

"EDR/XDR yakuniy tugunlarini yakuniy nuqtalarini) himoya qilish tizimlari" texnik topshirig'iga ___-ilova

Ishtirokchi 1

Talab raqami	Talab nomi/texnik xususiyatlar	Ishtirokchining nomi		
		Muvofiq/ muvofiq emas	Tavsifga havola (hujjat)	Izoh
TX-1	Dasturiy ta'minot 3 yil muddatga yetkazib berilishi kerak (obuna, shu jumladan texnik qo'llab-quvvatlash)	Muvofiq/ muvofiq emas		
TX-2	Yechim Extended Detection and Response (XDR) sinfiga tegishli bo'lishi kerak	Muvofiq/ muvofiq emas		
TX-3	Platforma 24x7 rejimida ishlash imkoniyatiga ega markazlashtirilgan boshqaruv konsolini qo'llab-quvvatlaydi.	Muvofiq/ muvofiq emas		
TX-4	SaaS modellarini yetkazib berishda quyidagi shartlar bajarilishi shart: - Buyurtmachi ma'lumotlarini izolyatsiya qilish; - ma'lumotlarni sertifikatlangan ma'lumotlar markazlariga joylashtirish; - ma'lumotlarni uzatish va saqlashda shifrlashdan foydalanish.	Muvofiq/ muvofiq emas		
TX-5	Yechim arxitekturasini xizmatlarni to'xtatmasdan gorizontallashtirishni ta'minlaydi.	Muvofiq/ muvofiq emas		
TX-6	Quyidagi funksiyalar bo'lishi shart: - zaifliklardan foydalanishning oldini olish; - fayl va faylsiz hujumlardan himoya; - zararli skriptlardan himoya qilish; - ransomware turidagi hujumlarni aniqlash va oldini olish	Muvofiq/ muvofiq emas		
TX-7	Turli xil xavfsizlik manbalaridan olingan telemetriya ma'lumotlarining avtomatik korrelyatsiyasi mavjudligi	Muvofiq/ muvofiq emas		
TX-8	Tizim hujum zanjirini vizuallashtirishni ta'minlaydi	Muvofiq/ muvofiq emas		
TX-9	Yechim tarmoq himoya vositalari (tarmoqlararo ekranlar, bosqinchilikning oldini olish tizimlari) bilan tabiiy integratsiyani qo'llab-quvvatlaydi.	Muvofiq/ muvofiq emas		
TX-10	Yechim javob ssenariylari doirasida tarmoq ulanishlari, IP-manzillar va domenlarni avtomatik ravishda bloklashni qo'llab-quvvatlaydi.	Muvofiq/ muvofiq emas		
TX-11	Integratsiya tashqi ma'lumotlar brokerlaridan foydalanmasdan amalga oshirilishi kerak.	Muvofiq/ muvofiq emas		
TX-12	Yechim ishlab chiqaruvchining 100 dan ortiq tayyor pleybuklari bilan xavfsizlik hodisalariga javob berishning avtomatlashtirilgan ssenariylarini taqdim etadi, jumladan: - oxirgi nuqtani izolyatsiyalash; - zararli jarayonlarni tugatish; - fayllarni xesh bo'yicha bloklash; - forenzik artefaktlarni to'plash.	Muvofiq/ muvofiq emas		
TX-13	Yechim dastur kodini yozmasdan maxsus javob ssenariylarini yaratish imkoniyatini qo'llab-quvvatlaydi.	Muvofiq/ muvofiq emas		
TX-14	Yechim real vaqt rejimida yangilanadigan global kibertahdid manbalaridan foydalanadi.	Muvofiq/ muvofiq emas		
TX-15	Yechim hodisalarni dolzarb xavf indikatorlari (IoC) bilan avtomatik ravishda bog'lashni qo'llab-quvvatlaydi.	Muvofiq/ muvofiq emas		

TX-16	<p>Yechim quyidagilarni qo'llab-quvvatlaydi:</p> <ul style="list-style-type: none"> - kirishning rolli modeli (RBAC); - foydalanuvchilar harakatlarining auditi; - hodisalar haqidagi barcha to'plangan xizmat ma'lumotlarini (telemetriya) kamida 30 kun saqlash, hodisalar tarixini esa 12 oygacha saqlash. 	Muvofiq/ muvofiq emas		
TX-17	<p>Qaror quyidagilarni shakllantirishni qo'llab-quvvatlaydi:</p> <ul style="list-style-type: none"> - tezkor boshqaruv panellari; - axborot xavfsizligi bo'limi rahbariyati uchun hisobotlar; - ma'lumotlarni tashqi SIEM tizimlariga yuklash. 	Muvofiq/ muvofiq emas		
TX-18	<p>Yechim zaifliklarni nazorat qilish va o'rnatilgan agentlarsiz tarmoq va aktivlarni skanerlashni amalga oshirish uchun ishlab chiqaruvchidan oraliq (proksi) server asosidagi zaifliklarni tarmoq skaneridan foydalanish imkoniyatini qo'llab-quvvatlashi kerak.</p> <p>Yechim zaifliklarni nazorat qilish uchun yagona platforma doirasida kengayishni qo'llab-quvvatlashi kerak:</p> <ul style="list-style-type: none"> - muayyan zaiflikdan foydalanishni avtomatik ravishda to'xtatishga qodir bo'lgan himoya mexanizmlari (aniqlash va javob berish platformasining faol oldini olish qoidalarini) mavjudligini hisobga oladigan kritiklikni darajalash algoritmlarini o'z ichiga olishi; - uchinchi tomon zaiflik skanerlaridan zaifliklar haqidagi ma'lumotlarni avtomatik ravishda to'plash va ularni zaifliklarni boshqarishning yagona tizimiga integratsiya qilishni ta'minlash; - eng muhim xavflarni, vaqt o'tishi bilan xavf darajasining o'zgarish dinamikasini va ularni bartaraf etish jarayonini ko'rish uchun maxsus monitoring panelini o'z ichiga olishi; - zaifliklarni bartaraf etish uchun avtomatlashtirilgan o'rnatilgan pleybuklarni ta'minlash, shu jumladan jiddiy zaifliklarni qo'lda aralashuvsiz bartaraf etish uchun to'liq avtomatlashtirilgan harakatlarni qo'llab-quvvatlash; - muayyan tugunlardagi zaifliklardan tarmoq ichida tajovuzkorni harakatlantirish uchun foydalanish mumkinligini ko'rsatuvchi "hujum yo'llari" vizualizatsiyasini taqdim etish; - nafaqat CVSS baholashini, balki ushbu EPSS zaifligidan foydalanish belgilarini ham hisobga oladigan zaifliklar xavfini baholash mexanizmini taqdim etish; - yagona platforma doirasida hujumning tashqi yuzasini nazorat qilish va tashqi zaifliklarni hamda boshqa tahdidlar bilan bog'liq tashqi hujum vektorlarini baholash uchun qo'shimcha modul qo'shish imkoniyati; - aniqlangan zaifliklarni aniqlash va javob berish platformasida qayd etilgan faol axborot xavfsizligi hodisalar bilan avtomatik solishtirish imkoniyatini o'z ichiga olishi. 	Muvofiq/ muvofiq emas		
TX-19	<p>Yechim quyidagilar bilan integratsiyani qo'llab-quvvatlaydi:</p> <ul style="list-style-type: none"> - Active Directory / LDAP; - REST API ni qo'llab-quvvatlovchi platformalar; - ogohlantirishlar va audit jurnallarini yuborish uchun tashqi Syslog Receivers bilan. 	Muvofiq/ muvofiq emas		
TX-20	Hisoblarni qo'lda boshqarmasdan avtomatik sinxronlash imkoniyati mavjud	Muvofiq/ muvofiq emas		
TX-21	Yechimda REST API mavjud	Muvofiq/ muvofiq emas		
TX-22	<p>Foydalanish jarayonida quyidagi funksiyalar bajarilishi lozim:</p> <ul style="list-style-type: none"> - imzolar, detektorlash modellari va tahlil komponentlarini yangilash avtomatik ravishda amalga oshirilishi lozim, - yechim komponentlarni yangilashda uzluksiz himoyani ta'minlashi kerak, - Vender 24x7 darajasidan past bo'lmagan texnik yordamni ta'minlashi kerak. 	Muvofiq/ muvofiq emas		
TX-23	Yechim yakuniy nuqtaga masofadan ulanish imkoniyatini qo'llab-quvvatlashi lozim.	Muvofiq/ muvofiq emas		
TX-24	Yechim ISO 27001 sertifikatiga ega bo'lishi shart	Muvofiq/ muvofiq emas		

TX-25	Yechim quyidagi qurilmalarni boshqarish funksiyalariga ega bo'lishi kerak: - Windows va macOS operatsion tizimlari uchun shifrlashni boshqarishni ta'minlash	Muvofiq/ muvofiq emas		
TX-26	Yechim quyidagilardan telemetriyani barqaror qayta ishlashni ta'minlaydi: - bitta mantiqiy tenant doirasida kamida 10 000 ta yakuniy nuqta; - arxitekturasini o'zgartirmasdan keyinchalik kengaytirish imkoniyati bilan.	Muvofiq/ muvofiq emas		
TX-27	Yechim LLM va bulutli omborlarda ma'lumotlar uzatilishini nazorat qilish va yakuniy nuqtalarda ma'lumotlar sizib chiqishining oldini olish imkoniyatini yagona tahdidlarni boshqarish platformasi va yakuniy nuqtalarga o'rnatiladigan yagona agent doirasida qo'llab-quvvatlashi kerak.	Muvofiq/ muvofiq emas		
TX-28	Yakuniy nuqta agenti o'rtacha quyidagilardan ortiq iste'mol qilmasligi kerak: - 5% CPU odatiy rejimda; - 500 MB operativ xotira; - 1 GB disk maydoni.	Muvofiq/ muvofiq emas		
TX-29	Yechim ma'lumotlar va telemetriyani yo'qotmasdan tahlil va boshqaruv tarkibiy qismlarining barqaror ishlashini ta'minlashi lozim.	Muvofiq/ muvofiq emas		
TX-30	Yechim sun'iy intellekt yordamida xatdagi niyatlarni chuqur tahlil qilish orqali fishing xatlarini aniqlash va o'chirish uchun maxsus modulni qo'llash imkoniyatini qo'llab-quvvatlashi lozim.	Muvofiq/ muvofiq emas		
TX-31	Integratsiya quyidagilarni ta'minlashi lozim: - foydalanuvchilar, guruhlar va rollar haqida ma'lumot olish; - xavfsizlik hodisalarining foydalanuvchi hisoblari bilan o'zaro bog'liqligini; - hodisalar kontekstini yaratish uchun katalog ma'lumotlaridan foydalanish.	Muvofiq/ muvofiq emas		
TX-32	Tashqi SIEM tizimlari bilan ikki tomonlama integratsiya ta'minlanadi, jumladan: - hodisalar va hodisalarni uzatish; - boyitilgan voqealarni uzatish.	Muvofiq/ muvofiq emas		
TX-33	Quyidagilar orqali integratsiya qo'llab-quvvatlanadi: - REST API; - Syslog; - mahalliy konnektorlar.	Muvofiq/ muvofiq emas		
TX-34	Yechimdan quyidagicha foydalanish mumkin: - SIEM uchun hodisalar manbasi; - SIEM ulanishi shart bo'lmagan avtonom XDR platformasi.	Muvofiq/ muvofiq emas		
TX-35	Integratsiya quyidagilarni ta'minlashi lozim: - xavfsizlik telemetriyasini olish; - fishing hujumlari va hisob qaydnomalarining buzilishi holatlarini aniqlash.	Muvofiq/ muvofiq emas		
TX-36	Yechim quyidagilar uchun ochiq, hujjatlashtirilgan REST API'ni taqdim etishi lozim: - hodisalar va hodisalarni qabul qilish; - himoya obyektlarini boshqarish; - javob berish ssenariylarini ishga tushirish.	Muvofiq/ muvofiq emas		
TX-37	API quyidagilarni qo'llab-quvvatlaydi: - tokenlar orqali autentifikatsiya qilish; - kirish huquqlarini chegaralash; - murojaatlarni qayd etish.	Muvofiq/ muvofiq emas		

TX-38	Yechim quyidagilar uchun ITSM toifasidagi tizimlar bilan integratsiyani qo'llab-quvvatlashi lozim: - hodisalarni avtomatik ravishda yaratish; - tergov maqomlarini o'tkazish; - javob berish natijalariga ko'ra hodisalarni yopish.	Muvofiq/ muvofiq emas		
TX-39	Quyidagilar doirasida integratsiyalardan foydalanish imkoniyati qo'llab-quvvatlanishi lozim: - avtomatik pleybuklar; - yarim avtomatik javob ssenariylari.	Muvofiq/ muvofiq emas		
TX-40	Qarorni litsenziyalash himoyalangan yakuniy nuqtalar soniga qarab, litsenziyalanadigan hajmni moslashuvchan tarzda ko'paytirish imkoniyati bilan amalga oshirilishi lozim.	Muvofiq/ muvofiq emas		
TX-41	Litsenziya qiymatiga quyidagilar kiritilishi kerak: - yakuniy nuqtalarda hujumlarning oldini olish funksiyalari; - aniqlash va javob berish funksiyalari (EDR/XDR); - markazlashtirilgan boshqaruv konsoli; - mashinaviy o'rganish va xulq-atvor modellari asoslangan tahlil; - o'rnatilgan avtomatik javob berish ssenariylari.	Muvofiq/ muvofiq emas		
TX-42	Quyidagi funksiyalar uchun qo'shimcha to'lovga yo'l qo'yilmaydi: - hodisalarning o'zaro bog'liqligini.	Muvofiq/ muvofiq emas		
TX-43	Litsenziya yechimdan foydalanish huquqini o'z ichiga olishi kerak: - kecha-kunduz rejimida; - hodisalar va hodisalar soniga cheklovlarisiz.	Muvofiq/ muvofiq emas		
TX-44	Litsenziya doirasida quyidagilar taqdim etilishi kerak: - imzolarni muntazam ravishda yangilab borish; - analitik modellarni yangilash; - platformaning funksional komponentlarini yangilash.	Muvofiq/ muvofiq emas		
TX-45	Litsenziya quyidagilarni o'z ichiga olishi kerak: - 24x7 darajadagi texnik yordam; - bilim bazasi va harakat qilish bo'yicha tavsiyalardan foydalanish imkoniyati.	Muvofiq/ muvofiq emas		
TX-46	Litsenziyalash quyidagilarga bog'liq bo'lmazligi kerak: - qayta ishlanadigan trafik hajmi; - tahliliy qoidalar soni; - boshqaruv konsoli foydalanuvchilari soni.	Muvofiq/ muvofiq emas		
TX-47	Tizimning ishlash rejimlariga qo'yiladigan talablar Tizimning asosiy ishlash rejimi avtomatlashtirilgan bo'lib, administrator tomonidan boshqariladi. Tizim quyidagi rejimlarda ishlash imkoniyatini ta'minlashi lozim: shtat rejimi (tun-u kun uzluksiz ishlash); avtonom rejim (tizim komponentlari o'rtasida yoki tashqi tarmoqlar bilan aloqa mavjud bo'lmagan taqdirda).	Muvofiq/ muvofiq emas		
TX-48	Dasturiy majmuani yetkazib berish va tizimni ishga tushirishni ta'minlash uchun Ijrochining xodimlari soni va malakasiga qo'yiladigan talablar: Ijrochining xodimlari tarkibida kamida bitta texnik qo'llab-quvvatlash muhandisi shtat birligi bo'lishi kerak; texnik qo'llab-quvvatlash muhandisi Buyurtmachida Tizimga shtatdagi texnik va avariya xizmatini ko'rsatish uchun zarur bo'lgan hajmdagi bilimlarga ega bo'lishi kerak.	Muvofiq/ muvofiq emas		

TX-49	Audit, monitoring va hisobotga qo'yiladigan talablar tizim foydalanuvchilar va ma'murlarning xatti-harakatlari auditini, xavfsizlik va foydalanish hodisalarini qayd etishni, shuningdek, tarkibiy qismlarning holati va ulardan foydalanish imkoniyatini monitoring qilishni ta'minlashi lozim; tizim shubhali faollik aniqlanganda xabar yuborish imkoniyati bilan real vaqt rejimida auditni qo'llab-quvvatlashi kerak; barcha hodisalar sana va vaqt, harakat manbai va natijasi ko'rsatilgan holda qayd etilishi kerak; tizim jurnallarni ruxsatsiz o'zgartirish va o'chirishdan himoya qilishni ta'minlashi kerak; hisobotlar so'rov bo'yicha va/yoki jadval asosida, standart formatlarga (PDF, CSV) eksport qilish imkoniyati bilan mavjud bo'lishi shart. auditorlik va monitoring ma'lumotlarini (loglarini) saqlash muddati - kamida 12 oy	Muvofiq/ muvofiq emas
TX-50	Himoyalangan yakuniy nuqtalar soni – kamida 2000 ta	Muvofiq/ muvofiq emas
TX-51	Loyiha montaj ishlarini o'z ichiga oladi.	Muvofiq/ muvofiq emas
TX-52	Loyiha loyihalash ishlarini o'z ichiga oladi.	Muvofiq/ muvofiq emas
TX-53	Loyihaga Buyurtmachi mutaxassislarini o'qitish kiritilgan	Muvofiq/ muvofiq emas
TX-54	Loyihaga dasturiy ta'minotni MKBda sertifikatlash kiritilgan	Muvofiq/ muvofiq emas
TX-55	Ijrochida MAFning mavjudligi	Muvofiq/ muvofiq emas

Sana: 03.06.2028.

kun/oy/yil 03.06.2028.

Tuzildi:

AX bo'limi boshlig'i

Lavozim



R.A. Abdulvaat

F.I.Sh,

Kelishildi:

AX va RB direktor

Lavozim



B.A. Olatov

F.I.Sh,