

«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. Olatov

2026-yil “03”- 

**EDR/XDR yakuniy tugunlarni (yakuniy nuqtalarni) himoya qilish tizimini
yetkazib berish, o'rnatish va ishga tushirish uchun
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 va xizmatlar ro'yxati hamda 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	10
7	Ishlarni bajarish va xizmatlar ko'rsatish xavfsizligiga doir talablar	11
8	Bajarilgan ishlar va ko'rsatilgan xizmatlar natijalari bo'yicha texnik va boshqa hujjatlarni topshirishga oid talablar	11
9	Buyurtmachi xodimlarini o'qitishga oid talablar	12
10	Kafolat majburiyatlari	12
11	Servis va texnik qo'llab-quvvatlash shartlari	12
12	Texnik qo'llab-quvvatlashga doir talablar	13
13	Ishlar, xizmatlar va ularni ko'rsatish shartlariga doir boshqa talablar	14
14	Foydalanilgan atamalar va qisqartmalar	15
15	Ilovalar ro'yxati	16

1 Umumiy ma'lumotlar

Mazkur Texnik topshiriqda EDR/XDR yakuniy tugunlarni (yakuniy nuqtalarni) himoya qilish tizimiga (keyingi o'rinlarda – Tizim, AT) qo'yiladigan talablar bayon etilgan. Ular 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 oid talablarini tavsiflash uchun yetarlidir.

Axborotlashtirish obyektining tavsifi 1-ilovada keltirilgan.

1.1 Bajariladigan ishlar va ko'rsatiladigan xizmatlarning nomi

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

Ishlar Buyurtmachining infratuzilmasida 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 shart.

1.2 Bajariladigan ishlar va ko'rsatiladigan xizmatlardan foydalanish maqsadlari

Loyihaning asosiy maqsadi – "UMS" MChJ infratuzilmasida Yakuniy tugunlarni (endpoint) himoya qilish EDR/XDR tizimining dasturiy ta'minotini joriy etishdan iborat.

Tizim tomonidan hal etiladigan asosiy vazifalar:

- Yakuniy nuqtalar va tarmoq infratuzilmasidagi murakkab kiberhujumlar va anomaliyalarni aniqlash;
- turli manbalardan xavfsizlik telemetriyasini markazlashgan holda yig'ish, muvofiqlashtirish va tahlil qilish;
- maqsadli hujumlar, zararli faoliyat va komprometatsiya urinishlarini barvaqt aniqlash;
- axborot xavfsizligi hodisalarini aniqlash va ularga javob qaytarish vaqtini qisqartirish;
- hodisalarga javob qaytarishni avtomatlashtirish va hujumlarning biznes-jarayonlarga ta'sirini minimallashtirish;
- hujumlar zanjiri va tahdidlar kontekstini vizualizatsiya qilish orqali hodisalar shaffofligini oshirish;
- hodisalarni tekshirish va raqamli forenzikani qo'llab-quvvatlash;
- "UMS" MChJ AT-infratuzilmasining umumiy himoyalanganlik darajasini oshirish.

Tizimning asosiy maqsadi – kiberxatarlar tavakkalchiligini va ularning biznes-jarayonlarga ta'sirini kamaytirish uchun "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 Budjeti).

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

Yakuniy tugunlarni (yakuniy nuqtalarni) himoya qiluvchi EDR/XDR tizimini joriy etish Buyurtmachining mavjud AT-infratuzilmasi ish qobiliyatini buzmaganda, mavjud qurilmalarni dastlabki yuzaki ko'zdan kechirib, Buyurtmachining mas'ul shaxslari bilan birgalikda amalga oshirilishi kerak. Har qanday korporativ tizimlarni to'xtatib qo'yishni talab etadigan barcha ishlar Buyurtmachi bilan oldindan kelishilishi 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

Ushbu bosqich Buyurtmachining loyiha uchun mas'ul xodimlari bilan o'zaro hamkorlik qilishni va uning AT-infratuzilmasini birgalikda o'rganishni o'z ichiga oladi. Bunda xodimlar quyidagilarni aniqlashlari lozim:

- Buyurtmachi tarmog'i topologiyasining eng muhim tafsilotlarini;
- Tizimni joriy etish jarayonida Buyurtmachi va Ijrochining mas'uliyat doiralarini;
- Tizim tomonidan himoya qilinadigan 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.

Tizim ishida Buyurtmachining IT infratuzilmasi obyektlari bilan bog'liq bo'lmagan xatolar tufayli nosozliklar aniqlangan taqdirda, Ijrochi bajarilgan ishlar dalolatnomasi imzolanmaguncha mahsulot funksionaliga tuzatishlar kiritish majburiyatini 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 layoqatliligini hamda ularning Texnik topshiriq talablariga muvofiqligini tasdiqlashdan iborat.

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

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

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

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

Kamchiliklar, nuqsonlar yoki tizimga qo'yiladigan talablardan boshqa chetga chiqishlar bartaraf etilgan paytdan boshlab besh ish kuni ichida qabul komissiyasi tegishli komponentni qayta qabul qilish sinovlaridan o'tkazishi va Tizimni doimiy foydalanishga qabul qilishi shart.

3.4 Xodimlarni o'qitish.

Mazkur Texnik topshiriqning 9-bandiga muvofiq o'qitish.

4 Ishlarni bajarish va xizmatlar ko'rsatish joyi

Ijrochi dasturiy ta'minotni quyidagi manzil bo'yicha yetkazib berishi, o'rnatishi va sozlab berishi

kerak: O'zbekiston Respublikasi, Toshkent sh., 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 va Ijrochi o'rtasida shartnoma munosabatlari imzolangan kundan boshlab 90 kalendar kundan oshmasligi kerak.

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 tegishli bo'lishi hamda yagona platforma doirasida yakuniy nuqtalar, tarmoq manbalari va bulutli muhitlardan kelib tushadigan xavfsizlik hodisalarining o'zaro bog'liqligini ta'minlashi kerak.

5.1.2 Platforma 24x7 rejimida ishlash imkoniyatiga ega bo'lgan markazlashtirilgan boshqaruv konsolini qo'llab-quvvatlashi kerak.

5.1.3 Quyidagi shartlar asosida bulutli modeldan (SaaS) foydalanishga ruxsat etiladi:

- Buyurtmachining ma'lumotlarini ajratish;
- ma'lumotlarni sertifikatlangan ma'lumot markazlariga joylashtirish;
- ma'lumotlarni uzatish va saqlashda shifrlashdan foydalanish.

5.1.4 Yechim arxitekturasi servislarni to'xtatmagan holda gorizontaal kengayishni ta'minlashi kerak.

5.2 Yakuniy nuqtalarni himoyalash (Endpoint Protection & EDR)

5.2.1 Yechim quyidagilardan foydalangan holda chekka qurilmalarni (Windows, Linux, macOS) himoyalashni ta'minlashi kerak:

- xulq-atvor tahlili;
- mashinali o'rganish;
- hujum zanjirlari tahlili.

5.2.2 Chekka qurilma agenti alohida komponentlarni o'rnatishni talab etmasdan oldini olish, aniqlash va javob qaytarish funksiyalarini o'zida birlashtirishi lozim.

5.2.3 Quyidagi funksiyalar qo'llab-quvvatlanishi kerak:

- zaifliklardan foydalanishning oldini olish;
- faylli va faylsiz hujumlardan himoya;
- zararli skriptlardan himoya;
- tovon talab qiluvchi dasturiy ta'minot (ransomware) turidagi hujumlarni aniqlash.

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

5.3 XDR-korrelyatsiya va tahlil

5.3.1 Yechim yagona insident doirasida turli xavfsizlik manbalaridan olingan telemetriyaning avtomatik korrelyatsiyasini ta'minlashi kerak.

5.3.2 Quyidagilarga asoslangan tahlil qo'llab-quvvatlanishi lozim:

- xulq-atvor modellari;
- mashinali o'rganish;
- hujumchining taktikasi, texnikasi va proseduralari (TTP) tahlili.

5.3.3 Platforma dastlabki komprometatsiya vektorini va tajovuzkorning keyingi qadamlarini ko'rsatgan holda hujum zanjirini (attack storyline) vizualizatsiya qilishni ta'minlashi kerak.

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

5.4 Tarmoq xavfsizligi bilan integratsiya

Javob qaytarish senariylari doirasida tarmoq ulanishlari, IP-manzillar va domenlarni avtomatik bloklash imkoniyati ta'minlanishi kerak.

IP-адресов и доменов в рамках сценариев реагирования.

5.5 Javob qaytarish va avtomatlashtirish (SOAR-funksiyalari)

5.5.1 Yechim ishlab chiqaruvchining 100 dan ortiq tayyor pleybukini o'z ichiga olgan holda xavfsizlik hodisalariga javob berishning avtomatlashtirilgan ssenariylarini ta'minlashi kerak, jumladan:

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

5.5.2 Dasturiy kod yozmasdan, moslashtirilgan javob ssenariylarini yaratish imkoniyati qo'llab-quvvatlanishi lozim.

5.5.3 Javob choralari ham avtomatik, ham qo'lda boshqariladigan rejimlarda mavjud bo'lishi kerak.

5.6 Tahdidlar tahlili (Threat Intelligence)

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

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

5.6.3 Platforma uchinchi tomon xizmatlarini ulashga ehtiyoj sezmasdan, hodisalarni tahdidlar haqidagi kontekstli ma'lumotlar bilan boyitishni ta'minlashi lozim.

5.7 Boshqaruv, hisobotdorlik va audit

5.7.1 Platforma quyidagilarni ta'minlashi kerak:

- kirishning rolga asoslangan modelini (RBAC);
- foydalanuvchilar harakatlari auditini;
- voqealar haqidagi barcha yig'iladigan xizmat ma'lumotlarini (telemetriya) kamida 30

kun, hodisalar tarixini esa 12 oygacha saqlashni.

5.7.2 Quyidagilarni shakllantirish imkoniyati qo'llab-quvvatlanishi kerak:

- tezkor asboblarni panellarini (dashbordlar);
- axborot xavfsizligi bo'limi rahbariyati uchun hisobotlarni;
- ma'lumotlarni tashqi SIEM-tizimlarga yuklab olishni.

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

5.8 AT-infratuzilma bilan integratsiya

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

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

bilan.

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

5.9 Foydalanishga oid talablar

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

– Yechim o'z komponentlarini yangilash jarayonida himoyaning uzluksizligini ta'minlashi lozim.

- Vendor kamida 24x7 darajasidagi texnik yordamni ta'minlashi shart.

5.10 Masofadan ulanish imkoniyatlari

Taklif etilayotgan yechim real vaqt rejimida ulanish orqali Yakuniy qurilmada buyruqlarni to'liq qo'llab-quvvatlagan holda buyruqlar satrini ishga tushirish imkoniyatini ta'minlashi kerak.

5.11 Sertifikatsiya:

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

5.12 Qurilmalarni nazorat qilish

Taklif etilayotgan yechim quyidagi imkoniyatlarga ega bo'lishi kerak:

- Windows va macOS operatsion tizimlari uchun shifrlashni boshqarishni ta'minlash;
- Windows va macOS operatsion tizimlari uchun USB qurilmalarni nazorat qilish

funksiyalarini ta'minlash.

5.13 Ishlash samaradorligi va kengaytiriluvchanlikka oid talablar

5.13.1 Yechim quyidagi manbalardan keladigan telemetriyani barqaror qayta ishlashni ta'minlashi kerak:

- bitta mantiqiy tenant doirasida kamida 10 000 ta Yakuniy nuqta;
- keyinchalik arxitekturasini o'zgartirmasdan 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 samaradorligi quyidagi hollarda pasaymasligi lozim:

- xulq-atvor tahlili yoqilganda;
- mashinali o'rganishdan foydalanilganda;
- avtomatik javob ssenariylari faollashtirilganda.

5.13.4 Yakuniy nuqta agenti o'rtacha hisobda quyidagilardan ko'p resurs sarflamasligi kerak:

- oddiy ish rejimida markaziy protsessorning 5% ini;
- 500 MB tezkor xotirani;
- 1 GB disk maydoni.

5.13.5 Yechim ma'lumotlar va telemetriyani yo'qotmagan holda tahlil va boshqaruv komponentlarining uzilishlarsiz ishlashini ta'minlashi lozim.

5.14 AT va AX tizimlari bilan integratsiyalashuvga qo'yiladigan talablar

5.14.1 Hisob qaydnomalarini boshqarish tizimlari bilan integratsiyalashuv

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

- Microsoft Active Directory;
- LDAP bilan mos keluvchi kataloglar.

b) Integratsiyalashuv quyidagilarni ta'minlashi lozim:

- foydalanuvchilar, guruhlar va rollar haqidagi ma'lumotlarni olishni;
- xavfsizlik hodisalarini foydalanuvchi hisob qaydnomalari bilan o'zaro bog'lashni;
- insidentlar kontekstini yaratish uchun katalog ma'lumotlaridan foydalanishni.

c) Hisob qaydnomalarini qo'lda sozlash zaruratisiz avtomatik sinxronizatsiya qilish imkoniyati qo'llab-quvvatlanishi kerak.

5.14.2 SIEM tizimi bilan integratsiyalashuv

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

- insidentlar va ogohlantirishlarni uzatishni;
- boyitilgan hodisalarni uzatishni;

b) Integratsiyalashuv quyidagilar orqali amalga oshirilishi lozim:

- REST API;
- Syslog;
- nativ konnektorlar.

c) Yechim quyidagi maqsadlarda foydalanishni qo'llab-quvvatlashi kerak:

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

sifatida.

5.14.3 Integratsiyalashuv quyidagilarni ta'minlashi lozim:

- xavfsizlik telemetriyasini olishni;
- fishing hujumlari va hisob qaydnomalari buzilishini aniqlashni.

5.14.4 API va kengaytiriluvchanlik

- d) Yechim quyidagilar uchun ochiq, hujjatlashtirilgan REST APIni taqdim etishi lozim:
- hodisalar va insidentlarni olish;
 - himoya obyektlarini boshqarish;
 - javob chorasi ssenariylarini ishga tushirish.
- e) API quyidagilarni qo'llab-quvvatlashi kerak:
- tokenlar orqali autentifikatsiyani;
 - kirish huquqlarini chegaralashni;
 - murojaatlar jurnalini yuritishni.
- f) API va integratsiyalardan foydalanish qo'shimcha litsenziyalarni sotib olishni talab qilmasligi lozim.

5.14.5 Avtomatlashtirish va orkestrlash

- g) Yechim quyidagilar uchun ITSM tizimlari bilan integratsiyani qo'llab-quvvatlashi kerak:
- insidentlarni avtomatik tarzda yaratish;
 - tekshiruv holatlarini uzatish;
 - munosabat bildirish natijalari bo'yicha insidentlarni yopish.
- h) Integratsiyalardan quyidagilar doirasida foydalanish imkoniyati qo'llab-quvvatlanishi lozim:
- avtomatik pleybuklar;
 - yarim avtomatik munosabat bildirish ssenariylari.
- i) Integratsiyalar dasturiy kod yozmasdan, grafik interfeys orqali sozlanishi kerak.

5.14.6 Litsenziyalash va yetkazib berish to'plami

5.14.6.1 Yechimni litsenziyalash himoyalanadigan yakuniy nuqtalar soniga qarab, litsenziyalanadigan hajmni moslashuvchan tarzda oshirish imkoniyati bilan amalga oshirilishi kerak.

5.14.6.2 Litsenziya narxiga quyidagilar kiritilishi lozim:

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

5.14.6.3 Quyidagilar uchun qo'shimcha to'lov undirishga yo'l qo'yilmaydi:

- insidentlar korrelyatsiyasi;
- hujumlar zanjirini vizuallashtirish;
- avtomatik munosabat bildirish;
- asosiy hisobotlar va asboblarni panellari

;

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

- kecha-yu kunduz rejimida;
- insidentlar va hodisalar soniga cheklavlarsiz.

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 yordam;
- bilimlar bazasi va javob choralari bo'yicha tavsiyalardan foydalanish imkoniyati.

5.14.6.7 Litsenziyalash quyidagilarga bog'liq bo'lmisligi 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 oy.

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

5.15 XDR-yechimga oid miqdoriy talablar

№	Ko'rsatkich	Talab
1	Himoyalangan Yakuniy nuqtalar soni	kamida 2000 ta
2	Tayyor aniqlash qoidalari	kamida 350 ta
3	Tayyor javob choralari ssenariylari	kamida 50 ta
4	Hujumlar zanjirini avtomatik tarzda	majburiy
5	Agent tomonidan resurslar iste'moli (CPU)	shtat rejimida 5 % dan ko'p bo'lmagan
6	Yakuniy nuqtalar bo'yicha litsenziyalash	majburiy, hodisalar va Yakuniy nuqtalardan yig'iladigan axborot hajmi bo'yicha cheklolrsiz
7	Platformaning ishga yaroqliligi 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 jamlash, dastlabki 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 oid talablar

Tizimning asosiy ishlash rejimi – avtomatlashtirilgan bo'lib, administrator tomonidan boshqariladi.

Tizim quyidagi rejimlarda ishlash imkoniyatini ta'minlashi kerak:

- shtat rejimi (uzluksiz tunu kun ishlash);
- avtonom rejim (tizim komponentlari o'rtasida yoki tashqi tarmoqlar bilan aloqa bo'lmagan hollarda, konfiguratsiya va arxiv ma'lumotlaridan foydalanish uchun).

5.18 Ijrochi xodimlarining soni va malakasiga doir talablar.

Dasturiy ta'minot majmuasini yetkazib berishni va Tizimning ishga tushirilishini ta'minlash uchun Ijrochining xodimlari tarkibida kamida bitta shtatdagi texnik qo'llab-quvvatlash muhandisi bo'lishi shart.

Texnik qo'llab-quvvatlash muhandisi Buyurtmachida Tizimga muntazam texnik xizmat ko'rsatish va nosozliklarni bartaraf etish uchun zarur bo'lgan darajadagi bilimlarga ega bo'lishi lozim.

5.19 Audit, monitoring va hisobotga doir talablar

Tizim foydalanuvchilar va administratorlar harakatlari auditini, xavfsizlik va ekspluatatsiya hodisalarining qayd etilishini, shuningdek, komponentlarning holati va ishlashga tayyorligi monitoringini ta'minlashi kerak.

Tizim shubhali faollik aniqlanganda xabarnomalar yuborish imkoniyati bilan real vaqt rejimida

auditni qo'llab-quvvatlashi kerak.

Barcha hodisalar sana va vaqt, amal manbai va natijasi ko'rsatilgan holda jurnalga kiritilishi lozim.

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

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

Audit va monitoring ma'lumotlarini (loglarni) saqlash muddati – kamida 12 oyni tashkil etadi.

5.20 Yechim zaifliklarni nazorat qilish va o'rnatilgan agentlarsiz tarmoq hamda aktivlarni skanerlash uchun ishlab chiqaruvchining oraliq (proksi) serveriga asoslangan tarmoq zaifliklari skaneridan foydalanish imkoniyatini qo'llab-quvvatlashi kerak.

5.20.1. Yechim zaifliklarni nazorat qilish uchun yagona platforma doirasida kengayishni qo'llab-quvvatlashi lozim:

- muayyan zaiflikdan foydalanishni avtomatik bloklay oladigan himoya mexanizmlari (aniqlash va javob qaytarish platformasining faol oldini olish qoidalari) mavjudligini hisobga oluvchi muhimlikni darajalash algoritmlarini o'z ichiga olishi;

- tashqi zaiflik skanerlaridan ma'lumotlarni avtomatik yig'ishni va ularni zaifliklarni boshqarishning yagona tizimiga integratsiyalashni ta'minlashi;

- eng muhim xatarlarni, vaqt o'tishi bilan xatar darajasining o'zgarish dinamikasini va ularni bartaraf etish jarayonini vizualizatsiya qilish uchun maxsus monitoring panelini o'z ichiga olishi;

- zaifliklarni bartaraf etish uchun avtomatlashtirilgan o'rnatilgan pleybuklarni taqdim etishi, jumladan, jiddiy zaifliklarni qo'lda aralashuvsiz bartaraf etish uchun to'liq avtomatlashtirilgan harakatlarni qo'llab-quvvatlashi;

- tajovuzkorning tarmoq ichida harakatlanishi uchun muayyan tugunlardagi qaysi zaifliklardan foydalanishi mumkinligini ko'rsatuvchi "hujum yo'llari" vizualizatsiyasini taqdim etishi;

- zaiflik xatarini baholashda nafaqat CVSS bahosini, balki mazkur zaiflikdan foydalanilganlik alomatlari (EPSS) mavjudligini ham hisobga oladigan mexanizmni taqdim etishi;

- tashqi hujum yuzasini nazorat qilish hamda yagona platforma doirasida boshqa tahdidlar bilan bog'liq bo'lgan tashqi zaifliklar va hujum vektorlarini baholash uchun qo'shimcha modul qo'shish imkoniyati mavjud bo'lishi;

- aniqlash va javob qaytarish platformasida qayd etilgan axborot xavfsizligiga doir faol hodisalar bilan topilgan zaifliklarni avtomatik tarzda taqqoslash imkoniyatini o'z ichiga olishi;

5.21 Yechim LLM va bulutli saqlagichlarga ma'lumotlar uzatilishini nazorat qilish hamda Yakuniy nuqtalarda ma'lumotlar sizib chiqishining oldini olish imkoniyatini yagona tahdidlarni boshqarish platformasi va Yakuniy nuqtalarga o'rnatiladigan yagona agent doirasida qo'llab-quvvatlashi kerak.

5.22 Yechim sun'iy intellekt yordamida xatning mazmunidagi maqsadlarni chuqur tahlil qilish orqali fishing xatlarini aniqlash va o'chirish uchun maxsus modulni qo'llash imkoniyatini qo'llab-quvvatlashi kerak.

6 Ijrochiga qo'yiladigan talablar

6.1 Ijrochiga qo'yiladigan umumiy talablar

Ijrochi quyidagi talablarga javob berishi lozim:

- belgilangan xizmatlarni ko'rsatish (dasturiy ta'minotni 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 Yakuniy foydalanuvchilarga tarqatish uchun hujjatli tasdiqnomaga ega bo'lishi;

- to'lovga layoqatsiz yoki bankrot bo'lmashligi, tugatish jarayonida bo'lmashligi, mol-mulki xatlanmagan bo'lishi, shuningdek, iqtisodiy faoliyati to'xtatib qo'yilmagan bo'lishi kerak.

- tarkibida ushbu dasturiy ta'minotni o'rnatish, sozlash, ishlatish va texnik qo'llab-quvvatlash bo'yicha malakasini tasdiqlovchi sertifikatlarga ega bo'lgan kamida 2 (ikki) nafar mutaxassisning mavjud bo'lishi;

- Ijrochi ekspertizadan o'tish niyati to'g'risidagi kafolat xatini yoxud "Kiberxavfsizlik markazi" DUKdan olingan axborot va kiberxavfsizlikni ta'minlash talablariga muvofiqlik yuzasidan ekspertizadan o'tganlik to'g'risidagi sertifikatni taqdim etish majburiyatini oladi.

Ijrochi maxfiy ma'lumotlarni o'z ichiga olgan hujjatlar va ma'lumotlar bilan ishlashga oid O'zbekiston Respublikasining amaldagi qonunchiligi talablariga rioya etishi hamda xizmatlar ko'rsatish jarayonida o'ziga ma'lum bo'lib qolgan maxfiy ma'lumotlarni oshkor etmasligi shart.

6.2 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 vakolatli xatning nusxasi;

- ishlab chiqaruvchi kompaniyadan olingan kamida 2 ta muhandislik sertifikatining nusxalari.

- yakuniy 3 yil ichida amalga oshirilgan AT-loyihalar ro'yxati.

6.3 Ishlab chiqaruvchiga qo'yiladigan talablar

Vendor-kompaniya bozorda kamida 5 yildan buyon faoliyat yuritayotgan bo'lishi va O'zbekiston bozorida vakolatli hamkorlarga ega bo'lishi kerak.

7 Ishlarni bajarish va xizmatlar ko'rsatish xavfsizligiga doir talablar

Ishlarni bajarishda xavfsizlik bo'yicha quyidagi talablar qo'yiladi:

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

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

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

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

Tizimni joriy etish va sanoat tartibida foydalanishga topshirish yakunlangandan so'ng Ijrochi, Tizimning amalda joriy qilingan holatini **aks ettiruvchi** ish (ijro) hujjatlarini tayyorlashi **shart**.

Hujjatlar quyidagi ko'rinishda taqdim etiladi:

- qog'oz tashuvchida 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);
- qisqa foydalanish hujjatlari;
- axborot xavfsizligi bo'yicha amalga oshirilgan chora-tadbirlar tavsifi.

Hujjatlar dolzarb, to'liq bo'lishi, Tizimning amaldagi joriy etilishiga mos kelishi, shuningdek, Ijrochini jalb qilmasdan undan foydalanish uchun yetarli bo'lishi kerak.

9 Buyurtmachi xodimlarini o'qitishga oid talablar

Mazkur Texnik topshiriq doirasida Ijrochi quyidagi o'quv dasturlarini ta'minlaydi;

a) ushbu majmuani boshqarish bo'yicha Buyurtmachining ikki nafar AX mutaxassisini sertifikatlashtirilgan tarzda o'qitish.

Tinglovchilar soni: 2 nafar.

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

Ta'lim 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 hujjat (sertifikatlar).

b) tizim foydalanuvchilarini o'qitish.

Tinglovchilar soni: 10 nafargacha.

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 sifati texnik topshiriqqa hamda Buyurtmachi tomonidan ko'rsatilgan talablarga muvofiq bo'lishini kafolatlashi shart.

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

DT obunasining amal qilish davri – **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 kerak.

11 Servis va texnik qo'llab-quvvatlash shartlari

Ishlab chiqaruvchining servis qo'llab-quvvatlash muddati — dasturiy ta'minot joriy qilingan paytdan boshlab **36 (o'ttiz olti) oyni tashkil etadi**. Dasturiy ta'minot komponentlari uchun servis qo'llab-quvvatlash ham Ishlab chiqaruvchi, ham Ijrochi tomonidan ko'rsatilishi shart.

Ijrochi hujjatlarni, yangilanishlarni va relizlarni mustaqil yuklab olish uchun dasturiy ta'minot ishlab chiqaruvchisi kompaniyasining axborot resurslari to'g'risidagi ma'lumotlarni taqdim etishi shart.

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

Dasturiy ta'minotga servis xizmat ko'rsatish ishlari quyidagilarni o'z ichiga olishi kerak:

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 imkoniyati (yangilanishlarni yuklab olish, texnik forum va hujjatlardan foydalanish imkoniyati).
- e) Tizim yangilangan taqdirda, Tizimning 2 nafar ma'muriga yo'riqnoma o'tkazish.
- f) Yuzaga kelgan muammolarni hal qilish, Tizimning ishlashi bilan bog'liq maslahatlar berish uchun "UMS" MChJ talabiga binoan mutaxassisni VPN orqali ulash.
- g) Tizimning ish qobiliyatini tiklash:
 - dasturiy vositalardagi nosozlikdan keyin Tizimning ish qobiliyatini shtat rejimida 2 ish kunidan kechiktirmay tiklash;
 - dasturiy majmuani qayta sozlash, qayta konfiguratsiyalash, yangilash va/yoki to'liq qayta o'rnatish, shuningdek, nosozlikka olib kelgan sabablarni bartaraf etish (agar nosozlik kompaniya mahsulotlari tufayli yuzaga kelgan bo'lsa);
 - tiklash ishlarini o'tkazish uchun nosozlik vaqtida Tizimni o'chirib qo'yish imkoniyati (baypas rejimi);
 - dasturiy nosozliklar, elektr ta'minotidagi uzilishlar va hokazolardan so'ng Tizim faoliyatini tiklash;
 - zaxira nusxalardan ma'lumotlarni tiklash amaliyotlari;
 - bajarilgan ishlar to'g'risida hisobotlar taqdim etish.

12 Texnik qo'llab-quvvatlashga doir talablar

12.1 Ijrochi yetkazib beriladigan dasturiy majmuani 36 oy davomida texnik qo'llab-quvvatlashni ta'minlashi shart.

12.2 Qo'llab-quvvatlash dasturiy ta'minot ishlab chiqaruvchisi yoki ishlab chiqaruvchining vakolatli servis hamkori tomonidan ko'rsatilishi kerak.

12.3 Qo'llab-quvvatlash darajasi ishlab chiqaruvchi darajasiga (L3) eskalatsiya qilish imkoniyatini nazarda tutishi lozim.

12.4 Qo'llab-quvvatlash quyidagilarga nisbatan amal qilishi kerak:

- dasturiy qism (software).

12.5 Qo'llab-quvvatlash quyidagi rejimda taqdim etilishi kerak:

- 24x7x365 – kritik insidentlar uchun;
- 8x5 dan kam bo'lmagan – nokritik insidentlar uchun (Buyurtmachi bilan kelishuvga asosan).

12.6 Insidentlarga javob qaytarish vaqti:

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

12.7 Tiklash (yoki aylanib o'tish yechimini taqdim etish) vaqti:

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

12.8 Ijrochi texnik qo'llab-quvvatlashga (TQQ) arizalarni ro'yxatdan o'tkazish uchun yagona kanalni ta'minlashi kerak:

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

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

13.1 Litsenziyalar/Dasturiy ta'minot, tomonlar vakillari ishtirokida jismoniy inventarizatsiya o'tkazilib, dasturiy ta'minotning ishga yaroqliligi tekshirilgach hamda tuzilgan shartnomaga muvofiq tegishli qabul qilish-topshirish dalolatnomasi imzolangandan so'ng qabul qilingan hisoblanadi. Ushbu Texnik topshiriqda va uning ilovalarida ko'rsatilmagan boshqa shartlar shartnomada belgilanadi.

13.2 Xizmat 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 e'lon qilingan muammolarni hal qilish bo'yicha Ijrochi bilan aloqa qilish vakolatiga ega bo'lgan xodimlarning ro'yxati va aloqa ma'lumotlarini taqdim etadi.

13.3 Butlanishiga doir talab

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

13.4 Integratsiyaga doir talab

Integratsiyada Buyurtmachi infratuzilmasi ishining o'ziga xos xususiyatlari inobatga olinishi kerak.

13.5 Yangiligi to'g'risidagi ma'lumotlar

Yetkazib beriladigan dasturiy ta'minot mahsulot va uning tarkibiy qismlari uchun barcha zarur litsenziyalarga ega bo'lgan, amaldagi eng yakuniy versiyada bo'lishi shart.

13.6 Sug'urta

Talablar qo'yilmaydi.

13.7 Xizmat ko'rsatishda mas'uliyatni taqsimlash matritsasi

Texnik xizmat ko'rsatish	Ijrochi	Buyurtmachi
Tizimning ishlashga tayyorligi		
Muammo ustuvorligini aniqlash va tasniflash, yechim uchun Huquq egasiga so'rov ochish	A	R
So'rov bo'yicha Buyurtmachining dasturiy ta'minotini sozlash	A	R
Hisobot davri uchun muammolarning yechimi bo'yicha statistikani taqdim etish	R	A
Barcha so'rovlarni Huquq egasining portalida ro'yxatdan o'tkazish	R	A
Dasturiy ta'minot yangilanishlari, tuzatishlari va moslashtirishlari		
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
Servislar va tavsiyalar		
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 yordamiga murojaat qiladigan, muayyan sohadagi mutaxassis yoki ekspert);

I (ingl. Informed) – kuzatuvchi, xabardor qilinadigan shaxs (vazifaning bajarilishi (yoki natijalari) haqida xabardor qilinishi lozim bo'lgan shaxs).

14 Foydalanilgan atamalar va qisqartmalar

Qisqartma	Qisqartma yoyilmasi
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 Yakuniy qurilma (server, ish stansiyasi, virtual mashina)
Agent	Endpoint'ga o'rnatiladigan hamda telemetriyani yig'ish, himoya qilish va EDR/XDR platformasi bilan o'zaro aloqani ta'minlaydigan dasturiy modul
EDR	Endpoint Detection and Response (Yakuniy nuqtalarda tahdidlarni aniqlash va javob qaytarish)
NGFW	Next-Generation Firewall (Yangi avlod xavfsizlik devori)
SOC	Security Operations Center (Xavfsizlik operatsiyalari markazi)
SIEM	Security Information and Event Management (Xavfsizlik ma'lumotlari va hodisalarini boshqarish)
IOC	Indicator of Compromise (Komprometatsiya indikatori)
MITRE ATT&CK	Tajovuzkorlarning taktikasi 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	Dastlabki komprometatsiyadan so'ng tajovuzkorning infratuzilma ichida harakatlanishi
Prevention	Tahdidlarning ishga tushirilishiga yo'l qo'ymaslik mexanizmlari
Detection	Shubhali yoki zararli faollikni aniqlash jarayoni
Response	Tahdidni lokalizatsiya qilish va bartaraf etish bo'yicha avtomatlashtirilgan yoki qo'lda bajariladigan harakatlar
Incident	Kompaniya aktivlariga ta'sir ko'rsatuvchi, axborot xavfsizligiga oid tasdiqlangan hodisa
SLA	Service Level Agreement (Xizmat ko'rsatish darajasi to'g'risidagi kelishuv: reaksiya vaqti, ishga yaroqlilik va h.k.)
MTTR	Mean Time To Respond (Insidentga javob qaytarishning 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 o'zaro hamkorlik interfeysi)
Application Programming Interface	Transport Layer Security (Tarmoq ulanishlarini himoya qiluvchi kriptografik protokol)
CVE	Umumiy zaifliklar va xavflar (Axborot xavfsizligi zaifliklarining umumiy

	qabul qilingan identifikatori)
VM	Virtual mashina
Cloud Console	Ishlab chiqaruvchining infratuzilmasida joylashtirilgan XDR bulutli boshqaruv konsoli
Telemetriya	Hodisalarni tahlil qilish va korrelyatsiyalash uchun agentlar tomonidan uzatiladigan ma'lumotlar majmuyi
Siyosat	Yakuniy nuqta yoki qurilmalar guruhiga qo'llanadigan xavfsizlik qoidolari va sozlamalari to'plami

15 Ilovalar ro'yxati

1-ilova – Axborotlashtirish obyektining tavsifi.

2-ilova – Texnik talablarga muvofiqlik jadvali.

TTni ishlab chiquvchi:

AXvaRBD Axborot xavfsizligi bo'limi
boshlig'i

imzo

R.A. Abdulvaat

AXvaRB direktor

imzo

B.A. Olmatov

Axborotlashtirish obyektining xususiyatlari

“UMS” MChJ – 2014-yil 1-dekabrda 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-sonli qaroriga asosan tashkil etilgan bo‘lib, O‘zbekiston Respublikasining yetakchi mobil operatorlaridan biri hisoblanadi.

O‘zbekiston Respublikasi Prezidentining 2021-yil 19-iyuldagi PQ-5187-sonli qaroriga muvofiq, O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi “UMS” MChJning ta’sischisidir.

Kompaniyaning shtat birligi 1800 kishini tashkil etadi.

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

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

Muvofiqlik jadvali

Talab raqami	Talabning nomi / texnik tavsiflar
1	Dasturiy ta'minot 3 yil muddatga (obuna, texnik yordamni o'z ichiga olgan holda) yetkazib berilishi kerak.
2	Yechim "Extended Detection and Response" (XDR) sinfiga mansub bo'lishi kerak.
3	Platforma 24/7 rejimida ishlash imkoniyatiga ega markazlashtirilgan boshqaruv konsolini qo'llab-quvvatlashi lozim.
4	SaaS modelida yetkazib berilganda quyidagi shartlarga rioya qilinishi kerak: - Buyurtmachining ma'lumotlarini ajratib qo'yish; - ma'lumotlarni sertifikatlangan data-markazlarda joylashtirish; - ma'lumotlarni uzatish va saqlashda shifrlashdan foydalanish.
5	Yechim arxitekturasini servislarni to'xtatmasdan gorizontol kengayishni ta'minlashi kerak.
6	Quyidagi funksiyalarning mavjud bo'lishi majburiy: - zaifliklardan foydalanishning oldini olish; - faylli va faylsiz hujumlardan himoya qilish; - zararli skriptlardan himoya qilish; - tovlamachi dastur (ransomware) turidagi hujumlarni aniqlash va 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 tarmoq himoya vositalari (tarmoqlararo ekranlar, tajovuzlarning oldini olish tizimlari) bilan nativ integratsiyani qo'llab-quvvatlashi kerak.
10	Yechim javob berish ssenariylari doirasida tarmoq ulanishlari, IP-manzillar va domenlarni avtomatik bloklashni qo'llab-quvvatlashi kerak.
11	Integratsiya uchinchil tomon ma'lumotlar brokerlaridan foydalanilmagan holda amalga oshirilishi kerak.
12	Ushbu yechim xavfsizlik hodisalariga javob berishning avtomatlashtirilgan ssenariylarini ta'minlaydi va ishlab chiqaruvchining 100 dan ortiq tayyor pleybukini o'z ichiga oladi, jumladan: - chekka nuqtalarni izolyatsiyalash; - zararli jarayonlarni yakunlash; - fayllarni xesh bo'yicha bloklash; - sud-texnik ekspertiza artefaktlarini yig'ish.
13	Yechim dasturiy kod yozmasdan turib, javob qaytarishning maxsus ssenariylarini yaratish imkoniyatini qo'llab-quvvatlaydi.
14	Yechim real vaqtga yaqin rejimda yangilanib turadigan global kibertahdid manbalaridan foydalanadi.
15	Yechim hodisalarni dolzarb komprometatsiya indikatorlari (IoC) bilan avtomatik korrelyatsiyalashni qo'llab-quvvatlaydi.
16	Yechim quyidagilarni qo'llab-quvvatlaydi: - rollarga asoslangan kirish modeli (RBAC); - foydalanuvchilar harakatlari auditini; - barcha yig'iladigan hodisalar haqidagi xizmat ma'lumotlarini (telemetriya) kamida 30 kun saqlashni, hodisalar tarixini 12 oygacha saqlashni.

17	<p>Yechim quyidagilarni shakllantirishni qo'llab-quvvatlaydi:</p> <ul style="list-style-type: none"> - tezkor boshqaruv panellarini; - AX bo'limi rahbariyati uchun hisobotlarni; - ma'lumotlarni tashqi SIEM-tizimlariga yuklab olishni.
18	<p>Yechim zaifliklarni nazorat qilish hamda o'rnatilgan agentlarsiz tarmoq va aktivlarni skanerlash uchun ishlab chiqaruvchining oraliq (proksi) serveriga asoslangan tarmoq zaifliklari skaneridan foydalanish imkoniyatini qo'llab-quvvatlashi kerak.</p> <p>Yechim zaifliklarni nazorat qilish uchun yagona platforma doirasida quyidagi kengaytmalarni qo'llab-quvvatlashi lozim:</p> <ul style="list-style-type: none"> - muayyan zaiflikning ekspluatatsiyasini avtomatik bloklay oladigan himoya mexanizmlari (aniqlash va javob berish platformasining faol oldini olish qoidalari) mavjudligini hisobga oluvchi muhimlikni baholash algoritmlarini o'z ichiga olishi; - uchinchi tomon zaiflik skanerlaridan zaifliklar to'g'risidagi ma'lumotlarni avtomatik yig'ishni va ularni zaifliklarni boshqarishning yagona tizimiga integratsiya qilishni ta'minlashi; - eng jiddiy xatarlarni, vaqt o'tishi bilan xatar darajasining o'zgarish dinamikasini va ularni bartaraf etish jarayonini vizualizatsiya qilish uchun maxsus monitoring panelini o'z ichiga olishi; - zaifliklarni bartaraf etish uchun avtomatlashtirilgan o'rnatilgan pleybuklarni taqdim etishi, jumladan, jiddiy zaifliklarni qo'lda aralashuvsiz bartaraf etish uchun to'liq avtomatlashtirilgan harakatlarni qo'llab-quvvatlashi; - tarmoq ichida tajovuzkorning harakatlanishi uchun ma'lum tugunlardagi qaysi zaifliklardan foydalanish mumkinligini ko'rsatuvchi "hujum yo'llari" vizualizatsiyasini taqdim etishi; - zaiflik xatarini baholash mexanizmini taqdim etishi, bunda nafaqat CVSS bahosi, balki mazkur zaiflikning ekspluatatsiya belgilari (EPSS) mavjudligi ham hisobga olinishi; - tashqi hujum yuzasini nazorat qilish hamda tashqaridan keladigan tashqi zaifliklar va hujum vektorlarini baholash uchun qo'shimcha modul qo'shish imkoniyati, ular yagona platforma doirasida boshqa tahdidlar bilan korrelyatsiya qilinishi; - aniqlangan zaifliklarni aniqlash va javob berish platformasida qayd etilgan faol axborot xavfsizligi insidentlari bilan avtomatik tarzda bog'lash imkoniyatini o'z ichiga olishi.
19	<p>Yechim quyidagilar bilan integratsiyani qo'llab-quvvatlaydi:</p> <ul style="list-style-type: none"> - Active Directory / LDAP; - REST API'ni qo'llab-quvvatlaydigan platformalar bilan; - ogohlantirishlar va audit jurnallarini yuborish uchun tashqi Syslog Receiver'lar bilan.
20	Hisob qaydnomalarini qo'lda boshqarish zaruratisiz avtomatik sinxronlashtirish qo'llab-quvvatlanadi.
21	Yechimda REST API mavjud.
22	<p>Foydalanish jarayonida quyidagi funksiyalar bajarilishi kerak:</p> <ul style="list-style-type: none"> - signaturalar, deteksiya modellari va tahlil komponentlari avtomatik tarzda yangilanishi kerak, - yechim komponentlarni yangilash vaqtida uzluksiz himoyani ta'minlashi kerak, - vendor kamida 24x7 darajasidagi texnik yordamni ta'minlashi kerak.
23	Yechim Yakuniy nuqtaga masofadan ulanish imkoniyatini qo'llab-quvvatlashi kerak.
24	Yechim ISO 27001 sertifikatiga ega bo'lishi shart.
25	<p>Yechim qurilmalarni nazorat qilish bo'yicha quyidagi funksiyalarga ega bo'lishi kerak:</p> <ul style="list-style-type: none"> - Windows va macOS OT uchun shifrlashni boshqarishni ta'minlashi; - Windows va macOS OT uchun USB-qurilmalarni nazorat qilish funksiyalarini ta'minlashi; - Bluetooth-qurilmalarni bloklash imkoniyatiga ega bo'lishi; - muayyan qurilmalarda chop etishni taqiqlash imkoniyatiga ega bo'lishi.
26	<p>Yechim quyidagilardan olinadigan telemetriyani barqaror qayta ishlashni ta'minlaydi:</p> <ul style="list-style-type: none"> - bitta mantiqiy tenant doirasida kamida 10 000 ta Yakuniy nuqtadan; - arxitekturani o'zgartirmagan holda keyinchalik kengaytirish imkoniyati bilan.

27	Yechim yagona tahdidlarni boshqarish platformasi va yakuniy nuqtalarga o'rnatiladigan yagona agent doirasida LLM va bulutli omborlarga ma'lumotlar uzatilishini nazorat qilish hamda yakuniy nuqtalarda ma'lumotlar sizib chiqishining oldini olish imkoniyatini qo'llab-quvvatlashi kerak.
28	Yakuniy nuqta agenti odatiy rejimda o'rtacha quyidagilardan ko'p resurs sarflamasligi kerak: - Markaziy protsessorning (CPU) 5 foizini; - 500 MB tezkor xotirani; - 1 GB disk maydonini.
29	Yechim ma'lumotlar va telemetriyani yo'qotmagan holda tahlil hamda boshqaruv komponentlarining ishdan chiqishga bardoshlilikini ta'minlashi kerak.
30	Yechim xatning mazmunidagi niyatlarni sun'iy intellekt yordamida chuqur tahlil qilish orqali fishing xatlarini aniqlash va o'chirish uchun maxsus modulni qo'llash imkoniyatini qo'llab-quvvatlashi kerak.
31	Integratsiya quyidagilarni ta'minlashi kerak: - foydalanuvchilar, guruhlar va rollar haqida ma'lumot olishni; - xavfsizlik hodisalarini foydalanuvchi qaydnomalari bilan o'zaro bog'lashni; - hodisalar kontekstini yaratish uchun katalog ma'lumotlaridan foydalanishni.
32	Tashqi SIEM-tizimlar bilan ikki tomonlama integratsiya ta'minlanadi, jumladan: - insidentlar va ogohlantirishlarni uzatish; - boyitilgan hodisalarni uzatish.
33	Quyidagilar orqali integratsiyani qo'llab-quvvatlash: - REST API; - Syslog; - maxsus konnektorlar.
34	Yechimdan quyidagilar sifatida foydalanish mumkin: - SIEM uchun hodisalar manbai sifatida; - SIEM'ga majburiy ulanishni talab qilmaydigan avtonom XDR-platforma sifatida.
35	Integratsiya quyidagilarni ta'minlashi kerak: - xavfsizlik telemetriyasini olishni; - fishing hujumlari va qaydnomalarning komprometatsiyasini aniqlashni.
36	Yechim quyidagilar uchun ommaviy, hujjatlashtirilgan REST API taqdim etishi kerak: - voqea va hodisalarni qabul qilish; - himoya obyektlarini boshqarish; - javob choralari ssenariylarini ishga tushirish.
37	API quyidagilarni qo'llab-quvvatlashi lozim: - tokenlar orqali autentifikatsiya qilish; - kirish huquqlarini cheklash; - murojaatlarni jurnallashtirish.
38	Yechim ITSM toifasidagi tizimlar bilan quyidagi maqsadlarda integratsiyani qo'llab-quvvatlashi kerak: - hodisalarni avtomatik tarzda yaratish; - tekshiruv holatlarini uzatish; - javob choralari natijalariga ko'ra hodisalarni yopish.
39	Quyidagilar doirasida integratsiyalardan foydalanish imkoniyati qo'llab-quvvatlanishi kerak: - avtomatik playbook-lar; - yarim avtomatik javob choralari ssenariylari.
40	Yechimni litsenziyalash himoyalangan yakuniy nuqtalar soniga qarab, litsenziyalanadigan hajmni moslashuvchan tarzda oshirish imkoniyati bilan amalga oshirilishi kerak.

41	<p>Litsenziya narxiga quyidagilar kiritilishi lozim:</p> <ul style="list-style-type: none"> - yakuniy nuqtalarda hujumlarning oldini olish funksiyalari; - aniqlash va javob choralari ko'rish funksiyalari (EDR/XDR); - markazlashtirilgan boshqaruv konsoli; - mashinaviy ta'lim va xulq-atvor modellariga asoslangan tahlil; - o'rnatilgan avtomatik javob choralari ssenariylari.
42	<p>Quyidagi funksiyalar uchun qo'shimcha to'lovga yo'l qo'yilmaydi:</p> <ul style="list-style-type: none"> - hodisalar korrelyatsiyasi; - hujum zanjirlarini vizualizatsiya qilish; - avtomatik javob choralari; - asosiy hisobotlar va asboblarni panellari.
43	<p>Litsenziya yechimidan foydalanish huquqini quyidagi shartlar bilan o'z ichiga olishi kerak:</p> <ul style="list-style-type: none"> - kecha-yu kunduz rejimida; - voqea va hodisalar soniga cheklolrsiz.
44	<p>Litsenziya doirasida quyidagilar taqdim etilishi kerak:</p> <ul style="list-style-type: none"> - signaturalarni muntazam yangilash; - tahliliy modellarni yangilash; - platformaning funksional komponentlarini yangilash.
45	<p>Litsenziya quyidagilarni o'z ichiga olishi kerak:</p> <ul style="list-style-type: none"> - 24x7 darajasidagi texnik yordam; - bilimlar bazasi va javob choralari bo'yicha tavsiyalardan foydalanish imkoniyati.
46	<p>Litsenziyalash quyidagilarga bog'liq bo'lmashligi lozim:</p> <ul style="list-style-type: none"> - ishlov beriladigan trafik hajmiga; - tahliliy qoidalar soniga; - boshqaruv konsoli foydalanuvchilari soniga.
47	<p>- Tizimning ishlash rejimlariga doir talablar</p> <p>Tizimning asosiy ishlash rejimi avtomatlashtirilgan bo'lib, administrator tomonidan boshqariladi. Tizim quyidagi rejimlarda ishlash imkoniyatini ta'minlashi lozim: shtat rejimi (uzluksiz kecha-kunduz ishlash); avtonom rejim (tizim komponentlari o'rtasida yoki tashqi tarmoqlar bilan aloqa bo'lmagan hollarda).</p>
48	<p>- Dasturiy ta'minot majmuasini yetkazib berish hamda tizimning ishga tushirilishini ta'minlash uchun Ijrochi xodimlarining soni va malakasiga doir talablar:</p> <p>Ijrochi xodimlari tarkibida texnik qo'llab-quvvatlash muhandisining kamida bitta shtat birligi bo'lishi shart;</p> <p>texnik qo'llab-quvvatlash muhandisi Buyurtmachida Tizimga rejali texnik va avariya xizmat ko'rsatish uchun zarur hajmda bilimga ega bo'lishi kerak.</p>
49	<p>- Audit, monitoring va hisobotlarga doir talablar</p> <p>Tizim foydalanuvchilar va ma'murlarning harakatlari auditini, xavfsizlik va ekspluatatsiya hodisalarini qayd etishni, shuningdek, komponentlarning holati va mavjudligini monitoring qilishni ta'minlashi kerak;</p> <p>Tizim shubhali faollik aniqlanganda ogohlantirishlar yuborish imkoniyati bilan real vaqt rejimida auditni qo'llab-quvvatlashi lozim;</p> <p>Barcha hodisalar sana va vaqt, manba va harakat natijasi ko'rsatilgan holda qayd etilishi kerak;</p> <p>Tizimda jurnallarni ruxsatsiz o'zgartirish va o'chirishdan himoya qilish ta'minlanishi lozim;</p> <p>Hisobotlar so'rov bo'yicha va/yoki jadval asosida, standart formatlarga (PDF, CSV) eksport qilish imkoniyati bilan taqdim etilishi shart.</p> <p>Auditorlik va monitoring ma'lumotlarini (loglarni) saqlash muddati – kamida 12 oy.</p>
50	<p>Himoyalangan yakuniy nuqtalar soni – kamida 2000 ta</p>
51	<p>Loyiha montaj ishlarini o'z ichiga oladi.</p>

52	Loyiha loyihalash ishlarini o'z ichiga oladi.
53	Loyihaga Buyurtmachi mutaxassislarini o'qitish kiritilgan
54	Loyihaga dasturiy ta'minotni MKBda sertifikatlash kiritilgan
55	Ijrochida MAFning mavjudligi