

"Fayllarni xavfsiz ijro etish uchun izolyatsiyalangan tizim (Sandbox)" texnik topshirig'iga ___-sonli ilova

Talab raqami	Talablar nomi/texnik tavsiflar	Ishtirokchi		
		Mos/ Mos emas	Tavsifga havola (hujjat)	Izoh
1	Yechim Sandbox sinfiga tegishli bo'lishi kerak	Соответствие/ Не соответствие		
2	Tizimni joylashtirish: On-Premise (dasturiy-qurilmaviy majmua)	Соответствие/ Не соответствие		
3	DQM tarkibidagi dasturiy ta'minot 3 yil muddatga yetkazib berilishi lozim (obuna turi bo'yicha, texnik qo'llab-quvvatlashni hisobga olgan holda).	Соответствие/ Не соответствие		
4	Yechim tahdidlarni tahlil qilishning quyidagi usullarini qo'llab-quvvatlaydi: • nolinch kun fishing saytlarini, shu jumladan spam va zararli dasturlarni o'z ichiga olgan saytlarni real vaqt rejimida aniqlash imkoniyati; • sniffer rejimida tarmoq tahdidlarini aniqlashni qo'llab-quvvatlash; • botnetlar va tarmoq hujumlari faoliyatini, zararli URL-manzillarga tashriflarni aniqlash; • obyektlarni antivirus skanerlash orqali tekshirishni ta'minlash.	Соответствие/ Не соответствие		
5	Fayl kengaytmalarining majburiy turlari: • Windowsning bajariladigan fayllari: .bat, .cab, .cmd, .dll, .exe, .js, .msi, .ps1, .vbs, .vbe, WSF • Microsoft Office: .doc, .docm, .docx, .dot, .dotm, .dotx, .ics, .iqy, .one, .pot, .potm, .potx, .ppt, .pptm, .pptx, .ppam, .pps, .ppsm, .ppsx, .pub, .rtf, .sldm, .sldx, .xlam, .xls, .xlsb, .xslm, .xlsx, .xlt, .xltm, .xltx • hujjatlar va elektron pochta fayllari: .eml, .pdf, .rl • Android uchun fayllar: .apk • Linux fayllari: .elf, .sh, ObjectFiles • MacOS fayllari: .app, .dmg, Mach-O • veb-fayllar: .asp, .hta, .htm, .html, .lnk, .js, .lnk, .url, WEblink • quyidagi fayllarni siqish: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .udf, .upx, .xz, .z, .zip	Соответствие/ Не соответствие		
6	Emulyatsiya uchun quyidagi turdagi operatsion tizimlarni qo'llab-quvvatlash imkoniyati mavjudligi: • Windows (bir nechta versiyalari, shu jumladan joriy versiyalari); • Linux (Redhat, OEL, Ubuntu, CentOS); • 32/64-bitni qo'llab-quvvatlash; • virtual obrazlarni moslashtirish imkoniyati.	Соответствие/ Не соответствие		
7	Tizim quyidagilar bilan integratsiyani qo'llab-quvvatlashi kerak: • fayervollar (NGFW); • elektron pochta shlyuzi (Email Gateway); • Web Gateway; • antivirus (Endpoint Protection) • EDR / XDR tizimi bilan • SIEM tizimi (istiqbolda).	Соответствие/ Не соответствие		
8	Ma'lumotlar almashinuvi quyidagilarni qo'llab-quvvatlashi kerak: • REST API; • STIX/ standarti; • Syslog.	Соответствие/ Не соответствие		
9	Tizimni endpoint yechimlari (antivirus) bilan integratsiyalash • antivirusning endpoint-agentlaridan shubhali fayllarni avtomatik uzatish imkoniyati. • yakuniy nuqtalarda buzilish belgilarini avtomatik ravishda bloklash imkoniyati. • xostni avtomatik izolyatsiyalashni qo'llab-quvvatlash (agar integratsiya mavjud bo'lsa).	Соответствие/ Не соответствие		
10	Tizim unumdorligi: • qurilmadagi lokal virtual mashinalar soni bo'yicha unumdorlik: kamida 14; • 80 tagacha virtual mashinani bulutga kengaytirish imkoniyati; • Sandbox ning samarali o'tkazish qobiliyati: soatiga kamida 10 000 ta fayl; • obyektlarni dastlabki filtrlash (statistik tahlil) orqali tekshirish unumdorligi: soatiga kamida 20 000 ta fayl; • virtual muhitda emulyatsiya orqali obyektlarni tekshirish unumdorligi (dinamik tahlil): soatiga kamida 500 ta fayl; • pochmani himoya qilish yechimi bilan integratsiyalashgandagi unumdorlik: soatiga 100 000 ta xat; • MTA Adapter orqali obyektlarni tekshirish unumdorligi soatiga 25 000 ta xat; • snifer rejimidagi unumdorlik: kamida 500 Mbit/s.	Соответствие/ Не соответствие		

11	<p>Tizimni boshqarish va ma'murlash</p> <ul style="list-style-type: none"> • WEB-boshqaruv interfeysi; • rollarni farqlash (rolli model); • administratorlar harakatlarini qayd etish; • AD/LDAP bilan integratsiya; • Tizim ma'murlari uchun ikki bosqichli autentifikatsiyani qo'llab-quvvatlash. 	Соответствие/ Не соответствие		
12	<p>Yechim quyidagi hisobotlarni taqdim etadi:</p> <ul style="list-style-type: none"> • batafsil xulq-atvor hisoboti: - fayl faolligi, - reyestrda o'zgarishlar, - tarmoq ulanishlari, - jarayonlar, • kiberhujum bosqichlarini boshidan to nishongacha grafik tasvirlash, • xavf-xatar belgilarini shakllantirish (hash, IP, URL, domen), • hisobotlarni PDF formatga eksport qilish. 	Соответствие/ Не соответствие		
13	<p>Tizimni litsenziyalash</p> <ul style="list-style-type: none"> • litsenziya quyidagilarni qamrab olishi kerak: - tahlil qilinayotgan obyektlar soni, - integratsiya qilinadigan qurilmalar soni, - signaturalar va dvigatellarni yangilash. • VM soni - kamida 4 dona. (qo'shimcha litsenziyani faollashtirish orqali yanada kengaytirish imkoniyati bilan); • dasturiy ta'minotga obuna bo'lish muddati - 3 yil; • texnik qo'llab-quvvatlash muddati - kamida 3 yil. 	Соответствие/ Не соответствие		
14	<p>Qo'shimcha talablar</p> <ul style="list-style-type: none"> • ishlab chiqaruvchidan o'z tadqiqot markazlarini qo'llab-quvvatlash; • XDR toifasidagi platformalar bilan integratsiya 	Соответствие/ Не соответствие		
15	Loyihaga o'rnatish ishlari ham kiritilgan.	Соответствие/ Не соответствие		
16	Loyihaga loyihalash kiritilgan	Соответствие/ Не соответствие		
17	Loyihaga Buyurtmachining 2 nafar mutaxassisini o'qitish ham kiritilgan.	Соответствие/ Не соответствие		
18	Loyihaga KXMda dasturiy ta'minot/DQMni sertifikatlash ham kiritilgan.	Соответствие/ Не соответствие		
19	Interfeys tili - rus/ingliz	Соответствие/ Не соответствие		
20	Ijrochida MAF mavjudligi	Соответствие/ Не соответствие		

* barcha bandlar majburiy va bloklovchi kuchga ega.

Sana:

kun/oy/yil

Tuzdi:

Axborot xavfsizligi bo'limi boshlig'i

Abdulvaat R.A.

Lavozimi

FISh

Kelishildi:

AXvaR departamenti direktori

Olmatorov B.A.

Lavozimi

FISh

