META DATA LARGA BO'LADIGAN HUJUMLARDAN HIMOYALANISH USULLARI

Madatov Islom Shukurullo o'g'li
Jo'ramirzayev Islomjon Adxamjon o'g'li
Odilov Ozod Rahmatullo o'g'li
Avazbekov Mirsaid A'zamjon o'g'li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnalogiyalari universiteti talabalari

Anatatsiya: *berilgan maqolada virtual Internet olamida meta data larga bo'ladigan hujumlardan himoyalanish usullari ko'rib chiqilagan hamda tahlil qilingan.*

Kalit so'zlar: *Mate data, Skyhigh Cloud Native, CloudWatch, IMDSv2, konfiguratsiya, kod, anomaliya.*

Metadata ma'lumotlarning kelib chiqishi, ma'nosi, joylashuvi, egaligi va yaratilishi kabi ma'lumotlarni taqdim etadi. Misol uchun, raqamli tasvirning metama'lumotlari uning o'lchami, ruxsati, yaratilish vaqti va rang chuqurligi kabi ma'lumotlardan iborat bo'lishi mumkin. U ma'lumotlarni tasniflash, tartibga solish, etiketlash, saralash va qidirishda foydalidir.

Meta data larni himoyalash usullari

AWS misol metama'lumotlariga hujumlarni qanday kamaytiradi.?

Ushbu xizmat xavfsizligini yaxshilash uchun AWS bir nechta yangi himoya qatlamlarini qo'shadigan IMDSv2 ni chiqardi.

IMDSv2 da tashqi foydalanuvchilarning hisob ma'lumotlarini olishi bloklanadi, bu esa ularni faqat ilova resurslariga olish imkonini beradi.

Biroq, IMDSv1 hali ham davom etishi qiyin. AWS'da mijozlarning IMDSv1'dan foydalanishiga to'sqinlik qiladigan hech narsa yo'q va siz hali ham barcha EC2 namunalaringiz uchun sukut bo'yicha undan foydalanishingiz mumkin. Yuqorida aytib o'tganimizdek, bulutdan xavfsiz foydalanayotganingizga ishonch hosil qilish AWS mas'uliyati emas. Bu mas'uliyat faqat mijozning zimmasiga tushadi.

Biz ta'riflagan hujumda teskari proksi-server tashqi so'rovlarning ichki manbalarga kirishiga ruxsat berish uchun noto'g'ri sozlangan. Agar jamoa o'zining hisoblash namunasini IMDSv2 dan foydalanish uchun sozlagan bo'lsa, tashqi tahdid ishtirokchisi tomonidan ruxsatsiz kirish bloklangan bo'lar edi.

Skyhigh Cloud Native ilovalarini himoya qilish qanday yordam berishi mumkin

Skyhigh Security-da bizda bu kabi hujumlarni aniqlash va oldini olishga yordam beradigan bir nechta yondashuvlar mavjud. Skyhigh Cloud Native Application Protection Platform (CNAPP) - bu AWS, Azure, GCP-dagi konfiguratsiyalarni kuzatish va yangilash hamda keng ko'lamli qo'shimcha xavfsizlik choralari.

AWS bilan to‘g‘ridan-to‘g‘ri API integratsiyasidan foydalangan holda, Skyhigh CNAPP har bir EC2 misolida qaysi IMDS versiyasidan foydalanayotganingizni ko‘rsatish uchun Amazon CloudWatch – ilova va infratuzilma monitoringi xizmatini doimiy ravishda kuzatib boradi.

CloudWatch IMDSv1 yordamida namunani faol ravishda qayd qilganda, Skyhigh CNAPP xavfsizlik hodisasini yaratadi va konfiguratsiyangizni IMDSv2 ga yangilash haqida sizni xabardor qiladi, bu tashqi foydalanuvchilar tomonidan hisob ma'lumotlaringizga ruxsatsiz kirishning oldini oladi.

IMDS versiyasi konfiguratsiyasi uchun Skyhigh CNAPP siyosati hodisalari

Barcha mahalliy kodlar va foydalanuvchilar uchun EC2 nusxalarida IMDSv2 ni qo'llash eng yaxshi amaliyotdir. IMDSv2 dan foydalanish kerakligini belgilaganingizdan so'ng, IMDSv1 endi ishlamaydi. AWS bu yerda IMDSv2 dan foydalanish uchun namunalaringizni qanday sozlash bo‘yicha bosqichma-bosqich ko‘rsatmalarga ega.

Ushbu hujum misolidan tashqari, Skyhigh CNAPP sizga bulutli ilovalarni himoya qilish uchun bir qator eng yaxshi amaliyotlarni amalga oshirish imkonini beradi:

- Konfiguratsiyalaringizni doimiy ravishda tekshirib turish. Skyhigh CNAPP yordamida siz AWS CloudFormation shablonlarini ishlab chiqarishga kirishdan oldin skanerlashingiz va vaqt o‘tishi bilan konfiguratsiyalaringizdagi har qanday “drift”ni aniqlashingiz mumkin. Bu sizga noto‘g‘ri konfiguratsiyalarni aniqlash va resurs ruxsati uchun eng kam imtiyozli modelni qo‘llash imkonini beradi.
- Nol-ishonchni ta'minlash. Metodologiya sifatida nol ishonchdan foydalaning, bu erda faqat ma'lum resurslar ishlashi va bir-biri bilan muloqot qilishiga ruxsat beriladi. Qolgan hamma narsa bloklangan.
- Kod zaifliklarini skanerlang. Ayniqsa, Docker kabi ochiq dasturiy ta’minotni tarqatish modellari bilan ilova resurslaringizni zaifliklar uchun doimiy ravishda kuzatib borish muhimdir.
- Anomaliyalar va tahdidlarni aniqlash. User and Entity Behavior Analytics (UEBA) yordamida siz anomal faollik va hisob ma’lumotlarini o‘g‘irlash kabi haqiqiy tahdidlarni aniqlash uchun millionlab bulutli hodisalarni baholash mumkin.

•DLP-ni saqlash obyektlarida ishga tushirish. Siz ruxsat bergan boshqa bulut xizmatlari, tarmog‘ingiz yoki so‘nggi nuqtalar kabi, AWS doirasida siz ham ma’lumotlaringizni S3 doirasida tasniflashingiz va eksfiltratsiyaga urinishlarni to‘xtatish uchun ma’lumotlar yo‘qolishining oldini olishni amalga oshirishingiz mumkin va kerak.

XULOSA

Metadata raqamli aktivlarni boshqarish, saqlash va ulardan samarali foydalanishda muhim ahamiyatga ega. Biz har xil turdagi metama’lumotlarni, jumladan, strukturaviy, ta'riflovchi, saqlash,aniq, ma’muriy va kelib chiqish metama’lumotlarini ko‘rib chiqdik. Ularning har biri raqamli aktivlardan foydalanish va tushunishni yaxshilash uchun noyob tushunchalarni taklif etadi.

AWS bilan to‘g‘ridan-to‘g‘ri API integratsiyasidan foydalangan holda, Skyhigh CNAPP har bir EC2 misolida qaysi IMDS versiyasidan foydalanayotganingizni ko‘rsatish uchun Amazon CloudWatch – ilova va infratuzilma monitoringi xizmatini doimiy ravishda kuzatib boradi.

CloudWatch IMDSv1 yordamida namunani faol ravishda qayd qilganda, Skyhigh CNAPP xavfsizlik hodisasini yaratadi va konfiguratsiyangizni IMDSv2 ga yangilash haqida sizni xabardor qiladi, bu tashqi foydalanuvchilar tomonidan hisob ma'lumotlaringizga ruxsatsiz kirishning oldini oladi.

FOYDALANILGAN ADABIYOTLAR:

1. Алтаев Ж. ГИС и земелный кадастр Казахстана. — М.,: ARGREVIEW. Современные геоинформационные технологии. - 2003.-№2.-С.2-5.,с14

2. Артамонов Б.Н., Брякалов Г.А., Гофман В.Э. и др. Основы современных компютерных технологий. — СанктПетербург.,: «Корона принт». 2002.-445с.

3. Валков В.М., Вершин В.Е. Автоматизированные системы управления технологическими процессами. —Д.: Политехника, 1991.-269 с.

4. https://atlan.com/types-of-metadata/#6-usage-metadata

5. https://www.skyhighsecurity.com/about/resources/resource-center.html

6. https://www.metadataetc.org/metadatabasics/types.htm