"Axborot va xavfsizlik hodisalarini boshqarish tizimi (SIEM) " texnik topshirig'iga 2-ilova

Talab raqami	Talab nomi/texnik xususiyatlar	Mezon turi
1	Dasturiy ta'minot 12 oylik obuna litsenziyalari bilan yetkazib beriladi (Yechimni litsenziyalash shaffof bo'lib, arxitekturani to'liq almashtirish zaruratisiz qayta ishlanadigan/indekslanadigan ma'lumotlar va/yoki funksional modullar hajmi bo'yicha kengaytirish imkonini beradi)	Bloklovchi
2	Dasturiy ta'minot (yechim) SIEM (Security Information and Event Management) sinfiga tegishli bo'lishi lozim	Bloklovchi
3	Tizim qayd etish, xavfsizlikni kuzatish, hodisalarni tekshirish, hisobot berish, vizualizatsiya qilish va boshqarish vazifalari uchun yagona interfeys va yagona ma'lumotlar omborini taqdim etishi lozim.	Bloklovchi
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 lozim.	Bloklovchi
5	Tizim barcha manbalarni oldindan yagona relyatsion modelga aylantirish zaruratisiz turli xil mashina ma'lumotlari bilan ishlashni ta'minlashi lozim.	Bloklovchi
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.	Bloklovchi
7	Tizim jismoniy infratuzilma, virtual muhit, xususiy/ommaviy bulut yoki gibrid modelda joylashtirishni qo'llab-quvvatlaydi va ishlab chiqaruvchining maxsus jismoniy qurilmalaridan majburiy foydalanishni talab qilmaydi.	Bloklovchi
8	Yechim arxitekturasi tizimni to'liq qayta o'rnatmasdan yig'ish, indekslash/saqlash va qidirish komponentlarini gorizontal miqyosda kengaytirishni qo'llab-quvvatlaydi.	Bloklovchi
9	Tizim bir nechta saqlash/indekslash tugunlari bo'yicha taqsimlangan qidiruvni ta'minlaydi va qidiruv so'rovlarini parallel qayta ishlashni qo'llab-quvvatlaydi.	Bloklovchi
10	Tizim qidiruv unumdorligini optimallashtirish, kirishni cheklash va saqlash muddatlarini boshqarish uchun turli xil ma'lumotlarni alohida mantiqiy omborlarga joylashtirishni qo'llab-quvvatlaydi.	Bloklovchi
11	Tizim katta hajmdagi mashina ma'lumotlarini qayta ishlashni qo'llab-quvvatlaydi va infratuzilmani tegishli tarzda loyihalashda kuniga o'nlab TB ma'lumotlarni kengaytirish imkoniyatiga ega ekanligi hujjatlar bilan tasdiqlangan.	Bloklovchi
12	Tizim ma'lumotlarni 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, skriptli va modulli manbalar orqali yig'ishni ta'minlaydi.	Bloklovchi
13	Agentlik dasturiy ta'minoti ma'lumotlar uzatishni shifrlashni, markaziy komponentlar mavjud bo'lmaganda keshlashni, qabul qiluvchi tugunlar o'rtasidagi yuklamani muvozanatlashni va ma'lumotlarni ishonchli transport protokoli orqali uzatishni qo'llab-quvvatlaydi.	Bloklovchi
14	Tizim ma'lumotlarni yig'ishning ham agentli, ham 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.	Bloklovchi
15	Tizim ko'p qatorli va murakkab hodisalarni hodisa tuzilishi va dastlabki vaqt belgisini yo'qotmasdan indekslashni qo'llab-quvvatlaydi.	Bloklovchi
16	Tizim ma'lumotlarni qabul qilishni boshlashdan oldin har bir manbaning tuzilishini oldindan tavsiflashni talab qilmasligi kerak.	Bloklovchi
17	Tizim har qanday manbadan dastlabki, o'zgartirilmagan mashina ma'lumotlarini qabul qilish, indekslash va saqlashni ta'minlashi lozim.	Bloklovchi
18	Tizim turli vaqt mintaqalaridan olingan vaqt belgilarini to'g'ri qayta ishlaydi va tizimga kelib tushgan vaqt bilan bir qatorda hodisaning asl vaqtini ham saqlab qoladi.	Bloklovchi
19	Tizim faqat ishlab chiqaruvchining tayyor konnektorlariga bog'liq emas: yangi manbalarni ulash va mahsulotning dastlabki kodini o'zgartirmasdan jurnal formatlarining o'zgarishiga moslashish imkoniyati bo'lishi kerak.	Bloklovchi
20	Manbalarning mavjudligini avtomatik tekshirish, kiruvchi hodisalarning to'liqligini nazorat qilish va muhim manbalardan ma'lumotlar kelishi to'xtatilganda ogohlantirishni qo'llab-quvvatlash.	Bloklovchi
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 ilovalari, Service Desk/ITSM, CMDB va foydalanuvchi ilovalari bilan integratsiyani qo'llab-quvvatlaydi.	Bloklovchi
22	Tizim dastlabki, o'zgartirilmagan mashina ma'lumotlarini indekslaydi va ushbu ma'lumotlarni keyinchalik qidirish, o'rganish va hisobot berishni ta'minlaydi, shuningdek, disk maydonidan foydalanishni optimallashtirish uchun indekslangan ma'lumotlarni avtomatik ravishda siqishni qo'llab-quvvatlaydi.	Bloklovchi
23	Tizimda tezkor, issiq va arxiv ma'lumotlarini manba turlari, indekslari, muhimligi va muvofiqlik talablari bo'yicha saqlash muddatlarini moslashuvchan sozlash imkoniyati mavjud.	Bloklovchi
24	Tizim ma'lumotlarning eskirishiga qarab ularni batafsil boshqarishni qo'llab-quvvatlaydi: arzonroq/tashqi xotiraga o'tkazish, arxivlash va/yoki Buyurtmachining qoidalariga muvofiq o'chirish.	Bloklovchi
25	Tizim foydalanish imkoniyati, yaxlitlik, nosozliklarga chidamlilik va qidiruv samaradorligini oshirish uchun ma'lumotlar/indekslarni takrorlashni qo'llab-quvvatlaydi.	Bloklovchi
26	Butun tizimni to'xtatmasdan xotirani kengaytirish imkoniyati mavjud	Bloklovchi
27	Jurnallar va auditorlik ma'lumotlarini ruxsatsiz o'zgartirish va o'chirishdan himoya qilish, jumladan yaxlitlikni tekshirish mexanizmlari mavjud.	Bloklovchi
28	Tizim xavfsizlikning namunaviy ssenariylari uchun hodisalarni yagona ma'lumotlar modeliga normallashtirishni qo'llab-quvvatlaydi, bunda dastlabki xom ma'lumotlar qidirish va tekshirish uchun ochiq bo'lishi lozim.	Bloklovchi
29	Maydonlar, ma'lumotnomalar, normallashtirish yoki boyitish qoidalarini ajratib olish mantiqini o'zgartirish avval saqlangan hodisalarni qayta yuklashni talab qilmaydi.	Bloklovchi
30	Tizim hodisalarni toifalash va hodisalarni 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-quvvatlaydi.	Bloklovchi
31	Foydalanuvchilarning atributlarini olish uchun korporativ kataloglar bilan integratsiya qo'llab-quvvatlanadi: login, to'liq ism, bo'linma, lavozim, rahbar, telefon raqami, joylashuv, imtiyozli belgi, ishning boshlanish/tugash sanasi va boshqa atributlar.	Bloklovchi
32	Bir nechta hisob/loginlarni bitta xodim yoki subyekt bilan bog'lash qo'llab-quvvatlanadi	Bloklovchi
33	Qurilmalar haqidagi ma'lumotlarni olish uchun aktivlar ma'lumotlar bazasi (CMDB) bilan integratsiya qo'llab-quvvatlanadi: xost nomi, IP, MAC, joylashuv, egasi, muhimlik darajasi, maxfiy ma'lumotlarning mavjudligi, me'yoriy talablarga muvofiqlik.	Bloklovchi
34	Tizim yangi ma'lumotnomalar va kontekst ma'lumotlarini avvalgi davrlar uchun qidirish va hisobot berish maqsadida ilgari indekslangan hodisalarga qo'llash imkonini beradi.	Bloklovchi
35	Tizim kalit so'zlar, vaqt oraliqlari, mantiqiy operatorlar, muntazam ifodalar va almashtirish belgilaridan foydalangan holda indekslangan ma'lumotlarning istalgan maydoni bo'yicha interaktiv to'liq matnli qidiruvni qo'llab-quvvatlaydi.	Bloklovchi
36	Tizim ham real vaqtdagi, ham rejalashtirilgan qidiruvlarni, shuningdek, bir nechta qidiruv so'rovlarini parallel ravishda bajarishni qo'llab-quvvatlaydi.	Bloklovchi
37	Tizim shunday yondashuvni qo'llab-quvvatlaydiki, unda dastlabki hodisalar to'liq saqlanadi va maydonlarni ajratib olish, ma'lumotlarni normallashtirish, boyitish va talqin qilish qabul qilish bosqichida ham, avval saqlangan ma'lumotlarni qidirish va tahlil qilish bosqichida ham amalga oshirilishi mumkin.	Bloklovchi
38	Tizim kirishning rol modelini hisobga olgan holda qidiruv so'rovlarini saqlash, tahrirlash, qayta foydalanish va boshqa foydalanuvchilarga uzatish imkonini beradi.	Bloklovchi
39	Tizim statistik tahlilni qo'llab-quvvatlaydi: hisoblash, novob qiymatlar, yig'indi, minimum, maksimum, o'rtacha, mediana, moda, standart og'ish, dispersiya, persentillar, qiymatning birinchi/oxirgi paydo bo'lishi	Bloklovchi
40	Tizim kam uchraydigan va g'ayritabiiy qiymatlarni aniqlash, asosiy xatti-harakat profillarini tuzish va og'ishlarni aniqlashni, jumladan, noma'lum tahdid ssenariylari va imzolarga qat'iy bog'liq bo'lmagan APTlarni qo'llab-quvvatlaydi.	Bloklovchi
41	Tizim vaqt, mantiqiy, xulq-atvor va statistik qoidalar, shu jumladan ko'p bosqichli hujum ssenariylari bo'yicha hodisalarni o'zaro bog'lashni qo'llab-quvvatlaydi.	Bloklovchi
42	Tizim aniqlash ssenariylarini tasniflash va tavsiflash uchun kill chain, MITRE ATT&CK yoki shunga o'xshash modellardan foydalanishni qo'llab-quvvatlaydi.	Bloklovchi

43	Tizim o‘z korrelyatsiya qoidalarini yaratish, mavjud qoidalarni o‘zgartirish va ularni sanoat ekspluatatsiyasiga kiritishdan oldin sinovdan o‘tkazish imkonini beradi.	Bloklovchi
44	Tizim oldindan tayyorlangan SIEM kontentini taqdim etadi: korrelyatsiya qoidalari, boshqaruv panellari, hisobotlar, ma’lumotlar modellari, tergov ssenariylari va xavfsizlik monitoringi andozalarini Buyurtmachining infratuzilmasiga moslashtirish imkoniyati bilan.	Bloklovchi
45	Tizim real vaqtga yaqin rejimda monitoringni qo‘llab-quvvatlaydi va qidiruv natijalari, korrelyatsiya qoidalari hamda tahliliy ssenariylar bo‘yicha ogohlantirishlarni shakllantiradi.	Bloklovchi
46	Ogohlantirishlar ustuvorliklarni belgilash, takroriy ishga tushirishlarni to‘xtatish, ishga tushirish chastotasini cheklash va mas’ul guruhlarga yo‘naltirishni qo‘llab-quvvatlaydi.	Bloklovchi
47	Tizim elektron pochta, tashqi tizimlar bilan integratsiya, Webhook/API, foydalanuvchi skriptlarini ishga tushirish yoki boshqa avtomatlashtirish mexanizmlari orqali xabarnomalar yuborishni qo‘llab-quvvatlaydi.	Bloklovchi
48	Tizim hodisalarni tekshirishning ish jarayonlarini taqdim etadi: hodisa kartochkasi/obyekti, boshlang‘ich voqealar va kontekstni bog‘lash, tergov tarixi, holatlar, izohlar, mas’ul shaxslarni tayinlash va natijalarni hujjatlashtirish imkoniyati.	Bloklovchi
49	Tizim yig‘ma hodisa/boshqaruv paneli/korrelyatsion ishga tushirishdan batafsil tekshiruv uchun dastlabki hodisalarga o‘tishni ta’minlaydi.	Bloklovchi
50	Tizim interaktiv boshqaruv panellari va hisobotlarni, jumladan jadvallar, vaqt diagrammalari, chiziqli, ustunli, maydonli, doiraviy va nuqtali grafiklar, holat ko‘rsatkichlari hamda IP/Geo-IP bo‘yicha geografik vizualizatsiyalarni tuzishni qo‘llab-quvvatlaydi.	Bloklovchi
51	Vizualizatsiyalar real vaqt rejimida yangilash, jamlangan ko‘rsatkichlardan boshlang‘ich hodisalarga o‘tish va anomaliyalar/emissiyalarni ajratib ko‘rsatishni qo‘llab-quvvatlaydi.	Bloklovchi
52	Tizim texnik va texnik bo‘lmagan foydalanuvchilarga hisobotlar va boshqaruv panellarini yaratish, jumladan panellarni vizual tahrirlash hamda sarlavhalar, afsonalar, o‘qlar va filtrlarni sozlash imkonini beradi.	Bloklovchi
53	Tizim rejalashtirilgan hisobotlarni shakllantirish va hisobotlarni PDF, CSV, XLS/XLSX va mahsulotda mavjud bo‘lgan boshqa formatlar kabi keng tarqalgan formatlarga eksport qilish/yuborishni qo‘llab-quvvatlaydi.	Bloklovchi
54	Tizim axborot xavfsizligi va tartibga solish talablariga, jumladan ISO 27002, NIST, PCI DSS va shunga o‘xshash standartlarga muvofiqlik masalalari uchun hisobotlar va monitoring panellarini qo‘llab-quvvatlaydi.	Bloklovchi
55	Tizim foydalanuvchilar va API uchun moslashuvchan rolli 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.	Bloklovchi
56	Tizim Active Directory/LDAP va korporativ yagona kirish tizimlari (SSO) bilan integratsiyani qo‘llab-quvvatlaydi.	Bloklovchi
57	Komponentlar o‘rtasida ma’lumotlar uzatish zamonaviy kriptografik protokollardan foydalangan holda himoyalangan kanallar orqali amalga oshiriladi.	Bloklovchi
58	Tizim foydalanuvchilar va ma’murlarning xatti-harakatlarini to‘liq tekshiradi: kirish, qidiruv so‘rovlari, hisobotlarni ko‘rish, sozlamalarni o‘zgartirish, foydalanuvchilarni boshqarish, qoidalarni yaratish/o‘zgartirish va boshqa muhim harakatlarni amalga oshiradi.	Bloklovchi
59	Auditorlik hodisalari Tizimlar sana va vaqtni, foydalanuvchi/subyektni, manbani, bajarilgan harakatni va bajarish natijasini o‘z ichiga oladi.	Bloklovchi
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.	Bloklovchi
61	Tizim o‘z konfiguratsiyasi, tarkibiy qismlarning mavjudligi va tizim xizmatlarining holatini ogohlantirish imkoniyati bilan nazorat qilishni ta’minlaydi.	Bloklovchi
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.	Bloklovchi
63	Tizim Python, Java, JavaScript, C# yoki shunga o‘xshash keng tarqalgan dasturlash tillari uchun SDK yoki kutubxonalarni qo‘llab-quvvatlashi lozim	Bloklovchi
64	Tizim konfiguratsiyalarini veb-interfeys, CLI va/yoki konfiguratsiya fayllari orqali boshqarish mumkin bo‘lishi lozim.	Bloklovchi
65	Tizim tashqi vizualizatsiya tizimlari, BI, ITSM/SOAR, CMDB, threat intelligence, monitoring tizimlari va Buyurtmachining boshqa korporativ platformalari bilan integratsiyani qo‘llab-quvvatlaydi.	Bloklovchi
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.	Bloklovchi
67	Tizim ommabop mahsulotlar va xavfsizlik ssenariylari uchun ommaviy va/yoki ishlab chiqaruvchi tomonidan taqdim etiladigan ilovalar/integratsiya paketlaridan foydalanishni qo‘llab-quvvatlaydi.	Bloklovchi
68	Tizim N+1 maqsadli arxitekturasida asosiy komponentlarni zaxiralash, klasterlash, muhim ma’lumotlarni takrorlash va yagona nosozlik nuqtasining yo‘qligini qo‘llab-quvvatlaydi.	Bloklovchi
69	Tizim avtomatik tiklanishni ta’minlaydi yoki tarkibiy qismlar ishlamay qolganda hujjatlashtirilgan tiklash tartibiga ega.	Bloklovchi
70	Tizimning asosiy ishlash rejimi - administrator nazorati ostida avtomatlashtirilgan rejimda uzluksiz, kecha-yu kunduz ishlashdir.	Bloklovchi
71	Tizim shtat, xizmat ko‘rsatish va avtonom rejimlarni qo‘llab-quvvatlaydi, shu jumladan markaziy komponentlar vaqtincha ishlamaganda ma’lumotlarni mahalliy buferlash imkoniyati mavjud.	Bloklovchi
72	Hodisalarni qabul qilish bo‘yicha o‘rtacha samaradorlik (EPS) - kamida 80 000 EPS (yoki o‘rtacha hodisa o‘lchami bo‘yicha hisoblangan ekvivalent ma’lumotlar hajmi)	Bloklovchi
73	Hodisalarni qabul qilish bo‘yicha eng yuqori samaradorlik - kamida 150 000 EPS	Bloklovchi
74	Qisqa muddatli portlash yuklamasi imkoniyati - 250 000 EPS gacha (to‘g‘ri hisoblangan arxitektura va buferlashda hodisalarni yo‘qotmasdan)	Bloklovchi
75	Indekslanadigan ma’lumotlarning kunlik hajmi - kuniga kamida 100 GB (platformani o‘zgartirmasdan yanada oshirish imkoniyati bilan)	Bloklovchi
76	"Qaynoq" ma’lumotlarni saqlash muddati (tezkor kirish) - kamida 180 kun.	Bloklovchi
77	"Iliq" ma’lumotlarni saqlash muddati - kamida 12 oy	Bloklovchi
78	Arxiv ma’lumotlarini saqlashning umumiy muddati - kamida 3 yil (36 oy).	Bloklovchi
79	Xabarnomagacha bo‘lgan hodisani qayta ishlashning maksimal kechikishi - shtat yuklamasi mavjud bo‘lgan kritik korrelyatsiya ssenariylari uchun 3 soniyadan oshmasligi lozim.	Bloklovchi
80	Manbalar va uzatish kanallari to‘g‘ri sozlanganda, odatiy yuklamada hodisalarning yo‘qolishi 0% ni tashkil etadi.	Bloklovchi
81	Bir vaqtning o‘zida ulangan manbalar soni - kamida 2000 ta	Bloklovchi
82	Taqsimlangan kollektorlar/agentlarni qo‘llab-quvvatlash - kamida 10 ta masofaviy maydoncha	Bloklovchi
83	Bir vaqtning o‘zida ishlaydigan SOC foydalanuvchilari soni - kamida 20 ta	Bloklovchi
84	90 kunlik ma’lumotlar bo‘yicha qidiruv so‘rovini bajarish vaqti - kelishilgan namunaviy qidiruv so‘rovlari uchun 120 soniyadan oshmasligi kerak.	Bloklovchi
85	6 oylik agregatsion hisobotni bajarish vaqti 10 daqiqadan oshmasligi kerak.	Bloklovchi
86	Tizimni to‘liq to‘xtatmasdan, gorizontal ravishda unumdorlikni kengaytirish	Bloklovchi
87	Arxitektura yondashuvini o‘zgartirmasdan EPSni kamida 3 baravar oshirish imkoniyati	Bloklovchi

88	Alohida saqlashni qo‘llab-quvvatlash (hot/warm/archive tiers) talab etiladi	Bloklovchi
89	Buzilishga chidamlilik - yagona buzilish nuqtasining yo‘qligi (N+1)	Bloklovchi
90	Tizim bir marta to‘plangan va indekslangan ma’lumotlardan turli ssenariylarda foydalanish imkonini beradi: axborot xavfsizligi monitoringi, muvofiqlik, hodisalarni tekshirish, firibgarlikni aniqlash, IT-operatsiyalar, ilovalar monitoringi, raqamli tahlil va biznes tahlili.	Bloklovchi
91	Tizim ma’lumotlarni alohida platformaga ko‘chirish zaruratisiz qo‘shimcha modullar, ilovalar yoki integratsiyalar orqali funksionallikni kengaytirishni qo‘llab-quvvatlaydi.	Bloklovchi
92	Tizim javobni avtomatlashtirish, SOAR/ITSM bilan integratsiyalashuv va foydalanuvchilar hamda obyektlar xatti-harakatlarining kengaytirilgan tahlili tomon keyingi rivojlanish imkoniyatini ta’minlaydi.	Bloklovchi
93	Yechimning kafolatli qo‘llab-quvvatlanishi - kamida 1 yil	Bloklovchi
94	Loyihaga o‘rnatish va integratsiya ishlari kiritilgan.	Bloklovchi
95	Loyihaga loyihalash kiritilgan	Bloklovchi
96	Loyihaga Buyurtmachi mutaxassislarining sertifikatlangan ta’limi kiritilgan.	Bloklovchi
97	Loyihaga Kiberxavfsizlik markazi dasturiy ta’minotni sertifikatlash kiritilgan.	Bloklovchi
98	Interfeys tili - rus/ingliz	Bloklovchi
99	Tizimda ma’lumotlarni oldindan normallashtirmasdan yoki alohida SQL ma’lumotlar bazasiga yuklamasdan, bevosita dastlabki indekslangan hodisalar bo‘yicha qidirish, tekshirish, korrelyatsiya qilish va hisobot tuzish imkoniyati mavjud bo‘lishi kerak, bu esa tizimning qo‘shimcha afzalligi hisoblanadi.	Bloklanmaydigan
100	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, bu me’yoriy ilova, qo‘shimcha, modul yoki SIEMning boshqa maxsus tarkibiy qismi sifatida amalga oshirilishi lozim.	Bloklanmaydigan
101	Shtat integratsiyasi Cortex XDR’dan kamida quyidagilarni o‘z ichiga olgan o‘zaro bog‘liq ma’lumotlarni avtomatik ravishda olishni ta’minlashi lozim: hodisalar, ogohlantirishlar, batafsil hodisalar, yakuniy qurilmalar, foydalanuvchilar, jarayonlar, tarmoq ulanishlari, tahdid obyektlari, artefaktlar va hodisalarni qayta ishlash holatlari haqidagi ma’lumotlar.	Bloklanmaydigan
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 va tegishli Cortex XDR insidenti o‘rtasidagi o‘zaro bog‘liqlik saqlanib qoladi.	Bloklanmaydigan
103	Olingan Cortex XDR ma’lumotlari boshlang‘ich qiymatlar va obyektlar o‘rtasidagi munosabatlarni saqlab qolgan holda, standart integratsiya vositalari yordamida SIEM ma’lumotlarining yagona me’yorlashtirilgan modeliga avtomatik ravishda o‘zgartirilishi lozim.	Bloklanmaydigan
104	Me’yorlashtirilgan Cortex XDR ma’lumotlari bevosita SIEMning asosiy mexanizmlari, jumladan qidiruv, korrelyatsiya, tahliliy qoidalar, vizualizatsiya, hodisalarni tekshirish, xavf-xatarga asoslangan tahlil va xavfsizlik kontenti tomonidan qo‘shimcha ma’lumotlarni o‘zgartirish zaruratisiz qo‘llanilishi lozim.	Bloklanmaydigan
105	SIEM Cortex XDR ma’lumotlarini Asset va Identity obyektlari, jumladan yakuniy nuqta, IP-manzil, DNS nomi, foydalanuvchi hisobi va boshqa identifikatorlar bilan avtomatik ravishda taqqoslashni ta’minlashi hamda ushbu kontekstdan keyingi tahlilda foydalanish imkoniyatini yaratishi lozim.	Bloklanmaydigan
106	Cortex XDR ma’lumotlari foydalanuvchilar, yakuniy qurilmalar va boshqa obyektlar uchun xavf hodisalarini shakllantirish, to‘plash va jamlash imkoniyatiga ega bo‘lgan SIEM xavfga yo‘naltirilgan tahlilning doimiy mexanizmida bevosita ishtirok etishi lozim.	Bloklanmaydigan
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.	Bloklanmaydigan
108	SIEM Cortex XDR ma’lumotlari uchun alohida tahliliy kontur yaratmasdan, Cortex XDR hodisalari va boshqa ulangan manbalar hodisalari to‘plami asosida yagona hodisa yoki tahliliy obyektni shakllantirishni ta’minlashi lozim.	Bloklanmaydigan
109	Cortex XDR ma’lumotlari SIEM ishlab chiqaruvchisi tomonidan yetkazib beriladigan oldindan o‘rnatilgan xavfsizlik kontentida, 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.	Bloklanmaydigan
110	SIEM uzluksiz aloqani ta’minlashi kerak: Cortex XDR hodisasi → normallashtirilgan hodisa SIEM → Asset/Identity → Risk → Correlation → Incident yagona tergov interfeysi doirasida ko‘rsatilgan obyektlar o‘rtasida o‘tish imkoniyati bilan	Bloklanmaydigan
111	Hodisani tekshirishda SIEM jamlangan hodisa, korrelyatsion hodisa yoki xavf obyektidan tortib Cortex XDR boshlang‘ich ma’lumotlarigacha bo‘lgan batafsil ma’lumotni taqdim etishi lozim, bunda bog‘liq yakuniy nuqta, foydalanuvchi, jarayon, fayl, IP-manzil, domen, tarmoq aloqasi va boshqa mavjud atributlar aks ettirilishi lozim.	Bloklanmaydigan
112	SIEM Cortex XDR ma’lumotlarini boshqa manbalar ma’lumotlari bilan birgalikda, Cortex XDR dan dastlabki ma’lumotlarni qayta olmasdan, tarixiy qidiruv va retrospektiv tahlil qilish imkoniyatini ta’minlashi lozim.	Bloklanmaydigan
113	SIEM o‘zgartirilgan yoki yangi yaratilgan me’yorlashtirish, tasniflash, boyitish va korrelyatsiya qoidalarini avval olingan Cortex XDR ma’lumotlariga tarixiy ma’lumotlar massivini qayta yuklash zaruratisiz qo‘llashni ta’minlashi lozim.	Bloklanmaydigan
114	Cortex XDR ma’lumotlari tezkor va tarixiy boshqaruv panellari hamda tahliliy ko‘rinishlar yaratish uchun boshqa manbalardan olingan ma’lumotlar bilan birgalikda, dastlabki hodisagacha o‘rganish imkoniyati bilan mavjud bo‘lishi lozim.	Bloklanmaydigan
115	SIEM tahdidlarni tahlil qilishda Cortex XDR va MITRE ATT&CK ma’lumotlaridan foydalanishni ta’minlashi, bunda tegishli taktikalar, usullar va tegishli hodisalarni yagona tergov doirasida aks ettirish imkoniyatiga ega bo‘lishi lozim.	Bloklanmaydigan
116	SIEM Cortex XDR integratsiyasining shtatli tarkibiy qismining ishlash qobiliyatini, jumladan ulanish holatini, ma’lumotlarni qabul qilishni, qayta ishlash xatolarini, ma’lumotlar kelishining kechikishini va ma’lumotlar kelishining to‘xtash belgilarini nazorat qilishni ta’minlashi lozim.	Bloklanmaydigan
117	99-118-talablarni (SoC) amalga oshirish uchun Buyurtmachi tomonidan mustaqil ishlab chiqilgan skriptlar, parserlar, ETL protseduralari, oraliq ma’lumotlar bazalari yoki ishlab chiqaruvchi tomonidan qo‘llab-quvvatlanadigan SIEMning Cortex XDR bilan integratsiyalashuviga kirmaydigan boshqa dasturiy komponentlardan majburiy foydalanishga yo‘l qo‘yilmaydi.	Bloklanmaydigan
118	SIEM va XDR integratsiyasining barcha ko‘rsatilgan mexanizmlari yagona SIEM texnologik konturi doirasida ishlashi va me’yorlashtirish, korrelyatsiya, xavf-xatar tahlili, vizualizatsiya yoki tergovni amalga oshirish uchun Cortex XDR ma’lumotlarini alohida tahliliy platformaga uzatishni talab qilmasligi lozim.	Bloklanmaydigan

Sana:

Tuzildi
AXB boshlig'i
Lavozim

kun/oy/yil

R.A. Abdulvaat
F.I.Sh.

Kelishildi:
AX va RB direktor
Lavozim

B.A. Olmatov
F.I.Sh.