



**«TASDIQLAYMAN»**  
**“Biznesni rivojlantirish banki” ATB**  
**Boshqaruv raisining birinchi**  
**o'rinbosari v.b.:**  
**Sh.Yusupov**

**«8» oktabr 2026 y.**  
**№ 640**

## **TEXNIK TOPSHIRIQ**

**session va tranzaksion antifrod tizimlarini xarid qilish va joriy etish**

## 1. Loyihaning maqsadi va vazifalari

Ushbu texnik topshiriq firibgarlikning oldini olishga mo'ljallangan kompleks yechimni xarid qilish va joriy etish bo'yicha Buyurtmachining talablarini belgilaydi. Yechim quyidagilarni o'z ichiga oladi:

- sessiyaviy antifrod tizimi (keyingi o'rinlarda — SAT), u firibgarlik va bot-faolligini mijoz sessiyasi boshlanishidan oldin hamda sessiya davomida aniqlash maqsadida Buyurtmachining masofadan xizmat ko'rsatish kanallarida (jismoniy shaxslar va yuridik shaxslar uchun masofaviy bank xizmati, P2P, 3-D Secure) sessiyaviy va xulq-atvor ma'lumotlarini yig'ish hamda tahlil qilishni ta'minlaydi;
- tranzaksion antifrod avtomatlashtirilgan tizimi (keyingi o'rinlarda — TA AT), u har bir mijoz operatsiyasi bo'yicha firibgarlik xavfini imkon qadar real vaqtga yaqin rejimda (operatsiya bajarilishidan oldin va/yoki keyin) baholashni ta'minlaydi.

SAT va TA AT yagona, o'zaro integratsiyalashgan himoya konturi sifatida ko'riladi: TA AT moliyaviy operatsiya bo'yicha qaror qabul qilishdan oldin SAT shakllantiradigan sessiyaviy va xulq-atvor ma'lumotlaridan foydalanadi, SAT esa qo'shimcha xulosalarni TA AT va boshqa tizimlarga uzatadi.

Litsenziya qiymatini hisoblash uchun mo'ljallangan taxminiy hajmlar:

- ⌚ masofaviy bank xizmatlari kanallaridagi faol (yuridik va jismoniy) mijozlar soni (MAU) — 250 mingtagacha;
- ⌚ masofaviy bank xizmatlari kanallaridagi operatsiyalarning o'rtacha soni — oyiga 1,0 milliontagacha;
- ⌚ litsenziyaning amal qilish muddati — 1 yil.

Mazkur ko'rsatkichlar tijorat taklifini hisoblash hamda session va tranzaksion antifrod litsenziyalari qiymatini aniqlash uchun foydalaniladi va tizimning funksional imkoniyatlarini cheklamaydi.

### Joriy etish maqsadlari

- masofaviy xizmat ko'rsatish kanallari, bank karta va boshqa operatsiyalar bo'yicha firibgarlikni real vaqt rejimida (operatsiya bajarilishidan oldin) va/yoki keyingi nazorat rejimida aniqlash, ogohlantirish va oldini olish;
- moliyaviy monitoringni (sessiyaviy va tranzaksion) real vaqt rejimida avtomatlashtirish;
- SAT va TA AT o'rtasidagi o'zaro aloqani ta'minlash, shu jumladan moliyaviy operatsiyani bajarish to'g'risida qaror qabul qilinishidan oldin sessiyaviy antifrod tizimidan olingan ma'lumotlarni hisobga olish;
- har bir operatsiya uchun firibgarlik xavfini baholash, xavf darajasini belgilash va oldindan sozlangan javob choralarini qo'llash;
- moliyaviy yo'qotishlar, operatsion xavf va tartibga solish bilan bog'liq xavflarni kamaytirish;

- O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son «Kiberxavfsizlik to‘g‘risida»gi Qonuni talablariga rioya etilishini ta‘minlash;
- O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-son «Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida»gi qarori talablariga rioya etilishini ta‘minlash;
- «To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta‘minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarni oldini olish choralari ko‘rish to‘g‘risida»gi nizom (AVda 21.05.2024y, 3513-son) talablariga rioya etilishini ta‘minlash;
- O‘zbekiston Respublikasi Prezidentining «O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta‘minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi PQ-167-son qarori talablariga rioya etilishini ta‘minlash;
- «Kredit va to‘lov tashkilotlari, to‘lov tizimi operatorlari tomonidan jismoniy shaxslarga masofadan moliyaviy xizmatlar ko‘rsatishda axborot xavfsizligi va kiberxavfsizlikni ta‘minlash hamda frod holatlarining oldini olish bo‘yicha minimal talablar to‘g‘risida»gi nizom (AVda 21.01.2026y, 3759-son) talablariga rioya etilishini ta‘minlash;

**Loyihaning kutilayotgan natijasi: SAT va TA AT Buyurtmachining infratuzilmasida joylashtiriladi, o‘zaro hamda Buyurtmachining maqsadli tizimlari bilan integratsiya qilinadi; mijozlarning sessiyalari va tranzaksiyalari bo‘yicha qarorlarni avtomatik aniqlaydigan qoidalar/senariylar sozlanadi va zarur sinovlar bajariladi.**

## 2. Umumiy ma’lumotlar

### 2.1. Atamalar va qisqartmalar

| Atama                   | Ta’rif                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Buyurtmachi (Tashkilot) | «Biznesni rivojlantirish banki» ATB                                                                                                                                                                                                                                                                                                                                   |
| Mijoz (Foydalanuvchi)   | Buyurtmachi tomonidan turli xizmat ko‘rsatish kanallari orqali taqdim etiladigan xizmatlar iste’molchisi; 12 oy davomida kamida bir marta tizimga kirgan jismoniy yoki yuridik shaxslar uchun masofaviy bank xizmati tizimi foydalanuvchisi.                                                                                                                          |
| AT                      | Avtomatlashtirilgan tizim                                                                                                                                                                                                                                                                                                                                             |
| SAT                     | Sessiyaviy antifrod tizimi — Buyurtmachining raqamli resurslarida (jismoniy va yuridik shaxslar uchun masofaviy bank xizmati, P2P, 3-D Secure) sessiyaviy va xulq-atvor ma’lumotlarini yig‘ish hamda tahlil qilish orqali firibgarlik, bot-faolligi, daromadlarni legallashtirish va boshqa noqonuniy harakatlarni aniqlashga xizmat qiladigan kompleks yechim qismi. |

| Atama                                                                                  | Ta'rif                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TA AT (tranzaksion antifrod avtomatlashtirilgan tizimi, tranzaksion monitoring tizimi) | Har bir to'lov operatsiyasini (tranzaksiyani) imkon qadar real vaqtga yaqin rejimda, amalda bajarilishidan oldin tahlil qiladigan qoidalar va algoritmlar tizimi. Operatsiya parametrlari yoki atributlari odatiy holatdan chetga chiqqanda firibgarlik harakatlarini aniqlash va oldini olishga mo'ljallangan. |
| Antifrod                                                                               | Mijozlarga xizmat ko'rsatishning turli kanallarida sessiyalar va moliyaviy operatsiyalar bilan bog'liq firibgarlik xavfini kamaytirishga mo'ljallangan SAT va TA AT majmuasi.                                                                                                                                   |
| JSh uchun masofaviy bank xizmati                                                       | Jismoniy shaxslarga masofaviy bank xizmati (mobil banking).                                                                                                                                                                                                                                                     |
| YSh uchun masofaviy bank xizmati                                                       | Yuridik shaxslarga masofaviy bank xizmati (internet-banking, mobil banking).                                                                                                                                                                                                                                    |
| P2P                                                                                    | Kartadan kartaga pul o'tkazish uchun Tashkilot sahifasi.                                                                                                                                                                                                                                                        |
| 3-D Secure                                                                             | Internet orqali tovar uchun to'lovni tasdiqlash.                                                                                                                                                                                                                                                                |
| Emissiya                                                                               | To'lov tizimi ishtirokchisi bo'lgan Buyurtmachining to'lov kartalarini chiqarish va ularga xizmat ko'rsatish faoliyati.                                                                                                                                                                                         |
| Operator                                                                               | SAT foydalanuvchisi bo'lib, SAT qoidalarini tahlil qilish va sozlashni amalga oshiradi.                                                                                                                                                                                                                         |
| Atomar qoidalar                                                                        | Tranzaksiya/Mijozning bitta aniq belgisi yoki parametriga asoslangan bazaviy mantiqiy tekshiruvlar; imkon qadar real vaqtga yaqin rejimda ishlaydigan «HA/YO'Q» turidagi sodda shartlar.                                                                                                                        |
| Qoida (sessiyaviy)                                                                     | Foydalanuvchilarning joriy xulq-atvori va qurilmasi haqidagi ma'lumotlarni ilgari to'plangan ma'lumotlar bilan solishtirish, nomuvofiqlik belgilarini aniqlash va anomaliyalarni topish uchun mantiqiy amallar bilan birlashtirilgan bir yoki bir nechta mezonlar to'plami.                                     |
| Senariylar                                                                             | Tranzaksiya shartlarini alohida belgilar va/yoki parametrlar bo'yicha tekshiradigan bir nechta atomar qoidalar birikmasi; sessiyaviy va tranzaksion parametrlarni birlashtirishi mumkin.                                                                                                                        |
| Xavfni baholash, skoring                                                               | Mijoz harakatlarining raqamli bahosi bo'lib, operatsiyaning Mijoz uchun odatiy operatsiyalardan qanchalik farq qilishini ko'rsatadi. Atomar qoidalar va/yoki senariylar asosida hisoblanadi; yakuniy skoring — senariyda ishga tushgan barcha qoidalar                                                          |

| Atama                  | Ta'rif                                                                                                                                                                                                                                                                                     |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | skoringlari yig'indisi.                                                                                                                                                                                                                                                                    |
| Qaror                  | Ishga tushgan atomar qoidalar yoki senariylarning chegaraviy qiymatlari asosida Buyurtmachi tomonida amalga oshiriladigan qaror (block / step-up / allow).                                                                                                                                 |
| Hodisa (tranzaksiya)   | Mijoz tomonidan istalgan xizmat ko'rsatish kanalida to'lov yoki to'lovga oid bo'lmagan operatsiyani bajarish uchun boshlangan harakat.                                                                                                                                                     |
| To'lov tranzaksiyasi   | Mijoz boshlagan va moliyaviy operatsiyaga olib keladigan hodisa (o'tkazmalar, to'lovlar, kreditni so'ndirish va boshqalar).                                                                                                                                                                |
| Sessiya                | So'rov manbalaridan yakuniy obyektlargacha ma'lumot almashinuvi uzluksiz bajariladigan, umumiy identifikator va yakuniy natijaga ega operatsiyalar sikli.                                                                                                                                  |
| Sessiyaviy ma'lumotlar | Bitta sessiya doirasida uzatiladigan ma'lumotlar.                                                                                                                                                                                                                                          |
| SDK                    | Buyurtmachining mobil ilovasiga integratsiya qilish uchun mo'ljallangan metodlar va kutubxonalar to'plami.                                                                                                                                                                                 |
| Veb-sensor             | SATning JavaScript-kod shaklida yetkaziladigan va raqamli xizmat kanali veb-sahifasiga (internet-banking, P2P, 3-D Secure) o'rnatiladigan qismi; firibgarlik yoki avtomatlashtirilgan faollik alomatlarini aniqlash uchun zarur ma'lumotlarni yig'adi.                                     |
| Mobil sensor           | SATning iOS/Android uchun SDK shaklida yetkaziladigan va Buyurtmachining mobil ilovasiga o'rnatiladigan qismi; firibgarlik alomatlarini aniqlash va xavfga asoslangan autentifikatsiyani tayyorlash uchun zarur ma'lumotlarni yig'adi.                                                     |
| Evaluate API           | TA ATning operatsiyani dastlabki skoring qilish uchun maxsus dasturiy interfeysi; TA AT protsessingiga ma'lumotlarni yig'ish, qabul qilish va uzatishni ta'minlaydi hamda operatsiya bajarilishidan oldin chaqiriladi.                                                                     |
| Ingest API             | TA ATning operatsiya faktini tarixni to'plash uchun yuklashga mo'ljallangan maxsus dasturiy interfeysi; operatsiyaning yakuniy maqomi olinganidan keyin chaqiriladi hamda mijoz operatsiyalari tarixini yakuniy qarorlar (BLOCK, STEP-UP, ALLOW) bilan boyitish va to'plashni ta'minlaydi. |
| UQ                     | Hisob qaydnomasi                                                                                                                                                                                                                                                                           |

| Atama                 | Ta'rif                                                                                                                                                                                                             |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| API                   | Application Programming Interface — dasturiy mahsulot tomonidan boshqa dasturiy mahsulotlarda foydalanish uchun taqdim etiladigan tayyor sinflar, protseduralar, funksiyalar, tuzilmalar va konstantalar to'plami. |
| Cookie                | Sessiya tokeni — veb-server yuboradigan va foydalanuvchi kompyuterida saqlanadigan kichik ma'lumot bo'lagi.                                                                                                        |
| Proxy / proksi-server | Kompyuter tarmoqlarida foydalanuvchilarga boshqa tarmoq xizmatlariga bilvosita so'rov yuborish imkonini beruvchi oraliq server (dasturlar majmuasi).                                                               |
| TOR                   | Tinglashdan himoyalangan anonim tarmoq ulanishini o'rnatish imkonini beruvchi proksi-serverlar tizimi; ma'lumotlarni shifrlangan ko'rinishda uzatuvchi virtual tunnellingning anonim tarmog'i.                     |
| Veb-inyeksiyalar      | Mijoz tomonida (brauzerda) veb-sahifa mazmunini o'zgartirish yoki unga qo'shimcha mazmun kiritish.                                                                                                                 |
| Obfuskatsiya          | Dastur matni yoki bajariladigan kodning funkcionalligini saqlagan holda, tahlil qilish, ishlash algoritmlarini tushunish va dekomplyatsiya paytida o'zgartirishni qiyinlashtiradigan ko'rinishga keltirish.        |
| On-premise formati    | Tizimni Buyurtmachining infratuzilmasiga integratsiya qilgan holda ekspluatatsiya qilish.                                                                                                                          |
| Cloud formati         | Tizimni Ijrochining infratuzilmasiga integratsiya qilgan holda ekspluatatsiya qilish.                                                                                                                              |
| TSE                   | Tajriba-sanoat ekspluatatsiyasi                                                                                                                                                                                    |

### 3. Qo'llanish sohasi va operatsiyalar qamrovi

Kompleks yechim (SAT + TA AT) jismoniy (JSh) va yuridik (YSh) shaxslarning operatsiyalari bo'yicha sessiyaviy hamda xulq-atvor ma'lumotlarini yig'ish va tahlil qilishni, shuningdek, barcha yuqori xavfli raqamli va masofaviy kanallarda firibgarlik xavfini baholashni ta'minlashi kerak.

Operatsiyalarning minimal turlari ro'yxati quyidagilarni o'z ichiga oladi, biroq ular bilan cheklanmaydi:

- bankning hisob-kitob, depozit va karta hisobvaraqlari bo'yicha operatsiyalar (mablag'larni kirim qilish/yechish, o'tkazmalar, to'lovlar);
- mobil ilovalar va internet-kanallar orqali amalga oshiriladigan operatsiyalar (shu jumladan agentlar ilovalari);
- elektron hamyonlar bilan bog'liq operatsiyalar;

- QR-kodlar/kartalardan foydalangan holda amalga oshiriladigan operatsiyalar;
- mamlakat ichidagi va xalqaro pul o'tkazmalari (agar tegishli kanallar ulangan bo'lsa);
- virtual aktivlar hamyonlariga va/yoki xorijiy virtual aktiv operatorlari/birjalari hisobvaraqlariga o'tkazmalar (qo'llaniladigan hollarda);
- naqd pul yechish, kartalar bo'yicha operatsiyalar, bankomatlar/terminallar orqali operatsiyalar (agar tegishli kanallar ulangan bo'lsa);
- Buyurtmachi yuqori xavfli deb tasniflagan boshqa operatsiyalar.

TA AT moliyaviy operatsiyani bajarish to'g'risida qaror qabul qilinishidan oldin firibgarlik alomatlarini aniqlash maqsadida SAT yig'adigan sessiyaviy va xulq-atvor ma'lumotlarini hisobga olishi kerak.

Dasturiy ta'minot ishlab chiqaruvchi tomonidan e'lon qilingan foydalanish maqsadlari va ushbu texnik topshiriqda ko'rsatilgan funksional imkoniyatlarga mos bo'lishi kerak. Dasturiy ta'minotda zararli dasturlar bo'lmasligi lozim. Buyurtmachining ushbu dasturiy ta'minotdan foydalanishi, jumladan, quyidagi holatlarga olib kelmasligi kerak:

#### **4. Tizimga qo'yiladigan umumiy talablar**

##### **4.1. Kanallararo ishlash va tashqi tizimlar bilan o'zaro aloqa**

4.1.1. Tizim sessiyaviy va tranzaksion tahlil konturlarini birlashtiradigan, firibgarlik operatsiyalarini aniqlashga mo'ljallangan kompleks kanallararo tizim bo'lishi kerak.

4.1.2. Tizim yangi ma'lumot manbalari/kanallarini ulash, yangi API turlari va skoring modellarini qo'shish hamda ulardan foydalanish imkoniyatiga ega bo'lishi kerak. Yangi manbalardan olingan ma'lumotlar qayta ishlanishi, saqlanishi va qoidalarda ishlatilishi lozim.

4.1.3. Tizim barcha xizmat ko'rsatish tizimlarida mijozlarning shubhali harakatlarini kuzatish, to'plash va aniqlashni ta'minlashi hamda barcha ulangan kanallardagi hodisalar asosida Mijozning yagona profilini shakllantirishi kerak.

4.1.4. Tizim qaror qabul qilishda tashqi ma'lumot tizimlaridan, jumladan federativ va markazlashtirilgan tizimlardan foydalanish imkoniyatiga ega bo'lishi kerak.

4.1.5. Tizim hodisalarni uzatish, shuningdek, ichki obyektlar — mijozlar, foydalanuvchilar, hisobvaraqlar va boshqalarning profillarini to'plash hamda yangilash uchun yangi ma'lumot manbalarini moslashuvchan tarzda qo'shish imkoniyatiga ega bo'lishi kerak.

##### **4.2. Tizim tarkibiy qismlari ro'yxati**

Tizim quyidagi tarkibiy qismlarni o'z ichiga olishi kerak:

- foydalanuvchi qurilmasidan ma'lumot yig'ish quyi tizimi (veb va mobil sensorlar) — SAT;
- bot-faolligini aniqlash va bloklash quyi tizimi — SAT;
- ma'lumotlarni qayta ishlash va korrelyatsiya qoidalarini boshqarish quyi tizimi — SAT;
- ma'lumotlar tahlili quyi tizimi — SAT;

- hisobot va vizualizatsiya quyi tizimi — SAT va TA AT uchun yagona;
- axborot almashinuvi quyi tizimi — SAT va TA AT uchun yagona;
- Markaziy bankning Markazlashtirilgan antifrod tizimi bilan axborot almashinuvi quyi tizimi — SAT;
- tranzaksiyalarni onlayn skoring qilish (Evaluate API) va ma'lumotlar bilan to'ldirish (Ingest API) quyi tizimi — TA AT;
- qoidalar/senariylar konstruktori va mexanizmi — SAT va TA AT uchun yagona;
- ro'yxatlar bilan ishlash quyi tizimi — SAT va TA AT uchun yagona;
- aloqalar grafigini tahlil qilish quyi tizimi — SAT va TA AT uchun yagona;
- operatsiyalarni belgilash va ML uchun ma'lumotlarni tayyorlash quyi tizimi — TA AT.

## **5. SATning mijoz tomonidagi qismiga qo'yiladigan talablar**

### **5.1. Veb-xizmatlarda**

Quyidagilar amalga oshirilishi kerak:

- foydalanuvchi qurilmasini uning parametrlari asosida identifikatsiya qilish (device fingerprinting);
- foydalanuvchi qurilmasini turli mijozlar kesimida global identifikatsiya qilish;
- mijozlarning hisob ma'lumotlaridan ruxsatsiz foydalanish holatlarini aniqlash;
- himoyalalanayotgan veb-ilovaga begona kod kiritilganini aniqlash;
- server tomonida veb-qismga firibgarlik maqsadida kiritilgan o'zgartirishlarni (veb-inyektsiyalarni) aniqlash;
- fishing holatlarini aniqlash;
- mijoz TOR, proxy va anonimlashtiruvchi vositalar orqali ishlayotganini aniqlash;
- komprometatsiya qilingan ajratilgan serverlar yoki hosting va kolokatsiya xizmatlarini ko'rsatuvchi kompaniyalar qurilmalaridan kirishni aniqlash;
- antidetekt-brauzerlardan (Dolphin, Incognition, CheBrowser, AdsPower va boshqalar) foydalanishni aniqlash;
- Buyurtmachining veb-resursidagi navigatsiya, kursor harakati, tugmalarni bosish tezligi va ketma-ketligi, pauzalar hamda shakllar bilan o'zaro aloqaga oid xulq-atvor ma'lumotlari asosida firibgar va qonuniy foydalanuvchini farqlash;
- hisob qaydnomalarini avtomatlashtirilgan tarzda buzishga urinishlarni («brute force») yoki boshqa resurslardan olingan komprometatsiyalangan hisob qaydnomalaridan foydalanishni («credential stuffing») aniqlash va bloklash;
- foydalanuvchi Buyurtmachi ilovasidan foydalanganda uning harakatlari haqidagi ma'lumotlarni yuborish;
- quyidagi brauzer turlaridan ma'lumot olish, shuningdek, ko'rsatilganidan eski versiyalar orqali ulanishni bloklash: Chromium 26 va undan yuqori (jumladan Google Chrome, Yandex Browser, Opera); Internet Explorer 9 va undan yuqori; Microsoft Edge 13 va undan yuqori; Mozilla Firefox va boshqa hujjatda ko'rsatilgan brauzerlar;

- Buyurtmachi tanlagan boshqa qoidalar (bir nechta hisob qaydnomasidan foydalanish, firibgarlik bilan bog‘liq quyi tarmoqlardan foydalanish va boshqalar) asosida foydalanuvchi va dasturiy ta‘minotning zararli faolligini aniqlash;
- ko‘p sahifali internet-resurslarda ham, Single Page Application texnologiyasi asosida yaratilgan resurslarda ham ishlash;
- maxfiy axborotni, shu jumladan shaxsga doir ma‘lumotlar va bank sirini tashkil etuvchi ma‘lumotlarni yig‘maslik hamda taqdim etmaslik (bunday ma‘lumotlar faqat SATga taqdim etiladi).

## 5.2. Mobil ilovalarda

Quyidagilar amalga oshirilishi va SATga uzatilishi kerak:

- mobil qurilmani identifikatsiya qilish;
- foydalanuvchi qurilmasini turli mijozlar kesimida global identifikatsiya qilish;
- Buyurtmachining mobil ilovasi soxtalashtirilganini aniqlash (imzoni tekshirish, yaxlitlikni nazorat qilish);
- operatsion tizim versiyasi va root-huquqlari mavjudligi haqida ma‘lumot berish, ilovaning mobil qurilma emulyatorida ishga tushirilganini aniqlash;
- mijoz qurilmasiga masofadan ulanishlarni aniqlash (masofaviy boshqaruv vositalaridan foydalanish): masofaviy kirish va boshqaruv dasturlarining mavjudligi; faol masofaviy boshqaruv sessiyalari; xulq-atvor belgilari asosida;
- mijoz SIM-kartasini almashtirganini aniqlash va bu haqdagi ma‘lumotni SATga uzatish;
- foydalanuvchining tegish, surish (swipe), ilova interfeysi elementlari bilan o‘zaro aloqasi va matn kiritish tezligi xususiyatlarini, shuningdek mobil qurilma sensorlari ma‘lumotlarini yig‘ish va SATga uzatish;
- SATga GPS ma‘lumotlari va foydalanilayotgan aloqa kanallari (Wi-Fi, mobil tarmoq, simli internet) haqidagi ma‘lumotlarni taqdim etish, jumladan GPS sensori orqali olingan uzunlik, kenglik, balandlik, yo‘nalish va harakat tezligi, shuningdek uyali aloqa minorasi identifikatorlari;
- foydalanuvchi qurilmasida debugger aniqlangani haqida ma‘lumot taqdim etish: dasturchi rejimini va mobil ilovaning faol debugging sessiyasini aniqlash;
- foydalanuvchi qurilmalarida Buyurtmachi ilovalari ishining sezilarli darajada sekinlashishiga yo‘l qo‘ymaslik;
- ma‘lumot yig‘ish jarayonida foydalanuvchiga dialog oynalari, tasdiqlash so‘rovlari yoki bildirishnomalar ko‘rsatilmasligi;
- foydalanuvchi qurilmasi bilan SAT o‘rtasidagi tarmoq faolligining sezilarli oshishiga yo‘l qo‘ymaslik;
- ham mahalliy (native) mobil ilovalarda, ham WebView komponentlaridan foydalanadigan gibrid ilovalarda ishlash;
- foydalanuvchi Buyurtmachi ilovasidan foydalanganda uning harakatlari haqidagi ma‘lumotlarni yuborish;
- brauzerlar hamda Android va iOS mobil operatsion tizimlarining standart funksiyalaridan foydalanish;

- Android v.5 (API 14) va undan yuqori, iOS v.10 va undan yuqori operatsion tizimlarda ishlash va ma'lumot olish;
- maxfiy axborotni, shu jumladan shaxsga doir ma'lumotlar va bank sirini tashkil etuvchi ma'lumotlarni yig'maslik hamda taqdim etmaslik (bunday ma'lumotlar faqat SATga taqdim etiladi).

## **6. Arxitekturaga qo'yiladigan talablar**

### 6.1. Integratsiya modeli

#### 6.1.1. Tizim quyidagi integratsiya ssenariylarini qo'llab-quvvatlashi kerak:

- onlayn skoring — xavfni baholash va tavsiya etiladigan qarorni olish uchun operatsiya bajarilishidan oldin tizimga murojaat qilish;
- ma'lumotlar bilan to'ldirish — operatsiya faktini, yakuniy holatini, qo'shimcha hodisalar va atributlarni operatsiyadan oldin hamda keyin uzatish;
- asinxron ma'lumot yuklash — tarixni to'plash va keyinchalik qoidalarda foydalanish uchun hodisalar, jurnallar, profillar va boshqa obyektlarni uzatish;
- tarixiy ma'lumotlarni yuklash — qoidalarni sozlash, ssenariylarni sinash va profillarni shakllantirish uchun oldingi davrlarga oid tarixni yuklash.

6.1.2. Tizim alohida oraliq integratsiya qatlamini yaratish zaruratisiz sessiyaviy va tranzaksion ma'lumotlarni tabiiy ravishda birlashtirishi kerak. Tranzaksion skoringda quyidagilardan foydalanilishi lozim:

- mijoz sessiyasining identifikatori;
- qurilma identifikatori;
- qurilma xavfi belgilari;
- emulyator, root/jailbreak va tampering belgilari;
- zararli dasturlar (malware) va masofaviy kirish vositalari belgilari;
- ekranni ulashish (screen sharing) belgilari;
- faol qo'ng'iroq / VoIP ssenariylari belgilari;
- IP, geolokatsiya, proxy, VPN va anonimlashtiruvchi vositalar signallari;
- mijoz bilan qurilma o'rtasidagi bog'liqlik tarixi;
- mijoz bilan mablag' oluvchi o'rtasidagi bog'liqlik tarixi;
- operatsiyagacha mijoz bajargan harakatlar ketma-ketligi.

6.1.3. Tizim quyidagi obyekt turlari uchun ma'lumotlar modellarini yaratish va kengaytirishni qo'llab-quvvatlashi kerak: operatsiyalar, hodisalar, mijozlar, foydalanuvchilar, hisobvaraqlar, kartalar, qurilmalar, mablag' oluvchilar, sessiyalar, ichki tizim hodisalari va tashqi xavf signallari. Tizim ma'lumotlar modelini kengaytirish imkonini berishi kerak.

### 6.2. Foydalanuvchi qurilmasidan ma'lumot olish quyi tizimiga qo'yiladigan talablar (SAT)

Quyi tizim quyidagilarni ta'minlashi kerak:

- Buyurtmachi tizimlarining ish qobiliyatini buzmaslik;
- firibgar quyi tizimning ishlashiga faol qarshilik ko'rsatishi mumkinligini hisobga olish: statik tahlildan himoyalash; veb-xizmatlar uchun SAT mijoz qismining kodini dinamik obfuskatsiya qilish; mijoz qismidan uzatiladigan ma'lumotlarni himoyalash;
- foydalanuvchi qurilmasi komprometatsiya qilinganini ko'rsatuvchi indikatorlarni aniqlash:
- veb-ilovalar uchun: mijoz qismiga (HTML, JS va boshqalar) inyeksiyalarni aniqlash; inyeksiyalarni qo'lda va avtomatik tasniflash; dinamik o'zgaruvchi inyeksiyalarni tasniflash; shubhali yoki firibgarlik bilan bog'liq internet-resurslarga murojaatlarni aniqlash;
- mobil ilovalar uchun: foydalanuvchi qurilmasidagi zararli dasturlarni signatura asosida tahlil qilish; zararli dasturlarning mavjudligi va ishlashini xulq-atvor asosida tahlil qilish, jumladan ilovaga administrator huquqlari berilishi, o'rnatish manbasi, overlay-faollik va avtomatlashtirilgan harakatlar;
- IPv4 manzil makonini proxy va VPN xizmatlari uchun ochiq tarmoq portlari mavjudligi bo'yicha profillash, domen nomlari va IP-manzillarni anonimlashtiruvchi vositalarni aniqlash uchun tahlil qilish orqali mijozning TOR, proxy va anonimlashtiruvchi vositalardan foydalanishini aniqlash;
- tarmoq qurilmalarini profillash bo'yicha tashqi manbalar hamda avtomatlashtirilgan faollikni aniqlash hodisalaridan foydalanib, komprometatsiya qilingan ajratilgan serverlar yoki hosting/kolokatsiya kompaniyalari qurilmalaridan kirishni aniqlash;
- ilova doirasida qurilma va SIM-karta, jumladan qurilma modeli yoki (e)SIM-karta o'zgarganda bir foydalanuvchining turli mobil qurilmalarini identifikatsiya qilish;
- tegish va surish xususiyatlari, interfeys elementlari bilan o'zaro aloqa, matn kiritish tezligi va qurilma sensorlari ma'lumotlari asosida, tugmalar bosilishi dinamikasi hamda kursor harakatlarini profillash orqali firibgar va qonuniy foydalanuvchini farqlash;
- GPS ma'lumotlari va aloqa kanallari turlari haqidagi ma'lumotlardan foydalangan holda firibgarlikni aniqlash: yuqori xavfli hodisalarni hisobga olib geolokatsiyalarni profillash va oxirgi foydalanuvchi qurilmasidagi geolokatsiya soxtalashtirilishini aniqlash;
- Buyurtmachi tanlagan boshqa qoidalar (bir nechta hisob qaydnomasi, firibgarlik tarmoq segmentlaridan foydalanish va boshqalar) asosida foydalanuvchi va dasturiy ta'minotning zararli faolligini aniqlash hamda yuqori xavf aniqlanganda uni bloklash/to'xtatish mexanizmlarini taqdim etish;
- debugger yoqilgan mijoz sessiyalarini aniqlash va mijoz harakatlarini tahlil qilishda buni hisobga olish;
- mobil API'ni botlar yoki begona mobil ilovalardan foydalanishdan himoyalash: mobil ilovaning server qismidagi API'ga to'g'ridan-to'g'ri murojaatlarni, soxta yoki begona mobil ilovadan API'ga murojaatlarni aniqlash va sessiya o'g'irlanishidan himoyalash;
- Buyurtmachining tashqi tizimlariga, masalan, TA ATga qo'shimcha xulosalarni taqdim etish;
- Buyurtmachining masofaviy bank xizmati tizimida (shaxsiy kabinetga kirish, tranzaksiya bajarish, profilni o'zgartirish) Buyurtmachi tanlagan yoki sozlagan qoidalar asosida mijoz sessiyasi yoki harakatini bloklash/to'xtatish;

- mobil operatsion tizim va brauzerlar haqidagi ma'lumotlar asosida harakat qonuniyligini baholash: antidekt-brauzerlarni, root qilingan/jailbreak mobil qurilmalarni hamda firibgarlik harakatlarini avtomatlashtirishda ishlatiladigan headless-brauzerlarni aniqlash;
- SAT modullari ma'lumotlarini uzatish uchun HTTPS (TLS va SSL) ulanishidan, mobil ilova tomonida esa SSL pinning imkoniyatidan foydalanish;
- Buyurtmachi ilovasida foydalanuvchi harakatlari haqidagi ma'lumotlarni qabul qilish va ularni ma'lumotlarni qayta ishlash quyi tizimiga uzatish;
- yig'ilgan ma'lumotlarni obfuskatsiya qilingan shaklda, yaxlitligi nazorati bilan uzatish;
- yig'ilgan ma'lumotlarni foydalanuvchi va Buyurtmachi o'rtasidagi aloqa kanallari orqali uzatishni qo'llab-quvvatlash;
- veb-sensor kodini dinamik obfuskatsiya qilishni, obfuskatsiya parametrlarini o'zgartirish va uning davriyligini belgilash imkoniyatini qo'llab-quvvatlash;
- mustaqillik, yaxlitlik va xavfsizlikni ta'minlash uchun veb-sensorni modullarga bo'linmagan monolit yetkazib berish arxitekturasiga ega bo'lish.

## 7. Funktsional talablar

### 7.1 Ma'lumotlarni qayta ishlash quyi tizimiga (SSA) qo'yiladigan talablar

Quyi tizim quyidagilarni bajarishi kerak:

- ma'lumotlarni yig'ish, qabul qilish va yaxlitligini tekshirish, jumladan, ma'lumotlar SSA server qismiga yetib borguniga qadar yo'lda firibgar tomonidan almashtirilmaganini tekshirish;
- ma'lumotlarni yig'ish quyi tizimlaridan olinadigan axborot asosida foydalanuvchi va uning qurilmalari profilini shakllantirish;
- Buyurtmachining har bir foydalanuvchisi ish seanslari bo'yicha ma'lumotlarni kanallararo korrelyatsiya qilish;
- korrelyatsiya qoidalaridan, jumladan, mashinaviy o'qitishdan foydalangan holda har bir foydalanuvchining harakatlarini tahlil qilish;
- SSA yig'ish tizimidan olingan mijoz identifikatori, qurilma raqamli izi, IP-manzil, seans identifikatori va boshqa parametrlar bo'yicha tezkor qidiruvni amalga oshirish;
- Buyurtmachi xodimlariga firibgarlik faolligini aniqlash va bloklash qoidalarini, shuningdek, har bir seans uchun xavf darajasini mustaqil sozlash imkonini berish;
- firibgarlik faolligini aniqlash bo'yicha yangi gipotezalarni tekshirish uchun amaldagi ma'lumotlarda onlayn rejimda sinov hodisalarini yaratish imkonini berish;
- uchinchi tomon ma'lumot manbalaridan indikatorlar bilan boyitish.

### 7.2 Ma'lumotlarni tahlil qilish quyi tizimiga (SSA) qo'yiladigan talablar

Quyi tizim quyidagilarni bajarishi kerak:

- Buyurtmachining boshqa foydalanuvchilariga tegishli boshqa seanslar bilan ma'lumotlar korrelyatsiyasini ta'minlash;

- ma'lumotlarni kanallararo darajada hamda SSAning boshqa buyurtmachilari darajasida identifikatsiya qilish va korrelyatsiyalash;
- tizimning boshqa buyurtmachilari roziligi bilan ulardan olingan bilimlardan foydalanib, Buyurtmachining mazkur va boshqa mijozlariga oid firibgarlik faolligi haqidagi ma'lumotlarni boyitish;
- mijoz masofaviy bank xizmatida (MBX) seans davomida uyali tarmoq yoki tezkor xabar almashish xizmatlari orqali kiruvchi/chiquvchi faol qo'ng'iroqni aniqlash;
- boshqa ishlab chiqaruvchilarning tashqi antifrod tizimlari bilan integratsiya qilish imkoniyatiga ega bo'lish;
- mijozlarning hisob ma'lumotlaridan ruxsatsiz foydalanish holatlarini aniqlash (MBXga yangi qurilmadan kirish, firibgarlik qurilmasidan MBXga kirish);
- aniqlangan yakka hodisalarni hamda foydalanuvchi qurilmasidagi brauzer ish seanslari bo'yicha guruhlangan hodisalarni ko'rish imkonini berish;
- mijozlararo darajada firibgarlikni global aniqlashni ta'minlash;
- aniqlangan har bir hodisa tafsilotlarini ko'rish imkonini berish, jumladan: hodisa vaqti, muhimlik darajasi, aniqlangan hodisa turi va turiga qarab hodisa tafsilotlari;
- mijoz profilini ko'rish uchun alohida vositani taqdim etish, bunda aloqalar asosiy obyektlar (qurilmalar, seanslar, geolokatsiyalar) bo'yicha guruhlanadi;
- Buyurtmachi sahifalariga kiritilgan veb-inyektsiyalarni ko'rish va toifalash;
- Buyurtmachi resurslarida foydalanuvchi seanslari davomida murojaatlar qayd etilgan domenlarni (masalan, zararli, shubhali, qonuniy) ko'rish va toifalash;
- foydalanuvchilar faolligi va ular orasida aniqlangan hodisalar soni bo'yicha statistikani chiqarish;
- SSA egasi tomonidan hisob yozuvlarini boshqarish, yangi rollar yaratish hamda rollar va hisob yozuvlari bo'yicha huquqlarni chegaralash imkoniyatini ta'minlash;
- ma'lumotlarni maxsus interfeysda tahlil qilish imkoniyatini ta'minlash.

### 7.3 Tranzaksiyalarni real vaqt rejimida monitoring qilish (TA AT)

7.3.1 TA AT sozlangan ssenariylar va qoidalar asosida, barcha mavjud manbalardan (shu jumladan SSA'dan) yig'ilgan xulq-atvor atributlari va seans hodisalarini hisobga olgan holda, mijoz tranzaksiyasi bo'yicha qaror qabul qilinishidan oldin o'zgarishlarga dinamik javob berib, firibgarlik va shubhali operatsiyalarni real vaqt rejimida aniqlash uchun tahlil o'tkazishi kerak.

7.3.2 Ulangan barcha ma'lumot manbalaridan keladigan hodisalarni tahlil qilish mijoz profilini shakllantirishni ta'minlashi kerak (qurilma bilan o'zaro aloqa, vaqt naqshlari, mobil ilovadagi harakatlar, operatsiyalar summalari); ushbu profil mijozning keyingi tranzaksiyalarini tahlil qilishda ishlatiladi.

7.3.3 Har bir operatsiya uchun tizim quyidagilarni bajarishi kerak: operatsiya ma'lumotlarini qabul qilish; ularni seans va profil belgilari bilan boyitish; qoidalar va agregatlarni hisoblash; yakuniy risk score'ni hisoblash; tavsiya etilgan qarorni shakllantirish; natijani Buyurtmachi tizimiga sinxron tarzda ham, asinxron tarzda ham (webhook xabarnomasi orqali) qaytarish.

## 7.4 Qoidalar va ssenariylar

7.4.1 Tizim monitoring qoidalarining oldindan sozlangan ro'yxatini o'z ichiga olishi kerak.

7.4.2 Tizim qoidalar va ssenariylarni faollashtirish/faolsizlantirish imkoniyatiga ega bo'lishi kerak.

7.4.3 Tizim operatsiyalar oqimi uchun operatsiya/seansni baholashga doir bir nechta ssenariyni bir vaqtning o'zida ishlata olishi kerak.

7.4.4 Tizim tarixiy ma'lumotlar bo'yicha agregatlarni sirg'aluvchi vaqt oynasida real vaqt rejimida (operatsiya amalga oshirilayotgan paytda) hisoblashni ta'minlashi kerak.

7.4.5 Tizim mijoz tranzaksiyasi va seansini tekshirish qoidalarini yaratish hamda sozlash imkoniyatiga ega bo'lishi kerak. Qoidalar quyidagi talablarga javob berishi lozim:

- skoring balli tranzaksiya/seansni avtomatik baholash natijasi sifatida hisobga olinadi;
- qoidalar dasturlash tillaridan foydalanmasdan, oddiy foydalanuvchilar uchun mavjud interfeys va usullar orqali sozlanadi;
- tizim qoidalarini tabiiy tilda shakllantirish va tavsiflash uchun AI funksiyalaridan foydalanishni qo'llab-quvvatlashi kerak;
- tizim operatsiya bo'yicha qarorni ishga tushgan atomar qoidalar va ssenariylar asosida ham, foydalanilayotgan ML-modellar asosida ham shakllantira olishi kerak;
- qaror chiqarishda qoidalar va ssenariylar operatsiya amalga oshirilayotgan paytdagi mijozga oid barcha seans, xulq-atvor, tranzaksiya va profil ma'lumotlarining kombinatsiyasini baholashi kerak.

7.4.6 Qoidalar quyidagilar kombinatsiyasidan foydalanishi kerak: tranzaksiya ma'lumotlari; seans ma'lumotlari; xulq-atvor belgilari; mijoz profillari; qurilma profillari; ro'yxatlar; agregatlar; tashqi xavf signallari.

7.4.7 Xavfni baholashga ta'sir qiluvchi har bir model va qoida uchun Tizim versiya, yaratilgan sana va muallif, o'qitish ma'lumotlarining manbasi va davri, ishlatilgan belgilar, parametrlar, sinov natijalari hamda Buyurtmachining mas'ul shaxsi tasdig'ini saqlashi kerak. Yangi model tasdiqlanguniga qadar sinov yoki yashirin rejimda ishga tushiriladi va amaldagi modelni mustaqil ravishda almashtirmasligi kerak.

## 7.5 Mijoz tranzaksiyasi bo'yicha qo'shimcha parametrlarni shakllantirish

7.5.1 Tizim mijoz tranzaksiyalari uchun quyidagi matematik formulalar asosida hisoblash funksiyalarini qo'llab-quvvatlashi kerak (shu bilan cheklanmagan holda): sirg'aluvchi va/yoki belgilangan vaqt oynasidagi operatsiyalar summasi; shu oynadagi operatsiyalar soni; biror hodisadan o'tgan vaqt; parametrdan qism satrni ajratib olish; ikki parametr nisbatini (shu jumladan foizlarda) aniqlash; biror qoida (quyi qoida) ishga tushganidan beri o'tgan vaqt; mamlakatlar va shaharlar orasidagi harakatlanish vaqtini aniqlash; operatsiya summasining balansga yoki tarixiy xulq-atvorga nisbati; matematik amallar.

7.5.2 Agregatlar ham real vaqt rejimida, ham asinxron rejimda hisoblanishi kerak.

## 7.6 Ro'yxatlar bilan ishlash

7.6.1 Tizim qora va oq ro'yxatlar bilan ishlashni, uchinchi tomon manbalaridan ro'yxatlarni import qilishni hamda tizim foydalanuvchilari tomonidan ro'yxatlar yaratishni qo'llab-quvvatlashi kerak, jumladan: oluvchilar ro'yxatlari; qurilmalar ro'yxatlari; hisobvaraqlar/kartalar ro'yxatlari; foydalanuvchilar, IP-manzillar va qurilma identifikatorlari bo'yicha maxsus ro'yxatlar (masalan, bloklash, istisnolar, shubhali qurilmalar ro'yxatlari va boshqalar).

## 7.7 Operatsiyalar tarixi bilan ishlash va ssenariylarni sinash

Tizim tarixiy tranzaksiyalar va seanslarni amaldagi ssenariylar bo'yicha baholash uchun qayta ishlash imkoniyatini qo'llab-quvvatlashi kerak.

## 7.8 Operatsiyalarni belgilash va MLga tayyorlash

Tizim mijozlar/foydalanuvchilar harakatlari va Buyurtmachi mutaxassislari tomonidan operatsiyalar tahlili natijalari haqida kelib tushadigan hamda to'planadigan ma'lumotlar asosida o'z-o'zini o'qitishni qo'llab-quvvatlashi kerak. Mijoz profili to'plangan tranzaksiya ma'lumotlari asosida yaratiladi va tizimdan foydalanish davomida moslashtirib boriladi.

## 7.9 Aloqalar grafigi

Tizim tranzaksiya va seans ishtirokchilari o'rtasidagi aloqalarni qurish funksiyasini taqdim etishi kerak. Bunda tahlil va firibgarlik hamda AML holatlarini tekshirish uchun seans va tranzaksiya ma'lumotlari yagona grafik sxemada birlashtiriladi; jumladan, Buyurtmachi mijozlari, qurilmalar, geolokatsiyalar va mijozlarning boshqa seans ma'lumotlari o'rtasidagi grafik aloqalar tahlil qilinadi.

## 7.10 Hisobotlar va foydalanuvchi interfeysi

7.10.1 Tizim quyidagilarni taqdim etishi kerak: operatsiyalar/seanslar ro'yxati; operatsiya/insident kartasi; filtrlar va saqlangan foydalanuvchi filtrlari (har bir foydalanuvchi hisob yozuvi uchun shaxsiy filtrlarni saqlash bilan); vidjetlar; boshqaruv panellari (dashboard); CSV/XLSX eksporti; qoidalar, ishga tushishlar, noto'g'ri ijobiy natijalar (false positive) va tasdiqlangan firibgarlik (confirmed fraud) bo'yicha hisobotlar.

7.10.2 Tizim operatsiyalar va hodisalar haqidagi axborotni turli ko'rinishlarda chiqaruvchi sozlanadigan vidjetlar orqali ham grafik, ham matnli shaklda hisobot taqdim etish funksiyasiga ega bo'lishi kerak.

## 7.11 Dasturiy interfeys (API)

7.11.1 API bilan o'zaro aloqa chaqirilayotgan funksiyalarga kirish huquqlarini tekshirgan holda, himoyalangan HTTPS protokoli orqali amalga oshiriladi.

7.11.2 API insidentlar/operatsiyalar haqidagi olingan ma'lumotlarni JSON formatida tashqi tizimlarga real vaqt rejimida taqdim etadi. Uzatiladigan ma'lumotlar tarkibiga quyidagilar kiradi: insidentning noyob identifikatori; insident turi bo'yicha tasnif; insident manbasi (kanal, seans,

qurilma, foydalanuvchi hisob yozuvi); insident vaqti; seansning noyob identifikatori; foydalanuvchi nomi; foydalanuvchi brauzeri va qurilmasi haqidagi ma'lumot; insident sodir bo'lgan URI; foydalanuvchining User-Agent ma'lumoti; umumiy xavf olinganda esa qo'shimcha ravishda ishga tushgan qoidalar identifikatorlari va har bir qoida bo'yicha xavf darajasi.

7.11.3 API aniqlangan hodisalarni ham real vaqt rejimida, ham so'rov rejimida olish imkonini berishi kerak. Bunda quyidagi parametrlar kombinatsiyasi bo'yicha aniqlangan hodisalar to'plamini olish mumkin bo'lishi lozim: vaqt oralig'i; Buyurtmachi seansining identifikatori (mavjud bo'lganda); belgilangan hodisa turlari to'plami.

7.11.4 API tizimni o'qitish va firibgarlik faolligini aniqlash sifatini oshirish maqsadida aniqlangan hodisalar bo'yicha qayta aloqa berish imkoniyatini taqdim etishi kerak.

7.11.5 Tizim ma'lumotlarni eksport/import qilish uchun sanoat standartidagi protokollar va usullardan foydalanishi, aniqlangan hodisalarda uzatiladigan ma'lumotlarning maxfiyligini ta'minlashi hamda pull, push va gibrud uzatish usullarini qo'llab-quvvatlashi kerak.

7.11.6 Tranzaksiya konturi (TA AT) uchun dasturiy interfeys qo'shimcha ravishda quyidagilarni o'z ichiga olishi kerak:

- Evaluate API — operatsiya amalga oshirilishidan oldin chaqiriladi, operatsiyani dastlabki skoringdan o'tkazish uchun TA AT protsessingiga ma'lumotlarni yig'ish, qabul qilish va uzatishni ta'minlaydi;
- Ingest API — operatsiyaning yakuniy maqomi olinganidan keyin chaqiriladi, operatsiya faktini yuklash, mijoz operatsiyalari tarixini ularning yakuniy qarorlari (BLOCK, STEP-UP, ALLOW) bilan boyitish va to'plashni ta'minlaydi.

7.11.7 Har bir API chaqiruvi autentifikatsiyadan va chaqiruvchi tizim vakolatlarini tekshirishdan o'tishi kerak. Tizimlararo aloqa uchun TLS, Buyurtmachi standarti nazarda tutgan bo'lsa, tomonlarning o'zaro autentifikatsiyasi qo'llanilishi lozim. Protokollarning aniq versiyalari va kriptografik himoya parametrlari tizim sanoat ekspluatatsiyasiga topshiriladigan sanada amal qiladigan me'yoriy talablar va Buyurtmachi standartiga muvofiq belgilanadi.

Tokenlar va kalitlar cheklangan vakolatlarga ega bo'lishi, Buyurtmachi tasdiqlagan maxfiy ma'lumotlar omborida saqlanishi, davriy almashtirilishi va bekor qilinishi kerak. API vaqt tamg'asi va so'rovning noyob identifikatorini tekshirishi yoki so'rovni takroran ijro etishdan teng darajadagi himoyani ta'minlashi lozim. Takroriy chaqiruvlar uchun Buyurtmachi bilan kelishilgan kutish vaqti (timeout) va so'rovlar chastotasini cheklash qoidalari qo'llanadi.

Imzolangan webhook va vaqt/noyoblikni tekshirish rekvizitlarini o'z ichiga olishi kerak; qabul qiluvchi takroran yuborilgan, muddati o'tgan yoki noto'g'ri imzolangan xabarlarni rad etishi lozim. Maxfiy ma'lumotlar, tokenlar va maxfiy maydonlarning to'liq qiymatlari jurnallarga yozilmasligi kerak.

7.12 Tizim shubhali va firibgarlik hodisalari bo'yicha ma'lumotlarini Markazlashgan antifrod tizimiga uzatish imkoniyatiga ega bo'lishi lozim.

## **8. Nofunksional talablar**

### **8.1 Unumdorlik**

8.1.1 Tizim operatsiyalarni real vaqt rejimida qayta ishlashni ta'minlashi kerak. Maqsadli ko'rsatkichlar:

- yuklama: kamida 250 TPS;
- P99 kechikish: ko'rsatilgan yuklamada 300 ms dan oshmasligi kerak;
- tashqi ma'lumot manbalari ishining yomonlashuvi skoringning to'liq to'xtashiga olib kelmasligi kerak.

### **8.2 Ishonchlilik va foydalanish imkoniyati**

8.2.1 Quyidagi talablar bajarilishi kerak:

- kamida ikkita maydonda nosozliklarga chidamli sxema asosida ishlash va avariya chidamli konfiguratsiyada ishlash sxemasiga, jumladan, seans va tranzaksiya ma'lumotlarini zaxira maydonga o'tkazish bo'yicha disaster recovery (DR) rejasiga ega bo'lish;
- asosiy maydondagi sozlamalar o'zgarganda zaxira maydon yangilanishi kerak; asosiy maydon mavjud bo'lmagan holatda to'g'ri ishlashi uchun qurilmalar va foydalanuvchilarning yaratilgan profillari zaxira maydonda avtomatik yangilanib borishi lozim;
- asosiy komponentlarni zaxiralashni ta'minlash;
- gorizontal masshtablash;
- Buyurtmachi tizimlari bilan o'zaro aloqa paytida tarmoq uzilishlari yuz berganda ma'lumotlar yaxlitligini saqlash;
- API so'rovlarining idempotentligi va xatolar yuz berganda xabarlarni qayta ishlash.

8.2.2 Tizim nosozliklarga chidamlilik nazorati talablariga javob berishi kerak:

- o'zining asosiy komponentlari holatini monitoring qilish va nazorat qilish;
- diskdagi bo'sh joy, protsessor va xotira resurslari sarfi, qayta ishlanayotgan mijoz tranzaksiyalari va seanslari sonini nazorat qilish mexanizmlarini ta'minlash.

8.2.3 Tizim aniqlangan muhim hodisalar, parametrlarning og'ishi va texnik nosozliklar haqida mas'ul xodimlarni bir nechta kanal orqali xabardor qilish funksiyasiga ega bo'lishi lozim. Qo'llab-quvvatlanadigan protokollar va yetkazish usullari:

- SMTP — Buyurtmachining pochta serveri orqali elektron pochta xabarnomalarini yuborish; autentifikatsiya protokollari (STARTTLS/SSL) va oluvchilar ro'yxatini rollar bo'yicha sozlash;

- Webhook (HTTP/HTTPS POST) —avtorizatsiya sarlavhalari (Bearer-token/HMAC) va kafolatlangan yetkazish mexanizmi (eksponensial kechikish bilan kamida 3 urinish) yordamida JSON paketlarni tashqi dasturiy interfeyslarga avtomatik yuborish. Mexanizm tashqi monitoring tizimlari (Zabbix, Grafana) va Buyurtmachining bot-platformalari bilan integratsiya qilish uchun mo'ljallangan bo'lishi lozim.

8.2.4 Tizim quyidagi ishonchlilik ko'rsatkichlariga javob berishi kerak:

- odatdagi ish rejimi — haftasiga 7 kun, sutkasiga 24 soat;
- haftalik umumiy to'xtab qolish vaqti 1 soatdan oshmasligi kerak;
- nosozlikdan keyin tiklanish vaqti 3 soatdan oshmasligi kerak;
- server qismining (frontend, backend va ma'lumotlar bazasi serverlari) yillik foydalanish imkoniyati kamida 99,95% bo'lishi kerak;
- veb-konsolning yillik foydalanish imkoniyati kamida 99,90% bo'lishi kerak.

8.2.5 Buyurtmachi tizimlari bilan o'zaro aloqa vaqtida ulanish uzilganda tizim ma'lumotlarning yaxlitligi va to'g'riligini ta'minlashi kerak.

8.2.6 Tizim quyidagilarni taqdim etishi kerak:

- komponentlar holati monitoringi;
- unumdorlik ko'rsatkichlari;
- xatolar ko'rsatkichlari;
- navbatlar va qayta ishlash kechikishlarini nazorat qilish;
- texnik ogohlantirishlar;
- shubhali operatsiyalar bo'yicha biznes-ogohlantirishlar.

### 8.3 Joylashtirish

8.3.1 Tizim bulutli joylashtirish hamda Buyurtmachi infratuzilmasida on-premise joylashtirish imkoniyatiga ega bo'lishi lozim.

### 8.4 Xavfsizlik

8.4.1 Tizim quyidagilarni qo'llab-quvvatlashi kerak:

- foydalanuvchilarning xizmat vazifalarini (administrator, katta tahlilchi, tahlilchi, auditor, operator) hisobga olgan holda tuziladigan va sozlanadigan rolli model asosida kirish huquqlarini chegaralash;
- foydalanuvchilar/operatorlar harakatlarini, jumladan, admin panelda operatorlar bajargan harakatlarni qayd etish auditi;
- qoidalar, ro'yxatlar va ssenariylardagi o'zgarishlar auditi;
- himoyalangan API aloqasi, zarur bo'lganda TLS/mTLS;
- boshqaruv veb-interfeysiga va Tizimning barcha tugunlari orasida himoyalangan shifrlangan ulanish;
- eskirgan seansdan himoya — ma'lum vaqt davomida faollik bo'lmaganda yoki brauzer yopilganda veb-interfeys bilan nafaol ulanishni uzish;

- operatsion tizim darajasida himoya mexanizmlari (kirish huquqlarini cheklash, foydalanilmaydigan tarmoq xizmatlarini o‘chirish va hokazo);
- Tizim ma’lumotlar bazasiga tarmoq orqali kirishni cheklash;
- maxfiy ma’lumotlarni Buyurtmachi talablariga muvofiq saqlash.

8.4.4 Ma’lumotlar bazasiga kirish tasdiqlangan tarmoq yo‘nalishlari va xizmat hisob yozuvlari bilan cheklanishi kerak. Uchinchi tomon tashkilotining ma’lumotlar bazasiga bevosita ulanishiga faqat qonunchilik va Buyurtmachi ruxsat bergan holatlar hamda tartibda yo‘l qo‘yiladi; tashqi tashkilot bilan ma’lumot almashinuvi kelishilgan veb-xizmat/API orqali amalga oshirilishi kerak. Ko‘rsatilgan qo‘llanish doirasidan tashqaridagi ma’lumotlarni shifrlash parametrlari Buyurtmachi standartlari bilan belgilanadi.

8.4.5 Tizim foydalanuvchilar va Tizimning o‘zi bajargan harakatlarni avtomatik qayd etishi kerak. Jumladan, muvaffaqiyatli va muvaffaqiyatsiz kirishlar, vakolatlarni berish va o‘zgartirish, ma’lumotlarni ko‘rish va eksport qilish, ma’muriy harakatlar, qoidalar va ro‘yxatlarni o‘zgartirish, modellarni chiqarish va oldingi holatga qaytarish, API xatolari hamda integratsiya sozlamalarini o‘zgartirish qayd etiladi. Har bir hodisa uchun sana-vaqt, subyekt, manba, obyekt, harakat, natija va korrelyatsiya identifikatori saqlanishi kerak.

Jurnallar Tizim foydalanuvchilari tomonidan o‘zgartirish va o‘chirishdan himoyalangan bo‘lishi kerak. 3759-son Nizom talablariga tegishli jurnallar ushbu Nizomda belgilangan muddatdan kam bo‘lmagan muddat davomida saqlanishi kerak; boshqa muddatlarni Buyurtmachi belgilaydi. Tizim kelishilgan hodisalarni QRadar SIEM tizimiga uzatishi va SOAR bilan kelishilgan ma’lumot almashinuvini qo‘llab-quvvatlashi kerak. Guardium bilan integratsiya Buyurtmachi ushbu yechim mavjudligi va undan foydalanish maqsadini tasdiqlagan taqdirda amalga oshiriladi.

## 9. Ma’lumotlarning ochiqligiga qo‘yiladigan talablar

Tizim Buyurtmachiga quyidagi maqsadlar uchun dastlabki va qayta ishlangan ma’lumotlardan foydalanish imkonini berishi kerak:

- ichki tahlil;
- hisobotlarni shakllantirish;
- o‘z ML-modellarini o‘qitish;
- DWH/Data Lake bilan integratsiya;
- tashqi tekshiruvlar;
- regulyator hisobotlari.

Server resurslariga qo‘yiladigan dastlabki talablar (Sizing) quyidagicha:

| Backend nodes required                  | each CPU | VCPU | RAM | Storage, GB |
|-----------------------------------------|----------|------|-----|-------------|
| 1                                       | 3GHz     | 16   | 64  | 100         |
| ML nodes required (optional)            | each CPU | VCPU | RAM | Storage, GB |
| 1                                       | 3GHz     | 16   | 64  | 2000        |
| Elastic nodes required                  | each CPU | VCPU | RAM | Storage, GB |
| 3                                       | 3GHz     | 16   | 64  | 1500        |
| Cassandra nodes required                | each CPU | VCPU | RAM | Storage, GB |
| 3                                       | 3GHz     | 16   | 64  | 1500        |
| Administrator + monitoring + ClickHouse | each CPU | VCPU | RAM | Storage, GB |

|                                                                                                              |                                       |                                                     |     |             |
|--------------------------------------------------------------------------------------------------------------|---------------------------------------|-----------------------------------------------------|-----|-------------|
| 1                                                                                                            | 3GHz                                  | 16                                                  | 64  | 500         |
| Risk Hub (tranzaksion modul)                                                                                 | each CPU                              | VCPU                                                | RAM | Storage, GB |
| 3                                                                                                            | 3GHz                                  | 16                                                  | 32  | 1000        |
| Additional data storage required (5 yil davomida saqlash)                                                    | Storage, GB                           |                                                     |     |             |
|                                                                                                              | 300                                   |                                                     |     |             |
| Additional backups storage required (kritik nosozlik holatida Tizim virtual mashinalarini to'liq zaxiralash) | (tanlash uchun 2 ta sxema) Xotira, GB |                                                     |     |             |
|                                                                                                              | Minimal qiymat                        | 1 nusxa<br>(RTO muhim)                              |     | 6000        |
|                                                                                                              | Tavsiya etiladi                       | 3 ta to'liq nusxa<br>(deduplikatsiyali GFS sxemasi) |     | 12000       |

kelishuvchilar: B.Shamsiev, J.Yusupov, Z.Orifkhojayev

<https://hujjat.brb.uz/?pin=rK43aB63&id=eac35809-744e-48a9-b798-ed161ab8a9f3>