«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" MChJning Axborot xavfsizligi
va rejim bo'yicha direktori

_____ B.A.Olmatov

2026-yil "____"_____

"UNIVERSAL MOBILE SYSTEMS" MCHJ ehtiyojlari uchun Axborot xavfsizligi va hodisalarini boshqarish tizimini (SIEM) yetkazib berish, o'rnatish va foydalanishga topshirish uchun

TEXNIK TOPSHIRIQ

Toshkent – 2026-yil

Mundarija:

1 Umumiy ma'lumotlar 3

2 Loyihani amalga oshirish uchun asos 3

3 Ijrochidan talab qilinadigan ishlar, xizmatlar ro'yxati va ularning hajmi (miqdori) 3

4 Ishlarni bajarish va xizmatlar ko'rsatish joyi 4

5 Tizimga qo'yiladigan texnik talablar 5

6 Ijrochiga qo'yiladigan talablar 13

7 Ishlarni bajarish va xizmatlar ko'rsatish xavfsizligiga qo'yiladigan talablar 14

8 Bajarilgan ishlar va ko'rsatilgan xizmatlar natijalari bo'yicha texnik va boshqa hujjatlarni topshirish talablari 14

9 Buyurtmachining xodimlarini o'qitishga qo'yiladigan talablar 14

10 Kafolat majburiyatlari 15

11 Xizmat ko'rsatish va texnik qo'llab-quvvatlash shartlari 15

12 Texnik yordamga qo'yiladigan talablar 16

13 Ishlar, xizmatlar va ularni ko'rsatish shartlariga qo'yiladigan boshqa talablar 16

14 Foydalaniladigan atamalar va qisqartmalar 17

15 Ilovalar ro'yxati 19

1 Umumiy ma'lumotlar

Ushbu Texnik topshiriqda SIEM axborot xavfsizligi va hodisalarini boshqarish tizimiga (keyingi o'rinlarda - Tizim, AT) qo'yiladigan talablar tavsiflangan bo'lib, ular Buyurtmachining dasturiy ta'minot tarkibiga qo'yiladigan talablarini tavsiflash uchun yetarli hisoblanadi hamda umuman loyihani "tayyor holda topshirish" shartlarida amalga oshirish uchun dasturiy ta'minot va xizmatlarni xarid qilish bo'yicha tender va/yoki tanlov e'lon qilish maqsadida ishlab chiqilgan.

Axborotlashtirish obyektining tavsifi 1-ilovada keltirilgan.

1.1 Bajariladigan ishlar va ko'rsatiladigan xizmatlar nomi

Loyihaning to'liq nomi: SIEM axborot xavfsizligi va hodisalarini boshqarish tizimi (bundan keyin matnda Tizim deb yuritiladi).

Ishlar Buyurtmachining infratuzilmasi va maydonchasida amalga oshiriladi.

Ushbu Texnik topshiriq doirasida Ijrochi dasturiy ta'minotni yetkazib berish, SIEM dasturiy majmuasini o'rnatish, joriy etish va ishga tushirish bo'yicha taklif taqdim etishi lozim.

1.2 Bajariladigan ishlar va ko'rsatiladigan xizmatlardan foydalanish maqsadlari

Loyihaning asosiy maqsadi "UMS" MCHJ infratuzilmasida Kompaniya infratuzilmasidagi axborot xavfsizligi hodisalari haqidagi ma'lumotlarni monitoring qilish va boshqarish vositasini joriy etishdan iborat.

Tizim tomonidan hal etiladigan asosiy vazifalar:

- xavfsizlik hodisalarini markazlashtirilgan tarzda to'plash va saqlash;
- IT va tarmoq infratuzilmasini uzluksiz monitoring qilish;
- axborot xavfsizligi insidentlarini aniqlash;
- insidentlarni tahlil va tekshirish;
- axborot xavfsizligi holatining yagona manzarasini shakllantirish;
- insidentlarga munosabat bildirishni qo'llab-quvvatlash;
- hisobot va tahliliy ma'lumotlarni tayyorlash;
- axborot xavfsizligi talablariga rioya etilishini nazorat qilish.

Tizimning asosiy vazifasi – "UMS" MCHJ kompaniyasida yuzaga keladigan noxush hodisalarni (insidentlarni) o'z vaqtida aniqlash, tekshirish va ularga munosabat bildirish maqsadida axborot xavfsizligi hodisalarini markazlashtirilgan tarzda to'plash, tahlil qilish va o'zaro bog'lashdan (korelyatsiya) iborat.

2 Loyihani amalga oshirish uchun asos

Axborot xavfsizligi va rejim departamentining 2026-yilga rejalashtirilgan rivojlantirish rejasi ("UMS" MCHJning 2026-yilga mo'ljallangan tasdiqlangan biznes-rejasi va byudjeti).

3 Ijrochidan talab qilinadigan ishlar, xizmatlar ro'yxati va ularning hajmlari (soni)

SIEM tizimini joriy etish Buyurtmachining mas'ul shaxslari bilan birgalikda, Buyurtmachining mavjud AT infratuzilmasining ishlash qobiliyatini buzmasdan, mavjud veb-resurslar va veb-ilovalarni oldindan yuzaki o'rganib chiqish orqali amalga oshirilishi lozim. Har qanday korporativ tizimlarni to'xtatishni talab qiladigan barcha ishlar Buyurtmachi bilan oldindan kelishilgan bo'lishi 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

Buyurtmachining Loyiha uchun mas'ul xodimlari bilan o'zaro hamkorlikni va Buyurtmachining AT infratuzilmasini birgalikda o'rganishni o'z ichiga oladi. Ushbu bosqichda xodimlar quyidagilarni aniqlashlari lozim:

- Buyurtmachi tarmog'i topologiyasining eng muhim detallarini;
- Tizimni joriy etish jarayonida Buyurtmachi va Ijrochining javobgarlik sohalarini;
- Tizim nazorat qiladigan va himoya qiladigan AT resurslari sonini.

3.2 Ishga tushirish-sozlash va integratsiya ishlari

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

- Tizimning dasturiy qismini o'rnatish va sozlashni;
- Buyurtmachining tarmoq infratuzilmasiga integratsiya qilishni;
- Tizim ishlashi uchun zarur bo'lgan modullarni faollashtirishni;
- zarur litsenziyalarni faollashtirishni.

Buyurtmachining AT infratuzilmasi obyektlari bilan bog'liq bo'lmagan xatolar tufayli Tizim ishida nosozliklar aniqlangan taqdirda, Ijrochi bajarilgan ishlar to'g'risidagi dalolatnoma imzolangunga qadar mahsulot funksionalligiga tuzatishlar kiritish majburiyatini oladi.

3.3 Tizimni nazorat qilish va qabul qilish tartibi

Tizimni qabul qilish qabul qilish sinovlarini o'tkazish orqali amalga oshirilishi lozim. Qabul qilish sinovlari Buyurtmachi va Ijrochining vakillari tomonidan amalga oshiriladi.

Qabul qilish sinovlarining maqsadi Tizim tarkibiy qismlarining ishlash qobiliyatini va ularning texnik topshiriq talablariga muvofiqligini tasdiqlashdan iborat.

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

Qabul qilish sinovlari natijalari qabul qilish komissiyasi a'zolari tomonidan imzolanadigan bayonnoma bilan rasmiylashtirilishi kerak. Qabul qilish sinovlari muvaffaqiyatli o'tkazilgandan so'ng Qabul qilish sinovlarini yakunlash dalolatnomasi imzolanadi.

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

- kamchiliklar (nuqsonlar) ro'yxati;
- qayd etilgan kamchiliklarning tizim ishlashiga ta'sir darajasi;
- kamchiliklarni (nuqsonlarni) bartaraf etishning talab qilinadigan muddatlari.

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

3.4 Xodimlarni o'qitish.

Ushbu texnik topshiriqning 9-bandiga muvofiq o'qitish.

4 Ishlarni bajarish va xizmatlar ko'rsatish joyi

Ijrochi quyidagi manzil bo'yicha dasturiy ta'minotni yetkazib berish, o'rnatish va sozlashni ta'minlashi lozim: O'zbekiston Respublikasi, Toshkent shahri, 100000, Amir Temur shoh ko'chasi, 24-uy, "UMS" MCHJ markaziy ofisi.

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

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 mansub bo'lishi hamda axborot xavfsizligi va IT infratuzilmasi hodisalarini markazlashgan holda yig'ish, saqlash, qayta ishlash, indekslash, izlash, korrelyatsiyalash va tahlil qilishni ta'minlashi lozim.

5.1.2 Tizim jurnallashtirish, xavfsizlikni monitoring qilish, hodisalarni surishtirish, hisobot berish, vizuallashtirish va ma'muriylashtirish vazifalari uchun yagona interfeys va yagona ma'lumotlar omborini taqdim etishi lozim.

5.1.3 Tizim dastlabki ma'lumotlarni keyinchalik qidirish va tahlil qilish imkoniyati bilan saqlashni ta'minlashi kerak, bunda dastlabki normallashtirish ma'lumotlarni qabul qilishning majburiy sharti bo'lmasligi kerak.

5.1.4 Tizim barcha manbalarni oldindan yagona relyatsion modelga o'zgartirmasdan, turli xil mashina ma'lumotlari bilan ishlashni ta'minlashi lozim.

5.1.5 Yechim yirik korporativ buyurtmachilarda tasdiqlangan sanoatda qo'llash amaliyotiga hamda hujjatlar, professional xizmatlar, o'qitish, qo'llab-quvvatlash va hamkorlarning rivojlangan ekotizimiga ega bo'lishi kerak.

5.1.6 Yechimni litsenziyalash shaffof bo'lishi va arxitekturani to'liq almashtirish zaruratisiz qayta ishlanadigan/indekslanadigan ma'lumotlar hajmi va/yoki funksional modullar bo'yicha masshtablash imkonini berishi kerak.

5.2 Arxitektura va masshtablanuvchanlik

5.2.1 Yechim dasturiy 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 joylashtirishni qo'llab-quvvatlashi lozim.

5.2.3 Tizim markaziy maydoncha va masofaviy maydonchalar uchun taqsimlangan arxitekturani, jumladan ma'lumotlarni yig'ish, buferlash, uzatish va markazlashtirilgan holda qayta ishlashni qo'llab-quvvatlashi lozim.

5.2.4 Arxitektura tizimni to'liq qayta o'rnatmasdan yig'ish, indekslash/saqlash va qidirish komponentlarini gorizontal masshtablashni qo'llab-quvvatlashi lozim.

5.2.5 Tizim bir nechta saqlash/indekslash tugunlari bo'yicha taqsimlangan qidiruvni ta'minlashi va qidiruv so'rovlarini parallel qayta ishlashni qo'llab-quvvatlashi lozim.

5.2.6 Tizim qidiruv unumdorligini optimallashtirish, kirishni chegaralash va saqlash muddatlarini boshqarish uchun turli xil turdagi ma'lumotlarni alohida mantiqiy omborlarga joylashtirishni qo'llab-quvvatlashi lozim.

5.2.7 Tizim katta hajmdagi mashina ma'lumotlarini qayta ishlashni qo'llab-quvvatlashi va tegishli infratuzilma loyihalashtirilganda sutkasiga o'nlab TB ma'lumotlargacha masshtablana olishining hujjat bilan tasdiqlangan imkoniyatiga ega bo'lishi kerak.

5.3 Ma'lumotlarni yig'ish, qabul qilish va integratsiya qilishga qo'yiladigan talablar

5.3.1 Tizim Syslog, TCP/UDP protokollari, himoyalangan TLS/SSL kanallari bo'yicha, agent dasturiy ta'minoti, API/REST, WMI, SNMP events orqali, shuningdek, log-fayllar, JSON, XML, CSV, ma'lumotlar bazalari, skriptli va modulli manbalardan ma'lumotlarni yig'ishni ta'minlashi lozim.

5.3.2 Agent dasturiy ta'minoti ma'lumotlar uzatishni shifrlashni, markaziy komponentlar mavjud bo'lmaganda keshlashshni, qabul qiluvchi uzellar o'rtasidagi yuklamani muvozanatlashni va ishonchli transport protokoli orqali ma'lumotlarni uzatishni qo'llab-quvvatlashi kerak.

5.3.3 Tizim ma'lumotlarni yig'ishning ham agentli, ham agentsiz usullarini, jumladan tarmoq orqali loglarga to'g'ridan-to'g'ri ulanishni, mavjud Syslog serverlaridan qabul qilishni va API orqali integratsiyani qo'llab-quvvatlashi lozim.

5.3.4 Tizim hodisa tuzilmasi va dastlabki vaqt belgisini yo'qotmagan holda ko'p qatorli va murakkab hodisalarni indekslashni qo'llab-quvvatlashi lozim.

5.3.5 Tizim ma'lumotlarni qabul qilishni boshlashdan oldin har bir manba tuzilishi oldindan tavsiflanishini talab qilmasligi kerak.

5.3.6 Tizim har qanday manbalardan dastlabki, o'zgartirilmagan mashina ma'lumotlarini 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 tushish vaqti bilan bir qatorda saqlashi kerak.

5.3.8 Tizim faqat ishlab chiqaruvchining tayyor konnektorlariga qaram bo'lmasligi kerak: yangi manbalarni ulash va mahsulotning dastlabki kodini o'zgartirmasdan log formatlarining o'zgarishiga moslashish imkoniyati bo'lishi kerak.

5.3.9 Manbalarning mavjudligini avtomatik tekshirish, kiruvchi hodisalarning to'liqligini nazorat qilish va muhim manbalardan ma'lumotlar kelib tushishi to'xtatilganda xabardor qilish qo'llab-quvvatlanishi kerak.

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 ilovalari, Service Desk/ITSM, CMDB va foydalanuvchi ilovalari bilan integratsiyani qo'llab-quvvatlashi lozim.

5.4 Ma'lumotlarni saqlash, indekslash va hayot sikliga qo'yiladigan talablar

5.4.1 Tizim dastlabki, modifikatsiyalanmagan mashina ma'lumotlarini indekslashi va ushbu ma'lumotlar bo'yicha keyingi qidiruv, surishtiruv va hisobotlarni ta'minlashi lozim.

5.4.2 Tizim disk xotirasidan foydalanishni optimallashtirish uchun indekslangan ma'lumotlarni avtomatik siqishni qo'llab-quvvatlashi lozim.

5.4.3 Tezkor, issiq va arxiv ma'lumotlarini manba turlari, indekslar, muhimlik darajasi va komplayens talablari bo'yicha saqlash muddatlarini moslashuvchan sozlash orqali saqlash imkoniyati ta'minlanishi lozim.

5.4.4 Tizim ma'lumotlarning eskirishiga qarab ularni batafsil boshqarishni qo'llab-quvvatlashi lozim: arzonroq/tashqi xotiraga o'tkazish, arxivlash va/yoki Buyurtmachining siyosatiga muvofiq o'chirish.

5.4.5 Tizim mavjudlik, yaxlitlik, nosozliklarga chidamlilikni ta'minlash va qidiruv

unumdorligini oshirish uchun ma'lumotlar/indekslar replikatsiyasini qo'llab-quvvatlashi lozim.

5.4.6 Butun tizimni to'xtatmasdan turib ma'lumotlarni saqlash tizimi miqyosini kengaytirish imkoniyati ta'minlanishi kerak.

5.4.7 Jurnallar va audit ma'lumotlarini ruxsatsiz o'zgartirish va o'chirishdan himoya qilish, shu jumladan yaxlitlikni tekshirish mexanizmlari ta'minlanishi lozim.

5.5 Normallashtirish, boyitish va kontekstga doir talablar

5.5.1 Tizim xavfsizlikning namunaviy ssenariylari uchun hodisalarni yagona ma'lumotlar modeliga normallashtirishni qo'llab-quvvatlashi, bunda dastlabki xom ma'lumotlar qidirish va tekshiruv o'tkazish uchun ochiq qolishi lozim.

5.5.2 Maydonlarni ajratib olish mantiqini, ma'lumotnomalarni, normallashtirish yoki boyitish qoidalarini o'zgartirish avval saqlangan hodisalarni majburiy ravishda qayta yuklashni talab qilmasligi kerak.

5.5.3 Tizim hodisalarni toifalash va 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, joylashuv, imtiyozlilik belgisi, ishning boshlanish/tugash sanasi va boshqa atributlar) olish uchun korporativ kataloglar bilan integratsiya qo'llab-quvvatlanishi kerak.

5.5.5 Bitta xodim yoki subyektga tegishli bir nechta hisob yozuvlari/loginlar o'rtasidagi korrelyatsiya qo'llab-quvvatlanishi lozim.

5.5.6 Qurilmalar haqidagi ma'lumotlarni (hostname, IP, MAC, joylashuv, egasi, muhimlik darajasi, nozik ma'lumotlarning mavjudligi, me'yoriy talablarga muvofiqligi) olish uchun aktivlar ma'lumotlar bazasi (CMDB) bilan integratsiya qo'llab-quvvatlanishi lozim.

5.5.7 Tizim o'tgan davrlar bo'yicha qidirish va hisobot tayyorlash uchun ilgari indekslangan hodisalarga yangi ma'lumotnomalar va kontekst ma'lumotlarini qo'llash imkonini berishi kerak.

5.6 Qidiruv, tahlil va korrelyatsiyaga qo'yiladigan talablar

5.6.1 Tizim kalit so'zlar, vaqt oraliqlari, mantiqiy operatorlar, regulyar ifodalar va o'rinbosar belgilaridan foydalangan holda 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, bir nechta qidiruv so'rovlarining parallel bajarilishini ham qo'llab-quvvatlashi kerak.

5.6.3 Tizimda ma'lumotlarni oldindan normallashtirmasdan yoki alohida SQL ma'lumotlar bazasiga yuklamasdan, bevosita boshlang'ich indekslangan hodisalar bo'yicha qidiruv, tekshiruv, korrelyatsiya va hisobot tuzish imkoniyati mavjudligi tizimning qo'shimcha afzalligi sifatida qaraladi.

5.6.4 Tizim shunday yondashuvni qo'llab-quvvatlashi kerakki, bunda boshlang'ich hodisalar to'liq saqlanadi, maydonlarni ajratib olish, ma'lumotlarni normallashtirish, boyitish va talqin qilish esa qabul qilish bosqichida ham, avval saqlangan ma'lumotlarni qidirish va tahlil qilish bosqichida ham amalga oshirilishi mumkin.

5.6.5 Tizim rollarga asoslangan ruxsat modelini hisobga olgan holda qidiruv so‘rovlarini saqlash, tahrirlash, qayta foydalanish va boshqa foydalanuvchilarga uzatish imkonini berishi kerak.

5.6.6 Tizim statistik tahlilni qo‘llab-quvvatlashi kerak: hisoblash, noyob qiymatlar, yig‘indi, minimum, maksimum, o‘rtacha, mediana, moda, standart og‘ish, dispersiya, persentillar, qiymatning birinchi/oxirgi uchrashi.

5.6.7 Tizim kam uchraydigan va anomal qiymatlarni aniqlashni, xatti-harakatlarning tayanch profillarini yaratishni hamda og‘ishlarni, shu jumladan signaturalarga qat’iy bog‘liq bo‘lmagan noma’lum tahdidlar va APT ssenariylarini aniqlashni qo‘llab-quvvatlashi kerak.

5.6.8 Tizim hodisalarni vaqt, mantiq, xulq-atvor va statistik qoidalar, shu jumladan ko‘p bosqichli hujum ssenariylari bo‘yicha korrelyatsiya qilishni qo‘llab-quvvatlashi kerak.

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 xususiy korrelyatsiya qoidalarini yaratish, mavjud qoidalarni o‘zgartirish va sanoat ekspluatatsiyasiga kiritishdan oldin ularni sinovdan o‘tkazish imkonini berishi kerak.

5.6.11 Tizim oldindan sozlangan SIEM kontentini taqdim etishi kerak: Buyurtmachi infratuzilmasiga moslashtirish imkoniyatiga ega korrelyatsiya qoidalari, dashbordlar, hisobotlar, ma’lumotlar modellari, insidentlarni tekshirish ssenariylari va xavfsizlik monitoringi shablonlari.

5.7 Monitoring, ogohlantirishlar va insidentlarni tekshirishga qo‘yiladigan talablar

5.7.1 Tizim real vaqtga yaqin rejimda monitoring qilishni va qidiruv natijalari, korrelyatsiya qoidalari hamda tahliliy ssenariylar bo‘yicha ogohlantirishlarni shakllantirishni qo‘llab-quvvatlashi kerak.

5.7.2 Ogohlantirishlar ustuvorliklarni sozlash, takroriy ishlashlarni bostirish, ishlash chastotasini cheklash va mas’ul guruhlarga yo‘naltirishni qo‘llab-quvvatlashi kerak.

5.7.3 Tizim elektron pochta, tashqi tizimlar bilan integratsiya, Webhook/API, foydalanuvchi skriptlarini ishga tushirish yoki boshqa avtomatlashtirish mexanizmlari orqali bildirishnomalar yuborishni qo‘llab-quvvatlashi kerak.

5.7.4 Tizim insidentlarni tekshirish ish jarayonlarini taqdim etishi kerak: insident kartochkasi/obyekti, dastlabki hodisalar va kontekstni bog‘lash, tekshiruv tarixi, maqomlar, izohlar, mas’ullarni tayinlash va natijalarni hujjatlashtirish imkoniyati.

5.7.5 Tizim umumlashtirilgan hodisa/dashbord/korrelyatsiya ishlashidan batafsil tekshiruv uchun dastlabki hodisalarga o‘tishni ta’minlashi lozim.

5.8 Vizualizatsiya va hisobot shakllantirish bo‘yicha talablar

5.8.1 Tizim interaktiv dashbordlar va hisobotlarni, jumladan jadvallar, vaqt diagrammalari, chiziqli, ustunli, maydonli, doiraviy va nuqtali grafiklar, holat indikatorlari hamda IP/Geo-IP bo‘yicha geografik vizualizatsiyalarni tuzishni qo‘llab-quvvatlashi lozim.

5.8.2 Vizualizatsiyalar real vaqt rejimida yangilanishni, jamlangan ko‘rsatkichlardan dastlabki hodisalarga o‘tishni (drill-down) va anomaliyalar/chetlashishlarni ajratib ko‘rsatishni qo‘llab-quvvatlashi lozim.

5.8.3 Tizim texnik va texnik bo‘lmagan foydalanuvchilarga hisobotlar va dashbordlar yaratish,

shu jumladan panellarni vizual tahrirlash hamda sarlavhalar, shartli belgilar, o'qlar va filtrlarni sozlash imkonini berishi kerak.

5.8.4 Tizim jadval asosida hisobotlarni shakllantirishni va ularni keng tarqalgan formatlarga, jumladan, PDF, CSV, XLS/XLSX hamda mahsulotda mavjud boshqa formatlarga eksport qilish/tarqatishni qo'llab-quvvatlashi lozim.

5.8.5 Tizim axborot xavfsizligi va regulyator talablariga, jumladan ISO 27002, NIST, PCI DSS va shunga o'xshash standartlarga muvofiqlik vazifalari uchun hisobotlar va monitoring panellarini qo'llab-quvvatlashi lozim.

5.9 Xavfsizlik, ruxsat va audit bo'yicha talablar

5.9.1 Tizim ma'lumotlar manbalari, ma'lumotlar turlari, vaqt oraliqlari, hisobotlar, dashbordlar, qidiruvlar va ma'muriy funksiyalarga kirishni cheklash imkoniyatiga ega bo'lgan foydalanuvchilar va API uchun moslashuvchan rolli kirish modelini (RBAC) qo'llab-quvvatlashi lozim.

5.9.2 Tizim Active Directory/LDAP va korporativ yagona kirish tizimlari (SSO) bilan integratsiyani qo'llab-quvvatlashi kerak.

5.9.3 Ma'lumotlarni komponentlar o'rtasida uzatish zamonaviy kriptografik protokollar yordamida himoyalangan kanallar orqali amalga oshirilishi shart.

5.9.4 Tizim foydalanuvchilar va ma'murlarning xatti-harakatlarini to'liq auditini yuritishi kerak: tizimga kirish, qidiruv so'rovlari, hisobotlarni ko'rish, konfiguratsiyani o'zgartirish, foydalanuvchilarni boshqarish, qoidalarni yaratish/o'zgartirish va boshqa muhim harakatlar.

5.9.5 Audit hodisalari sana va vaqtni, foydalanuvchi/subyektni, manbani, bajarilgan harakatni va bajarish natijasini o'z ichiga olishi kerak.

5.9.6 Tizim indekslangan hodisalarning yaxlitligini tasdiqlash mexanizmlarini, jumladan xeshlash va/yoki hodisalarning raqamli imzosini yoki haqiqiylikni nazorat qilishning funksional ekvivalent mexanizmini qo'llab-quvvatlashi lozim.

5.9.7 Tizim o'z konfiguratsiyasi, komponentlardan foydalanish imkoniyati va tizim xizmatlari holati monitoringini ta'minlashi hamda nosozliklar haqida ogohlantirish imkoniyatiga ega bo'lishi lozim.

5.10 Arxitekturaning ochiqligi va tashqi tizimlar bilan integratsiyalashuv

5.10.1 Tizim indekslangan ma'lumotlarga kirish, qidiruv so'rovlarini bajarish, konfiguratsiya obyektlarini boshqarish va tashqi tizimlar bilan integratsiyalashish uchun ochiq API interfeyslarini taqdim etishi lozim.

5.10.2 Tizim SDK'ni qo'llab-quvvatlashi yoki Python, Java, JavaScript, C# va shunga o'xshash keng tarqalgan dasturlash tillari uchun kutubxonalarga ega bo'lishi kerak.

5.10.3 Tizimning barcha konfiguratsiyalarini veb-interfeys, CLI va/yoki konfiguratsiya fayllari orqali boshqarish imkoni bo'lishi 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 Syslog TCP/UDP, raw TCP, fayl, API yoki shunga o'xshash mexanizm orqali tashqi tizimlarga yuborish imkoniyatiga ega bo'lishi kerak.

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

5.10.7 SIEM ishlab chiqaruvchi tomonidan rasman qo'llab-quvvatlanadigan Palo Alto Networks Cortex XDR bilan to'g'ridan-to'g'ri integratsiya mexanizmiga ega bo'lishi kerak, u shtatdagi ilova, Add-on, modul yoki SIEMning boshqa maxsus komponenti sifatida amalga oshirilgan bo'lishi lozim.

5.10.8 Shtatdagi integratsiya Cortex XDR'dan kamida quyidagilarni o'z ichiga olgan o'zaro bog'liq ma'lumotlarni avtomatlashtirilgan tarzda olinishini ta'minlashi kerak: insidentlar, ogohlantirishlar (alerts), batafsil hodisalar, oxirgi qurilmalar, foydalanuvchilar, jarayonlar, tarmoq ulanishlari, tahdid obyektlari, artefaktlar va insidentlarni qayta ishlash holatlari haqidagi ma'lumotlar.

5.10.9 Integratsiya insidentlar haqidagi jamlangan ma'lumotlarni ham, ular bilan bog'liq batafsil voqealar va telemetriyani ham olishni ta'minlashi kerak, bunda boshlang'ich hodisa, alert va tegishli Cortex XDR insidenti o'rtasidagi o'zaro bog'liqlik saqlanib qoladi.

5.10.10 Olingan Cortex XDR ma'lumotlari boshlang'ich qiymatlar va obyektlar o'rtasidagi aloqalarni saqlagan holda SIEM ma'lumotlarining yagona me'yorlashtirilgan modeliga standart integratsiya vositalari yordamida avtomatik ravishda aylantirilishi lozim.

5.10.11 Me'yorlashtirilgan Cortex XDR ma'lumotlari ma'lumotlarni qo'shimcha aylantirish zaruratisiz, bevosita SIEMning asosiy mexanizmlari, jumladan qidiruv, korrelyatsiya, tahliliy qoidalar, vizualizatsiya, insidentlarni tekshirish, xavfga yo'naltirilgan tahlil va security content tomonidan qo'llanilishi lozim.

5.10.12 SIEM Cortex XDR ma'lumotlarini Asset va Identity obyektlari, jumladan, endpoint, IP-manzil, DNS-nomi, foydalanuvchi hisobi va boshqa identifikatorlar bilan avtomatik moslashtirishni ta'minlashi lozim, bunda ushbu kontekstdan keyingi tahlilda foydalanish imkoniyati mavjud bo'ladi.

5.10.13 Cortex XDR ma'lumotlari foydalanuvchilar, oxirgi qurilmalar va boshqa obyektlar uchun xavf hodisalarini shakllantirish, to'plash va jamlash imkoniyatiga ega bo'lgan SIEMning xavfga yo'naltirilgan tahlilining standart mexanizmida bevosita ishtirok etishi lozim.

5.10.14 SIEM vaqt, identifikatsiya, tarmoq va boshqa o'zaro bog'liqliklar asosida Cortex XDR hodisalarini boshqa manbalar hodisalari bilan yagona tahliliy kontekstda avtomatik ravishda birlashtirishni ta'minlashi lozim.

5.10.15 SIEM Cortex XDR ma'lumotlari uchun alohida tahliliy kontur yaratish zaruratisiz, Cortex XDR hodisalari va boshqa ulangan manbalarning hodisalari to'plami asosida yagona insident yoki tahliliy obyektni shakllantirishni ta'minlashi lozim.

5.10.16 Cortex XDR ma'lumotlari SIEM ishlab chiqaruvchisi tomonidan taqdim etiladigan oldindan sozlangan xavfsizlik kontentida (security content), shu jumladan korrelyatsiya qoidalari, tahliliy ssenariylar, tahdidlarni aniqlash qoidalari va boshqa tahlil mexanizmlarida, Buyurtmachi tomonidan Cortex XDR ma'lumotlarini o'zgartirish bo'yicha maxsus mexanizmlarni ishlab chiqish zaruratisiz qo'llanilishi lozim.

5.10.17 SIEM boshdan oxirigacha bo'lgan bog'liqlikni ta'minlashi lozim:

- Cortex XDR hodisasi → normallashtirilgan SIEM hodisasi → Asset/Identity → Risk → Correlation → Incident

- bunda yagona tekshiruv interfeysi doirasida ko‘rsatilgan obyektlar o‘rtasida o‘tish imkoniyati bo‘lishi kerak.

5.10.18 Insidentni tekshirishda SIEM umumlashtirilgan insident, korrelyatsion hodisa yoki xavf obyektidan tortib Cortex XDRning dastlabki ma’lumotlarigacha chuqurlashtirilgan o‘tishni (drill-down) ta’minlashi lozim, bunda bog‘liq endpoint, foydalanuvchi, jarayon, fayl, IP-manzil, domen, tarmoq ulanishi va boshqa mavjud atributlar aks ettirilishi kerak.

5.10.19 SIEM Cortex XDRdan dastlabki ma’lumotlarni qayta olmasdan turib, Cortex XDR ma’lumotlarini boshqa manbalarning ma’lumotlari bilan birgalikda tarixiy qidiruv va retrospektiv tahlil qilish imkoniyatini ta’minlashi lozim.

5.10.20 SIEM o‘zgartirilgan yoki yangi yaratilgan normallashtirish, tasniflash, boyitish va korrelyatsiya qoidalarini avval olingan Cortex XDR ma’lumotlariga tarixiy ma’lumotlar massivini qayta yuklamasdan qo‘llashni ta’minlashi lozim.

5.10.21 Cortex XDR ma’lumotlari tezkor va tarixiy dashbordlar hamda tahliliy ko‘rinishlarni yaratish uchun boshqa manbalardagi ma’lumotlar bilan birgalikda, dastlabki hodisagacha chuqur tahlil qilish (drill-down) imkoniyati bilan ochiq bo‘lishi kerak.

5.10.22 SIEM tahdidlar va MITRE ATT&CK tahlilida Cortex XDR ma’lumotlaridan foydalanishni ta’minlashi, bunda tegishli taktikalar, texnikalar va aloqador hodisalarni yagona tekshiruv doirasida aks ettirish imkoniyatiga ega bo‘lishi lozim.

5.10.23 SIEM Cortex XDR bilan integratsiyaning shtatdagi komponenti ishlashini, jumladan ulanish holatini, ma’lumotlar olinishini, qayta ishlash xatolarini, ma’lumotlar kelishining kechikishini va ma’lumotlar kelishi to‘xtaganligi belgilarini nazorat qilishni ta’minlashi lozim.

5.10.24 5.10.7–5.10.25 talablarini amalga oshirish uchun Buyurtmachi tomonidan mustaqil ravishda ishlab chiqilgan skriptlar, parserlar, ETL-protseduralari, oraliq ma’lumotlar bazalari yoki ishlab chiqaruvchi tomonidan qo‘llab-quvvatlanadigan, SIEMning Cortex XDR bilan shtatdagi integratsiyasiga kirmaydigan boshqa dasturiy komponentlardan majburiy ravishda foydalanishga yo‘l qo‘yilmaydi.

5.10.25 Barcha ko‘rsatilgan mexanizmlar SIEMning yagona texnologik konturi doirasida ishlashi hamda normallashtirish, korrelyatsiya, xavflarni tahlil qilish, vizualizatsiya yoki tekshiruvni amalga oshirish uchun Cortex XDR ma’lumotlarini alohida tahliliy platformaga uzatishni talab qilmasligi kerak.

5.11 Nosozlikka chidamlilik va ishlash rejimlariga qo‘yiladigan talablar

5.11.1 Tizim N+1 maqsadli arxitekturasida asosiy komponentlarni zaxiralash, klasterizatsiya, muhim ma’lumotlarni replikatsiya qilish va yagona nosozlik nuqtasining yo‘qligini qo‘llab-quvvatlashi lozim.

5.11.2 Tizim komponentlarda nosozliklar yuz berganda avtomatik tiklanishni yoki hujjatlashtirilgan tiklash tartibini ta’minlashi lozim.

5.11.3 Tizimning asosiy ishlash rejimi — administrator boshqaruvi ostida avtomatlashtirilgan rejimda uzluksiz, tunu kun ishlash.

5.11.4 Tizim shtat, xizmat ko‘rsatish va avtonom rejimlarni, shu jumladan markaziy komponentlar vaqtincha ulanib bo‘lmaydigan holatda ma’lumotlarni mahalliy buferlash imkoniyatini qo‘llab-quvvatlashi lozim.

5.12 Unumdorlik va o‘tkazish qobiliyatiga qo‘yiladigan talablar

Yetkazib beriladigan yechim quyidagi talablarga javob berishi kerak:

№	Ko‘rsatkich	Talab qilinadigan qiymat
1	Hodisalarni qabul qilish bo‘yicha o‘rtacha unumdorlik (EPS)	kamida 80 000 EPS yoki hodisaning o‘rtacha o‘lchami bo‘yicha hisoblangan ekvivalent ma’lumotlar hajmi
2	Hodisalarni qabul qilish bo‘yicha eng yuqori (pik) unumdorlik	kamida 150 000 EPS
3	Qisqa muddatli burst (keskin) yuklama imkoniyati	to‘g‘ri hisoblangan arxitektura va buferlash sharoitida hodisalarni yo‘qotmasdan 250 000 EPS gacha
4	Indekslanadigan ma’lumotlarning sutkalik hajmi	platformani o‘zgartirmasdan yanada oshirish imkoniyati bilan sutkasiga kamida 100 GB
5	"Qaynoq" ma’lumotlarni saqlash hajmi (tezkor ruxsat)	kamida 180 sutka
6	"Iliq" ma’lumotlarni saqlash hajmi	kamida 12 oy
7	Arxiv ma’lumotlarini saqlashning umumiy muddati	kamida 3 yil
8	Ogohlantirishgacha hodisani qayta ishlashning maksimal kechikishi	me’yoriy yuklamada kritik korrelyatsiya ssenariylari uchun 3 soniyadan oshmasligi kerak
9	Me’yoriy yuklamada hodisalarning yo‘qotilishi	Manbalar va uzatish kanallari to‘g‘ri sozlanganda 0%
10	Bir vaqtda ulangan manbalar soni	kamida 2 000
11	Taqsimlangan kollektorlar/agentlarni qo‘llab-quvvatlash	kamida 10 ta masofaviy maydoncha
12	Bir vaqtning o‘zida ishlaydigan SOC foydalanuvchilari soni	kamida 20 ta
13	90 kunlik ma’lumotlar bo‘yicha qidiruv so‘rovining bajarilish vaqti	kelishilgan namunaviy qidiruv so‘rovlari uchun 120 soniyadan oshmasligi kerak
14	6 oylik agregatsiya hisobotining bajarilish vaqti	10 daqiqadan ortiq emas
15	Unumdorlikni masshtablash	gorizontal, tizimni to‘liq to‘xtatmasdan
16	EPSni oshirish imkoniyati	arxitektura yondashuvini o‘zgartirmasdan kamida 3 barobar
17	Alohida saqlashni qo‘llab-quvvatlash (hot/warm/archive tiers)	majburiy
18	Nosozliklarga bardoshlilik	yagona nosozlik nuqtasining yo‘qligi (N+1)

5.13 Qo‘shimcha foydalanish ssenariylariga qo‘yiladigan talablar

5.13.1 Tizim bir marta to‘plangan 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 ko‘chirish zaruratisiz qo‘shimcha modullar,

ilovalar yoki integratsiyalar orqali funksionallikni kengaytirishni qo'llab-quvvatlashi lozim.

5.13.3 Tizim reaksiyani avtomatlashtirish, SOAR/ITSM bilan integratsiya qilish hamda foydalanuvchilar va obyektlar xatti-harakatlarining kengaytirilgan tahlili yo'nalishida kelgusida rivojlantirish imkoniyatini ta'minlashi lozim.

6 Ijrochiga talablar

Ijrochiga quyidagi talablar qo'yiladi:

6.1 Xarid qilish tartib-taomili doirasida Ijrochi yetkazib beriladigan dasturiy ta'minotning batafsil spetsifikatsiyasini taqdim etishi shart;

6.2 Ijrochiga qo'yiladigan umumiy talablar

Ijrochi quyidagi talablarga javob berishi kerak:

- belgilangan xizmatlarni ko'rsatish bo'yicha tasdiqlangan ish tajribasi (dasturiy ta'minot yetkazib berish);
- vakolatli hamkor bo'lishi, shuningdek, amalga oshirilayotgan/joriy etilayotgan dasturiy ta'minotdan foydalanish va joriy etish huquqlarini yakuniy foydalanuvchilarga taqdim etish bo'yicha hujjatli tasdiqqa ega bo'lishi;
- Ijrochi taklif etilayotgan dasturiy ta'minot uchun "Kiberxavfsizlik markazi" DUK sertifikatini (axborot va kiberxavfsizlikni ta'minlash talablariga muvofiqligi bo'yicha) taqdim etish majburiyatini oladi yoki u mavjud bo'lmagan taqdirda, loyihani joriy etish bosqichida dasturiy ta'minotni sertifikatlash jarayonidan o'tishi shart.

Ijrochi O'zbekiston Respublikasining amaldagi qonunchiligida maxfiy ma'lumotlarni o'z ichiga olgan hujjatlar va ma'lumotlar bilan ishlashga qo'yiladigan talablarga rioya etishi hamda xizmatlar ko'rsatish jarayonida o'ziga ma'lum bo'lgan maxfiy ma'lumotlarni oshkor etmasligi shart.

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

- ishlab chiqaruvchi kompaniya bilan hamkorlik maqomi mavjudligi to'g'risidagi avtorizatsiya xati nusxasi;
- ishlab chiqaruvchi kompaniyaning kamida 2 ta muhandis sertifikati nusxalari;
- amalga oshirilgan IT-loyihalar ro'yxati.

7 Ishlarni bajarish va xizmatlar ko'rsatish xavfsizligiga qo'yiladigan talablar

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

8 Bajarilgan ishlar va ko'rsatilgan xizmatlar natijalari bo'yicha texnik va boshqa hujjatlarni topshirish talablari

Tizimni joriy etish va sanoat ekspluatatsiyasiga kiritish tugallangandan so'ng, Ijrochi ish (ijro) hujjatlarini tayyorlashi shart, **qaysiki u** Tizimning amalda amalga oshirilgan holatini aks ettirishi kerak.

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;
- apparat va dasturiy komponentlarning ro'yxati va konfiguratsiyasi;
- Buyurtmachining infratuzilmasi bilan integratsiyalashuv tavsifi;
- tarmoq manzillari (IP, portlar, protokollar);
- qisqacha ekspluatatsiya hujjatlari;
- axborot xavfsizligi bo'yicha amalga oshirilgan chora-tadbirlar tavsifi.

Hujjatlar dolzarb, to'liq va Tizimning amaldagi holatiga mos bo'lishi, shuningdek, uni Ijrochini jalb qilmasdan ekspluatatsiya qilish uchun yetarli bo'lishi kerak.

9 Buyurtmachi xodimlarini o'qitishga qo'yiladigan talablar

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

a) ushbu majmuani boshqarish bo'yicha Buyurtmachining ikkita axborot xavfsizligi mutaxassisini sertifikatlangan holda o'qitish.

Tinglovchilar soni: 2 nafar.

Format: yuzma-yuz / onlayn, amaliy mashg'ulotlar bilan.

O'qitish tili: rus / ingliz.

Materiallar: taqdimotlar, ko'rsatmalar, laboratoriya ishlari.

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

- o'quv materiallari;
- mashg'ulotlar yozuvlari;
- o'quvdan o'tganlikni tasdiqlash (sertifikatlar).

b) tizim foydalanuvchilarini o'qitish.

Tinglovchilar soni: 10 kishigacha.

Format: ko'rgazmali + amaliy.

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

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

O'qitish dasturi va vaqtini Buyurtmachi bilan oldindan kelishish lozim.

10 Kafolat majburiyatlari

Ijrochi bajarilgan ish sifati ishlab chiqaruvchi tomonidan hujjatlarda belgilangan dasturiy (dasturiy-apparat) ta'minotdan foydalanish qoidalariga rioya qilingan va o'rnatilgan dasturiy ta'minot ishiga ruxsatsiz aralashuvlar bo'lmagan taqdirda, texnik topshiriq va Buyurtmachi tomonidan ko'rsatilgan talablarga muvofiq bo'lishini kafolatlashi shart.

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

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

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

11 Servis qo'llab-quvvatlash va texnik hamrohlik shartlari

Ishlab chiqaruvchining Servis qo'llab-quvvatlash muddati – dasturiy ta'minot joriy etilgan kundan boshlab **12 (o'n ikki) oy.** Dasturiy komponentlarga Servis qo'llab-quvvatlash ham ishlab chiqaruvchi, ham Ijrochi tomonidan ko'rsatilishi kerak.

Ijrochi hujjatlar, yangilanishlar va relizlarni mustaqil ravishda yuklab olish uchun dasturiy ta'minot ishlab chiqaruvchi kompaniyaning axborot resurslari to'g'risidagi ma'lumotlarni taqdim etishi shart.

Ijrochi Ishlab chiqaruvchining veb-saytidagi Buyurtmachi kabinetida dasturiy ta'minotning identifikatsiya ma'lumotlarini bog'laydi.

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

a) SIEM 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 amalga oshirilgandan so'ng Tizimning odatiy rejimda ishlashini sinovdan o'tkazish.

b) Mavjud boshqaruv va monitoring tizimlari bilan integratsiya.

c) Tizimni kengaytirish bo'yicha maslahatlar.

d) Dasturiy ta'minot ishlab chiqaruvchisi portaliga kirish (yangilanishlarni yuklab olish imkoniyati, texnik forumga kirish, hujjatlarga kirish).

e) Tizim yangilangan taqdirda, Tizimning 2 nafar administratoriga yo'riqnoma berish.

f) "UMS" MCHJ talabiga ko'ra, Tizimning ishlashi bilan bog'liq yuzaga kelgan muammolarni hal qilish va maslahat berish uchun mutaxassisni VPN orqali ulash.

g) Dasturiy majmuaning ishlash qobiliyatini tiklash:

- dasturiy vositalar ishdan chiqqandan so'ng 2 ish kunidan kechiktirmay Tizimning ishlash qobiliyatini odatiy rejimda tiklash;
- dasturiy majmuani qayta sozlash, rekonfiguratsiya qilish, yangilash va/yoki to'liq qayta o'rnatish, shuningdek, nosozlikka olib kelgan sabablarni bartaraf etish (kompaniya mahsulotlari tufayli yuzaga kelgan nosozlik holatida);
- tiklash ishlarini amalga oshirish uchun nosozlik vaqtida Tizimni uzib qo'yish (baypas rejimi) imkoniyati;
- apparat nosozliklari, elektr ta'minotidagi uzilishlar va hokazolardan so'ng Tizim faoliyatini tiklash;
- ma'lumotlarni zaxira nusxalaridan tiklash amaliyotlari.
- bajarilgan ishlar to'g'risida hisobotlar taqdim etish.

12 Texnik qo'llab-quvvatlashga doir talablar

12.1 Ijrochi yetkazib berilayotgan dasturiy majmuani 12 oy davomida texnik jihatdan qo'llab-quvvatlashni ta'minlashi shart.

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

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

12.4 Qo'llab-quvvatlash quyidagilarni qamrab olishi kerak:

- dasturiy qismni (software).

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

- 24×7×365 – kritik insidentlar uchun;
- 8×5 dan kam bo'lmagan – kritik bo'lmagan insidentlar uchun (Buyurtmachi bilan kelishilgan holda).

12.6 Insidentlarga reaksiya bildirish vaqti:

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

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

- P1: 4 soatdan ko'p emas;
- P2: 8 soatdan ko'p emas;
- P3: 2 ish kunigacha;
- P4: Buyurtmachi bilan kelishilgan holda.

12.8 Ijrochi tomonidan texnik qo'llab-quvvatlash bo'yicha talabnomalarni ro'yxatga olishning yagona kanali taqdim etilishi lozim:

- Service Desk (portal);
- qaynoq liniya telefoni;
- e-mail.

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

13.1 Litsenziyalar/DTlar tomonlar vakillari ishtirokida dasturiy ta'minotning jismoniy inventarizatsiyasi va ishlash qobiliyati tekshirilgandan hamda tuzilgan shartnomaga muvofiq tegishli qabul qilish-topshirish dalolatnomasi imzolangandan so'ng qabul qilingan deb hisoblanadi. Ushbu TT (texnik topshiriq) va uning ilovalarida ko'rsatilmagan boshqa shartlar shartnomada ko'rsatiladi.

13.2 Buyurtmachining amaldagi ichki tartib-qoidalariga, nazorat-o'tkazish rejimiga, ichki nizomlarga, yo'riqnomalar va talablarga rioya etish xizmatlar ko'rsatishning majburiy sharti hisoblanadi, Buyurtmachi bu haqda Ijrochini xabardor qiladi. Buyurtmachi Ijrochiga dasturiy ta'minotga obunani faollashtirish bilan bog'liq muammolarni hal qilish uchun Ijrochi bilan bog'lanish vakolatiga ega bo'lgan xodimlarning ro'yxati va aloqa ma'lumotlarini taqdim etadi.

13.3 Taklif berishning batafsil shakli ushbu TTning 2-ilovasida keltirilgan.

13.4 Butlashga qo'yiladigan talablar

Tizim joriy TT doirasida taklif etilayotgan yechimning to'liq ishlashi uchun to'liq komplektatsiyaga ega bo'lishi lozim. DTning narxi to'liq butlashdan kelib chiqib shakllantirilishi kerak.

13.5 Integratsiyaga qo'yiladigan talablar

Integratsiya Buyurtmachi infratuzilmasining ishlash xususiyatlarini hisobga olishi kerak.

13.6 Yangi ekanligi to'g'risida ma'lumot

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

13.7 Sug'urta

Talablar qo'yilmaydi, biroq Ijrochi dasturiy (apparat-dasturiy) majmuaning Buyurtmachiga rasman topshirilguniga qadar but saqlanishi uchun javobgardir.

13.8 Xizmat ko'rsatishda javobgarlikni taqsimlash matritsasi

Texnik xizmat ko'rsatish	**Ijrochi**	**Buyurtmachi**
Tizimning mavjudligi		
Muammoni aniqlash va ustuvorligini tasniflash, uni hal qilish uchun Huquq egasida so'rov ochish	A	R
So'rov bo'yicha Buyurtmachining dasturiy ta'minotini sozlashni amalga oshirish	A	R
Hisobot davrida muammolarni hal qilish statistikasini taqdim etish	R	A
Barcha so'rovlarni Huquq egasining portalida ro'yxatdan o'tkazish	R	A
Dasturiy ta'minotni yangilash, to'g'rilash va tuzatishlar kiritish		
Jarayon uslubini 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
Xizmatlar va tavsiyalar		
Texnik talablarni taqdim etish	R	R
Texnik talablarni joriy etish	R	A
Texnik tavsiyalar taqdim etish	R	I

R (inglizcha Responsible) - bevosita ijrochi;
A (inglizcha Accountable) - ijrochi ishiga rahbarlik qiluvchi mas'ul shaxs;
C (inglizcha Consulted) - maslahatchi (aniq qaror qabul qilishdan oldin mas'ul shaxs yordam so'raydigan tegishli soha mutaxassisi yoki eksperti);
I (inglizcha Informed) - kuzatuvchi, xabardor qilinadigan shaxs (vazifaning bajarilishi (yoki natijalari) haqida xabardor qilinishi lozim bo'lgan shaxs)

14 Qo'llaniladigan atamalar va qisqartmalar

№	Atama / Qisqartma	Yoyilmasi	Ta'rifi
1	SIEM	Security Information and Event Management	Axborot xavfsizligi hodisalarini markazlashgan holda yig'ish, saqlash, korrelyatsiya qilish va tahlil qilish tizimi
2	SOC	Security Operations Center	Axborot xavfsizligi hodisalarini monitoring qilish va ularga munosabat bildirish markazi
3	EPS	Events Per Second	Soniyasiga ishlov beriladigan hodisalar soni
4	LPS	Logs Per Second	Bir soniyada tizimga kelib tushadigan loglar soni
5	GB/day	Gigabytes per day	Kelib tushadigan ma'lumotlarning kunlik hajmi
6	Correlation	Hodisalar korrelyatsiyasi	Bir nechta hodisani yagona insidentga bog'lash
7	Use Case	Aniqlash ssenariysi	Muayyan turdagi tahdidni aniqlash qoidalari to'plami
8	Rule	Korrelyatsiya qoidasi	Shubhali faoliyatni aniqlashning mantiqiy sharti
9	Incident	AX insidenti	Tasdiqlangan axborot xavfsizligi buzilishi hodisasi
10	Event	Hodisa	Tizimning qayd qilingan harakati yoki holati
11	Log	Hodisalar jurnali	Axborot tizimidagi hodisa yozuvi
12	Parsing	Parsing	Loglarni tuzilmali formatga aylantirish
13	Normalization	Normalizatsiya	Hodisalarni yagona tuzilmaga keltirish
14	Enrichment	Ma'lumotlarni boyitish	Hodisaga kontekstli ma'lumot qo'shish
15	IOC	Indicator of Compromise	Kompрometatsiya indikatori (IP, xesh, domen va boshqalar)
16	MITRE ATT&CK	-	Kiberhujum taktikasi va texnikasi 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	Reaksiyani orkestrlash va avtomatlashtirish
19	XDR	Extended Detection and Response	Kengaytirilgan aniqlash va javob berish tizimi
20	EDR	Endpoint Detection and Response	Ishchi stansiyalarda tahdidlarni aniqlash tizimi
21	NTA	Network Traffic Analysis	Tarmoq trafigini tahlil qilish
22	NetFlow	—	Tarmoq trafigi statistikasini yig'ish protokoli

№	Atama / Qisqartma	Yoyilmasi	Ta'rifi
23	Syslog	—	Loglarni uzatish protokoli
24	API	Application Programming Interface	Tizimlarning dasturiy o'zaro ta'siri interfeysi
25	AD	Active Directory	Microsoft kataloglar xizmati
26	LDAP	Lightweight Directory Access Protocol	Kataloglar xizmatiga kirish protokoli
27	RBAC	Role-Based Access Control	Ruxsatni rollar asosida cheklash
28	MFA	Multi-Factor Authentication	Ko'p omilli autentifikatsiya
29	SLA	Service Level Agreement	Xizmat ko'rsatish darajasi to'g'risidagi kelishuv
30	MTTR	Mean Time To Respond/Recover	O'rtacha javob berish/tiklanish vaqti
31	MTTD	Mean Time To Detect	Tahdidni aniqlashning o'rtacha vaqti
32	HA	High Availability	Nosozliklarga chidamlilik
33	DR	Disaster Recovery	Nosozlikdan so'ng tiklash rejasi
34	Hot Storage	-	Ma'lumotlarni tezkor (operativ) saqlash
35	Warm Storage	-	Oraliq saqlash ombori
36	Cold Storage	-	Arxiv ombori
38	Cluster	Klaster	Yagona tizim sifatida ishlaydigan serverlar guruhi
39	Node	Uzel	Klasterdagi alohida server
40	Dashboard	Dashbord	Hodisalar va ko'rsatkichlarni vizuallashtirish paneli

15 Ilovalar ro'yxati

1-ilova – Axborotlashtirish obyektining tavsifi.
2-ilova – Texnik talablarga muvofiqlik jadvali.

Texnik topshiriqni ishlab chiqdi:

AXvaRD Axborot xavfsizligi bo'limi boshlig'i _____ imzo R.A.Abdulvaat

AXvaRD direktori _____ imzo B.A.Olmatov

1-ilova

Axborotlashtirish obyektining xususiyatlari

"UMS" MCHJ — 2014-yil 1-dekabrdan boshlab O'zbekiston Respublikasining butun hududida mobil aloqa xizmatlarini ko'rsatuvchi telekommunikatsiya kompaniyasi.

"UMS" MCHJ O'zbekiston Respublikasi Vazirlar Mahkamasining 2014-yil 31-iyuldagi 208-son "Mobil aloqa xizmatlarini ko'rsatish bo'yicha "Universal Mobile Systems" qo'shma korxonasini tashkil etish to'g'risida"gi 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'sischisi hisoblanadi.

Kompaniyaning shtatdagi xodimlari soni – 1800 kishi.

Serverlarning umumiy soni (shu jumladan virtuallari) – 1000 donadan ko'p emas.

Tarmoq qurilmalarining umumiy soni – 150 donadan ko'p emas.

Ilovalarning umumiy soni – 10 ta

Axborot xavfsizligi axborot dasturiy vositalarining umumiy soni – kamida 10 ta

Umumiy o'tkazish qobiliyati – 1000 Mbit/s dan ko'p emas.

Generatsiya qilinadigan loglarning umumiy hajmi – sutkasiga 100 Gb dan ko'p emas.

2-ilova

Texnik talablarga muvofiqlik jadvali

Talab №	Talab nomi/ texnik xususiyatlari
1	DT 12 oylik obuna litsenziyalari bilan yetkazib beriladi (Yechimni litsenziyalash - shaffof bo'lishi va arxitekturani to'liq almashtirish zaruratisiz qayta ishlanadigan/indekslanadigan ma'lumotlar va/yoki funksional modullar hajmi bo'yicha masshtablashtirish imkonini berishi kerak)
2	DT (yechim) SIEM (Security Information and Event Management) sinfiga tegishli bo'lishi lozim
3	Tizim jurnallashtirish, xavfsizlikni nazorat qilish, hodisalarni tekshirish, hisobot berish, vizualizatsiya qilish va ma'muriylashtirish vazifalari uchun yagona interfeys va yagona ma'lumotlar omborini taqdim etishi lozim.
4	Tizim dastlabki ma'lumotlarni keyinchalik qidirish va tahlil qilish imkoniyati bilan saqlashni ta'minlashi lozim, bunda dastlabki normallashtirish ma'lumotlarni qabul qilishning majburiy sharti bo'lmasligi kerak.
5	Tizim barcha manbalarni oldindan yagona relyatsion modelga aylantirish zaruratisiz turli xil mashina ma'lumotlari bilan ishlashni ta'minlashi lozim.
6	Yechim yirik korporativ buyurtmachilarda sanoat miqyosida qo'llashning tasdiqlangan amaliyotiga hamda hujjatlar, professional xizmatlar, o'qitish, qo'llab-quvvatlash va hamkorlarning rivojlangan ekotizimiga ega bo'lishi lozim.
7	Tizim jismoniy infratuzilma, virtual muhit, xususiy/ommaviy bulut yoki gibrid modelda yoyishni qo'llab-quvvatlaydi va ishlab chiqaruvchining maxsus jismoniy qurilmalaridan majburiy foydalanishni talab qilmaydi.
8	Yechim arxitekturasi tizimni to'liq qayta o'rnatmasdan yig'ish, indekslash/saqlash va qidirish komponentlarini gorizontal miqyoslashni qo'llab-quvvatlaydi.
9	Tizim bir nechta saqlash/indekslash uzellari bo'yicha taqsimlangan qidiruvni ta'minlaydi va qidiruv so'rovlarini parallel qayta ishlashni qo'llab-quvvatlaydi.
10	Tizim qidiruv samaradorligini oshirish, kirish huquqlarini ajratish va saqlash muddatlarini boshqarish uchun turli xil ma'lumotlarni alohida mantiqiy omborlarga joylashtirishni qo'llab-quvvatlaydi.
11	Tizim katta hajmdagi mashina ma'lumotlarini qayta ishlashni qo'llab-quvvatlashi va tegishli infratuzilma loyihalashtirilganda kuniga o'nlab TB ma'lumotlargacha kengaytirishning hujjatlar bilan tasdiqlangan imkoniyatiga ega bo'lishi lozim
12	Tizim ma'lumotlarni Syslog, TCP/UDP protokollari, himoyalangan TLS/SSL kanallari, agent dasturiy ta'minoti, API/REST, WMI, SNMP hodisalari, jurnal fayllari, JSON, XML, CSV, ma'lumotlar bazalari, skriptli va modulli manbalar orqali yig'ishni ta'minlaydi.
13	Agent dasturiy ta'minoti ma'lumotlar uzatishni shifrlashni, markaziy komponentlar uzilib qolganda keshlashni, qabul qiluvchi tugunlar o'rtasida yuklamani muvozanatlashni va ma'lumotlarni ishonchli transport protokoli orqali uzatishni qo'llab-quvvatlaydi
14	Tizim ma'lumotlarni yig'ishning agentli va agentsiz usullarini, jumladan tarmoq orqali jurnallarga to'g'ridan-to'g'ri kirish, mavjud Syslog serverlaridan qabul qilish va API orqali integratsiyalashni qo'llab-quvvatlaydi
15	Tizim ko'p qatorli va murakkab hodisalarni hodisa tuzilishi va dastlabki vaqt belgisini yo'qotmasdan indekslashni qo'llab-quvvatlaydi

16	Tizim ma'lumotlarni qabul qilishni boshlashdan oldin har bir manbaning tuzilishini oldindan tavsiflashni talab qilmasligi kerak
17	Tizim har qanday manbadan dastlabki, o'zgartirilmagan mashina ma'lumotlarini qabul qilish, indekslash va saqlashni ta'minlashi lozim
18	Tizim turli vaqt mintaqalaridan olingan vaqt belgilarini to'g'ri qayta ishlashi va tizimga kelib tushgan vaqt bilan bir qatorda hodisaning asl vaqtini ham saqlashi kerak
19	Tizim faqatgina ishlab chiqaruvchining tayyor konnektorlariga bog'liq bo'lmasligi kerak: yangi manbalarni ulash va mahsulotning manba kodini o'zgartirmasdan log formatlarining o'zgarishiga moslashish imkoniyati bo'lishi lozim.
20	Manbalar mavjudligini avtomatik tekshirish, kelib tushayotgan hodisalar to'liqligini nazorat qilish va muhim manbalardan ma'lumotlar kelishi to'xtatilganda xabardor qilish 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 xizmatlar, biznes-ilovalar, Service Desk/ITSM, CMDB va foydalanuvchi ilovalari bilan integratsiyani qo'llab-quvvatlaydi.
22	Tizim dastlabki, o'zgartirilmagan mashina ma'lumotlarini indekslaydi va ushbu ma'lumotlar bo'yicha keyinchalik qidirish, surishtiruv o'tkazish va hisobot tayyorlashni ta'minlaydi, shuningdek, disk maydonidan foydalanishni optimallashtirish uchun indekslangan ma'lumotlarni avtomatik ravishda siqishni qo'llab-quvvatlaydi.
23	Tizimda tezkor, iliq va arxiv ma'lumotlarini manba turlari, indekslar, muhimlik va komplayens (muvofiqlik) talablari bo'yicha saqlash muddatlarini moslashuvchan sozlagan holda saqlash imkoniyati mavjud.
24	Tizim ma'lumotlarning eskirishiga qarab ularni batafsil boshqarishni qo'llab-quvvatlaydi: arzonroq/tashqi xotiraga o'tkazish, arxivlash va/yoki Buyurtmachining siyosatlariga muvofiq o'chirish.
25	Tizim mavjudlik, yaxlitlik, nosozliklarga chidamlilikni ta'minlash va qidiruv unumdorligini oshirish maqsadida ma'lumotlar/indekslar replikatsiyasini qo'llab-quvvatlaydi.
26	Butun tizimni to'xtatmasdan ma'lumotlar ombori miqyosini kengaytirish imkoniyati mavjud
27	Jurnallar va audit ma'lumotlarini ruxsatsiz o'zgartirish va o'chirishdan himoya qilish, shu jumladan yaxlitlikni tekshirish mexanizmlari mavjud
28	Tizim xavfsizlikning namunaviy ssenariylari uchun hodisalarni yagona ma'lumotlar modeliga normallashtirishni qo'llab-quvvatlaydi, bunda dastlabki xom ma'lumotlar qidirish va tekshiruvlar uchun ochiq qolishi lozim
29	Maydonlarni ajratib olish mantiqini, ma'lumotnomalarni, normallashtirish yoki boyitish qoidalarini o'zgartirish avval saqlangan hodisalarni majburiy qayta yuklashni talab qilmaydi
30	Tizim hodisalarni toifalash va 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	Foydalanuvchilarning atributlarini (login, F.I.Sh., bo'linma, lavozim, rahbar, telefon raqami, joylashuv, imtiyozlilik belgisi, ishning boshlanish/tugash sanasi va boshqa atributlar) olish uchun korporativ kataloglar bilan integratsiya qo'llab-quvvatlanadi
32	Bir nechta hisob yozuvlari/loginlarni bitta xodim yoki subyekt bilan korrelyatsiya qilish qo'llab-quvvatlanadi

33	Qurilmalar haqidagi ma'lumotlarni (xost nomi, IP, MAC, joylashuv, egasi, muhimlik darajasi, maxfiy ma'lumotlarning mavjudligi, me'yoriy talablarga muvofiqlik) olish uchun aktivlar bazalari (CMDB) bilan integratsiya qo'llab-quvvatlanadi
34	Tizim o'tgan davrlar bo'yicha qidirish va hisobot tayyorlash uchun yangi ma'lumotnomalar va kontekst ma'lumotlarini avval indekslangan hodisalarga qo'llash imkonini beradi
35	Tizim kalit so'zlar, vaqt oraliqlari, mantiqiy operatorlar, regulyar ifodalar va o'rinbosar 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'rovlarini parallel ravishda bajarishni qo'llab-quvvatlaydi
37	Tizim shunday yondashuvni qo'llab-quvvatlaydiki, unda dastlabki hodisalar to'liq saqlanadi, maydonlarni ajratib olish, ma'lumotlarni normallashtirish, boyitish va talqin qilish esa qabul qilish bosqichida ham, avval saqlangan ma'lumotlarni qidirish va tahlil qilish bosqichida ham amalga oshirilishi mumkin
38	Tizim rolli ruxsat modelini hisobga olgan holda qidiruv so'rovlarini saqlash, tahrirlash, qayta ishlatish va boshqa foydalanuvchilarga uzatish imkonini beradi
39	Tizim statistik tahlilni qo'llab-quvvatlaydi: hisoblash, noyob qiymatlar, yig'indi, minimum, maksimum, o'rtacha qiymat, mediana, moda, standart og'ish, dispersiya, persentillar, qiymatning birinchi/oxirgi paydo bo'lishi
40	Tizim kam uchraydigan va g'ayritabiiy qiymatlarni aniqlashni, xulq-atvorning tayanch profillarini yaratishni va og'ishlarni aniqlashni, shu jumladan signaturalarga qat'iy bog'liq bo'lmagan holda noma'lum tahdidlar va APT ssenariylarini qo'llab-quvvatlaydi.
41	Tizim vaqt, mantiqiy, xulq-atvor va statistik qoidalar asosida hodisalar korrelyatsiyasini, shu jumladan ko'p bosqichli hujum ssenariylarini qo'llab-quvvatlaydi.
42	Tizim aniqlash ssenariylarini tasniflash va tavsiflash uchun kill chain, MITRE ATT&CK modellari yoki shunga o'xshash freymvorklardan foydalanishni qo'llab-quvvatlaydi.
43	Tizim o'z korrelyatsiya qoidalarini yaratish, mavjud qoidalarni o'zgartirish va ularni sanoat ekspluatatsiyasiga kiritishdan oldin sinovdan o'tkazish imkonini beradi.
44	Tizim Buyurtmachi infratuzilmasiga moslashtirish imkoniyatiga ega bo'lgan oldindan sozlangan SIEM kontentini taqdim etadi: korrelyatsiya qoidalari, dashbordlar, hisobotlar, ma'lumotlar modellari, tekshiruv ssenariylari va xavfsizlik monitoringi shablonlari.
45	Tizim real vaqtga yaqin rejimda monitoringni va qidiruv natijalari, korrelyatsiya qoidalari hamda tahliliy ssenariylar bo'yicha ogohlantirishlarni shakllantirishni qo'llab-quvvatlaydi.
46	Ogohlantirishlar ustuvorliklarni sozlash, takroriy ishga tushishlarni bostirish, ishga tushish chastotasini cheklash va mas'ul guruhlarga yo'naltirishni qo'llab-quvvatlaydi.
47	Tizim elektron pochta, tashqi tizimlar bilan integratsiya, Webhook/API, foydalanuvchi skriptlarini ishga tushirish yoki boshqa avtomatlashtirish mexanizmlari orqali bildirishnomalar yuborishni qo'llab-quvvatlaydi.
48	Tizim hodisalarni tekshirish ish jarayonlarini taqdim etadi: hodisa kartochkasi/obyekti, dastlabki voqealar va kontekstni bog'lash, tekshirish tarixi, statuslar, izohlar, mas'ul shaxslarni tayinlash va natijalarni hujjatlashtirish imkoniyati.
49	Tizim batafsil tekshirish uchun yig'ma voqea/dashbord/korrelyatsiya ishlashidan boshlang'ich voqealarga o'tishni ta'minlaydi.

50	Tizim interaktiv dashbordlar va hisobotlarni, jumladan jadvallar, vaqt diagrammalari, chiziqli, ustunli, maydonli, doiraviy va nuqtali grafiklar, holat ko'rsatkichlari hamda IP/Geo-IP bo'yicha geografik vizualizatsiyalarni yaratishni qo'llab-quvvatlaydi.
51	Vizualizatsiyalar real vaqt rejimida yangilanishni, jamlangan ko'rsatkichlardan boshlang'ich voqealarga o'tishni (drill-down) va anomaliyalar/chetlanishlarni ajratib ko'rsatishni qo'llab-quvvatlaydi.
52	Tizim texnik va texnik bo'lmagan foydalanuvchilarga hisobotlar va dashbordlarni yaratish, jumladan panellarni vizual tahrirlash hamda sarlavhalar, shartli belgilar, o'qlar va filtrlarni sozlash imkonini beradi.
53	Tizim hisobotlarni jadval asosida shakllantirish hamda PDF, CSV, XLS/XLSX va mahsulotda mavjud bo'lgan boshqa keng tarqalgan formatlarga eksport qilish/tarqatishni qo'llab-quvvatlaydi.
54	Tizim axborot xavfsizligi va tartibga solish talablariga, jumladan ISO 27002, NIST, PCI DSS va shunga o'xshash standartlarga muvofiqlik vazifalari uchun hisobotlar va monitoring panellarini qo'llab-quvvatlaydi.
55	Tizim foydalanuvchilar va API uchun moslashuvchan rollarga asoslangan kirish modelini (RBAC) qo'llab-quvvatlaydi, bunda ma'lumotlar manbalari, ma'lumotlar turlari, vaqt oraliqlari, hisobotlar, boshqaruv panellari, qidiruvlar va ma'muriy funksiyalarga kirishni cheklash imkoniyati mavjud.
56	Tizim Active Directory/LDAP va korporativ yagona kirish tizimlari (SSO) bilan integratsiyani qo'llab-quvvatlaydi.
57	Komponentlar o'rtasida ma'lumotlarni uzatish zamonaviy kriptografik protokollardan foydalangan holda himoyalangan kanallar orqali amalga oshiriladi.
58	Tizim foydalanuvchilar va ma'murlarning xatti-harakatlarining to'liq auditini olib boradi: tizimga kirish, qidiruv so'rovlari, hisobotlarni ko'rish, konfiguratsiyani o'zgartirish, foydalanuvchilarni boshqarish, qoidalarni yaratish/o'zgartirish va boshqa muhim harakatlar.
59	Tizimning audit hodisalari sana va vaqtni, foydalanuvchi/subyektni, manbani, bajarilgan harakatni va uning natijasini o'z ichiga oladi.
60	Tizim indekslangan hodisalarning yaxlitligini tasdiqlash mexanizmlarini, jumladan xeshlash va/yoki hodisalarning raqamli imzosini yoki funksional jihatdan ekvivalent bo'lgan haqiqiylikni nazorat qilish mexanizmini qo'llab-quvvatlaydi.
61	Tizim o'z konfiguratsiyasi, komponentlarning mavjudligi va tizim xizmatlarining holatini xabardor qilish imkoniyati bilan monitoring qilishni ta'minlaydi.
62	Tizim indekslangan ma'lumotlarga kirish, qidiruv so'rovlarini bajarish, konfiguratsiya obyektlarini boshqarish va tashqi tizimlar bilan integratsiya qilish uchun ochiq API interfeyslarini taqdim etadi.
63	Tizim Python, Java, JavaScript, C# yoki shunga o'xshash keng tarqalgan dasturlash tillari uchun SDK ni qo'llab-quvvatlashi yoki kutubxonalarga ega bo'lishi lozim.
64	Tizim konfiguratsiyalarini veb-interfeys, CLI va/yoki konfiguratsiya fayllari orqali boshqarish imkoniyati mavjud bo'lishi lozim.
65	Tizim tashqi vizualizatsiya tizimlari, BI, ITSM/SOAR, CMDB, threat intelligence, monitoring tizimlari va Buyurtmachining boshqa korporativ platformalari bilan integratsiyani qo'llab-quvvatlaydi.
66	Tizim Syslog TCP/UDP, raw TCP, fayl, API yoki shunga o'xshash mexanizm orqali xom, o'zgartirilgan yoki boyitilgan hodisalarni tashqi tizimlarga yuborish imkoniyatiga ega.
67	Tizim ommabop mahsulotlar va xavfsizlik ssenariylari uchun ommaviy va/yoki ishlab chiqaruvchi tomonidan taqdim etiladigan ilovalar/integratsiya paketlaridan foydalanishni qo'llab-quvvatlaydi.

68	Tizim N+1 maqsadli arxitekturasida asosiy komponentlarni zaxiralash, klasterlash, muhim ma'lumotlar replikatsiyasini va yagona nosozlik nuqtasining yo'qligini qo'llab-quvvatlaydi.
69	Tizim avtomatik tiklanishni ta'minlaydi yoki komponentlar ishlamay qolganda hujjatlashtirilgan tiklash tartibiga ega.
70	Tizimning asosiy ishlash rejimi - ma'mur boshqaruvi ostida avtomatlashtirilgan rejimda tunu kun uzluksiz ishlashdir.
71	Tizim shtatli, xizmat ko'rsatish va avtonom rejimlarni, shu jumladan markaziy komponentlar vaqtincha mavjud bo'lmaganda ma'lumotlarni mahalliy buferlash imkoniyatini qo'llab-quvvatlaydi.
72	Hodisalarni qabul qilish bo'yicha o'rtacha unumdorlik (EPS) - kamida 80 000 EPS (yoki hodisaning o'rtacha o'lchami bo'yicha hisoblangan ekvivalent ma'lumotlar hajmi)
73	Hodisalarni qabul qilish bo'yicha eng yuqori unumdorlik - kamida 150 000 EPS
74	Qisqa muddatli burst-yuklama imkoniyati - 250 000 EPS gacha (to'g'ri hisoblangan arxitektura va buferlashda hodisalarni yo'qotmasdan)
75	Indekslanadigan ma'lumotlarning sutkalik hajmi - kamida 100 GB/sutka (platformani o'zgartirmasdan yanada oshirish imkoniyati bilan)
76	"Qaynoq" ma'lumotlarni saqlash hajmi (tezkor ruxsat) - kamida 180 sutka
77	"Iliq" ma'lumotlarni saqlash hajmi - kamida 12 oy
78	Arxiv ma'lumotlarini saqlashning umumiy muddati - kamida 3 yil (36 oy)
79	Hodisani qayta ishlashdan to xabardor qilishgacha bo'lgan maksimal kechikish - shtatli yuklamadagi kritik korrelyatsiya ssenariylari uchun 3 soniyadan ko'p emas
80	Shtatli yuklamada hodisalar yo'qotilishi - manbalar va uzatish kanallari to'g'ri sozlanganda 0%
81	Bir vaqtning o'zida ulangan manbalar soni - kamida 2 000 ta
82	Taqsimlangan kollektorlar/agentlarni qo'llab-quvvatlash - kamida 10 ta masofaviy maydoncha
83	Bir vaqtning o'zida ishlaydigan SOC foydalanuvchilari soni - kamida 20 ta
84	90 sutkalik ma'lumotlar bo'yicha qidiruv so'rovini bajarish vaqti - kelishilgan namunaviy qidiruv so'rovlari uchun 120 soniyadan ko'p emas
85	6 oylik agregatsion hisobotni bajarish vaqti - 10 daqiqadan ko'p emas
86	Unumdorlikni gorizontal masshtablash, tizimni to'liq to'xtatmasdan
87	Arxitektura yondashuvini o'zgartirmasdan EPSni kamida 3 baravar oshirish imkoniyati
88	Alohida saqlashni (hot/warm/archive tiers) qo'llab-quvvatlash majburiydir

89	Nosozliklarga chidamlilik - yagona nosozlik nuqtasining yo‘qligi (N+1)
90	Tizim bir marta to‘plangan va indekslangan ma’lumotlardan turli ssenariylarda foydalanish imkonini beradi: axborot xavfsizligi monitoringi, komplayens, hodisalarni tekshirish, firibgarlikni aniqlash, AT-operatsiyalari, ilovalar monitoringi, raqamli tahlil va biznes tahlili
91	Tizim ma’lumotlarni alohida platformaga ko‘chirish zaruratisiz qo‘shimcha modullar, ilovalar yoki integratsiyalar orqali funksionallikni kengaytirishni qo‘llab-quvvatlaydi
92	Tizim javob qaytarishni avtomatlashtirish, SOAR/ITSM bilan integratsiya qilish va foydalanuvchilar hamda obyektlar xatti-harakatlarining kengaytirilgan tahlili tomon keyingi rivojlanish imkoniyatini ta’minlaydi
93	Yechimni texnik qo‘llab-quvvatlash - kamida 1 yil
94	Loyihaga o‘rnatish va integratsiya ishlari kiritilgan
95	Loyihaga loyihalash kiritilgan
96	Loyihaga Buyurtmachi mutaxassislarini sertifikatlangan o‘qitish kiritilgan
97	Loyihaga MKBda dasturiy ta’minotni sertifikatlash kiritilgan
98	Interfeys tili - rus/ingliz
99	Tizimda ma’lumotlami oldindan normallashtirmasdan yoki alohida SQL ma’lumotlar bazasiga yuklamasdan turib, bevosita dastlabki indekslangan hodisalar bo‘yicha qidirish, tekshirish, korrelyatsiya qilish va hisobot tuzish imkoniyatining mavjudligi tizimning qo‘shimcha afzalligi sifatida ko‘rib chiqiladi
100	SIEM ishlab chiqaruvchi tomonidan rasman qo‘llab-quvvatlanadigan, Palo Alto Networks Cortex XDR bilan to‘g‘ridan-to‘g‘ri integratsiya qilish mexanizmiga ega bo‘lishi kerak hamda u standart ilova, qo‘shimcha (Add-on), modul yoki SIEMning boshqa maxsus tarkibiy qismi ko‘rinishida amalga oshirilgan bo‘lishi lozim
101	Standart integratsiya Cortex XDR’dan kamida quyidagilarni o‘z ichiga olgan o‘zaro bog‘liq ma’lumotlarni avtomatik ravishda olishni ta’minlashi lozim: insidentlar, ogohlantirishlar (alerts), batafsil hodisalar, oxirgi qurilmalar, foydalanuvchilar, jarayonlar, tarmoq ulanishlari, tahdid obyektlari, artefaktlar va insidentlarni qayta ishlash holatlari haqidagi ma’lumotlar.
102	Integratsiya insidentlar haqidagi jamlangan ma’lumotlarni ham, ular bilan bog‘liq batafsil hodisalar va telemetriyani ham olishni ta’minlashi lozim, bunda dastlabki hodisa, ogohlantirish (alert) va tegishli Cortex XDR insidenti o‘rtasidagi o‘zaro bog‘liqlik saqlanib qoladi.
103	Olingan Cortex XDR ma’lumotlari boshlang‘ich qiymatlar va obyektlar o‘rtasidagi o‘zaro bog‘liqliklarni saqlagan holda, standart integratsiya vositalari yordamida SIEM ma’lumotlarining yagona normallashtirilgan modeliga avtomatik ravishda aylantirilishi lozim.
104	Normallashtirilgan Cortex XDR ma’lumotlari bevosita SIEMning asosiy mexanizmlari, jumladan qidiruv, korrelyatsiya, tahliliy qoidalar, vizualizatsiya, insidentlarni tekshirish, xavfga asoslangan tahlil va xavfsizlik kontenti (security content) tomonidan, ma’lumotlarni qo‘shimcha o‘zgartirish zaruratisiz qo‘llanilishi lozim.
105	SIEM Cortex XDR ma’lumotlarini Asset va Identity obyektlari, jumladan oxirgi nuqta (endpoint), IP-manzil, DNS nomi, foydalanuvchi hisobi va boshqa identifikatorlar bilan avtomatik ravishda moslashtirishni ta’minlashi lozim, bunda ushbu kontekstdan keyingi tahlilda foydalanish imkoniyati yaratiladi.

106	Cortex XDR ma'lumotlari foydalanuvchilar, yakuniy qurilmalar va boshqa obyektlar uchun xavf hodisalarini shakllantirish, to'plash va jamlash imkoniyatiga ega bo'lgan SIEM'ning xavfga yo'naltirilgan tahlilining standart mexanizmida bevosita ishtirok etishi lozim.
107	SIEM vaqt, identifikatsiya, tarmoq va boshqa o'zaro bog'liqliklar asosida Cortex XDR hodisalarini boshqa manbalardagi hodisalar bilan yagona tahliliy kontekstda avtomatik ravishda birlashtirishni ta'minlashi lozim.
18	SIEM Cortex XDR ma'lumotlari uchun alohida tahliliy kontur yaratish zaruratisiz, Cortex XDR hodisalari va boshqa ulangan manbalar hodisalari to'plami asosida yagona insident yoki tahliliy obyektni shakllantirishni ta'minlashi lozim.
109	Cortex XDR ma'lumotlari SIEM ishlab chiqaruvchisi tomonidan yetkazib beriladigan oldindan sozlangan security content'da, jumladan korrelyatsiya qoidalari, tahliliy ssenariylar, tahdidlarni aniqlash qoidalari va boshqa tahlil mexanizmlarida, Buyurtmachi tomonidan Cortex XDR ma'lumotlarini o'zgartirishning maxsus mexanizmlarini ishlab chiqish zaruratisiz qo'llanilishi lozim.
110	SIEM quyidagi uzluksiz aloqani ta'minlashi lozim: Cortex XDR event → normallashtirilgan SIEM hodisasi → Asset/Identity → Risk → Correlation → Incident yagona tekshiruv interfeysi doirasida ko'rsatilgan obyektlar o'rtasida o'tish imkoniyati bilan
112	Hodisani tekshirishda SIEM jamlangan hodisa, korrelyatsion hodisa yoki xavf obyektidan tortib Cortex XDR boshlang'ich ma'lumotlarigacha bo'lgan drill-down'ni ta'minlashi lozim, bunda bog'liq endpoint, foydalanuvchi, jarayon, fayl, IP-manzil, domen, tarmoq ulanishi va boshqa mavjud atributlar aks ettirilishi kerak.
113	SIEM Cortex XDR dan boshlang'ich ma'lumotlarni qayta olmasdan turib, Cortex XDR ma'lumotlarini boshqa manbalar ma'lumotlari bilan birgalikda tarixiy qidiruv va retrospektiv tahlil qilish imkoniyatini ta'minlashi lozim.
114	SIEM tarixiy ma'lumotlar massivini qayta yuklash zaruratisiz, o'zgartirilgan yoki yangi yaratilgan normallashtirish, tasniflash, boyitish va korrelyatsiya qoidalarini avval olingan Cortex XDR ma'lumotlariga qo'llashni ta'minlashi lozim.
115	Cortex XDR ma'lumotlari boshqa manbalar ma'lumotlari bilan birgalikda tezkor va tarixiy dashboard'lar hamda tahliliy ko'rinishlarni yaratish uchun mavjud bo'lishi va bunda boshlang'ich hodisagacha drill-down imkoniyati bo'lishi lozim.
116	SIEM tahdidlar tahlilida va MITRE ATT&CK'da Cortex XDR ma'lumotlaridan foydalanishni ta'minlashi, bunda tegishli taktikalar, texnikalar va bog'liq hodisalarni yagona tekshiruv doirasida aks ettirish imkoniyati bo'lishi lozim.
117	SIEM Cortex XDR ning shtatli integratsiya komponenti ishlash qobiliyatini, jumladan ulanish holati, ma'lumotlarni qabul qilish, qayta ishlash xatolari, ma'lumotlar kelishining kechikishi va ma'lumotlar kelishi to'xtashi belgilarini nazorat qilishni ta'minlashi lozim.
118	5.10.7–5.10.25 talablarini amalga oshirish uchun Buyurtmachi tomonidan mustaqil ravishda ishlab chiqilgan skriptlar, parserlar, ETL-protseduralar, oraliq ma'lumotlar bazalari yoki ishlab chiqaruvchi tomonidan qo'llab-quvvatlanadigan SIEMning Cortex XDR bilan standart integratsiyasiga kirmaydigan boshqa dasturiy komponentlardan majburiy foydalanishga yo'l qo'yilmaydi.