



«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 “15” - 

**“UNIVERSAL MOBILE SYSTEMS” MChJ ehtiyojlari uchun
Axborot va xavfsizlik hodisalarini boshqarish tizimini (SIEM)
yetkazib berish, o'rnatish va ishga tushirish bo'yicha**

TEXNIK TOPSHIRIQ

Toshkent – 2026

Оглавление

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	11
7	Ishlarni bajarish va xizmatlar ko'rsatishda xavfsizlikka qo'yiladigan talablar	12
8	Bajarilgan ishlar va ko'rsatilgan xizmatlar natijalariga oid texnik va boshqa hujjatlarni topshirish bo'yicha talablar	12
9	Buyurtmachi xodimlarini o'qitishga doir talablar	12
10	Kafolat majburiyatlari	13
11	Servis va texnik qo'llab-quvvatlash shartlari	13
12	Texnik yordamga qo'yiladigan talablar	14
13	Ishlar, xizmatlar va ularni ko'rsatish shartlariga doir boshqa talablar	15
14	Foydalanilgan atamalar va qisqartmalar	16
15	Ilovalar ro'yxati	17

1 Umumiy ma'lumotlar

Mazkur Texnik topshiriqnomada loyihani 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 qo'yadigan talablarini ifodalash uchun yetarli bo'lgan SIEM axborot va xavfsizlik hodisalarini boshqarish tizimiga (keyingi o'rinlarda – Tizim, AT) qo'yiladigan talablar bayon etilgan.

Axborotlashtirish obyektining tavsifi 1-ilovada keltirilgan.

1.1 Bajariladigan ishlar va ko'rsatiladigan xizmatlarning nomi

Loyihaning to'liq nomi: SIEM axborot va xavfsizlik hodisalarini boshqarish tizimi (matnda bundan keyin – Tizim).

Ishlar Buyurtmachining infratuzilmasi va maydonchasida bajariladi.

Ushbu Texnik topshiriq doirasida Ijrochi dasturiy ta'minotni yetkazib berish, SIEM dasturiy majmuasini o'rnatish, joriy etish 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 Kompaniyaning axborot xavfsizligi hodisalari to'g'risidagi ma'lumotlarni monitoring qilish va boshqarish vositasini joriy etishdan iborat.

Tizim tomonidan hal etiladigan asosiy vazifalar:

- xavfsizlik hodisalarini markazlashtirilgan holda yig'ish va saqlash;
- AT va tarmoq infratuzilmasini uzluksiz monitoring qilish;
- axborot xavfsizligi hodisalarini aniqlash;
- hodisalarni tahlil qilish va tekshirish;
- axborot xavfsizligi holatining yagona manzarasini shakllantirish;
- hodisalarga javob choralarini qo'llab-quvvatlash;
- hisobotlar va tahliliy ma'lumotlarni tayyorlash;
- axborot xavfsizligi talablariga rioya etilishini nazorat qilish.

Tizimning asosiy maqsadi – "UMS" MChJ kompaniyasida yuzaga keladigan hodisalarni o'z vaqtida aniqlash, tekshirish va ularga javob choralarini ko'rish maqsadida axborot xavfsizligi hodisalarini markazlashtirilgan holda yig'ish, tahlil qilish va o'zaro bog'lashdan iborat.

2 Loyihani amalga oshirish uchun asos

Axborot xavfsizligi va rejim departamentining 2026-yilga mo'ljallangan 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)

SIEM tizimini joriy etish Buyurtmachining mas'ul shaxslari bilan birgalikda, uning mavjud AT-infratuzilmasi ishiga xalal yetkazmagan holda, mavjud veb-resurslar va veb-ilovalar dastlabki yuzaki o'rganib chiqilgach amalga oshirilishi lozim. Korporativ tizimlardan birortasini to'xtatishni talab qiladigan barcha ishlar Buyurtmachi bilan oldindan kelishilishi shart.

Loyiha doirasida Ijrochi quyidagi ish bosqichlarini bajarishi 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 o'zaro hamkorlik qilishni va Buyurtmachining AT-infratuzilmasini birgalikda o'rganishni o'z ichiga oladi. Mazkur bosqichda xodimlar quyidagilarni aniqlashlari lozim:

- Buyurtmachi tarmog'i topologiyasining eng muhim jihatlarini;
- Tizimni joriy etish davomida Buyurtmachi va Ijrochining mas'uliyat doiralarini;
- Tizim nazorat qiladigan va himoya qiladigan AT-resurslar 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;
- Tizim ishlashi uchun zarur bo'lgan modullarni faollashtirish;
- zarur litsenziyalarni faollashtirish.

Agar Tizim ishida Buyurtmachining AT-infratuzilmasi obyektlari bilan bog'liq bo'lmagan xatolar tufayli nosozliklar aniqlansa, Ijrochi bajarilgan ishlar to'g'risidagi dalolatnoma imzolangunga qadar mahsulotning funksionaliga tuzatishlar kiritish majburiyatini oladi.

3.3 Tizimni nazorat qilish va qabul qilib olish tartibi

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

Qabul sinovlarining maqsadi Tizim tarkibiy qismlarining ishga yaroqliligini hamda ularning Texnik topshiriq (TT) 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 tomonidan imzolanadigan bayonnoma bilan rasmiylashtirilishi kerak. Qabul sinovlari muvaffaqiyatli o'tkazilgach, qabul sinovlarini yakunlash dalolatnomasi imzolanadi.

Qabul sinovlari vaqtida kamchiliklar, nuqsonlar yoki TT 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 yaroqliligiga ta'sir darajasi;
- kamchiliklarni (nuqsonlarni) bartaraf etish uchun talab etiladigan muddatlar.

Kamchiliklar, nuqsonlar yoki tizimga qo'yiladigan talablardan boshqa chetga chiqishlar bartaraf etilgan paytdan e'tiboran besh ish kuni ichida qabul komissiyasi tegishli tarkibiy qismning takroriy qabul sinovlarini o'tkazishi va Tizimni doimiy foydalanishga qabul qilishi shart.

3.4 Xodimlarni o'qitish.

O'qitish ushbu TTning 9-bandiga muvofiq amalga oshiriladi.

4 Ishlarni bajarish va xizmatlar ko'rsatish joyi

Ijrochi dasturiy ta'minotni quyidagi manzil bo'yicha yetkazib berish, o'rnatish va sozlashni ta'minlashi shart: O'zbekiston Respublikasi, 100000, Toshkent shahri, 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 shartnomaviy munosabatlar imzolangan kundan boshlab 90 kalendar kunidan oshmasligi kerak.

5 Tizimga qo'yiladigan texnik talablar

Tizimga quyidagi asosiy texnik talablar qo'yiladi.

5.1 Umumiy talablar

- 5.1.1 Taklif etilayotgan tizim SIEM (Security Information and Event Management) sinfiga oid bo'lishi hamda axborot xavfsizligi va AT-infratuzilmasi hodisalarini markazlashtirilgan tarzda yig'ish, saqlash, qayta ishlash, indekslash, izlash, o'zaro bog'lash va tahlil qilishni ta'minlashi lozim.
- 5.1.2 Tizim loglarni yuritish, xavfsizlik monitoringi, hodisalarni tekshirish, hisobotlar tuzish, vizualizatsiya va ma'muriy boshqaruv vazifalari uchun yagona interfeys hamda yagona ma'lumotlar omborini taqdim etishi lozim.
- 5.1.3 Tizim hodisalarni oldindan majburiy normallashtirish, agregatlash yoki ma'lumotlarni belgilangan sxemagacha qisqartirishsiz, asl holatida yoxud asl holatiga maksimal darajada yaqin ko'rinishda saqlashi kerak.
- 5.1.4 Tizim ma'lumotlarning qat'iy belgilangan relyatsion modelisiz saqlash va qidiruv sxemasini qo'llab-quvvatlashi hamda inson o'qiy oladigan formatdagi har qanday manbalardan olingan turli xil mashina ma'lumotlari bilan ishlash imkonini berishi kerak.
- 5.1.5 Yechim yirik korporativ buyurtmachilar tomonidan sanoat miqyosida qo'llanilganligi tasdiqlangan amaliyotga hamda hujjatlar, professional servislar, o'qitish, qo'llab-quvvatlash va hamkorlarning rivojlangan ekotizimiga ega bo'lishi kerak.
- 5.1.6 Yechimni litsenziyalash shaffof bo'lishi hamda arxitekturani to'liq almashtirish zaruratisiz, ishlov beriladigan/indekslanadigan ma'lumotlar hajmi va/yoki funksional modullar bo'yicha miqyosni kengaytirish imkonini berishi kerak.

5.2 Arxitektura va miqyoslanuvchanlik

- 5.2.1 Yechim dasturiy ta'minot shaklida bo'lishi va ishlab chiqaruvchining maxsus jismoniy qurilmalaridan majburiy foydalanishni talab qilmasligi kerak.
- 5.2.2 Tizim jismoniy infratuzilma, virtual muhit, xususiy/ommaviy bulut yoki gibrid modelda joylashtirilishini qo'llab-quvvatlashi kerak.
- 5.2.3 Tizim markaziy va masofaviy maydonchalar uchun taqsimlangan arxitekturani, jumladan, ma'lumotlarni yig'ish, buferlash, uzatish va markazlashgan holda qayta ishlashni qo'llab-quvvatlashi kerak.
- 5.2.4 Arxitektura tizimni to'liq qayta o'rnatmasdan yig'ish, indekslash/saqlash va qidiruv komponentlarining gorizontal miqyoslanishini qo'llab-quvvatlashi kerak.
- 5.2.5 Tizim bir nechta saqlash/indekslash tugunlari bo'yicha taqsimlangan qidiruvni ta'minlashi va qidiruv so'rovlariga parallel ishlov berishni qo'llab-quvvatlashi kerak.
- 5.2.6 Tizim qidiruv samaradorligini optimallashtirish, foydalanish huquqlarini cheklash va saqlash muddatlarini boshqarish uchun turli turdagi ma'lumotlarni alohida mantiqiy omborlar/indekslarga joylashtirishni qo'llab-quvvatlashi kerak.
- 5.2.7 Tizim katta hajmdagi mashina ma'lumotlarini qayta ishlashni qo'llab-quvvatlashi va tegishli infratuzilma loyihalashtirilganda, bir sutkada o'nlab TB ma'lumotgacha masshtablanish imkoniyatiga ega ekanligi hujjatlar bilan tasdiqlangan bo'lishi kerak.

5.3 Ma'lumotlarni yig'ish, qabul qilish va integratsiyalashga doir talablar

- 5.3.1 Tizim Syslog, TCP/UDP protokollari, himoyalangan TLS/SSL kanallari, agentlik dasturiy ta'minoti, API/REST, WMI, SNMP events, jurnal fayllari, JSON, XML, CSV, ma'lumotlar bazalari hamda skriptli va modulli manbalardan ma'lumotlar yig'ishni ta'minlashi lozim.
- 5.3.2 Agentlik dasturiy ta'minoti ma'lumotlar uzatishni shifrlashni, markaziy komponentlar ishlamay qolganda keshlashni, qabul qiluvchi tugunlar o'rtasidagi yuklamani muvozanatlashni va ishonchli transport protokoli orqali ma'lumotlar uzatishni qo'llab-quvvatlashi kerak.
- 5.3.3 Tizim ma'lumotlarni yig'ishning ham agentli, ham agentsiz usullarini, jumladan, tarmoq orqali loglarga bevosita kirish, mavjud Syslog-serverlardan ma'lumotlarni qabul qilish va API orqali integratsiyalashni qo'llab-quvvatlashi lozim.
- 5.3.4 Tizim ko'p qatorli va murakkab hodisalarni, ularning strukturasi va dastlabki vaqt belgisini yo'qotmagan holda indekslashni qo'llab-quvvatlashi lozim.
- 5.3.5 Tizim hodisalarni qabul qilish va tahlil qilishni boshlashdan oldin qat'iy jadval sxemasini majburiy yaratishni talab qilmasligi kerak.
- 5.3.6 Tizim istalgan manbalardan olingan dastlabki, o'zgartirilmagan mashina ma'lumotlarini qat'iy relyatsion sxemaga majburan keltirmasdan qabul qilish, indekslash va saqlashni ta'minlashi kerak.
- 5.3.7 Tizim turli vaqt mintaqalaridagi vaqt belgilarini to'g'ri qayta ishlashi hamda hodisaning asl vaqtini tizimga kelib tushgan vaqti bilan birga saqlashi kerak.
- 5.3.8 Tizim faqat ishlab chiqaruvchining tayyor konnektorlariga bog'liq bo'lib qolmasligi lozim: mahsulotning dastlabki kodini o'zgartirmagan holda yangi manbalarni ulash va log formatlaridagi o'zgarishlarga moslashish imkoniyati mavjud bo'lishi kerak.
- 5.3.9 Manbalarning mavjudligi avtomatik tarzda tekshirilishi, kelib tushayotgan hodisalarning to'liqligi nazorat qilinishi va muhim manbalardan ma'lumotlar kelishi to'xtaganda xabar berilishi qo'llab-quvvatlanishi lozim.
- 5.3.10 Tizim Active Directory/LDAP, autentifikatsiya tizimlari, tarmoqlararo ekranlar, IDS/IPS, WAF, VPN, EDR/XDR/antiviruslar, DLP, zaiflik skanerlari, pochta va veb-shlyuzlar, DNS/DHCP, tarmoq qurilmalari, NetFlow/IPFIX, operatsion tizimlar, ma'lumotlar bazalari, virtualizatsiya tizimlari, bulutli xizmatlar, biznes-ilovalar, Service Desk/ITSM, CMDB va foydalanuvchi ilovalari bilan integratsiyani qo'llab-quvvatlashi kerak.

5.4 Ma'lumotlarni saqlash, indekslash va ularning hayotiy sikliga doir talablar

- 5.4.1 Tizim dastlabki, o'zgartirilmagan mashina ma'lumotlarini indekslashi va shu ma'lumotlar asosida keyingi qidiruv, tekshiruv va hisobotlarni ta'minlashi kerak.
- 5.4.2 Tizim diskdagi joydan foydalanishni optimallashtirish uchun indekslangan ma'lumotlarni avtomatik siqishni qo'llab-quvvatlashi kerak.
- 5.4.3 Manba turlari, indekslar, muhimlik darajasi va komplayens talablariga ko'ra saqlash muddatlarini moslashuvchan sozlash orqali tezkor, iliq va arxiv ma'lumotlarini saqlash imkoniyati ta'minlanishi kerak.
- 5.4.4 Tizim, ma'lumotlar eskirgan sari ularni Buyurtmachining siyosatiga muvofiq batafsil boshqarishni: arzonroq/tashqi saqlagichga o'tkazish, arxivlash va/yoki o'chirishni

qo'llab-quvvatlashi kerak.

- 5.4.5 Tizim mavjudlikni, yaxlitlikni, ishdan chiqishga chidamlilikni ta'minlash va qidiruv samaradorligini oshirish uchun ma'lumotlar/indekslar replikatsiyasini qo'llab-quvvatlashi lozim.
- 5.4.6 Saqlagichni butun tizimni to'xtatmasdan kengaytirish imkoniyati ta'minlanishi kerak.
- 5.4.7 Jurnallar va audit ma'lumotlarini ruxsatsiz o'zgartirish va o'chirishdan himoya qilish, jumladan, yaxlitlikni tekshirish mexanizmlari ham ta'minlanishi lozim.

5.5 Normallashtirish, boyitish va kontekstga oid talablar

- 5.5.1 Tizim odatiy xavfsizlik ssenariylari uchun hodisalarni yagona ma'lumotlar modeliga normallashtirishni qo'llab-quvvatlashi kerak, bunda asl xom ma'lumotlar qidirish va tekshirish uchun ochiq qolishi lozim.
- 5.5.2 Maydonlarni ajratib olish mantig'ini, ma'lumotnomalarni, normallashtirish yoki boyitish qoidalarini o'zgartirish ilgari saqlangan hodisalarni majburiy qayta yuklashni talab qilmasligi kerak.
- 5.5.3 Tizim hodisalarni toifalarga ajratishni va ularni qo'shimcha ma'lumotlar (kontekst, ma'lumotnomalar, aktivlar ro'yxatlari, foydalanuvchilar haqidagi ma'lumotlar, AD/IDM ma'lumotlari, tashqi va ichki tahdid turlari hamda boshqa ma'lumotnoma manbalari) bilan boyitishni qo'llab-quvvatlashi lozim.
- 5.5.4 Foydalanuvchilarning atributlarini: login, F.I.Sh., bo'linma, lavozim, rahbar, telefon, joylashuvi, imtiyozlilik belgisi, ishga kirgan/ishdan bo'shagan sanalar va boshqa atributlarni olish uchun korporativ kataloglar bilan integratsiya qo'llab-quvvatlanishi kerak.
- 5.5.5 Bitta xodim yoki subyektga bir nechta hisob qaydnomasi/login mos kelishini (korrelyatsiyasini) qo'llab-quvvatlash imkoniyati bo'lishi lozim.
- 5.5.6 Qurilmalar haqida ma'lumotlarni: xost nomi, IP, MAC, joylashuvi, egasi, muhimligi, maxfiy ma'lumotlar mavjudligi, me'yoriy talablarga muvofiqligini olish uchun aktivlar bazasi (CMDB) bilan integratsiyani qo'llab-quvvatlashi kerak.
- 5.5.7 Tizim o'tgan davrlar uchun qidirish va hisobot berish maqsadida yangi ma'lumotnomalar va kontekstli ma'lumotlarni avval indekslangan hodisalarga qo'llash imkonini berishi lozim.

5.6 Qidiruv, tahlil va korrelyatsiyaga oid talablar

- 5.6.1 Tizim kalit so'zlar, vaqt oraliqlari, mantiqiy operatorlar, muntazam ifodalar va umumiy belgilar yordamida indekslangan ma'lumotlarning istalgan maydoni bo'yicha interaktiv to'liq matnli qidiruvni qo'llab-quvvatlashi kerak.
- 5.6.2 Tizim real vaqtdagi qidiruvlarni ham, rejalashtirilgan qidiruvlarni ham, shuningdek, bir nechta qidiruv so'rovining parallel bajarilishini ham qo'llab-quvvatlashi lozim.
- 5.6.3 Tizim ma'lumotlarni oldindan normallashtirmasdan yoki alohida SQL-ma'lumotlar bazasiga yuklamasdan, bevosita dastlabki indekslangan hodisalar bo'yicha qidirish, tekshirish, korrelyatsiya qilish va hisobotlar yaratish imkonini berishi kerak.
- 5.6.4 Tizim shunday yondashuvni qo'llab-quvvatlashi lozimki, unda dastlabki hodisalar to'liq saqlanadi, maydonlarni ajratib olish, normallashtirish, ma'lumotlar bilan boyitish va talqin qilish esa ham qabul qilish bosqichida, ham avval saqlangan ma'lumotlarni qidirish

va tahlil qilish bosqichida bajarilishi mumkin bo'лади.

- 5.6.5 Tizim, kirish huquqlarining rolga asoslangan modelini hisobga olgan holda, qidiruv so'rovlarini saqlash, tahrirlash, qayta ishlatish va boshqa foydalanuvchilarga uzatish imkoniyatini berishi kerak.
 - 5.6.6 Tizim statistik tahlilni qo'llab-quvvatlashi lozim: sanash, noyob qiymatlar, yig'indi, minimum, maksimum, o'rtacha qiymat, mediana, moda, standart og'ish, dispersiya, persentillar, qiymatning birinchi/oxirgi uchragan holati.
 - 5.6.7 Tizim kamyob va anomal qiymatlarni aniqlash, xulq-atvorning bazaviy profillarini yaratish hamda og'ishlarni, jumladan, signaturalarga qat'iy bog'lanmagan noma'lum tahdidlar va APT-hujumlar ssenariylarini aniqlashni qo'llab-quvvatlashi kerak.
 - 5.6.8 Tizim hodisalarni vaqtinchalik, mantiqiy, xulq-atvorga oid va statistik qoidalar, shu jumladan ko'p bosqichli hujum ssenariylari bo'yicha o'zaro bog'lashni (korrelyatsiya) qo'llab-quvvatlashi lozim.
 - 5.6.9 Tizim aniqlash ssenariylarini tasniflash va tavsiflash uchun kill chain, MITRE ATT&CK modellari yoki shunga o'xshash freymvorklardan foydalanishni qo'llab-quvvatlashi kerak.
 - 5.6.10 Tizim shaxsiy korrelyatsiya qoidalarini yaratish, mavjud qoidalarni o'zgartirish va ularni sanoat miqyosida ishga tushirishdan oldin sinovdan o'tkazish imkonini berishi lozim.
 - 5.6.11 Tizim Buyurtmachining infratuzilmasiga moslashtirish imkoniyati bilan oldindan sozlab qo'yilgan SIEM-kontentni: korrelyatsiya qoidalari, asboblarni panellari, hisobotlar, ma'lumotlar modellari, tekshiruv ssenariylari va xavfsizlik monitoringi andozalarini taqdim etishi kerak.
- 5.7 Monitoring, ogohlantirishlar va hodisalarni tekshirishga oid talablar
- 5.7.1 Tizim real vaqtga yaqin rejimda monitoring olib borishni hamda qidiruv natijalari, korrelyatsiya qoidalari va tahliliy ssenariylar asosida ogohlantirishlarni shakllantirishni qo'llab-quvvatlashi lozim.
 - 5.7.2 Ogohlantirishlar ustuvorliklarni sozlash, takroriy ishga tushishlarning oldini olish, ishga tushish chastotasini cheklash va mas'ul guruhlariga yo'naltirishni qo'llab-quvvatlashi lozim.
 - 5.7.3 Tizim elektron pochta, tashqi tizimlar bilan integratsiyalar, Webhook/API orqali, foydalanuvchi skriptlarini ishga tushirish yoki boshqa avtomatlashtirish mexanizmlari yordamida bildirishnomalar yuborishni qo'llab-quvvatlashi kerak.
 - 5.7.4 Tizim insidentlarni tekshirish ish oqimlarini ta'minlashi lozim: insident kartochkasi/obyekti, dastlabki hodisalar va kontekstni bog'lash, tekshiruv tarixi, statuslar, izohlar, mas'ullarni tayinlash hamda natijalarni hujjatlashtirish imkoniyati.
 - 5.7.5 Tizim batafsil tekshiruv o'tkazish uchun yig'ma hodisa/dashboard/korrelyatsion ishga tushishdan dastlabki hodisalarga o'tishni ta'minlashi lozim.
- 5.8 Vizualizatsiya va hisobotlarga qo'yiladigan talablar
- 5.8.1 Tizim interaktiv dashboardlar va hisobotlar, jumladan, jadvallar, vaqtinchalik diagrammalar, chiziqli, ustunli, maydonli, doiraviy va nuqtali grafiklar, holat indikatorlari hamda IP/Geo-IP bo'yicha geografik vizualizatsiyalarni yaratishni qo'llab-quvvatlashi kerak.
 - 5.8.2 Vizualizatsiyalar real vaqtda yangilanishni, jamlangan ko'rsatkichlardan dastlabki

hodisalarga chuqurlashib o'tishni (drill-down) va anomaliya/chekinishlarni ajratib ko'rsatishni qo'llab-quvvatlashi lozim.

- 5.8.3 Tizim texnik va notexnik foydalanuvchilarga hisobotlar va dashboardlar yaratish, shu jumladan panellarni vizual tahrirlash hamda sarlavhalar, shartli belgilar, o'qlar va filtrlarni sozlash imkonini berishi kerak.
- 5.8.4 Tizim hisobotlarni jadval bo'yicha shakllantirishni hamda ularni PDF, CSV, XLS/XLSX kabi keng tarqalgan va mahsulotda mavjud bo'lgan boshqa formatlarda eksport qilish/jo'natishni qo'llab-quvvatlashi kerak.
- 5.8.5 Tizim axborot xavfsizligi va regulyatorlar talablariga, jumladan ISO 27002, NIST, PCI DSS va shunga o'xshash standartlarga muvofiqlikni ta'minlash vazifalari uchun hisobotlar va monitoring panellarini qo'llab-quvvatlashi kerak.

5.9 Xavfsizlik, kirish huquqi va auditga doir talablar

- 5.9.1 Tizim ma'lumotlar manbalari, turlari, vaqt oraliqlari, hisobotlar, boshqaruv panellari, qidiruvlar va ma'muriy funksiyalarga kirishni cheklash imkoniyati bilan foydalanuvchilar va API uchun moslashuvchan rollarga asoslangan kirish modelini (RBAC) qo'llab-quvvatlashi kerak.
- 5.9.2 Tizim Active Directory/LDAP va korporativ yagona autentifikatsiya (SSO) tizimlari bilan integratsiyani qo'llab-quvvatlashi lozim.
- 5.9.3 Komponentlar o'rtasida ma'lumotlar uzatish zamonaviy kriptografik protokollardan foydalangan holda himoyalangan kanallar orqali amalga oshirilishi kerak.
- 5.9.4 Tizim foydalanuvchilar va ma'murlarning harakatlari, xususan: tizimga kirishlar, qidiruv so'rovlari, hisobotlarni ko'rish, konfiguratsiyani o'zgartirish, foydalanuvchilarni boshqarish, qoidalarni yaratish/o'zgartirish va boshqa muhim amallarning to'liq auditini yuritishi kerak.
- 5.9.5 Audit qaydlari sana va vaqt, foydalanuvchi/subyekti, manba, bajarilgan harakat va uning natijasini o'z ichiga olishi lozim.
- 5.9.6 Tizim indekslangan hodisalarning yaxlitligini tasdiqlash mexanizmlarini, jumladan xeshlash va/yoki hodisalarni raqamli imzolash yoxud autentifiklikni nazorat qilishning funksional jihatdan ekvivalent mexanizmini qo'llab-quvvatlashi kerak.
- 5.9.7 Tizim o'z konfiguratsiyasini, komponentlarining mavjudligini va tizim servislarining holatini kuzatishni ta'minlashi hamda nosozliklar haqida xabar berish imkoniyatiga ega bo'lishi kerak.

5.10 Arxitekturaning ochiqligi va uchinchi tomon tizimlari bilan integratsiya

- 5.10.1 Tizim indekslangan ma'lumotlarga kirish, qidiruv so'rovlarini bajarish, konfiguratsiya obyektlarini boshqarish va tashqi tizimlar bilan integratsiyalashuv uchun ochiq API interfeyslarini taqdim etishi lozim.
- 5.10.2 Python, Java, JavaScript, C# kab i keng tarqalgan dasturlash tillari yoki shunga o'xshash tillar uchun SDK yoxud kutubxonalarni qo'llab-quvvatlashi maqsadga muvofiqdir.
- 5.10.3 Tizimning barcha konfiguratsiyalari veb-interfeys, CLI va/yoki konfiguratsiya fayllari orqali boshqarilishi kerak.
- 5.10.4 Tizim tashqi vizualizatsiya tizimlari, BI, ITSM/SOAR, CMDB, threat intelligence,

monitoring tizimlari va Buyurtmachining boshqa korporativ platformalari bilan integratsiyani qo'llab-quvvatlashi lozim.

5.10.5 Tizim xom, o'zgartirilgan yoki boyitilgan hodisalarni tashqi tizimlarga Syslog TCP/UDP, raw TCP orqali, fayl, API yoxud shunga o'xshash mexanizmlar yordamida yuborish imkoniyatiga ega bo'lishi kerak.

5.10.6 Tizim ommabop mahsulotlar va xavfsizlik ssenariylari uchun ommaviy va/yoki ishlab chiqaruvchi tomonidan taqdim etilgan ilovalardan/integratsiya paketlaridan foydalanishni qo'llab-quvvatlashi lozim.

5.11 Ishdan chiqishga chidamlilik va ishlash rejimlariga qo'yiladigan talablar

5.11.1 Tizim N+1 maqsadli arxitekturasida asosiy komponentlarni zaxiralashni, klasterlashni, muhim ma'lumotlarni replikasiya qilishni va yagona ishdan chiqish nuqtasi mavjud bo'lmashligini qo'llab-quvvatlashi kerak.

5.11.2 Tizim, uning komponentlarida nosozliklar yuzaga kelganda, avtomatik ravishda tiklanishni yoki hujjatlashtirilgan tiklash tartib-taomilini ta'minlashi kerak.

5.11.3 Tizim faoliyatining asosiy rejimi — administrator boshqaruvi ostida avtomatlashtirilgan rejimda uzluksiz, kecha-yu kunduz ishlashdir.

5.11.4 Tizim shtatli, servis va avtonom rejimlarni, shu jumladan, markaziy komponentlarga vaqtincha ulanish imkoni bo'lmaganda ma'lumotlarni lokal buferlash imkoniyatini qo'llab-quvvatlashi kerak.

5.12 Ishlash samaradorligi va o'tkazuvchanlik qobiliyatiga qo'yiladigan talablar

Yetkazib beriladigan yechim quyidagi talablarga javob berishi lozim:

№	Ko'rsatkich	Talab etiladigan qiymat
1.	Hodisalarni qabul qilish bo'yicha o'rtacha samaradorlik (EPS)	kamida 80 000 EPS yoki hodisaning o'rtacha hajmiga qarab hisoblangan ekvivalent hajmdagi ma'lumotlar
2.	Hodisalarni qabul qilish bo'yicha eng yuqori samaradorlik	kamida 150 000 EPS
3.	Qisqa muddatli "burst" (keskin) yuklanish imkoniyati	arxitektura va buferlash to'g'ri hisoblangan taqdirda hodisalarni yo'qotmasdan 250 000 EPSgacha
4.	Indekslandigan ma'lumotlarning sutkalik hajmi	platformani o'zgartirmasdan keyinchalik oshirish imkoniyati bilan sutkasiga kamida 100 GB
5.	"Qaynoq" ma'lumotlarni (tezkor kirish) saqlash hajmi	kamida 180 sutka
6.	"Iliq" ma'lumotlarni saqlash hajmi	kamida 12 oy
7.	Arxiv ma'lumotlarini saqlashning umumiy muddati	kamida 3 yil
8.	Hodisaga ishlov berishdan bildirishnomagacha bo'lgan maksimal kechikish	shtatli yuklanishda muhim korrelyatsion ssenariylar uchun 3 soniyadan oshmasligi kerak
9.	Shtatli yuklanishda hodisalarning yo'qolishi	manbalar va uzatish kanallari to'g'ri sozlanganida 0%
10.	Bir vaqtning o'zida ulangan manbalar soni	kamida 2 000

№	Ko'rsatkich	Talab etiladigan qiymat
11.	Taqsimlangan kollektorlar/agentlarni qo'llab-quvvatlash	kamida 10 ta masofaviy maydoncha
12.	Bir vaqtning o'zida ishlaydigan SOC foydalanuvchilarining soni	kamida 20 nafar
13.	90 kunlik ma'lumotlar bo'yicha qidiruv so'rovining bajarilish vaqti	kelishilgan namunaviy qidiruv so'rovlari uchun 120 soniyadan ko'p bo'lmasligi lozim
14.	6 oylik jamlanma hisobotni shakllantirish vaqti	10 daqiqadan oshmasligi kerak
15.	Ishlash samaradorligini kengaytirish	tizimni to'liq to'xtatmagan holda, gorizontol
16.	EPS'ni oshirish imkoniyati	arxitektura yondashuvini o'zgartirmasdan, kamida 3 baravarga
17.	Ma'lumotlarni alohida saqlashni qo'llab-quvvatlash (hot/warm/archive tiers)	majburiy
18.	Ishdan chiqishga chidamlilik	yagona ishdan chiqish nuqtasining mavjud emasligi (N+1)

5.13 Qo'shimcha foydalanish ssenariylariga doir talablar

- 5.13.1 Tizim bir marta yig'ilgan va indekslangan ma'lumotlardan turli ssenariylarda foydalanish imkonini berishi kerak: axborot xavfsizligi monitoringi, komplayens, insidentlarni tekshirish, firibgarlikni aniqlash, IT-operatsiyalar, ilovalar monitoringi, raqamli tahlil va biznes-tahlil.
- 5.13.2 Tizim ma'lumotlarni alohida platformaga o'tkazish zaruratisiz, qo'shimcha modullar, ilovalar yoki integratsiyalar hisobiga funksionallikni kengaytirishni qo'llab-quvvatlashi lozim.
- 5.13.3 Tizim munosabat bildirishni avtomatlashtirish, SOAR/ITSM bilan integratsiya qilish hamda foydalanuvchilar va obyektlar xatti-harakatlarining kengaytirilgan tahlili yo'nalishida yanada rivojlanish imkoniyatini ta'minlashi kerak.

6 Ijrochiga qo'yiladigan talablar

Ijrochiga quyidagi talablar qo'yiladi:

6.1 Xarid jarayoni doirasida Ijrochi quyidagi ma'lumotlarni taqdim etishi shart:

- yetkazib beriladigan dasturiy ta'minotning batafsil spetsifikatsiyasi;
- dasturiy ta'minotni yetkazib berish va o'rnatish muddatlari;
- kafolatdan keyingi servisli texnik yordam ko'rsatish shartlari va qiymati;
- dasturiy ta'minot litsenziyalari (obuna) shartlari va qiymati;
- taklif etilayotgan texnik yechimning o'ziga xos xususiyatlari.

6.2 Ijrochiga qo'yiladigan umumiy talablar

Ijrochi quyidagi talablarga javob berishi kerak:

- ko'rsatilgan xizmatlarni taqdim etish (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 oxirgi foydalanuvchilarga tarqatish uchun hujjatli tasdiqnomaga ega bo'lishi;

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

- Ijrochi "Kiberxavfsizlik markazi" DUKda dasturiy ta'minotni axborot va kiberxavfsizlik talablariga muvofiqligi yuzasidan ekspertizadan yoki sertifikatliyadan o'tkazish niyati to'g'risida kafolat xatini taqdim etish majburiyatini o'z zimmasiga oladi.

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

6.3 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 avtorizatsiya xatining nusxasi;

- ishlab chiqaruvchi kompaniyaning kamida 2 nafar muhandisining sertifikat nusxalari

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

6.4 Ishlab chiqaruvchiga qo'yiladigan talablar

Vendor-kompaniya bozorda kamida 5 yildan buyon mavjud bo'lishi va O'zbekiston bozorida o'zining vakolatli hamkorlariga ega bo'lishi shart.

7 Ishlarni bajarish va xizmatlar ko'rsatishda xavfsizlikka qo'yiladigan talablar

Loyihani amalga oshirishda faqat dasturiy yechimlardan foydalanilgani sababli, xavfsizlik bo'yicha maxsus talablar qo'yilmaydi.

8 Bajarilgan ishlar va ko'rsatilgan xizmatlar natijalariga oid texnik va boshqa hujjatlarni topshirish bo'yicha talablar

Tizimni joriy etish va sanoat tartibida foydalanishga topshirish yakunlanganidan so'ng, Ijrochi Tizimning amalda joriy etilgan holatini **aks ettiruvchi** ishchi (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;
- me'moriy va tarmoq sxemalari;
- apparat va dasturiy ta'minot komponentlarining ro'yxati va konfiguratsiyasi;
- Buyurtmachining infratuzilmasi bilan integratsiya tavsifi;
- tarmoq manzillari (IP, portlar, protokollar);
- foydalanish bo'yicha qisqacha hujjatlar;
- axborot xavfsizligi bo'yicha amalga oshirilgan chora-tadbirlar tavsifi.

Hujjatlar dolzarb, to'liq, Tizimning amaldagi joriy etilishiga muvofiq bo'lishi, shuningdek, Ijrochini jalb etmagan holda undan foydalanish uchun yetarli bo'lishi kerak.

9 Buyurtmachi xodimlarini o'qitishga doir talablar

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

a) Buyurtmachining ikki nafar axborot xavfsizligi mutaxassisini mazkur majmuani

boshqarish bo'yicha sertifikatlangan 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 materiallari;
- mashg'ulotlar yozuvlari;
- o'qishni yakunlaganlikni tasdiqlovchi hujjat (sertifikatlar).

b) Tizim foydalanuvchilarini o'qitish.

Tinglovchilar soni: 10 nafargacha.

Shakli: namoyishli va amaliy.

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

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

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

10 Kafolat majburiyatlari

Ijrochi, agar ishlab chiqaruvchi tomonidan hujjatlarda belgilangan dasturiy (dasturiy-apparat) ta'minotdan foydalanish qoidalariga rioya qilinsa va o'rnatilgan dasturiy ta'minot ishiga ruxsatsiz aralashuv bo'lmasa, bajarilgan ish sifatining Buyurtmachi tomonidan ko'rsatilgan texnik topshiriqqa hamda talablarga muvofiq bo'lishini kafolatlashi shart.

Tizimni joriy etish bo'yicha bajarilgan ishlar uchun kafolat muddati **12 (o'n ikki) oyni** tashkil etishi kerak va u Tomonlar ishlarni topshirish-qabul qilish dalolatnomasini imzolagan kundan boshlab hisoblanadi.

Litsenziyalarga obuna (Subscription) muddati **12 (o'n ikki) oyni** tashkil etishi kerak.

Sinov tariqasida foydalanish davri 1 (bir) oyni tashkil etadi va Tomonlar ishlarni topshirish-qabul qilish dalolatnomasini imzolagan kundan boshlab hisoblanadi.

11 Servis va texnik qo'llab-quvvatlash shartlari

Ishlab chiqaruvchining servis qo'llab-quvvatlash muddati – **12 (o'n ikki) oy**, dasturiy ta'minot joriy etilgan paytdan boshlab. Dasturiy ta'minot komponentlari uchun servis qo'llab-quvvatlash ham Ishlab chiqaruvchi, ham Ijrochi tomonidan ko'rsatilishi lozim.

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

Dasturiy ta'minotni texnik qo'llab-quvvatlash ishlari quyidagilarni o'z ichiga olishi kerak:

- a) WAF Tizimining server qismi uzluksiz ishlashini ta'minlash:
 - apparat va dasturiy resurslardan foydalanishni optimallashtirish uchun Tizim parametrlarini sozlash;
 - xavfsizlik siyosatini boshqarish uchun Tizim parametrlarini sozlash;
 - yangilanishlar o'tkazilganidan so'ng Tizimning shtat rejimida ishlashini sinovdan o'tkazish.
- b) Mavjud boshqaruv va monitoring tizimlari bilan integratsiya qilish.
- c) Tizim miqyosini kengaytirish bo'yicha maslahatlar berish.
- d) Dasturiy ta'minot ishlab chiqaruvchisi 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) Tizimning ishlashi bilan bog'liq yuzaga kelgan muammolarni hal etish va maslahatlar berish uchun "UMS" MChJ talabiga binoan mutaxassisni VPN orqali ulash.

g) Dasturiy majmuaning ish faoliyatini tiklash:

- dasturiy vositalardagi nosozlikdan keyin kamida 2 ish kuni ichida Tizimning ish faoliyatini shtat rejimida tiklash;

- dasturiy majmuani qayta sozlash, qayta konfiguratsiya qilish, yangilash va/yoki to'liq qayta o'rnatish, shuningdek, nosozlikka olib kelgan sabablarni bartaraf etish (nosozlik kompaniya mahsulotlari tufayli yuzaga kelgan taqdirda);

- tiklash ishlarini o'tkazish uchun nosozlik vaqtida Tizimni o'chirib qo'yish imkoniyati (baypas rejimi);

- apparatdagi nosozliklar, elektr ta'minotidagi uzilishlar va h.k.lardan so'ng Tizim faolligini tiklash;

- zaxira nusxalardan ma'lumotlarni tiklash amaliyotlari.

- bajarilgan ishlar to'g'risida hisobotlar taqdim etish.

12 Texnik yordamga qo'yiladigan talablar

12.1 Ijrochi yetkazib beriladigan dasturiy majmuaga 12 oy davomida texnik yordam ko'rsatilishini ta'minlashi shart.

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

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

12.4 Qo'llab-quvvatlash quyidagilarga nisbatan qo'llanilishi lozim:

- dasturiy qism (software).

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

- 24x7x365 – kritik insidentlar uchun;

- kamida 8x5 – nokritik insidentlar uchun (Buyurtmachi bilan kelishuvga ko'ra).

12.6 Insidentlarga munosabat bildirish vaqti:

- Kritik (P1): 15–30 daqiqadan oshmasligi kerak;

- Yuqori (P2): 1 soatdan oshmasligi kerak;

- O'rta (P3): 4 soatdan oshmasligi kerak;

- Past (P4): 1 ish kunidan oshmasligi kerak.

12.7 Tiklash (yoki muammoni aylanib o'tish) vaqti:

- P1: 4 soatdan oshmasligi kerak;

- P2: 8 soatdan oshmasligi kerak;

- P3: 2 ish kunigacha;

- 4-band: Buyurtmachi bilan kelishuvga ko'ra.

12.8 Ijrochi texnik qo'llab-quvvatlash uchun arizalarni ro'yxatga olishning yagona kanalini taqdim etishi 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 ishlash qobiliyati tekshirilgandan va tuzilgan shartnomaga muvofiq qabul qilish-topshirish dalolatnomasi imzolangandan so'ng qabul qilingan hisoblanadi. Ushbu Texnik topshiriqda va uning ilovalarida ko'rsatilmagan boshqa shartlar shartnomada keltiriladi.

13.2 Xizmatlar ko'rsatishning majburiy sharti – Buyurtmachining amaldagi ichki tartib qoidalariga, nazorat-o'tkazish rejimiga, ichki nizomlari, yo'riqnomalari va talablariga rioya qilishdir. Bu haqda Buyurtmachi Ijrochini xabardor qiladi. Buyurtmachi dasturiy ta'minot obunasini faollashtirish bilan bog'liq e'lon qilingan muammolarni hal qilish bo'yicha Ijrochi bilan aloqa qilishga vakolatli xodimlarning ro'yxati va aloqa ma'lumotlarini Ijrochiga taqdim etadi.

13.3 Taklifni taqdim etishning batafsil shakli ushbu Texnik topshiriqning 2-ilovasida keltirilgan.

13.4 Butlanishiga oid talab

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

13.5 Integratsiyaga oid talab

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

13.6 Yangiligi to'g'risida ma'lumot

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

13.7 Sug'urta

Talablar qo'yilmaydi, biroq Ijrochi dasturiy (apparat-dasturiy) majmuani Buyurtmachiga rasman topshirish paytigacha uning saqlanishi uchun javobgar bo'ladi.

13.8 Xizmatlarni ko'rsatishda mas'uliyatni taqsimlash matritsasi

Texnik xizmat ko'rsatish	Ijrochi	Buyurtma chi
Tizimdan foydalanish imkoniyati		
Muammoni aniqlash, uning ustuvorligini 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 statistik ma'lumotlarni taqdim etish	R	A
Barcha so'rovlarni Huquq egasining portalida ro'yxatdan o'tkazish	R	A
Dasturiy ta'minotni yangilash, tuzatish va to'g'rilashlar kiritish		
Jarayon 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 (muayyan qaror qabul qilishdan oldin mas'ul shaxs yordamiga

murojaat qiladigan soha mutaxassisi yoki ekspert);

I (ingl. *Informed*) – kuzatuvchi, xabardor qilinadigan shaxs (topshiriqning bajarilish jarayoni (yoki natijalari) to'g'risida xabardor qilinishi kerak bo'lgan shaxs).

14 Foydalanilgan atamalar va qisqartmalar

№	Atama / Qisqartma	Kengaytmasi	Ta'rifi
1	SIEM	Security Information and Event Management	Axborot xavfsizligi hodisalarini markazlashtirilgan holda yig'ish, saqlash, korrelyatsiya qilish va tahlil etish tizimi
2	SOC	Security Operations Center	Axborot xavfsizligi hodisalarini monitoring qilish va bartaraf etish markazi
3	EPS	Events Per Second	Bir soniyada ishlov beriladigan hodisalar soni
4	LPS	Logs Per Second	Tizimga bir soniyada kelib tushadigan loglar (qaydlar) soni
5	GB/day	Gigabytes per day	Kelib tushadigan ma'lumotlarning sutkalik hajmi
6	Correlation	Hodisalarni korrelyatsiya qilish	Bir nechta hodisani yagona insidentga bog'lash
7	Use Case	Aniqlash ssenariysi	Muayyan turdagi tahdidni aniqlashga doir qoidalar to'plami
8	Rule	Korrelyatsiya qoidasi	Shubhali faollikni aniqlashning mantiqiy sharti
9	Incident	AX insidenti	Axborot xavfsizligi buzilganligi tasdiqlangan hodisa
10	Event	Hodisa	Tizimda qayd etilgan harakat yoki holat
11	Log	Hodisalar jurnali	Axborot tizimidagi hodisa haqidagi yozuv
12	Parsing	Parsing (tahliliy ajratish)	Loglarni tuzilmaviy formatga o'tkazish
13	Normalization	Normallashtirish	Hodisalarni yagona tuzilmaga keltirish
14	Enrichment	Ma'lumotlarni boyitish	Hodisaga kontekstli ma'lumot qo'shish
15	IOC	Indicator of Compromise	Komprometatsiya indikator (IP, hesh, domen va b.)
16	MITRE ATT&CK	-	Kiberhujumlar taktikasi va texnikalari bo'yicha bilimlar bazasi
17	UEBA	User and Entity Behavior Analytics	Foydalanuvchilar va obyektlarning xulq-atvor anomaliyalarini tahlil qilish
18	SOAR	Security Orchestration, Automation and Response	Reaksiyalarni orkestrlash va avtomatlashtirish
19	XDR	Extended Detection and Response	Kengaytirilgan aniqlash va bartaraf etish tizimi
20	EDR	Endpoint Detection and Response	Ish stansiyalaridagi tahdidlarni aniqlash tizimi
21	NTA	Network Traffic Analysis	Tarmoq trafikini tahlil qilish
22	NetFlow	—	Tarmoq trafigi statistikasini yig'ish protokoli
23	Syslog	—	Loglarni uzatish protokoli
24	API	Application Programming Interface	Tizimlarning dasturiy hamkorlik interfeysi
25	AD	Active Directory	Microsoft katalog xizmati
26	LDAP	Lightweight Directory Access Protocol	Katalog xizmatiga murojaat qilish protokoli

№	Atama / Qisqartma	Kengaytmasi	Ta'rif
27	RBAC	Role-Based Access Control	Rollarga asoslangan kirishni cheklash
28	MFA	Multi-Factor Authentication	Ko'p faktorli autentifikatsiya
29	SLA	Service Level Agreement	Xizmat ko'rsatish darajasi to'g'risidagi bitim
30	MTTR	Mean Time To Respond/Recover	Reaksiya bildirish/qayta tiklashning o'rtacha vaqti
31	MTTD	Mean Time To Detect	Tahdidni aniqlashning o'rtacha vaqti
32	HA	High Availability	Ishdan chiqishga chidamlilik
33	DR	Disaster Recovery	Nosozlikdan so'ng tiklash rejasi
34	Hot Storage	-	Tezkor (operativ) ma'lumotlar ombori
35	Warm Storage	-	Oraliq ma'lumotlar ombori
36	Cold Storage	-	Arxiv ma'lumotlar ombori
38	Cluster	Klaster	Yagona tizim sifatida ishlaydigan serverlar guruhi
39	Node	Tizim qismi	Klasterdagi alohida server
40	Dashboard	Dashbord	Hodisa va ko'rsatkichlarni vizuallashtirish paneli

15 Ilovalar ro'yxati

1-ilova – Axborotlashtirish obyektining tavsifi.

2-ilova – Texnik talablarga muvofiqlik jadvali.

Texnik topshiriqni ishlab chiqdi:

AX va RBD Axborot xavfsizligi
bo'limi boshlig'i


imzo R.A. Abdulvaat

AX va RB direktor


imzo B.A. Olmatov

Axborotlashtirish obyektining tavsiflari

“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-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-son qaroriga muvofiq, O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi “UMS” MChJning ta’asischisidir.

Kompaniyaning shtat birligi — 1800 kishi.

Serverlarning umumiy soni (jumladan, virtual) — 1000 donadan ko‘p emas.

Tarmoq qurilmalarining umumiy soni — 150 donadan ko‘p emas.

Ilovalarning umumiy soni — 10 ta.

Axborot xavfsizligining axborot-dasturiy vositalari umumiy soni — 10 tadan kam emas.

Umumiy o‘tkazuvchanlik qobiliyati — 1000 Mbit/s dan ko‘p emas.

Yaratiladigan loglarning umumiy hajmi — sutkasiga 100 Gb dan ko‘p emas.

Texnik talablarga muvofiqlik jadvali

Talab raqami	Talab nomi
1	Dasturiy ta'minot 12 oylik obuna litsenziyalari bilan taqdim etiladi (Yechimni litsenziyalash shaffof bo'lishi va arxitekturani to'liq almashtirishni talab qilmasdan, ishlanadigan/indekslanadigan ma'lumotlar hajmi va/yoki funksional modullar bo'yicha kengayish imkonini berishi kerak).
2	Dasturiy ta'minot (yechim) SIEM (Security Information and Event Management) sinfiga mansub bo'lishi kerak.
3	Tizim loglarni yuritish, xavfsizlik monitoringi, hodisalarni tergov qilish, hisobotlar tayyorlash, vizuallashtirish va ma'muriy boshqaruv vazifalari uchun yagona interfeys hamda yagona ma'lumotlar omborini taqdim etadi.
4	Tizim voqealarni dastlabki yoki dastlabki holatga maksimal darajada yaqin ko'rinishda, ma'lumotlarni belgilangan sxemaga majburiy oldindan normallashtirmasdan, agregatsiyalamasdan yoki qisqartirmasdan saqlaydi.
5	Tizim qat'iy belgilangan relyatsion modelsiz ma'lumotlarni saqlash va qidirish sxemasini qo'llab-quvvatlaydi hamda inson o'qiy oladigan formatdagi har qanday manbadan olingan turli xil mashina ma'lumotlari bilan ishlashga imkon beradi.
6	Yechim yirik korporativ buyurtmachilar tomonidan sanoat miqyosida qo'llanishi bo'yicha tasdiqlangan amaliyotga hamda hujjatlar, professional servislari, o'qitish, qo'llab-quvvatlash va hamkorlardan iborat rivojlangan ekotizimga ega.
7	Tizim jismoniy infratuzilma, virtual muhit, xususiy/ommaviy bulut yoki gibridda joylashtirishni qo'llab-quvvatlaydi va ishlab chiqaruvchining ixtisoslashtirilgan jismoniy qurilmalaridan majburiy foydalanishni talab etmaydi.
8	Yechim arxitekturasi tizimni to'liq qayta o'rnatmasdan, yig'ish, indekslash/saqlash va qidirish komponentlarini gorizontallarga kengaytirishni qo'llab-quvvatlaydi.
9	Tizim bir nechta saqlash/indekslash tugunlari bo'yicha taqsimlangan qidiruvni ta'minlaydi va qidiruv so'rovlariga parallel ishlov berishni qo'llab-quvvatlaydi.
10	Tizim qidiruv samaradorligini optimallashtirish, foydalanish huquqini cheklash va saqlash muddatlarini boshqarish uchun turli turdagi ma'lumotlarni alohida mantiqiy omborlar/indekslarga joylashtirishni qo'llab-quvvatlaydi.
11	Tizim katta hajmdagi mashina ma'lumotlarini qayta ishlashni qo'llab-quvvatlaydi va infratuzilma tegishli tarzda loyihalashtirilganda, kuniga o'nlab TB ma'lumotlarga kengaytirilishi mumkinligi hujjatlar bilan tasdiqlangan.
12	Tizim Syslog, TCP/UDP protokollari, himoyalangan TLS/SSL kanallari, agent dasturiy ta'minoti, API/REST, WMI, SNMP events, jurnal fayllari, JSON, XML, CSV, ma'lumotlar bazalari, skript va modul manbalaridan ma'lumotlar yig'ishni ta'minlaydi.
13	Agent dasturiy ta'minoti ma'lumotlar uzatishini shifrlashni, markaziy komponentlar ishlamay qolganda keshlashni, qabul qiluvchi tugunlar o'rtasidagi yuklamani muvozanatlashni va ma'lumotlarni ishonchli transport protokoli orqali uzatishni qo'llab-quvvatlaydi.
14	Tizim ma'lumotlar yig'ishning agentli hamda agentsiz usullarini, jumladan, tarmoq orqali loglarga bevosita kirish, mavjud Syslog-serverlardan ma'lumotlarni qabul qilish va API orqali integratsiyalashuvni qo'llab-quvvatlaydi.
15	Tizim ko'p qatorli va murakkab hodisalarni ularning tuzilmasi va dastlabki vaqt belgisini saqlagan holda indekslashni qo'llab-quvvatlaydi.
16	Tizim hodisalarni qabul qilish va tahlil etishdan avval jadvallarning qat'iy sxemasini yaratishni talab qilmaydi.
17	Tizim har qanday manbadan olingan dastlabki, o'zgartirilmagan mashina ma'lumotlarini oldindan qat'iy relyatsion ma'lumotlar sxemasiga keltirish majburiyatisiz qabul qilish, indekslash va saqlashni ta'minlaydi.

18	Tizim turli vaqt mintaqalaridagi vaqt belgilarini to'g'ri qayta ishlaydi hamda hodisaning asl vaqtini Tizimga kelib tushgan vaqt bilan birga saqlaydi.
19	Tizim faqatgina ishlab chiqaruvchining tayyor konnektorlariga bog'liq bo'lib qolmasligi kerak: mahsulotning asl kodini o'zgartirmasdan yangi manbalarni ulash va log formatlaridagi o'zgarishlarga moslashish imkoniyati bo'lishi lozim.
20	Manbalarning mavjudligi avtomatik tarzda tekshirilishi, kiruvchi hodisalarning to'liqligi nazorat qilinishi va muhim manbalardan ma'lumotlar kelishi to'xtaganida bildirishnoma yuborilishi qo'llab-quvvatlanishi kerak.
21	Tizim Active Directory/LDAP, autentifikatsiya tizimlari, tarmoqlararo ekranlar, IDS/IPS, WAF, VPN, EDR/XDR/antiviruslar, DLP, zaiflik skanerlari, pochta va veb-shlyuzlar, DNS/DHCP, tarmoq qurilmalari, NetFlow/IPFIX, operatsion tizimlar, ma'lumotlar bazalari, virtualizatsiya tizimlari, bulutli servislar, biznes-ilovalar, Service Desk/ITSM, CMDB hamda foydalanuvchi ilovalari bilan integratsiyani qo'llab-quvvatlaydi.
22	Tizim dastlabki, o'zgartirilmagan mashina ma'lumotlarini indekslaydi hamda bu ma'lumotlar asosida keyinchalik qidiruv, tekshiruv va hisobotlar shakllantirishni, shuningdek, diskdagi joydan foydalanishni optimallashtirish uchun indekslangan ma'lumotlarni avtomatik siqishni ta'minlaydi.
23	Tizimda operativ, iliq va arxiv ma'lumotlarini manba turlari, indekslar, muhimlik darajasi va kompayens talablariga ko'ra saqlash muddatlarini moslashuvchan sozlash imkoniyati mavjud.
24	Tizim ma'lumotlar eskirgan sari ularni batafsil boshqarishni qo'llab-quvvatlaydi: Buyurtmachining siyosatiga muvofiq arzonroq/tashqi saqlash vositasiga o'tkazish, arxivlash va/yoki o'chirish.
25	Tizim foydalanish imkoniyati, yaxlitligi, ishdan chiqishga chidamliligi va qidiruv samaradorligini oshirishni ta'minlash uchun ma'lumotlar/indekslar replikatsiyasini qo'llab-quvvatlaydi.
26	Butun tizimni to'xtatmasdan saqlash omborini masshtablash imkoniyati mavjud.
27	Jurnallar va audit ma'lumotlarini ruxsatsiz o'zgartirish va o'chirishdan himoya qilish, jumladan, yaxlitlikni tekshirish mexanizmlari mavjud.
28	Tizim xavfsizlikning tipik ssenariylari uchun hodisalarni yagona ma'lumotlar modeliga normallashtirishni qo'llab-quvvatlaydi, bunda dastlabki xom ma'lumotlar qidiruv va tekshiruv uchun ochiq qolishi kerak.
29	Maydonlarni ajratib olish, ma'lumotnomalar, normallashtirish yoki boyitish qoidalari mantiqini o'zgartirish ilgari saqlangan hodisalarni majburiy qayta yuklashni talab qilmaydi.
30	Tizim hodisalarni tasniflashni va ularni qo'shimcha ma'lumotlar (kontekst, ma'lumotnomalar, aktivlar ro'yxatlari, foydalanuvchilar haqidagi ma'lumotlar, AD/IDM ma'lumotlari, tashqi va ichki tahdid turlari hamda boshqa ma'lumot manbalari) bilan boyitishni qo'llab-quvvatlaydi.
31	Foydalanuvchi atributlarini olish uchun korporativ kataloglar bilan integratsiya qo'llab-quvvatlanadi: login, F.I.Sh., bo'linma, lavozim, rahbar, telefon, joylashuv, imtiyozlilik belgisi, ishga kirgan/bo'shagan sana va boshqa atributlar.
32	Bir nechta hisob qaydnomasi/loginni bitta xodim yoki subyekt bilan o'zaro bog'lash qo'llab-quvvatlanadi.
33	Qurilmalar haqidagi ma'lumotlarni (xost nomi, IP, MAC, joylashuvi, egasi, muhimligi, maxfiy ma'lumotlar mavjudligi, me'yoriy talablarga muvofiqligi) olish uchun aktivlar ma'lumotlar bazasi (CMDB) bilan integratsiya qo'llab-quvvatlanadi.
34	Tizim o'tgan davrlar uchun qidiruv va hisobotlarni shakllantirish maqsadida yangi ma'lumotnomalar hamda kontekstli ma'lumotlarni avval indekslangan hodisalarga qo'llash imkonini beradi.
35	Tizim kalit so'zlar, vaqt oraliqlari, mantiqiy operatorlar, regular ifodalar va o'rniga qo'yish belgilaridan foydalangan holda indekslangan ma'lumotlarning istalgan maydoni bo'yicha interaktiv to'liq matnli qidiruvni qo'llab-quvvatlaydi.
36	Tizim ham real vaqtdagi, ham rejalashtirilgan qidiruvlarni, shuningdek, bir nechta qidiruv so'rovining parallel bajarilishini qo'llab-quvvatlaydi.

37	Tizim ma'lumotlarni oldindan normallashtirmasdan yoki alohida SQL ma'lumotlar bazasiga yuklamasdan, bevosita dastlabki indekslangan hodisalar bo'yicha qidirish, tekshirish, korrelyatsiya qilish va hisobot yaratish imkonini beradi.
38	Tizim dastlabki hodisalar to'liq saqlanadigan, maydonlarni ajratib olish, normallashtirish, ma'lumotlar bilan boyitish va ularni sharhlash esa ham qabul qilish, ham avval saqlangan ma'lumotlarni qidirish va tahlil qilish bosqichida bajarilishi mumkin bo'lgan yondashuvni qo'llab-quvvatlaydi.
39	Tizim ruxsat berishning rolga asoslangan modelini hisobga olgan holda qidiruv so'rovlarini saqlash, tahrirlash, qayta ishlatish va boshqa foydalanuvchilarga uzatish imkonini beradi.
40	Tizim statistik tahlilni qo'llab-quvvatlaydi: sanoq, noyob qiymatlar, yig'indi, minimum, maksimum, o'rtacha qiymat, mediana, moda, standart og'ish, dispersiya, persentillar, qiymatning birinchi/oxirgi marta paydo bo'lishi
41	Tizim kam uchraydigan va anomal qiymatlarni aniqlash, xulq-atvorning asosiy profillarini yaratish va og'ishlarni, jumladan, noma'lum tahdidlar ssenariylarini hamda signaturalarga qat'iy bog'liq bo'lmagan APT-hujumlarni aniqlashni qo'llab-quvvatlaydi.
42	Tizim vaqtinchalik, mantiqiy, xulq-atvorga oid va statistik qoidalar, jumladan, ko'p bosqichli hujum ssenariylari bo'yicha hodisalar korrelyatsiyasini qo'llab-quvvatlaydi.
43	Tizim aniqlash ssenariylarini tasniflash va tavsiflash uchun kill chain, MITRE ATT&CK yoki shunga o'xshash freymvork modellaridan foydalanishni qo'llab-quvvatlaydi.
44	Tizim o'zining korrelyatsiya qoidalarini yaratish, mavjud qoidalarni o'zgartirish va ularni sanoat miqyosida ishga tushirishdan oldin sinovdan o'tkazish imkonini beradi.
45	Tizim Buyurtmachining infratuzilmasiga moslashtirish imkoniyati bilan oldindan sozlab qo'yilgan SIEM-kontentni: korrelyatsiya qoidalari, asboblari panellari, hisobotlar, ma'lumotlar modellari, tekshiruv ssenariylari va xavfsizlik monitoringi andozalarini taqdim etadi.
46	Tizim real vaqtga yaqin rejimda monitoringni qo'llab-quvvatlaydi hamda qidiruv natijalari, korrelyatsiya qoidalari va tahliliy ssenariylar asosida bildirishnomalarni shakllantiradi.
47	Bildirishnomalar prioritetlarni sozlash, takroriy ishga tushishlarning oldini olish, ishga tushish chastotasini cheklash va mas'ul guruhlarga yo'naltirish imkoniyatlarini qo'llab-quvvatlaydi.
48	Tizim elektron pochta, tashqi tizimlar bilan integratsiyalar, Webhook/API orqali, shuningdek, foydalanuvchi skriptlarini ishga tushirish yoki boshqa avtomatlashtirish mexanizmlari yordamida bildirishnomalar yuborishni qo'llab-quvvatlaydi.
49	Tizim insidentlarni tekshirish ish jarayonlarini ta'minlaydi: insident kartochkasi/obyekti, dastlabki hodisalar va kontekstni bog'lash, tekshiruv tarixi, statuslar, izohlar, mas'ul shaxslarni tayinlash hamda natijalarni hujjatlashtirish imkoniyati.
50	Tizim batafsil tekshiruv o'tkazish uchun umumiy hodisa/asboblari paneli/korrelyatsion javobdan dastlabki hodisalarga o'tishni ta'minlaydi.
51	Tizim interaktiv asboblari panellari va hisobotlarni, jumladan, jadvallar, vaqt diagrammalari, chiziqli, ustunli, maydonli, doiraviy va nuqtali grafiklar, holat indikatorlari hamda IP/Geo-IP bo'yicha geografik vizualizatsiyalarni yaratishni qo'llab-quvvatlaydi.
52	Vizualizatsiyalar real vaqt rejimida yangilanishni, umumlashtirilgan ko'rsatkichlardan dastlabki hodisalarga chuqurroq kirish (drill-down) imkoniyatini va anomaliya/chekinishlarni ajratib ko'rsatishni qo'llab-quvvatlaydi.
53	Tizim ham texnik, ham notexnik foydalanuvchilarga hisobotlar va asboblari panellarini yaratish, jumladan, panellarni vizual tahrirlash hamda sarlavhalar, shartli belgilar, o'qlar va filtrlarni sozlash imkonini beradi.
54	Tizim hisobotlarni jadval asosida shakllantirishni hamda ularni PDF, CSV, XLS/XLSX kabi keng tarqalgan va mahsulotda mavjud bo'lgan boshqa formatlarda eksport qilishni/jo'natishni qo'llab-quvvatlaydi.
55	Tizim axborot xavfsizligi va me'yoriy talablarga, jumladan, ISO 27002, NIST, PCI DSS va shunga o'xshash standartlarga muvofiqlik masalalari uchun hisobotlar va monitoring panellarini qo'llab-quvvatlaydi.
56	Tizim foydalanuvchilar va API uchun rollarga asoslangan ruxsat berishning moslashuvchan modelini (RBAC) qo'llab-quvvatlaydi hamda ma'lumotlar manbalari, ma'lumotlar turlari, vaqt

	oraliqlari, hisobotlar, asboblarni panellari, qidiruvlar va ma'muriy funksiyalarga kirishni cheklash imkoniyatini beradi.
57	Tizim Active Directory/LDAP va korporativ yagona kirish (SSO) tizimlari bilan integratsiyani qo'llab-quvvatlaydi.
58	Komponentlar o'rtasida ma'lumotlar almashinuvi zamonaviy kriptografik protokollardan foydalangan holda himoyalangan kanallar orqali amalga oshiriladi.
59	Tizim foydalanuvchilar va ma'murlarning barcha harakatlari: tizimga kirishlar, qidiruv so'rovlar, hisobotlarni ko'zdan kechirish, konfiguratsiyani o'zgartirish, foydalanuvchilarni boshqarish, qoidalar yaratish/o'zgartirish va boshqa muhim amallarning to'liq auditini yuritadi.
60	Tizimning audit hodisalari sana va vaqt, foydalanuvchi/subjekt, manba, bajarilgan harakat va uning natijasini o'z ichiga oladi.
61	Tizim indekslangan hodisalarning yaxlitligini tasdiqlash mexanizmlarini, jumladan, hodisalarni xeshlash va/yoki raqamli imzolash yoxud funksional jihatdan ekvivalent bo'lgan haqiqiylikni nazorat qilish mexanizmini qo'llab-quvvatlaydi.
62	Tizim o'zining konfiguratsiyasi, komponentlarining ishlashi va tizim servislarning holati monitoringini yuritadi hamda bu haqda xabardor qilish imkoniyatini ta'minlaydi.
63	Tizim indekslangan ma'lumotlarga kirish, qidiruv so'rovlarini bajarish, konfiguratsiya obyektlarini boshqarish va tashqi tizimlar bilan integratsiya qilish uchun ochiq API interfeyslarini taqdim etadi.
64	Tizim keng tarqalgan dasturlash tillari, jumladan Python, Java, JavaScript, C# yoki shunga o'xshash tillar uchun SDK (dasturiy ta'minot ishlab chiqish to'plami) yoki kutubxonalarni qo'llab-quvvatlashi kerak.
65	Tizim konfiguratsiyalari veb-interfeys, CLI va/yoki konfiguratsiya fayllari orqali boshqarilishi kerak.
66	Tizim tashqi vizualizatsiya tizimlari, BI, ITSM/SOAR, CMDB, threat intelligence, monitoring tizimlari va Buyurtmachining boshqa korporativ platformalari bilan integratsiyani qo'llab-quvvatlaydi.
67	Tizim xom, o'zgartirilgan yoki boyitilgan hodisalarni Syslog TCP/UDP, raw TCP, fayl, API yoki shunga o'xshash mexanizm orqali tashqi tizimlarga yuborish imkoniyatiga ega.
68	Tizim ommabop mahsulotlar va xavfsizlik ssenariylari uchun ochiq va/yoki ishlab chiqaruvchi tomonidan taqdim etiladigan ilovalar/integratsiya paketlaridan foydalanishni qo'llab-quvvatlaydi.
69	Tizim N+1 maqsadli arxitekturasida asosiy komponentlarni zaxiralash, klasterlash, muhim ma'lumotlarni replikasiya qilish va yagona ishdan chiqish nuqtasining mavjud emasligini qo'llab-quvvatlaydi.
70	Tizim avtomatik tiklanishni ta'minlaydi yoki komponentlar ishdan chiqqan holatlar uchun hujjatlashtirilgan tiklash tartib-qoidasiga ega.
71	Tizimning asosiy ishlash rejimi – administrator nazorati ostida avtomatlashtirilgan rejimda kecha-yu kunduz uzluksiz ishlash.
72	Tizim shtatli, servis va avtonom rejimlarni, jumladan, markaziy komponentlar vaqtincha ishlamay qolganda ma'lumotlarni lokal buferlash imkoniyatini qo'llab-quvvatlaydi.
73	Hodisalarni qabul qilish bo'yicha o'rtacha unumdorlik (EPS) – kamida 80 000 EPS (yoki hodisaning o'rtacha hajmiga qarab hisoblangan ekvivalent ma'lumotlar hajmi).
74	Hodisalarni qabul qilish bo'yicha eng yuqori unumdorlik – kamida 150 000 EPS.
75	Qisqa muddatli "burst" yuklanish imkoniyati — 250 000 EPS gacha (arxitektura to'g'ri hisoblanganda va buferlash mavjud bo'lganda hodisalar yo'qolmaydi)

76	Indekslandigan ma'lumotlarning sutkalik hajmi — kamida 100 GB/sutka (platformani o'zgartirmasdan keyinchalik kengaytirish imkoniyati bilan)
77	“Qaynoq” ma'lumotlarni (tezkor kirish) saqlash hajmi — kamida 180 sutka
78	“Iliq” ma'lumotlarni saqlash hajmi — kamida 12 oy
79	Arxiv ma'lumotlarini saqlashning umumiy muddati — kamida 3 yil (36 oy)
80	Hodisani qayta ishlashdan xabarnoma yuborishgacha bo'lgan maksimal kechikish — shtatdagi yuklanmada muhim korrelyatsion ssenariylar uchun 3 soniyadan oshmasligi kerak
81	Shtatdagi yuklanmada hodisalarning yo'qolishi — manbalar va uzatish kanallari to'g'ri sozlanganida 0%
82	Bir vaqtning o'zida ulangan manbalar soni — kamida 2 000 ta
83	Taqsimlangan kollektorlar/agentlarni qo'llab-quvvatlash — kamida 10 ta masofaviy maydoncha
84	Bir vaqtning o'zida ishlaydigan SOC foydalanuvchilari soni — kamida 20 nafar
85	90 sutkalik ma'lumotlar bo'yicha qidiruv so'rovini bajarish vaqti — kelishilgan tipik qidiruv so'rovlari uchun 120 soniyadan oshmasligi kerak
86	6 oylik agregatsion hisobotni bajarish vaqti — 10 daqiqadan oshmasligi kerak
87	Ishlash samaradorligini gorizontol masshtablash (tizimni to'liq to'xtatmasdan)
88	Arxitekturaviy yondashuvni o'zgartirmasdan EPS'ni kamida 3 barobar oshirish imkoniyati
89	Ma'lumotlarni alohida saqlashni (hot/warm/archive tiers) qo'llab-quvvatlash majburiy
90	Ishdan chiqishga bardoshlilik — yagona nosozlik nuqtasining yo'qligi (N+1)
91	Tizim bir marta yig'ilgan va indekslangan ma'lumotlardan turli ssenariylarda foydalanish imkonini beradi: axborot xavfsizligi monitoringi, komplayens, hodisalarni tergov qilish, firibgarlikni aniqlash, AT-operatsiyalar, ilovalar monitoringi, raqamli tahlil va biznes-tahlil.
92	Tizim ma'lumotlarni alohida platformaga o'tkazish zaruratisiz, qo'shimcha modullar, ilovalar yoki integratsiyalar hisobiga funktsionallikni kengaytirishni qo'llab-quvvatlaydi.
93	Tizim javob qaytarishni avtomatlashtirish, SOAR/ITSM bilan integratsiyalashuv hamda foydalanuvchilar va obyektlar xatti-harakatlarining kengaytirilgan tahlili yo'nalishida yanada rivojlanish imkoniyatini ta'minlaydi.
94	Yechimni texnik qo'llab-quvvatlash — kamida 1 yil.
95	Loyihaga o'rnatish va integratsiya ishlari kiritilgan.
96	Loyihaga loyihalashtirish ishlari kiritilgan.
97	Loyihaga Buyurtmachi mutaxassislarini o'qitish kiritilgan.

98	Loyihaga dasturiy ta'minotni MKBda sertifikatlash kiritilgan.
99	Interfeys tili — rus/ingliz.
100	Ijrochida MAF mavjudligi.