mumkin:

AVZALLIKLAR:

1. Komplekslik: Xavfsizlik vositalarini boshqarish arxitekturasi kompleks va murakkab bo'lishi mumkin. Bu, xavfsizlik operatsiyalarini o'zgartirish, yangilash va jarayonlarni boshqarishda katta tajribaga ega IT xodimlarni talab qiladi.

2. Moliyaviy resurslar: Xavfsizlik vositalarini qo'llab-quvvatlash, ulardan foydalanish va ularni yangilash uchun moliyaviy resurslar talab qiladi. Bu, vositalar uchun narxlarni, litsenziyalarni, xavfsizlik konsultatsiyalarini olish va texnik xodimlar bilan hamkorlik qilishni talab qiladi.

3. Uzluksiz integratsiya: Xavfsizlik vositalari o'rtasidagi integratsiya muhimdir. Boshqarish arxitekturasi, xavfsizlik vositalarining bir-biriga va asosiy tizimga integratsiyasini ta'minlashga ahamiyat beradi. Bu integratsiya, ma'lumot almashish, ma'lumotlar ustida ishlash va holat ma'lumotlarini to'plashni osonlashtiradi.

KAMCHILIKLAR:

1. Narx: Xavfsizlik vositalarining o'rtacha narxi qimmat bo'lishi mumkin. Bu, tashkilotlar uchun moliyaviy muammo bo'lishi va xavfsizlikni to'liq ta'minlash uchun katta mablag' sarflashni talab qilishi mumkin.

2. Jarayonlar va sozlovchilar bo'lgan integratsiya: Xavfsizlik vositalarini o'rganish, ulardan foydalanish va ularni integratsiya qilish jarayonlarini boshqarish IT xodimlar uchun qo'ng'iroq bo'lishi mumkin. Bu, boshqarishni osonlashtirish, integratsiya ko'rsatkichlarini o'rnatish va vositalar orasidagi boshqaruvni ta'minlashni talab qiladi.

3. False positives va false negatives: Xavfsizlik vositalarining tahlili va monitoringi orqali hosil bo'lgan alarm va hodisalar soni katta bo'lishi mumkin. False positives (yolg'on alarm) va false negatives (haqiqiy hodisa niqobi) tashkilotlar uchun kamchiliklar yaratadi. Bu, vositalarni ustunlikliligi va to'g'ri sozlovchilarni o'rnatishni talab qiladi.

4. Sozlovchilarning yetarlicha tayyorlanmaganligi: Xavfsizlik vositalarini boshqarish arxitekturasi muvaffaqiyatli amalga oshirilish uchun tayyor va tajribali sozlovchilarni talab qiladi. Agar tashkilotda bu xil mutaxassislar bo'lmagan bo'lsa, vositalar to'g'ri sozlovchilar yordamida to'g'ri ishlashi kamayadi.

5. Monitoring va tahlilning qo'shimcha resurslarni talab qilishi: Xavfsizlik vositalarini boshqarish arxitekturasi monitoring va tahlil jarayonlarini o'rnatish va o'zgartirish uchun qo'shimcha resurslar va vositalar talab qiladi. Bu, moliyaviy resurslarni va katta tahlil vositalarini qo'llab-quvvatlashni talab qiladi.

6. Xavfsizlik bo'yicha strategiyalar va yangilanishlar: Xavfsizlik vositalarini boshqarish arxitekturasi, tashkilotning xavfsizlik strategiyalarini va yangilanishlarini to'liq o'z ichiga olishni talab qiladi. Bu, tashkilotning xavfsizlik holatiga mos keladigan vositalarni o'rganish va ularga qisqa vaqt ichida reaksiya berish imkonini beradi.

7. Maxsus talablar va integratsiya: Xavfsizlik vositalarini boshqarish arxitekturasi xavfsizlikning maxsus talablarini qondirish va ulardan foydalanishni ta'minlashni talab

qiladi. Bu, ma'lumotlarni o'zaro almashish, maxsus xavfsizlik protokollari va standartlar bilan integratsiya qilishni talab qiladi.

Xavfsizlik vositalarini boshqarish arxitekturasi misollar bilan quyidagicha ko'rsatilishi mumkin:

1. SIEM (Security Information and Event Management) Platform: SIEM platformasi, tashkilotdagi xavfsizlik hodisalarni va ma'lumotlarni birlashtiradi va tahlil qiladi. Uning boshqarish arxitekturasi tahlil markazining yaratilishini, log va hodisa ma'lumotlarini to'plashni, xavfsizlik qonunlarini o'zgartirishni, ma'lumotni o'rganishni va alarm tizimlarini boshqarishni o'z ichiga oladi.

2. IDS/IPS (Intrusion Detection/Prevention System): IDS/IPS vositalari tashkilotdagi hujumlarni aniqlash va ularga javob berishda foydalaniladi. Boshqarish arxitekturasi, hujumlarni va hujumga qarshi maslahat berishni o'rganish, vositalarni konfiguratsiya qilishni, jarayonlarni monitoring qilishni va otomatisatsiya qilishni ta'minlaydi.

3. FW (Firewall): Keng doiradagi xavfsizlik vositalaridan biri firewall'dir. Boshqarish arxitekturasi, ichki va tashqi xavfsizlik qoidalari va vositalari orasidagi hamkorlikni ta'minlayadi. U firewallni sozlovchilashni, xavfsizlikni monitoring qilishni, yangilanishlarni o'rnatishni va amalga oshirishni o'z ichiga oladi.

4. AV (Antivirus) va AM (Anti-Malware): AV va AM vositalari tizimdagi zararli dasturlarni aniqlash, izolyatsiya qilish va uning tarqatilmasini ta'minlash uchun foydalaniladi. Boshqarish arxitekturasi bu vositalarning tizimga integratsiyasini, o'zgartirishlarni va yanada yaxshi tan olishni ta'minlashni o'z ichiga oladi.

5. DLP (Data Loss Prevention) Platform: DLP platformasi ma'lumotlarning yo'qolishini va yo'qolishini oldini olishga yordam beradi. Boshqarish arxitekturasi ma'lumotlarni tan olishni, ma'lumotlar ustida monitoring qilishni, yo'qolish hodisalariga javob berishni va tahlil qilishni o'z ichiga oladi.

6. Vulnerability Management System: Vulnerability Management System tashkilotdagi nusxalarni aniqlash, tahlil qilish, yangilanishlarni o'rnatish va tashkilotni nusxalardan himoya qilishda yordam beradi. Boshqarish arxitekturasi nusxalarni topish, o'zgartirishlarni qabul qiladi.

7. SIEM platformasining integratsiyasi: Xavfsizlik vositalarini boshqarish arxitekturasi SIEM platformasining qo'shimcha integratsiyasini o'z ichiga olishi mumkin. Bu integratsiya tizimdagi boshqa vositalar bilan ma'lumot almashishni, ma'lumotlarni tahlil qilishni va yo'qolish hodisalarini aniqlashni osonlashtiradi.

8. Identity and Access Management (IAM) platformasi: Xavfsizlik vositalarini boshqarish arxitekturasi IAM platformasining integratsiyasini o'z ichiga olishi mumkin. Bu integratsiya tashkilotning xodimlarining kirish va kirish ruxsatlarini boshqarishni, kirishlarni monitoring qilishni va ruxsat bermaslik holatlarida xavfsizlikni ta'minlashni osonlashtiradi.

9. Network Security Monitoring (NSM) vositalari: Boshqarish arxitekturasi NSM vositalarining integratsiyasini ta'minlayishi mumkin. NSM vositalari tarmoq trafiklarini

monitoring qilish, anomal qo'llanmalar va hujumlarni aniqlashni, tarmoqdagi xavfsizlik holatlarini tahlil qilishni osonlashtiradi.

10. Vulnerability Scanning vositalari: Xavfsizlik vositalarini boshqarish arxitekturasi vulnarablik skennirlarining integratsiyasini o'z ichiga olishi mumkin. Bu integratsiya tashkilot tizimlaridagi potensial nusxalarni aniqlash, ularga javob berish va ulardan foydalanishni osonlashtiradi.

11. Patch Management vositalari: Boshqarish arxitekturasi tashkilotdagi patchlarni to'plab olish va ulardan foydalanishning osonlashtirilgan yo'li bo'lishini ta'minlash uchun patch boshqaruv vositalarining integratsiyasini o'z ichiga oladi.

12. Incident Response platformasi: Boshqarish arxitekturasi holat hodisalariga javob berishning oson yo'li bo'lishi uchun incident tartibga soluvchi platformaning integratsiyasini o'z ichiga oladi. Bu platforma tashkilotga xavfsizlik hodisalaridan xabar berish, ularga javob berish va holatni normalga qaytarishni ta'minlaydi.

13. Data Encryption vositalari: Xavfsizlik vositalarini boshqarish arxitekturasi ma'lumotlarni himoya qilish uchun kriptografiya vositalarining integratsiyasini o'z ichiga oladi. Bu integratsiya ma'lumotlar ustida kriptografiya.

Xulosa: Xavfsizlik vositalarini boshqarish arxitekturasi, tashkilotning xavfsizlikni ta'minlash va xavfsizlik hodisalariga qisqa vaqt ichida javob berish imkonini beradi. Bu arxitektura tizimdagi xavfsizlik vositalarini bir-biriga integratsiya qilish, ulardan olingan ma'lumotlarni to'plash, tahlil qilish va monitoring qilishni osonlashtiradi. Misollar, SIEM platformalari, IDS/IPS vositalari, firewall, antivirus, DLP platformalari, va boshqa xavfsizlik vositalarini o'z ichiga oladi. Bu integratsiya, xavfsizlik tizimini hamkorlikda ishlashga imkon beradi, xavfsizlikni oshirish, xavfsizlik hodisalarini aniqlash va ularga javob berishni osonlashtiradi. Xavfsizlik vositalarini boshqarish arxitekturasi, tashkilotning xavfsizlik darajasini yuqori qilish va xavfsizlik risklarini minimalga tushirishga yordam beradi.

FOYDALANILAGAN ADABIYOTLAR:

1. «Axborot texnologiyasi. Ma’lumotlami kriptografik muho- fazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O‘zbekiston Davlat standard. 0‘z DSt 1092:2005.

2.«Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006

3. «Axborot texnologiyasi. Ochiq tizimlar o‘zaro bogMiqligi. Elek tron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzil- masi» 0‘zbekiston Davlat standarti. 0‘zDSt 1108:2006.

4.С.В. Симонов. Анализ рисков в информационнмх систе- мах. Практические советь! // Конфидент. -2001. -№2.

5.S.S.Qosimov. Axborot texnologiyalari. 0‘quv qoMlanma. - T.: «Aloqachi», 2006.

6.S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tar- moqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qoMlanma. —Toshkent Davlat texnika universiteti, 2003.