

«Universal Mobile Systems»  
Mas'uliyati cheklangan jamiyati

Общество с ограниченной  
ответственностью  
«Universal Mobile Systems»

O'zbekiston, 100000  
Toshkent shahri, Amir  
Temur shoh ko'chasi, 24.  
Tel: (+99897) 403 83 35  
Faks: (+99871) 235 81 60,  
e-mail: info@mobi.uz  
www.mobi.uz

## TASDIQLAYMAN

“UMS” MChJ Axborot xavfsizligi  
va rejim bo'yicha direktori



B.A. Olmatov

2026-yil “ 08 ” anprel

Oxirgi tugunlarni (oxirgi nuqtalarni) himoya qilish EDR/XDR tizimini  
yetkazib berish, o'rnatish va ishga tushirishga doir

## TEXNIK TOPSHIRIQ

“UNIVERSAL MOBILE SYSTEMS” MChJ ehtiyojlari uchun



## Mundarija

1	Umumiy ma'lumotlar .....	3
2	Loyihani amalga oshirish uchun asos.....	3
3	Ijrochidan talab etiladigan ishlar, xizmatlar ro'yxati va ularning hajmi (miqdori).....	3
4	Ishlarni bajarish va xizmatlar ko'rsatish joyi .....	4
5	Tizimga qo'yiladigan texnik talablar.....	5
6	Ijrochiga qo'yiladigan talablar.....	9
7	Ishlarni bajarish va xizmatlarni ko'rsatishda xavfsizlikka oid talablar .....	10
8	Bajarilgan ishlar va ko'rsatilgan xizmatlar natijalari bo'yicha texnik hamda boshqa hujjatlarni topshirishga oid talablar.....	10
9	Buyurtmachi xodimlarini o'qitishga qo'yiladigan talablar .....	11
10	Kafolat majburiyatlari.....	11
11	Servis yordami ko'rsatish shartlari va texnik qo'llab-quvvatlash .....	11
12	Texnik ko'makka doir talablar .....	12
13	Ishlar, xizmatlar va ularni ko'rsatish shartlariga doir boshqa talablar .....	13
14	Qo'llaniladigan atamalar va qisqartmalar.....	14
15	Ilovalar ro'yxati .....	15



## **1 Umumiy ma'lumotlar**

Mazkur Texnik topshiriqda loyihani umuman "to'liq tayyor holda topshirish" shartlari asosida amalga oshirish uchun dasturiy ta'minot va xizmatlarni xarid qilish bo'yicha tender va/yoki tanlov e'lon qilish maqsadida Buyurtmachining dasturiy ta'minot tarkibiga bo'lgan talablarini bayon etish uchun yetarli bo'lgan Oxirgi tugunlarni (oxirgi nuqtalarni) himoya qilish EDR/XDR tizimiga (keyingi o'rinlarda – Tizim, AT) qo'yiladigan talablar keltirilgan.

Axborotlashtirish obyektining tavsifi 1-ilovada keltirilgan.

### **1.1 Bajariladigan ishlar va ko'rsatiladigan xizmatlarning nomi**

Loyihaning to'liq nomi: Oxirgi tugunlarni (oxirgi nuqtalarni) himoya qilish tizimi EDR/XDR (matnda keyingi o'rinlarda – Tizim).

Ishlar Buyurtmachining infratuzilmasi va maydonchasida bajariladi.

Mazkur Texnik topshiriq doirasida Ijrochi dasturiy ta'minotni yetkazib berish, EDR/XDR dasturiy majmuasini integratsiya qilish va foydalanishga topshirish bo'yicha tijorat taklifini taqdim etishi kerak.

### **1.2 Bajariladigan ishlar va ko'rsatiladigan xizmatlardan foydalanish maqsadlari**

Loyihaning asosiy maqsadi – "UMS" MChJ infratuzilmasida Oxirgi tugunlarni (oxirgi nuqtalarni) himoya qilish tizimi EDR/XDR dasturiy ta'minotini joriy etishdir.

Tizim tomonidan hal etiladigan asosiy vazifalar:

- oxirgi nuqtalar va tarmoq infratuzilmasida murakkab kiberhujumlar hamda anomaliyalarni aniqlash;
- turli manbalardan xavfsizlik telemetriyasini markazlashgan holda yig'ish, o'zaro bog'lash va tahlil qilish;
- maqsadli hujumlarni, zararli faoliyatni va tizimga putur yetkazishga urinishlarni barvaqt aniqlash;
- axborot xavfsizligi hodisalarini aniqlash va ularga javob qaytarish vaqtini qisqartirish;
- hodisalarga javob qaytarishni avtomatlashtirish va hujumlarning biznes jarayonlariga ta'sirini minimallashtirish;
- hujumlar zanjiri va tahdidlar kontekstini vizuallashtirish orqali hodisalar shaffofligini oshirish;
- hodisalarni tekshirish va raqamli forenzikani qo'llab-quvvatlash;
- "UMS" MChJ AT-infratuzilmasining umumiy himoyalanganlik darajasini oshirish.

Tizimning asosiy vazifasi – kibertahdidlar xatarlarini minimallashtirish va ularning biznes jarayonlariga ta'sirini kamaytirish maqsadida "UMS" MChJ AT-infratuzilmasida axborot xavfsizligi hodisalarini markazlashgan holda aniqlash, tahlil qilish va ularga javob qaytarishni ta'minlashdan iborat.

## **2 Loyihani amalga oshirish uchun asos**

Xavfsizlik va rejim departamentining 2026-yil uchun rejalashtirilgan rivojlanish rejasi ("UMS" MChJning 2026-yil uchun tasdiqlangan Biznes-rejasi va Byudjeti).

## **3 Ijrochidan talab etiladigan ishlar, xizmatlar ro'yxati va ularning hajmi (miqdori).**

Yakuniy tugunlarni (oxirgi nuqtalarni) himoya qilish bo'yicha EDR/XDR tizimini joriy etish Buyurtmachining mavjud AT-infratuzilmasi ishiga ziyon yetkazmagan holda, mavjud qurilmalarni dastlabki yuzaki ko'rikdan o'tkazgan holda Buyurtmachining mas'ul shaxslari bilan birgalikda amalga oshirilishi kerak. Har qanday korporativ tizimlarni to'xtatishni talab qiladigan barcha ishlar Buyurtmachi bilan oldindan kelishib olinishi shart.

Loyiha doirasida Ijrochi tomonidan quyidagi ish bosqichlari bajarilishi lozim:



- tayyorgarlik bosqichi;
- ishga tushirish-sozlash va integratsiya ishlari;
- Buyurtmachi xodimlarini o'qitish.

### 3.1 Tayyorgarlik bosqichi

Bu bosqich Buyurtmachining Loyiha uchun mas'ul xodimlari bilan hamkorlik qilishni va Buyurtmachining IT-infratuzilmasini birgalikda o'rganishni o'z ichiga oladi. Ushbu bosqichda xodimlar quyidagilarni aniqlashi lozim:

- Buyurtmachining tarmoq topologiyasining eng muhim tafsilotlarini;
- Tizimni joriy etish jarayonida Buyurtmachi va Ijrochining mas'uliyat doiralarini;
- Tizim himoya qiladigan yakuniy nuqtalar sonini.

### 3.2 Ishga tushirish-sozlash va integratsiya ishlari

Buyurtmachining Loyiha uchun mas'ul xodimlari bilan hamkorlikda amalga oshiriladigan ishga tushirish-sozlash ishlari quyidagilarni o'z ichiga oladi:

- Tizimning dasturiy qismini o'rnatish va sozlash;
- Buyurtmachining tarmoq infratuzilmasiga integratsiya qilish;
- monitoring uchun zarur bo'lgan modullarni faollashtirish;
- zarur litsenziyalarni faollashtirish.

Buyurtmachining AT infratuzilmasi obyektlari bilan bog'liq bo'lmagan xatolar sababli Tizim ishida nosozliklar aniqlangan taqdirda, Ijrochi bajarilgan ishlar dalolatnomasi imzolanmasdan oldin mahsulotning funksionaliga tuzatishlar kiritish majburiyatini o'z zimmasiga oladi.

### 3.3 Tizimni nazorat qilish va qabul qilib olish tartibi

Tizimni qabul qilib olish qabul sinovlarini o'tkazish yo'li bilan amalga oshirilishi kerak. Qabul sinovlari Buyurtmachi va Ijrochining vakillari tomonidan o'tkaziladi.

Qabul sinovlarining maqsadi Tizim komponentlarining ishga yaroqliligini hamda ularning Texnik topshiriq talablariga muvofiqligini tasdiqlashdan iborat.

Sinovlarning turlari, tarkibi, hajmi va usullari qabul sinovlari dasturi bilan belgilanishi lozim. Qabul sinovlari dasturi Ijrochi tomonidan ishlab chiqiladi va sinovlar boshlanishidan kamida 1 kun oldin Buyurtmachi bilan kelishib olinadi.

Qabul sinovlari natijalari qabul komissiyasi a'zolari imzolaydigan bayonnoma bilan rasmiylashtirilishi kerak. Qabul sinovlari muvaffaqiyatli o'tkazilganidan so'ng Qabul sinovlarini yakunlash to'g'risidagi dalolatnoma imzolanadi.

Qabul sinovlari vaqtida kamchiliklar, nuqsonlar yoki Texnik topshiriq talablaridan boshqa chetga chiqishlar aniqlansa, tegishli faktlar bayonnomada qayd etilishi lozim, unda, jumladan, quyidagilar ko'rsatiladi:

- kamchiliklar (nuqsonlar) ro'yxati;
- qayd etilgan kamchiliklarning tizimning ishga yaroqliligiga ta'sir darajasi;
- kamchiliklarni (nuqsonlarni) bartaraf etish uchun talab etiladigan muddatlar.

Kamchiliklar, nuqsonlar yoki tizimga qo'yiladigan talablardan boshqa og'ishlar bartaraf etilgan paytdan boshlab besh ish kuni ichida qabul komissiyasi tegishli komponentning takroriy qabul sinovlarini o'tkazishi va Tizimni doimiy foydalanishga qabul qilishi shart.

### 3.4 Xodimlarni o'qitish.

Ushbu Texnik topshiriqning 9-bandiga muvofiq o'qitish.

## 4 Ishlarni bajarish va xizmatlar ko'rsatish joyi

Ijrochi quyidagi manzil bo'yicha dasturiy ta'minotni yetkazib berish, o'rnatish va sozlashni



ta'minlashi kerak: O'zbekiston Respublikasi, Toshkent shahri, 100000, Amir Temur shoh ko'chasi, 24-uy, "UMS" MChJ markaziy ofisi.

Tizimni yetkazib berish muddatlari Buyurtmachi va Ijrochi o'rtasidagi Shartnomada belgilanadi, lekin u Buyurtmachi bilan Ijrochi o'rtasida shartnoma munosabatlari imzolangan kundan boshlab 90 kalendar kundan oshmasligi lozim.

## **5 Tizimga qo'yiladigan texnik talablar**

Tizimga quyidagi texnik talablar qo'yiladi.

### **5.1 Arxitektura va yetkazib berish modeli**

5.1.1 Yechim Extended Detection and Response (XDR) sinfiga mansub bo'lishi hamda yagona platforma doirasida so'nggi nuqtalar, tarmoq manbalari va bulutli muhitlardan kelib tushadigan xavfsizlik hodisalarining o'zaro bog'liqligini (korrelyatsiyasini) ta'minlashi lozim.

5.1.2 Platforma 24/7 rejimida ishlash imkoniyatiga ega markazlashtirilgan boshqaruv konsolini qo'llab-quvvatlashi kerak.

5.1.3 Bulutli modeldan (SaaS) foydalanishga quyidagi shartlar asosida yo'l qo'yiladi:

- Buyurtmachining ma'lumotlarini ajratish (izolyatsiya qilish);
- ma'lumotlarni sertifikatlangan ma'lumotlar markazlarida joylashtirish;
- ma'lumotlarni uzatish va saqlashda shifrlashdan foydalanish.

5.1.4 Yechim arxitekturasini xizmatlarni to'xtatmagan holda gorizontol kengayishni (masshtablashni) ta'minlashi kerak.

### **5.2 So'nggi nuqtalarni himoya qilish (Endpoint Protection & EDR)**

5.2.1 Yechim quyidagilardan foydalangan holda so'nggi nuqtalarni (Windows, Linux, macOS) himoya qilishni ta'minlashi kerak:

- xulq-atvor tahlili;
- mashinaviy o'qitish;
- hujumlar zanjiri tahlili.

5.2.2 So'nggi nuqta agenti alohida komponentlarni o'rnatishni talab etmasdan, oldini olish, aniqlash va chora ko'rish funksiyalarini o'zida birlashtirishi lozim.

5.2.3 Quyidagi funksiyalar qo'llab-quvvatlanishi kerak:

- zaifliklardan foydalanishning oldini olish;
- faylli va faylsiz hujumlardan himoya qilish;
- zararli skriptlardan himoya qilish;
- tovon talab qiluvchi dastur (ransomware) turidagi hujumlarni aniqlash.

5.2.4 Agent tizim resurslarini kam iste'mol qilishi va avtomatik yangilanishni qo'llab-quvvatlashi lozim.

### **5.3 XDR-korrelyatsiya va tahlil**

5.3.1 Yechim yagona hodisa doirasida turli xavfsizlik manbalaridan olingan telemetriya ma'lumotlarining avtomatik korrelyatsiyasini ta'minlashi kerak.

5.3.2 Quyidagilarga asoslangan tahlil qo'llab-quvvatlanishi lozim:

- xulq-atvor modellariga;
- mashinaviy ta'limga;
- tajovuzkorning taktikalari, texnikalari va protseduralari (TTP) tahliliga.

5.3.3 Platforma hujum zanjirining (attack storyline) vizual tasvirini taqdim etishi, unda komprometatsiyaning birlamchi vektori va tajovuzkorning keyingi qadamlari ko'rsatilishi kerak.

5.3.4 Avtomatik korrelyatsiya va kontekstli tahlil hisobiga yolg'on ijobiy natijalar sonini kamaytirish mexanizmi joriy etilishi lozim.

### **5.4 Tarmoq xavfsizligi bilan integratsiya**

Chora ko'rish ssenariylari doirasida tarmoq ulanishlarini,



IP-manzillar va domenlarni avtomatik bloklash imkoniyati ta'minlanishi kerak.

#### 5.5 Chora ko'rish va avtomatlashtirish (SOAR funksiyalari)

5.5.1 Yechim xavfsizlik hodisalariga chora ko'rishning avtomatlashtirilgan ssenariylarini ta'minlashi kerak, jumladan:

- chekka nuqtani izolyatsiyalash;
- zararli jarayonlarni yakunlash;
- fayllarni xesh bo'yicha bloklash;
- forenzika artefaktlarini yig'ish.

5.5.2 Dasturiy kod yozmasdan maxsus (kastom) munosabat bildirish ssenariylarini yaratish imkoniyati qo'llab-quvvatlanishi lozim.

5.5.3 Munosabat bildirish ham avtomatik, ham qo'lda boshqariladigan rejimlarda mavjud bo'lishi kerak.

#### 5.6 Kiberxavflar tahlili (Threat Intelligence)

5.6.1 Yechim real vaqtga yaqin rejimda yangilanadigan kiberxavflarning global manbalaridan foydalanishi lozim.

5.6.2 Insidentlarning komprometatsiya indikatorlari (IoC) bilan avtomatik korrelyatsiyasi qo'llab-quvvatlanishi kerak.

5.6.3 Platforma chetdan xizmatlarni ulashga ehtiyoj sezmasdan, insidentlarni tahdidlar haqidagi kontekstli ma'lumotlar bilan boyitishni ta'minlashi lozim.

#### 5.7 Boshqaruv, hisobotdorlik va audit

5.7.1 Platforma quyidagilarni ta'minlashi lozim:

- rollarga asoslangan kirish modeli (RBAC);
- foydalanuvchilar harakatlari auditi;
- insidentlar tarixini 12 oygacha saqlash.

5.7.2 Quyidagilarni shakllantirish imkoniyati qo'llab-quvvatlanishi kerak:

- operativ asboblarni panellari (dashboard);
- AX bo'limi rahbariyati uchun hisobotlar;
- ma'lumotlarni tashqi SIEM tizimlariga yuklab olish.

5.7.3 Boshqaruv interfeysi ingliz tilini qo'llab-quvvatlashi kerak.

#### 5.8 IT-infratuzilmasi bilan integratsiya

5.8.1 Yechim quyidagilar bilan integratsiyani qo'llab-quvvatlashi lozim:

- REST API-ni qo'llab-quvvatlaydigan platformalar;
- Active Directory / LDAP;
- ogohlantirishlar va audit jurnallarini yuborish uchun tashqi Syslog qabul qilgichlari.

5.8.2 Ommaviy, hujjatlashtirilgan REST API mavjud bo'lishi shart.

#### 5.9 Ekspluatatsiya talablari

– Signaturalar, detektlash modellari va tahlil komponentlari avtomatik tarzda yangilanib borishi kerak.

- Yechim komponentlarni yangilash vaqtida uzluksiz himoyani ta'minlashi lozim.
- Vender 24x7 darajasidan kam bo'lmagan texnik yordamni ta'minlashi shart.

#### 5.10 Masofadan ulanish imkoniyatlari

Taklif etilayotgan yechim oxirgi qurilmada real vaqt rejimida ulanish orqali buyruqlarni to'liq qo'llab-quvvatlaydigan buyruqlar satrini ishga tushirish imkoniyatini ta'minlashi lozim.

#### 5.11 Sertifikatlash:

Taklif etilayotgan yechim ISO 27001 sertifikatiga ega bo'lishi kerak.

#### 5.12 Qurilmalarni nazorat qilish

Taklif etilayotgan yechim quyidagilarni ta'minlashi lozim:

- Windows va macOS operatsion tizimlari uchun shifrlashni boshqarish;
- Windows va macOS operatsion tizimlari uchun USB qurilmalarni nazorat qilish



funksiyalari.

#### 5.13 Ishlash unumdorligi va kengayuvchanlikka doir talablar

5.13.1 Yechim quyidagilardan keladigan telemetriyani barqaror qayta ishlashni ta'minlashi lozim:

- bitta mantiqiy tenant doirasida kamida 10 000 ta oxirgi nuqta;
- arxitekturasini o'zgartirmasdan keyinchalik kengaytirish imkoniyati bilan.

5.13.2 Platforma xavfsizlik hodisalarini real vaqtga yaqin rejimda oqimli qayta ishlashni qo'llab-quvvatlashi kerak.

5.13.3 Tahliliy va korrelyatsion mexanizmlarning ishlash unumdorligi quyidagi hollarda pasaymasligi kerak:

- xulq-atvor tahlili yoqilganda;
- mashinaviy ta'limdan foydalanilganda;
- avtomatik javob ssenariylari faollashtirilganda.

5.13.4 Oxirgi nuqta agenti o'rtacha hisobda quyidagilardan ortiq resurs sarflamasligi kerak:

- shtat rejimida protsessor (CPU) resurslarining 5 %i;
- 500 MB tezkor xotira;
- 1 GB disk maydoni.

5.13.5 Yechim ma'lumotlar va telemetriyani yo'qotmagan holda tahlil va boshqaruv komponentlarining ishdan chiqishga bardoshlilikini ta'minlashi lozim.

#### 5.14 AT va XT tizimlari bilan integratsiyaga doir talablar

5.14.1 Hisob qaydnomalarini boshqarish tizimlari bilan integratsiya

a) Yechim quyidagilar bilan integratsiyani qo'llab-quvvatlashi kerak:

- Microsoft Active Directory;
- LDAP-ga mos kataloglar.

b) Integratsiya quyidagilarni ta'minlashi kerak:

- foydalanuvchilar, guruhlar va rollar haqidagi ma'lumotlarni olish;
- xavfsizlik hodisalarini foydalanuvchi qaydnomalari bilan o'zaro bog'lash;
- insidentlar kontekstini yaratish uchun katalog ma'lumotlaridan foydalanish.

c) Qaydnomalarni qo'lda boshqarish zaruratisiz avtomatik sinxronlashtirish qo'llab-quvvatlanishi kerak.

5.14.2. SIEM tizimi bilan integratsiya

a) Yechim tashqi SIEM tizimlari bilan ikki tomonlama integratsiyani ta'minlashi kerak, jumladan:

- insidentlar va alertlarni uzatish;
- boyitilgan hodisalarni uzatish;

b) Integratsiya quyidagilar orqali amalga oshirilishi kerak:

- REST API;
- Syslog;
- nativ konnektorlar.

c) Yechim undan quyidagicha foydalanishni qo'llab-quvvatlashi kerak:

- SIEM uchun hodisalar manbai sifatida;
- SIEM tizimiga majburiy ulanishni talab qilmaydigan avtonom XDR-platforma

sifatida.

5.14.3. Integratsiya quyidagilarni ta'minlashi kerak:

- xavfsizlik telemetriyasini olish;
- fishing hujumlarini va qaydnomalarning komprometatsiyasini aniqlash.

5.14.4. API va kengaytiriluvchanlik

d) Yechim quyidagilar uchun ochiq, hujjatlashtirilgan REST API ni taqdim etishi kerak:

- hodisalar va insidentlarni olish;



- himoya obyektlarini boshqarish;
- javob qaytarish ssenariylarini ishga tushirish.
- e) API quyidagilarni qo'llab-quvvatlashi kerak:
  - tokenlar orqali autentifikatsiya;
  - kirish huquqlarini cheklash;
  - murojaatlarni jurnallashtirish.
- f) API va integratsiyalardan foydalanish qo'shimcha litsenziyalar xarid qilishni talab qilmasligi kerak.

#### 5.14.5. Avtomatlashtirish va orkestratsiya

- g) Yechim quyidagilar uchun ITSM tizimlari bilan integratsiyani qo'llab-quvvatlashi kerak:
  - insidentlarni avtomatik yaratish;
  - tekshiruv statuslarini uzatish;
  - javob qaytarish natijalariga ko'ra insidentlarni yopish.
- h) Quyidagilar doirasida integratsiyalardan foydalanish imkoniyati qo'llab-quvvatlanishi kerak:
  - avtomatik pleybuklar;
  - yarim avtomatik javob berish ssenariylari.
- i) Integratsiyalar dasturiy kod yozmasdan, grafik interfeys orqali sozlanishi kerak.

#### 5.14.6. Litsenziyalash va yetkazib berish jamlanmasi

5.14.6.1. Yechimni litsenziyalash litsenziyalanadigan hajmning miqdorini moslashuvchan tarzda oshirish imkoniyati bilan himoyalangan so'nggi nuqtalar soni bo'yicha amalga oshirilishi lozim.

5.14.6.2. Litsenziya narxiga quyidagilar kiritilishi lozim:

- so'nggi nuqtalarda hujumlarning oldini olish funksiyalari;
- aniqlash va javob berish funksiyalari (EDR/XDR);
- markazlashtirilgan boshqaruv konsoli;
- mashinaviy ta'lim va xulq-atvor modellariga asoslangan tahlil;
- o'rnatilgan avtomatik javob berish ssenariylari;

5.14.6.3. Quyidagilar uchun qo'shimcha to'lov undirishga

- hodisalarni korrelyatsiya qilish;
- hujumlar zanjirini vizualizatsiya qilish;
- avtomatik javob berish;
- asosiy hisobotlar va axborot panellari

yo'l qo'yilmaydi.

5.14.6.4. Litsenziya yechimdan foydalanish huquqini o'z ichiga olishi kerak:

- kecha-kunduz rejimida;
- hodisalar va voqealar soniga cheklovlarisiz.

5.14.6.5. Litsenziya doirasida quyidagilar taqdim etilishi kerak:

- signaturalarni muntazam yangilash;
- tahliliy modellarni yangilash;
- platformaning funksional komponentlarini yangilash.

5.14.6.6. Litsenziya quyidagilarni o'z ichiga olishi kerak:

- 24x7 rejimida texnik qo'llab-quvvatlash;
- bilimlar bazasi va javob berish bo'yicha tavsiyalardan foydalanish imkoniyati.

5.14.6.7. Litsenziyalash quyidagilarga bog'liq bo'lmasligi kerak:

- ishlov beriladigan trafik hajmiga;
- tahliliy qoidalar soniga;



– boshqaruv konsoli foydalanuvchilari soniga.

5.14.6.8. Obuna amal qilish muddati – uzaytirish imkoniyati bilan kamida 36 oyni tashkil etadi.

5.14.6.9. 36 oy muddatga litsenziyalar xarid qilish imkoniyati qo'llab-quvvatlanishi kerak.

#### 5.15. XDR-yechimga qo'yiladigan miqdoriy talablar

<b>№</b>	<b>Ko'rsatkich</b>	<b>Talab</b>
1	Himoyalangan so'nggi nuqtalar soni	kamida 2000 ta
2	Tayyor aniqlash qoidalari	kamida 350
3	Tayyor javob berish ssenariylari	kamida 50 ta
4	Hujumlar zanjirini avtomatik tarzda	majburiy
5	Agent tomonidan resurslar iste'moli (CPU)	ko'pi bilan 5% (shtat rejimida)
6	So'nggi nuqtalar bo'yicha litsenziyalash	majburiy, hodisalar bo'yicha cheklovlarisiz
7	Platforma ishchanligi bo'yicha SLA	kamida 99,9%

#### 5.16. Boshqa axborot tizimlari bilan o'zaro hamkorlikka oid talablar

Tizim mahalliy manbalar va segmentlangan tarmoqlardan ma'lumotlarni agregatsiya qilish, oldindan ishlov berish va boshqaruv konsoliga xavfsiz uzatish uchun mo'ljallangan dasturiy komponentni (virtual applayans) joylashtirish uchun VMware ESXi virtual infratuzilmasini qo'llab-quvvatlashi kerak.

#### 5.17. Tizimning ishlash rejimlariga qo'yiladigan talablar

Tizimning asosiy ishlash rejimi avtomatlashtirilgan bo'lib, administrator tomonidan boshqariladi. Tizim quyidagi rejimlarda ishlash imkoniyatini ta'minlashi lozim:

- shtat rejimi (uzluksiz, kecha-yu kunduz ishlash);
- avtonom rejim (tizim komponentlari o'rtasida yoki tashqi tarmoqlar bilan aloqa uzilgan hollarda, konfiguratsiyaviy va arxiv ma'lumotlaridan foydalanish uchun).

#### 5.18. Ijrochi xodimlarining soni va malakasiga qo'yiladigan talablar.

Dasturiy ta'minot majmuasini yetkazib berish va Tizimning ishga tushirilishini ta'minlash uchun Ijrochi xodimlari tarkibida kamida bitta texnik yordam muhandisi shtat birligi bo'lishi shart.

Texnik yordam muhandisi Buyurtmachida Tizimga rejali texnik va avariya xizmat ko'rsatish uchun zarur bo'lgan hajmda bilim ega bo'lishi kerak.

#### 5.19. Audit, monitoring va hisobotga oid talablar

Tizim foydalanuvchilar va ma'murlarning harakatlari auditini, xavfsizlik va ekspluatatsiya hodisalarining qayd etilishini, shuningdek, komponentlarning holati va mavjudligi monitoringini ta'minlashi lozim.

Tizim shubhali faollik aniqlanganda bildirishnomalar yuborish imkoniyati bilan real vaqt rejimida auditni qo'llab-quvvatlashi kerak.

Barcha hodisalar sana va vaqt, harakat manbasi va natijasi ko'rsatilgan holda jurnalga qayd etib borilishi lozim.

Jurnallarning ruxsatsiz o'zgartirilishi va o'chirilishidan himoyalaniishi ta'minlanishi kerak.

Hisobotlar so'rov bo'yicha va/yoki jadval asosida taqdim etilishi hamda ularni standart formatlarga (PDF, CSV) eksport qilish imkoniyati mavjud bo'lishi kerak.

Audit va monitoring ma'lumotlarini (loglarni) saqlash muddati – kamida 12 oy.

### 6. Ijrochiga qo'yiladigan talablar

#### 6.14. Ijrochiga qo'yiladigan umumiy talablar



Ijrochi quyidagi talablarga javob berishi kerak:

- ko'rsatilgan xizmatlarni taqdim etish (dasturiy ta'minot yetkazib berish) bo'yicha kamida 3 yillik tasdiqlangan ish tajribasiga ega bo'lishi;
- vakolatli hamkor bo'lishi, shuningdek, sotilayotgan/joriy etilayotgan dasturiy ta'minotdan foydalanish va uni joriy etish huquqlarini oxirgi foydalanuvchilarga tarqatish uchun hujjatli tasdiqnomaga ega bo'lishi;
- to'lovga layoqatsiz yoki bankrot bo'lmasligi, tugatish jarayonida turmasligi, mol-mulki xatlanmagan bo'lishi, shuningdek, iqtisodiy faoliyati to'xtatib qo'yilmagan bo'lishi;
- o'z tarkibida mazkur dasturiy ta'minotni o'rnatish, sozlash, ishlatish va unga texnik yordam ko'rsatish bo'yicha malakasini tasdiqlovchi sertifikatlariga ega kamida 2 (ikki) nafar mutaxassisning mavjud bo'lishi;
- Ijrochi "Kiberxavfsizlik markazi" DUKdan olingan axborot va kiberxavfsizlikni ta'minlash talablariga muvofiqlik bo'yicha ekspertizadan o'tish niyati to'g'risida kafolat xatini yoxud ekspertizadan o'tganligi haqidagi sertifikatni taqdim etish majburiyatini o'z zimmasiga oladi.

Ijrochi O'zbekiston Respublikasining amaldagi qonunchiligida maxfiy axborotni o'z ichiga olgan hujjatlar va ma'lumotlar bilan ishlashga doir belgilangan talablarga rioya etishi hamda xizmatlar ko'rsatish jarayonida o'ziga ma'lum bo'lib qolgan maxfiy axborotni oshkor qilmasligi shart.

6.15. Ijrochi o'zining yuqorida ko'rsatilgan talablarga muvofiqligini tasdiqlovchi quyidagi hujjatlarni taklif tarkibiga kiritishi lozim:

- ishlab chiqaruvchi kompaniya bilan hamkorlik maqomi mavjudligi to'g'risidagi rasmiy xat nusxasi;
- ishlab chiqaruvchi kompaniya tomonidan berilgan kamida 2 ta muhandislik sertifikatining nusxalari.
- so'nggi 3 yil ichida amalga oshirilgan AT-loyihalar ro'yxati.

6.16. Ishlab chiqaruvchiga qo'yiladigan talablar

VENDOR kompaniyasi bozorda kamida 5 yillik faoliyat tajribasiga hamda O'zbekiston bozorida vakolatli hamkorlarga ega bo'lishi shart.

## **7. Ishlarni bajarish va xizmatlarni ko'rsatishda xavfsizlikka oid talablar**

Ishlarni bajarishda quyidagi xavfsizlik talablari qo'yiladi:

7.14. Dasturiy ta'minot majmuasini o'rnatish, sozlash va foydalanishga topshirish bo'yicha barcha ishlar elektr xavfsizligi talablariga, shuningdek, amaldagi ichki me'yoriy hujjatlarga muvofiq bajarilishi kerak.

7.15. Ijrochi ishlarni bajarish jarayonida axborot xavfsizligi talablariga rioya qilinishi uchun to'liq javobgar bo'ladi.

7.16. Ishlarni faqat Buyurtmachi tomonidan tasdiqlangan, kelishilgan muddatlarda va vaqt oralig'ida bajarishga ruxsat etiladi.

## **8. Bajarilgan ishlar va ko'rsatilgan xizmatlar natijalari bo'yicha texnik hamda boshqa hujjatlarni topshirishga oid talablar**

Tizimni joriy etish va sanoat miqyosida foydalanishga topshirish yakunlangach, Ijrochi ishchi (ijro) hujjatlarini – Tizimning amalda joriy qilingan holatini **aks ettiruvchi hujjatlarni** tayyorlashi **shart**.

Hujjatlar quyidagi ko'rinishda taqdim etiladi:

- qog'ozda 2 (ikki) nusxada;
- elektron shaklda (DOCX va PDF formatlarida).

Hujjatlarning majburiy tarkibi:



- Tizimning umumiy tavsifi;
- arxitektura va tarmoq sxemalari;
- dasturiy komponentlarning ro'yxati va konfiguratsiyasi;
- Buyurtmachining infratuzilmasi bilan integratsiya tavsifi;
- tarmoq manzillari (IP, portlar, protokollar);
- foydalanish bo'yicha qisqacha yo'riqnoma;
- axborot xavfsizligi bo'yicha amalga oshirilgan chora-tadbirlar tavsifi.

Hujjatlar dolzarb, to'liq va Tizimning haqiqiy realizatsiyasiga mos bo'lishi, shuningdek, Ijrochini jalb etmagan holda undan foydalanish uchun yetarli bo'lishi kerak.

## 9. Buyurtmachi xodimlarini o'qitishga qo'yiladigan talablar

Ushbu Texnik topshiriq doirasida Ijrochi quyidagi o'qitish dasturlarini ta'minlaydi;

a) Buyurtmachining axborot xavfsizligi bo'yicha ikki nafar mutaxassisini ushbu majmuani boshqarish yuzasidan sertifikatlangan o'qitish.

Tinglovchilar soni: 2 kishi.

Shakli: kunduzgi / onlayn, amaliy mashg'ulotlar bilan.

O'qitish tili: rus / ingliz.

Materiallar: taqdimotlar, yo'riqnomalar, laboratoriya ishlari.

O'qitish yakunlari bo'yicha Ijrochi quyidagilarni taqdim etadi:

- o'quv materiallarini;
- mashg'ulotlar yozuvlarini;
- o'qitishdan o'tganlikni tasdiqlovchi hujjatlarni (sertifikatlar).

b) Tizim foydalanuvchilarini o'qitish.

Tinglovchilar soni: 10 kishigacha.

Shakli: namoyishli + amaliy.

O'qitish maqsadi: tizimning funksional imkoniyatlarini o'zlashtirish.

O'qitishdan o'tganlik fakti tegishli sertifikat bilan tasdiqlanishi kerak.

O'qitish dasturi va vaqti Buyurtmachi bilan oldindan kelishilishi lozim.

## 10. Kafolat majburiyatlari

Ijrochi, ishlab chiqaruvchi tomonidan hujjatlarda belgilangan dasturiy ta'minotdan foydalanish qoidalariga rioya qilingan va o'rnatilgan dasturiy ta'minot ishiga ruxsatsiz aralashuv bo'lmagan taqdirda, bajarilgan ish sifatining texnik topshiriqqa hamda Buyurtmachi tomonidan ko'rsatilgan talablarga mos kelishini kafolatlashi shart.

Tizimni joriy etish bo'yicha bajarilgan ishlarga beriladigan kafolat muddati **36 (o'ttiz olti) oyni** tashkil etishi kerak va u Tomonlar ishlarni topshirish-qabul qilish dalolatnomasini imzolagan kundan boshlab hisoblanadi.

Dasturiy ta'minotga obuna amal qilish muddati – **36 (o'ttiz olti) oy**.

Tajriba tariqasida ishlatish davri 1 (bir) oyni tashkil etishi va Tomonlar ishlarni topshirish-qabul qilish dalolatnomasini imzolagan kundan boshlab hisoblanishi lozim.

## 11. Servis yordami ko'rsatish shartlari va texnik qo'llab-quvvatlash

Ishlab chiqaruvchining servis yordami ko'rsatish muddati – Dasturiy ta'minot joriy etilgan paytdan boshlab **36 (o'ttiz olti) oy**. Dasturiy komponentlarga servis yordami ham Ishlab chiqaruvchi, ham Ijrochi tomonidan ko'rsatilishi kerak.

Ijrochi hujjatlar, yangilanishlar va relizlarni mustaqil ravishda yuklab olish uchun dasturiy ta'minot ishlab chiqaruvchisi bo'lgan kompaniyaning axborot resurslari to'g'risidagi ma'lumotlarni



taqdim etishi shart.

Ijrochi Ishlab chiqaruvchining saytida, Buyurtmachining shaxsiy kabinetida dasturiy ta'minotning identifikatsiya ma'lumotlarini bog'lashni amalga oshiradi.

Dasturiy ta'minotni servis bo'yicha qo'llab-quvvatlash ishlari quyidagilarni o'z ichiga olishi lozim:

- a) EDR/XDR tizimining dasturiy qismi uzluksiz ishlashini ta'minlash:
  - Buyurtmachining apparat (server) resurslaridan foydalanishni optimallashtirish uchun Tizim parametrlarini sozlash;
  - xavfsizlik siyosatini boshqarish uchun Tizim parametrlarini sozlash;
  - yangilanishlar o'tkazilgandan so'ng Tizimning shtat rejimida ishlashini sinovdan o'tkazish.
- b) Buyurtmachining mavjud boshqaruv va monitoring tizimlari bilan integratsiya qilish.
- c) Tizim miqyosini kengaytirish bo'yicha maslahatlar berish.
- d) Dasturiy ta'minot ishlab chiqaruvchisining portalidan foydalanish (yangilanishlarni yuklab olish, texnik forum va hujjatlardan foydalanish imkoniyati).
- e) Tizim yangilangan taqdirda, Tizimning 2 nafar ma'muriga yo'riqnoma o'tkazish.
- f) "UMS" MChJ talabiga binoan, Tizimning ishlashi bilan bog'liq yuzaga kelgan muammolarni hal etish, maslahatlar berish uchun mutaxassisni VPN orqali ulash.
- g) Tizimning ish qobiliyatini tiklash:
  - dasturiy vositalardagi nosozlikdan so'ng, 2 ish kunidan kechiktirmay Tizimning ish qobiliyatini shtat rejimida tiklash;
  - dasturiy majmuani qayta sozlash, qayta konfiguratsiyalash, yangilash va/yoki to'liq qayta o'rnatish, shuningdek, nosozlikka olib kelgan sabablarni bartaraf etish (nosozlik kompaniya mahsulotlari sababli yuzaga kelgan taqdirda);
  - tiklash ishlarini o'tkazish uchun nosozlik vaqtida Tizimni o'chirib qo'yish imkoniyati (aylanma rejim);
  - dasturiy nosozliklar, elektr ta'minoti uzilishi va hokazolardan so'ng Tizim faolligini tiklash;
  - zaxira nusxalardan ma'lumotlarni tiklash amaliyotlari.
  - bajarilgan ishlar to'g'risida hisobotlar taqdim etish.

## **12. Texnik ko'makka doir talablar**

12.1 Ijrochi yetkazib beriladigan dasturiy majmuani 36 oy davomida texnik ko'mak bilan ta'minlashi shart.

12.2 Texnik ko'mak dasturiy ta'minot ishlab chiqaruvchisi yoki ishlab chiqaruvchining vakolatli servis hamkori tomonidan ko'rsatilishi lozim.

12.3 Texnik ko'mak darajasi masalani ishlab chiqaruvchi darajasiga (L3) eskalatsiya qilish imkoniyatini nazarda tutishi kerak.

12.4 Texnik ko'mak quyidagilarga nisbatan tatbiq etilishi lozim:

- dasturiy qism (software).

12.5 Texnik ko'mak quyidagi rejimda taqdim etilishi kerak:

- 24x7x365 – o'ta muhim insidentlar uchun;
- kamida 8x5 – o'ta muhim bo'lmagan insidentlar uchun (Buyurtmachi bilan kelishuvga ko'ra).

12.6 Insidentlarga munosabat bildirish vaqti:

- O'ta muhim (P1): 15–30 daqiqadan oshmasligi kerak;
- Yuqori (P2): 1 soatdan oshmasligi kerak;
- O'rta (P3): 4 soatdan ko'p bo'lmagan vaqtda;
- Past (P4): 1 ish kunidan ko'p bo'lmagan vaqtda.

12.7 Tiklash (yoki aylanma yechim) vaqti:



- P1: 4 soatdan ko'p bo'lmagan vaqtda;
- P2: 8 soatdan ko'p bo'lmagan vaqtda;
- P3: 2 ish kunigacha;
- P4: Buyurtmachi bilan kelishuvga ko'ra.

12.8 Ijrochi texnik qo'llab-quvvatlashga (TQQ) so'rovlarni ro'yxatdan o'tkazish uchun yagona kanalni taqdim etishi kerak:

- Service Desk (portal);
- ishonch telefoni;
- elektron pochta (e-mail).

### 13. Ishlar, xizmatlar va ularni ko'rsatish shartlariga doir boshqa talablar

13.14. Litsenziyalar/Dasturiy ta'minot tomonlar vakillari ishtirokida jismoniy inventarizatsiya o'tkazilganidan hamda dasturiy ta'minotning ishlash qobiliyati tekshirilganidan va tuzilgan shartnomaga muvofiq qabul qilish-topshirish dalolatnomasi imzolanganidan so'ng qabul qilingan hisoblanadi. Ushbu Texnik topshiriqda va uning ilovalarida ko'rsatilmagan boshqa shartlar shartnomada keltiriladi.

13.15. Xizmatlarni ko'rsatishning majburiy sharti — Buyurtmachining amaldagi ichki tartib qoidalariga, nazorat-o'tkazish rejimiga, ichki nizomlari, yo'riqnomalari va talablariga rioya qilishdir. Buyurtmachi bu haqda Ijrochini xabardor qiladi. Buyurtmachi Ijrochiga dasturiy ta'minotga obunani faollashtirish bilan bog'liq bildirilgan muammolarni hal qilish bo'yicha Ijrochi bilan aloqa qilishga vakolatli xodimlarning ro'yxati va aloqa ma'lumotlarini taqdim etadi.

#### 13.16. Butlashga doir talab

Tizim joriy Texnik topshiriq doirasida taklif etilayotgan yechimning to'laqonli ishlashi uchun to'liq butlangan bo'lishi kerak. Dasturiy ta'minotning narxi to'liq butlanishdan kelib chiqib shakllantirilishi lozim.

#### 13.17. Integratsiyaga doir talab

Integratsiyada Buyurtmachi infratuzilmasining ishlash xususiyatlari hisobga olinishi kerak.

#### 13.18. Yangiligi to'g'risida ma'lumotlar

Yetkazib beriladigan dasturiy ta'minot mahsulot va uning tarkibiy qismlari uchun barcha zarur litsenziyalarga ega, eng so'nggi aktual versiya bo'lishi kerak.

#### 13.19. Sug'urta

Talablar qo'yilmaydi.

#### 13.20. Xizmat ko'rsatishda mas'uliyatni taqsimlash matritsasi

Texnik xizmat ko'rsatish	Ijrochi	Buyurtmachi
<b>Tizimning ishlashga tayyorligi</b>		
Muammoni aniqlash, uning ustuvorligini tasniflash va hal qilish uchun Huquq egasiga so'rov ochish	A	R
So'rov bo'yicha Buyurtmachining dasturiy ta'minotini sozlash	A	R
Hisobot davri uchun muammolarning yechimi statistikasini taqdim etish	R	A
Barcha so'rovlarni Huquq egasining portalida ro'yxatdan o'tkazish	R	A
<b>Dasturiy ta'minot yangilanishlari, tuzatishlari va moslashtirishlari</b>		
Protsedura usulini taqdim etish	R	A
O'rnatish vaqtini belgilash	A	R
Dasturiy ta'minotni o'rnatish	R	A
O'rnatilgan dasturiy ta'minotning ishlashini tekshirish	A	R



<b>Servislar va tavsiyalar</b>		
Texnik talablarni taqdim etish	R	R
Texnik talablarni joriy etish	R	A
Texnik tavsiyalarni taqdim etish	R	I

*R (ingl. Responsible) – bevosita ijrochi;*

*A (ingl. Accountable) – ijrochining ishiga rahbarlik qiluvchi mas’ul shaxs;*

*C (ingl. Consulted) – maslahatchi (mas’ul shaxs aniq qarorlar qabul qilishdan oldin yordam so‘rab murojaat qiladigan, muayyan soha bo‘yicha mutaxassis yoki ekspert);*

*I (ingl. Informed) – kuzatuvchi, xabardor qilinadigan shaxs (topshiriqning bajarilishi (yoki natijalari) haqida xabardor qilinishi kerak bo‘lgan shaxs)*

#### 14. Qo‘llaniladigan atamalar va qisqartmalar

<b>Qisqartma</b>	<b>Qisqartmaning yoyilmasi</b>
TT	Texnik topshiriq
DT	Dasturiy ta’minot
AT	Axborot tizimi
AT	Axborot texnologiyalari
MB	Ma’lumotlar bazasi
AX	Axborot xavfsizligi
WEB	World Wide Web
Endpoint	EDR/XDR agenti o‘rnatilgan oxirgi qurilma (server, ishchi stansiya, virtual mashina)
Agent	Endpointga o‘rnatiladigan, telemetriya yig‘ish, himoya va EDR/XDR platformasi bilan o‘zaro aloqani ta’minlaydigan dasturiy modul
EDR	Endpoint Detection and Response
NGFW	Next-Generation Firewall
SOC	Security Operations Center
SIEM	Security Information and Event Management
IOC	Indicator of Compromise
MITRE ATT&CK	Tajovuzkorlarning taktika va texnikalari haqidagi bilimlar bazasi. Insidentlarni tasniflash uchun ishlatiladi
Malware	Zararli dasturiy ta’minot
Ransomware	To‘lov talab qilish maqsadida ma’lumotlarni shifrlaydigan zararli dasturiy ta’minot turi
Phishing	Maxfiy ma’lumotlarni qo‘lga kiritishga yo‘naltirilgan ijtimoiy muhandislik usuli
Lateral Movement	Tajovuzkorning dastlabki komprometatsiyadan so‘ng infratuzilma ichida harakatlanishi
Prevention	Tahdidlarni ular ishga tushishidan oldin bartaraf etish mexanizmlari
Detection	Shubhali yoki zararli faoliyatni aniqlash jarayoni
Response	Tahdidni cheklash va bartaraf etish bo‘yicha avtomatlashtirilgan yoki qo‘lda bajariladigan harakatlar
Incident	Kompaniya aktivlariga ta’sir ko‘rsatuvchi, tasdiqlangan axborot xavfsizligi hodisasi
SLA	Xizmat ko‘rsatish darajasi to‘g‘risidagi kelishuv (reaksiya vaqti, mavjudlik va h.k.)
MTTR	Mean Time To Respond (Insidentga reaksiya bildirishning o‘rtacha vaqti)
MTTD	Mean Time To Detect (Insidentni aniqlashning o‘rtacha vaqti)



RBAC	Role-Based Access Control (Rollarga asoslangan kirishni boshqarish modeli)
API	Application Programming Interface (Tizimlarning dasturiy hamkorlik interfeysi)
Amaliy dasturlash interfeysi	Transport Layer Security (Tarmoq ulanishlarini himoya qilish kriptografik protokoli)
CVE	Common Vulnerabilities and Exposures (Axborot xavfsizligi zaifliklarining umumiy qabul qilingan identifikatori)
VM	Virtual mashina
Cloud Console	Ishlab chiqaruvchining infratuzilmasida joylashtirilgan XDR bulutli boshqaruv konsoli
Telemetry	Hodisalarni tahlil qilish va o'zaro bog'lash uchun agentlar tomonidan uzatiladigan ma'lumotlar majmui
Siyosat	Endpoint yoki qurilmalar guruhiga qo'llanadigan xavfsizlik qoidalari va sozlamalari to'plami

## 15. Ilovalar ro'yxati


1-ilova – Axborotlashtirish obyektining tavsifi.

2-ilova – Texnik talablarga muvofiqlik jadvali.

TTni ishlab chiqdi:

AX va RBD Axborot xavfsizligi  
bo'limi boshlig'i

imzo



R. A. Abdulvaat

AX va RBD direktori

imzo



B. A. Olmatov



Axborotlashtirish obyektining tavsiflari

“UMS” MChJ – 2014-yil 1-dekabrdan boshlab O‘zbekiston Respublikasining butun hududida mobil aloqa xizmatlarini ko‘rsatib kelayotgan telekommunikatsiya kompaniyasi.

“UMS” MChJ O‘zbekiston Respublikasi Vazirlar Mahkamasining 2014-yil 31-iyuldagi “Mobil aloqa xizmatlarini ko‘rsatish bo‘yicha “Universal Mobile Systems” qo‘shma korxonasini tashkil etish to‘g‘risida”gi 208-son qarori asosida tashkil etilgan bo‘lib, O‘zbekiston Respublikasining yetakchi mobil aloqa operatorlaridan biri hisoblanadi.

O‘zbekiston Respublikasi Prezidentining 2021-yil 19-iyuldagi PQ-5187-sonli qaroriga muvofiq, “UMS” MChJning ta‘sischisi O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi hisoblanadi.

Kompaniyaning shtatdagi xodimlari soni – 1800 kishi.

Ish stansiyalarining (endpoints) umumiy soni – 1500 donadan ko‘p emas.

Serverlarning (Windows, Linux, shu jumladan virtual) umumiy soni – 500 donadan ko‘p emas.



## Muvofiqlik jadvali

Talab raqami	Talab nomi / Texnik xususiyatlari
1	Dasturiy ta'minot 3 yil muddatga (obuna, texnik qo'llab-quvvatlashni o'z ichiga olgan holda) yetkazib berilishi lozim.
2	Yechim Kengaytirilgan aniqlash va javob berish (Extended Detection and Response, XDR) sinfiga mansub bo'lishi kerak.
3	Platforma 24/7 rejimida ishlash imkoniyatiga ega markazlashtirilgan boshqaruv konsolini qo'llab-quvvatlashi zarur.
4	SaaS modelini yetkazib berishda quyidagi shartlarga rioya etilishi shart: - Buyurtmachining ma'lumotlarini ajratib qo'yish; - ma'lumotlarni sertifikatlangan ma'lumotlar markazlarida joylashtirish; - ma'lumotlarni uzatish va saqlashda shifrlashdan foydalanish.
5	Yechim arxitekturasini servislarni to'xtatmagan holda gorizontol kengayishni ta'minlashi kerak.
6	Quyidagi funksiyalarning bo'lishi majburiy: - zaifliklardan foydalanishning oldini olish; - faylli va faylsiz hujumlardan himoya qilish; - zararli skriptlardan himoya qilish; - to'lov talab qiluvchi zararli dastur (ransomware) turidagi hujumlarni aniqlash va ularning oldini olish.
7	Turli xavfsizlik manbalaridan olingan telemetriya ma'lumotlarining avtomatik korrelyatsiyasi mavjud bo'lishi kerak.
8	Tizim hujum zanjirining vizualizatsiyasini ta'minlashi lozim.
9	Yechim tarmoqni himoyalash vositalari (tarmoqlararo ekranlar, tajovuzlarning oldini olish tizimlari) bilan uzviy integratsiyani qo'llab-quvvatlashi kerak.
10	Yechim munosabat bildirish ssenariylari doirasida tarmoq ulanishlarini, IP-manzillarni va domenlarni avtomatik bloklashni qo'llab-quvvatlaydi.
11	Integratsiya tashqi ma'lumotlar brokerlaridan foydalanmagan holda amalga oshirilishi lozim.
12	Yechim axborot xavfsizligi hodisalariga munosabat bildirishning avtomatlashtirilgan ssenariylarini ta'minlaydi, jumladan: - so'nggi nuqtani izolyatsiyalash; - zararli jarayonlarni yakunlash; - fayllarni xesh bo'yicha bloklash; - forensik-artefaktlarni yig'ish.
13	Yechim dasturiy kod yozmasdan, munosabat bildirishning maxsus ssenariylarini yaratish imkoniyatini qo'llab-quvvatlaydi.
14	Munosabat bildirish ham avtomatik, ham qo'lda boshqariladigan rejimlarda mavjud.
15	Yechim real vaqtga yaqin rejimda yangilanib turadigan global kiberxavf manbalaridan foydalanadi.
16	Yechim hodisalarning dolzarb komprometatsiya indikatorlari (IoC) bilan avtomatik korrelyatsiyasini qo'llab-quvvatlaydi.
17	Yechim quyidagilarni qo'llab-quvvatlaydi: - rollarga asoslangan kirish modeli (RBAC); - foydalanuvchi harakatlari audit; - hodisalar tarixini 12 oygacha saqlash.



18	<p>Yechim quyidagilarni shakllantirishni qo'llab-quvvatlaydi:</p> <ul style="list-style-type: none"> <li>- operativ asboblarni panellari;</li> <li>- AX bo'limi rahbariyati uchun hisobotlar;</li> <li>- ma'lumotlarni tashqi SIEM-tizimlarga yuklash.</li> </ul>
19	Boshqaruv interfeysi rus yoki ingliz tillarini qo'llab-quvvatlaydi.
20	Yechim quyidagilar bilan integratsiyani qo'llab-quvvatlaydi: - Active Directory / LDAP; - REST API-ni qo'llab-quvvatlaydigan platformalar; - bildirishnomalar va audit jurnallarini yuborish uchun tashqi Syslog Receiver-lar.
21	Hisob qaydnomalarini qo'lda boshqarish zaruratsiz avtomatik sinxronlashtirish qo'llab-quvvatlanadi.
22	Yechimda REST API mavjud.
23	<p>Foydalanish jarayonida quyidagi funksiyalar bajarilishi kerak:</p> <ul style="list-style-type: none"> <li>- signaturalar, aniqlash modellari va tahlil komponentlari avtomatik tarzda yangilanishi lozim,</li> <li>- yechim komponentlarni yangilash vaqtida uzluksiz himoyani ta'minlashi lozim,</li> <li>- Vender kamida 24x7 darajasida texnik yordam ko'rsatishni ta'minlashi lozim.</li> </ul>
24	Yechim oxirgi nuqtaga masofadan ulanish imkoniyatini qo'llab-quvvatlashi lozim.
25	Yechim ISO 27001 sertifikatiga ega bo'lishi shart.
26	<p>Yechim qurilmalarni nazorat qilish bo'yicha quyidagi funksiyalarga ega bo'lishi lozim:</p> <ul style="list-style-type: none"> <li>- Windows va macOS OT uchun shifrlashni boshqarishni ta'minlash;</li> <li>- Windows va macOS OT uchun USB qurilmalarni nazorat qilish funksiyalarini ta'minlash;</li> <li>- Bluetooth qurilmalarini bloklash imkoniyatiga ega bo'lish;</li> <li>- muayyan qurilmalarda chop etishni taqiqlash imkoniyatiga ega bo'lish.</li> </ul>
27	<p>Yechim quyidagi manbalardan keluvchi telemetriyani barqaror qayta ishlashni ta'minlaydi:</p> <ul style="list-style-type: none"> <li>- bitta mantiqiy tenent doirasida kamida 10 000 ta oxirgi nuqtadan;</li> <li>- keyinchalik arxitekturaning o'zgartirish imkoniyati bilan.</li> </ul>
28	<p>Yechim quyidagilarni ta'minlaydi:</p> <ul style="list-style-type: none"> <li>- bir vaqtning o'zida kamida 100 ta faol tahliliy so'rovning ishlashini;</li> <li>- samaradorlik pasaymasdan kamida 1 000 ta insidentni parallel qayta ishlashni.</li> </ul>
29	<p>Oxirgi nuqta agenti o'rtacha hisobda quyidagilardan ko'p resurs sarflamasligi kerak:</p> <ul style="list-style-type: none"> <li>- shtat rejimida Markaziy protsessorning (CPU) 5%;</li> <li>- 500 MB tezkor xotira;</li> <li>- 1 GB disk maydoni.</li> </ul>
30	Yechim ma'lumotlar va telemetriyani yo'qotmagan holda tahlil va boshqaruv komponentlarining ishdan chiqishga bardoshlilikini ta'minlashi lozim.
31	<p>Yechim quyidagilar bilan integratsiyani ta'minlashi kerak:</p> <ul style="list-style-type: none"> <li>- Microsoft Active Directory;</li> <li>- LDAP-ga mos keluvchi kataloglar.</li> </ul>
32	<p>Integratsiya quyidagilarni ta'minlashi kerak:</p> <ul style="list-style-type: none"> <li>- foydalanuvchilar, guruhlar va rollar haqidagi ma'lumotlarni olishni;</li> <li>- xavfsizlik hodisalarini foydalanuvchi hisoblari bilan o'zaro bog'lashni;</li> <li>- insidentlar kontekstini yaratish uchun katalog ma'lumotlaridan foydalanishni.</li> </ul>
33	<p>Tashqi SIEM-tizimlar bilan ikki tomonlama integratsiya ta'minlanadi, jumladan:</p> <ul style="list-style-type: none"> <li>- insidentlar va alertlarni (ogohlantirishlarni) uzatish;</li> <li>- boyitilgan hodisalarni uzatish.</li> </ul>



34	<p>Integratsiya quyidagilar orqali qo'llab-quvvatlanadi:</p> <ul style="list-style-type: none"> <li>- REST API;</li> <li>- Syslog;</li> <li>- nativ konnektorlar.</li> </ul>
35	<p>Yechimdan quyidagicha foydalanish mumkin:</p> <ul style="list-style-type: none"> <li>- SIEM uchun hodisalar manbai sifatida;</li> <li>- SIEM'ga majburiy ulanishni talab qilmaydigan avtonom XDR-platforma sifatida.</li> </ul>
36	<p>Integratsiya quyidagilarni ta'minlashi kerak:</p> <ul style="list-style-type: none"> <li>- xavfsizlik telemetriyasini olishni;</li> <li>- fishing hujumlari va hisob yozuvlarining komprometatsiyasini aniqlashni.</li> </ul>
37	<p>Yechim quyidagilar uchun ommaviy, hujjatlashtirilgan REST API taqdim etishi kerak:</p> <ul style="list-style-type: none"> <li>- hodisalar va insidentlarni olish;</li> <li>- himoya obyektlarini boshqarish;</li> <li>- reksiya ssenariylarini ishga tushirish.</li> </ul>
38	<p>API quyidagilarni qo'llab-quvvatlaydi:</p> <ul style="list-style-type: none"> <li>- tokenlar orqali autentifikatsiyani;</li> <li>- kirish huquqlarini chegaralashni;</li> <li>- murojaatlar jurnalini yuritishni.</li> </ul>
39	<p>Yechim ITSM toifasidagi tizimlar bilan integratsiyani qo'llab-quvvatlashi kerak, bu quyidagilarni o'z ichiga oladi:</p> <ul style="list-style-type: none"> <li>- insidentlarni avtomatik yaratish;</li> <li>- tekshiruv statuslarini uzatish;</li> <li>- reksiya natijalariga ko'ra insidentlarni yopish.</li> </ul>
40	<p>Integratsiyalardan quyidagilar doirasida foydalanish imkoniyati qo'llab-quvvatlanishi kerak:</p> <ul style="list-style-type: none"> <li>- avtomatik pleybuklar;</li> <li>- yarim avtomatik reksiya ssenariylari.</li> </ul>
41	<p>Integratsiyalar dasturiy kod yozmasdan, grafik interfeys orqali sozlanadi.</p>
42	<p>Yechimni litsenziyalash himoyalanganadigan so'nggi nuqtalar soni bo'yicha, litsenziyalanadigan hajmni moslashuvchan tarzda oshirish imkoniyati bilan amalga oshirilishi kerak.</p>
43	<p>Litsenziya narxiga quyidagilar kiritilishi lozim:</p> <ul style="list-style-type: none"> <li>- so'nggi nuqtalardagi hujumlarning oldini olish funksiyalari;</li> <li>- aniqlash va javob qaytarish funksiyalari (EDR/XDR);</li> <li>- markazlashtirilgan boshqaruv konsoli;</li> <li>- mashinaviy ta'lim va xulq-atvor modellari asoslangan tahlil;</li> <li>- o'rnatilgan avtomatik javob qaytarish ssenariylari.</li> </ul>
44	<p>Quyidagi funksiyalar uchun qo'shimcha haq olinishiga yo'l qo'yilmaydi:</p> <ul style="list-style-type: none"> <li>- hodisalarni o'zaro bog'lash;</li> <li>- hujumlar zanjirini vizuallashtirish;</li> <li>- avtomatik javob qaytarish;</li> <li>- asosiy hisobotlar va asboblarni panellari.</li> </ul>
45	<p>Litsenziya yechimdan foydalanish huquqini o'z ichiga olishi kerak:</p> <ul style="list-style-type: none"> <li>- kecha-kunduz rejimida;</li> <li>- hodisalar va voqealar soniga cheklolrsiz.</li> </ul>
46	<p>Litsenziya doirasida quyidagilar taqdim etilishi kerak:</p> <ul style="list-style-type: none"> <li>- signaturalarni muntazam yangilash;</li> <li>- tahliliy modellarni yangilash;</li> <li>- platformaning funksional komponentlarini yangilash.</li> </ul>



47	Litsenziyaga quyidagilar kiritilishi lozim: - 24/7 rejimida texnik qo'llab-quvvatlash; - bilimlar bazasi va javob qaytarish bo'yicha tavsiyalardan foydalanish imkoniyati.
48	Litsenziyalash quyidagilarga bog'liq bo'lmasligi lozim: - ishlov beriladigan trafik hajmiga; - tahliliy qoidalar soniga; - boshqaruv konsoli foydalanuvchilari soniga.
49	Himoyaladigan so'nggi nuqtalar soni – kamida 2000 ta.
50	Loyihaga o'rnatish ishlari kiritilgan.
51	Loyihaga loyihalashtirish ishlari kiritilgan.
52	Loyihaga Buyurtmachi mutaxassislarini o'qitish kiritilgan.
53	Loyihaga dasturiy ta'minotni MKBda sertifikatlash kiritilgan.
54	Interfeys tili - ruscha/inglizcha
55	Ijrochida MAF mavjudligi