



«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”

“UNIVERSAL MOBILE SYSTEMS” MChJ
Axborot xavfsizligi va rejim bo'yicha direktori



 B.A. Olatov
2026-y. “ ” _____

“Universal Mobile Systems” MChJ ehtiyojlari uchun fayllarni xavfsiz ijro etish uchun
izolyatsiyalangan tizimni (Sandbox) yetkazib berish, o'rnatish va ishga tushirish bo'yicha

TEXNIK TOPSHIRIQ

Mundarija:

1 Umumiy ma'lumotlar	3
2 Loyihani amalga oshirish uchun asos.....	3
Xavfsizlik va rejim departamentining 2026-yilga mo'ljallangan rivojlanish rejasi ("UMS" MChJning 2026-yil uchun tasdiqlangan biznes-rejasi va budjeti).	3
3 Ijrochidan talab qilinadigan ishlar, xizmatlar ro'yxati va ularning hajmlari (miqdori).....	3
4 Ishlarni bajarish va xizmatlar ko'rsatish joyi	4
5 Tizimga texnik talablar	4
6. Ijrochiga qo'yiladigan talablar.....	9
7. Ishlarni bajarish va xizmatlar ko'rsatish uchun xavfsizlik talablari	10
8. Bajarilgan ishlar va ko'rsatilgan xizmatlar natijalariga ko'ra texnik va boshqa hujjatlarni topshirish bo'yicha talablar	10
10. Kafolat majburiyatlari.....	11
11. Servis va texnik qo'llab-quvvatlash shartlari	11
13. Ishlar, xizmatlar va ularni taqdim etish shartlariga qo'yiladigan boshqa talablar	13
14. Qo'llaniladigan atamalar va qisqartmalar.....	14
15. Ilovalar ro'yxati	14
"UMS" MChJ - 2014-yil 1-dekabrda boshlab O'zbekiston Respublikasining butun hududida mobil aloqa xizmatlarini ko'rsatuvchi telekommunikatsiya kompaniyasi.	15

1 Umumiy ma'lumotlar

Ushbu texnik topshiriqda fayllarni xavfsiz ijro etish uchun ajratilgan tizimga (Sandbox) (keyingi o'rinlarda - Tizim, AT) loyihani to'liq foydalanishga tayyor holda amalga oshirish uchun dasturiy ta'minot va xizmatlarni sotib olish bo'yicha tender va/yoki tanlov e'lon qilish maqsadida Buyurtmachining dasturiy ta'minot tarkibiga qo'yiladigan talablarini tavsiflash uchun yetarli bo'lgan talablar tavsiflangan

Axborotlashtirish obyektining tavsifi 1-ildovada keltirilgan.

1.1 Bajarilayotgan ishlar (ko'rsatilayotgan xizmatlar) nomi

Loyihaning to'liq nomi: Fayllarni xavfsiz ijro etish uchun izolyatsiyalangan tizim (Sandbox) (keyingi o'rinlarda – Tizim).

Ishlar Buyurtmachining infratuzilmasi va maydonchasida olib borilmoqda.

Ushbu Texnik topshiriq doirasida Ijrochi Sandbox apparat-dasturiy kompleksini yetkazib berish, o'rnatish, integratsiya qilish va foydalanishga topshirish bo'yicha tijorat taklifini taqdim etishi lozim.

1.2 Bajarilayotgan ishlar va ko'rsatilayotgan xizmatlardan foydalanish maqsadlari

Loyihaning asosiy maqsadi – Buyurtmachining axborot infratuzilmasi himoyalanganlik darajasini oshirish uchun zararli kodni dinamik tahlil qilish tizimini joriy etish.

Tizim tomonidan hal qilinadigan asosiy vazifalar:

- zararli va ilgari noma'lum bo'lgan (Zero-day) dasturiy ta'minotni aniqlash;
- emulyatsiya qilinadigan operatsion muhitda obyektlarning xatti-harakatlarini tahlil qilish;
- aniqlangan obro'sizlantirish ko'rsatkichlari (IOC) bo'yicha hisobotlarni shakllantirish;
- mavjud himoya vositalari (SIEM, EDR/XDR, pochta shlyuzlari, NGFW) bilan integratsiyalashuv;

- tahlil natijalarini javob berish tizimlariga avtomatik ravishda uzatish;

- "UMS" MChJ IT-infratuzilmasining umumiy himoya darajasini oshirish.

Tizimning asosiy vazifasi - nazorat qilinadigan virtual muhitda shubhali fayllar, havolalar, ilovalar va tarmoq trafigi obyektlarini alohida ishga tushirish va ularning xatti-harakatini tahlil qilish orqali maqsadli va noma'lum kibertahdidlarni aniqlash, tahlil qilish va oldini olishdan iborat.

2 Loyihani amalga oshirish uchun asos

Xavfsizlik va rejim departamentining 2026-yilga mo'ljallangan rivojlanish rejasi ("UMS" MChJning 2026-yil uchun tasdiqlangan biznes-rejasi va budjeti).

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

Fayllarni xavfsiz ijro etish uchun izolyatsiyalangan tizimni (Sandbox) joriy etish Buyurtmachining mas'ul shaxslari bilan birgalikda, Buyurtmachining mavjud IT-infratuzilmasining ishlash qobiliyatini buzmasdan, mavjud qurilmalarni oldindan yuzaki tekshirish orqali amalga oshirilishi lozim. Har qanday korporativ tizimlarni to'xtatishni talab qiladigan barcha ishlar Buyurtmachi bilan oldindan kelishilgan bo'lishi kerak.

Loyiha doirasida Ijrochi tomonidan ishlarning quyidagi bosqichlari bajarilishi kerak:

- tayyorgarlik bosqichi;
- ishga tushirish-sozlash va integratsiya ishlari;
- Buyurtmachi xodimlarini o'qitish.

3.1 Tayyorgarlik bosqichi

Loyiha uchun mas'ul bo'lgan Buyurtmachi xodimlari bilan o'zaro hamkorlikni va Buyurtmachining AT infratuzilmasini birgalikda tekshirishni o'z ichiga oladi. Ushbu bosqichda xodimlar quyidagilarni aniqlashlari kerak:

- Buyurtmachi tarmog'i topologiyasining eng muhim tafsilotlari;
- ulanadigan interfeyslarning turlari;

- Tizimni yoyish jarayonida Buyurtmachi va Ijrochining javobgarlik zonalarini;

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 apparat qismini o'rnatish va konfiguratsiyalash;
- Buyurtmachining tarmoq infratuzilmasiga integratsiyalash;
- monitoring uchun zarur bo'lgan modullarni faollashtirish;
- zarur litsenziyalarni faollashtirish.

Buyurtmachining AT infratuzilmasi obyektlari bilan bog'liq bo'lmagan xatolar tufayli Tizim ishida uzilishlar aniqlangan taqdirda, Ijrochi bajarilgan ishlar to'g'risidagi dalolatnoma imzolanganiga qadar mahsulotning funksional qismiga tuzatishlar kiritish majburiyatini oladi.

3.3 Tizimni nazorat qilish va qabul qilish tartibi

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

Qabul qilish sinovlarining maqsadi Tizim komponentlarining ishlash qobiliyatini va ularning TT talablariga muvofiqligini tasdiqlashdan iborat.

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

Qabul sinovlari natijalari qabul komissiyasi a'zolari tomonidan imzolanadigan bayonnoma bilan rasmiylashtirilishi kerak. Qabul sinovlari muvaffaqiyatli o'tkazilganligi fakti bo'yicha Qabul sinovlarini yakunlash dalolatnomasi imzolanadi.

Qabul sinovlari vaqtida kamchiliklar, nuqsonlar yoki TT talablaridan boshqa chetga chiqishlar aniqlangan taqdirda tegishli faktlar bayonnomada qayd etilishi kerak, unda, shu jumladan quyidagilar ko'rsatiladi:

- kamchiliklar (nuqsonlar) ro'yxati;
- qayd etilgan kamchiliklarning tizimning ishlash qobiliyatiga ta'siri darajasi;
- kamchiliklarni (nuqsonlarni) bartaraf etishning talab qilinadigan muddatlari.

Qabul komissiyasi kamchiliklar, nuqsonlar yoki tizimga qo'yiladigan talablardan boshqa chetga chiqishlar bartaraf etilgan paytdan boshlab besh ish kuni ichida tegishli komponentni takroriy qabul sinovlaridan o'tkazishi va Tizimni doimiy foydalanishga qabul qilishi kerak.

3.4 Xodimlarni o'qitish.

O'qitish ushbu TTning 9-bandiga muvofiq

4 Ishlarni bajarish va xizmatlar ko'rsatish joyi

Ijrochi DTni yetkazib berish, o'rnatish va sozlashni quyidagi manzil bo'yicha ta'minlashi kerak: O'zbekiston Respublikasi, Toshkent shahri, 100000, Amir Temur shoh ko'chasi, 24, "UMS" MChJ markaziy ofisi.

Tizimni yetkazib berish muddatlari Buyurtmachi va Ijrochi o'rtasidagi Shartnomada belgilanadi, biroq Buyurtmachi va Ijrochi o'rtasidagi shartnomaviy munosabatlar imzolangan kundan boshlab 90 kalendar kundan oshmasligi kerak.

5 Tizimga texnik talablar

Tizimga quyidagi texnik talablar qo'yiladi.

5.1 Umumiy talablar

5.1.1 Yechim Sandbox/Advanced Malware Analysis toifasiga mansub bo'lishi lozim.

5.1.2 Tizimning vazifasi - noma'lum zararli dasturiy ta'minot (zero-day), APT tahdidlari va yuklangan ijro etiladigan fayllar ko'rinishidagi maqsadli hujumlarni aniqlash.

5.1.3 Yoyishni qo'llab-quvvatlash:

- On-Premise (standart telekommunikatsiya ustuniga o'rnatishni qo'llab-quvvatlovchi dasturiy-apparat majmuasi)

- Tizim Vendorining bulutli xizmatlari bilan integratsiya qilish imkoniyati.

5.1.4 Izolyatsiyalangan segmentda ishlashni qo'llab-quvvatlash

5.1.5 Unumdorlik bo'yicha masshtablash imkoniyati.

5.2 Funksional talablar

5.2.1 Tahlil usullari

- Real vaqt rejimida nolinchi kun fishing saytlarini, shu jumladan spam va zararli dasturlarni o'z ichiga olgan saytlarni aniqlash imkoniyati.
- Sniffer rejimida tarmoq tahdidlarini aniqlashni qo'llab-quvvatlash. Botnetlar faoliyati va tarmoq hujumlarini, zararli URL manzillarga tashriflarni aniqlash.
- Antivirus skanerlash orqali obyektlarni tekshirishni ta'minlash;
- Qurilmalarning SOCga fayl va URL manzillarini yuborishini qo'llab-quvvatlash.
- NGFW bilan integratsiyani qo'llab-quvvatlash, protokollar qismida: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM va ularning SSL shifrlangan ekvivalent versiyalari.
- SMTP, POP3, IMAP protokollari doirasida pochta himoyasi bilan integratsiyani qo'llab-quvvatlash.
- HTTP, FTP, SMB protokollari bo'yicha yakuniy nuqtalarni himoya qilish yechimi bilan integratsiyani qo'llab-quvvatlash.
- WAF bilan integratsiyani qo'llab-quvvatlash, protokollar qismida: HTTP, HTTPS.
- Sniffer rejimini qo'llab-quvvatlash. HTTP, FTP, POP3, IMAP, SMTP, SMB.
- ICAP orqali proksi-serverni tekshirish imkoniyati.
- SMTP orqali MTA/BCC rejimida ishlash imkoniyati.
- FTP, sFTP, CIF, NFS orqali tarmoq umumiy xotiralarini skanerlash rejimini qo'llab-quvvatlash.
- Vaziyatni tuzatish uchun zararli DT namunalari va ko'rsatkichlarini yuklashni avtomatlashtirish uchun JSON API mavjudligi.
- CEF serverlari va syslog serverlari yordamida jurnallarni masofadan va xavfsiz saqlash hamda SIEMga yuborish imkoniyati.
- Integratsiyalashgan qurilmadan (qurilmalardan) fayllarni yuborish imkoniyati.
- Mijozning shubhali server bilan ulanishini qayta tiklash uchun TCP RST qo'llab-quvvatlaydigan sniffer rejimini yoyish imkoniyati.
- Katta fayllarni (masalan, ISO-tasvirlar, umumiy tarmoq papkalari, SMB/NFS) qo'llab-quvvatlaydigan tarmoq resurslarini skanerlash imkoniyati.
- Zaxiralash uchun birlamchi va ikkilamchi tugunlar bilan yuqori qulaylikni qo'llab-quvvatlash.
- Klasterning nosozliklarga chidamliligini ta'minlash uchun portlar monitoringi.
- O'tkazish qobiliyatini oshirish uchun tugunlarni klasterlash imkoniyati.
- O'tkazish qobiliyatini oshirish va zaxiralash uchun jamlangan interfeyslarni qo'llab-quvvatlash.
- Ma'muriy trafikni virtual mashina obrazlari trafigidan ajratish.
- Taqdim etilgan materiallarga qarab "Sandbox" resurslarini optimallashtiruvchi intellektual moslashuvchan skanerlash profilini sozlash imkoniyati.
- Bir vaqtning o'zida bir nechta turli xil VMlarni ishga tushirish uchun parallel skanerlashni qo'llab-quvvatlash.
- Hujjatlarga o'rnatilgan fayllarni ajratib olish va skanerlash imkoniyati.
- Hujjatlar va QR-kodlarga o'rnatilgan URL-manzilni ajratib olish va skanerlash imkoniyati.
- OCR yordamida hujjatlardagi tasvirlarni ajratib olish va skanerlash imkoniyati.
- Yara uchinchi tomon ishlab chiqaruvchilari qoidalari bilan integratsiyani qo'llab-quvvatlash.

- Fayllar nazorat yig'indilarining oq va qora ro'yxatlari parametrlarini belgilash imkoniyati.
- Yuborilgan xatlar va fayllardan URL manzillarni skanerlash imkoniyati.
- VMdan samarali foydalanish uchun VMni skanerlash koeffitsiyentini monitoring qilish.
- Zararli dasturlarga xos xulq-atvor belgilarini aniqlash maqsadida virtual muhitda emulyatsiya (dinamik tahlil) orqali obyektlarni tekshirishni ta'minlaydi.
- Sun'iy intellektga asoslangan xulq-atvor tahlilini qo'llab-quvvatlash.
- Sandboxning bir vaqtdagi nusxalarini qo'llab-quvvatlash.
- Qo'llab-quvvatlanadigan OT turlari: Windows 11/10, Linux, MacOS, Android.
- Windows va Linux operatsion tizimlari uchun sozlanadigan virtual mashinalarni qo'llab-quvvatlash.
- Internet Explorer, Microsoft Edge, Google Chrome va Mozilla Firefox qo'llab-quvvatlaydigan sozlanuvchi internet-brauzer.
- "Sandbox" interaktiv rejimini qo'llab-quvvatlash, zararli dasturiy ta'minot bilan o'zaro ta'sirni videoga olish va VM skrinshotlari.

5.2.2 Aylanib o'tish holatlarini aniqlash uchun zarur texnikalar:

Aylanib o'tishni aniqlashning zarur usullari:

Необходимые техники обнаружения обходов:

- API obfuscatsiyasi;
- bare-metal aniqlash;
- Command and Control;
- Bevosita tizim qo'ng'iroqlari;
- Bajarilishning kechikishi;
- Payload faqat xotira uchun;
- Jarayonlarga inyeksiya qilish;
- Bajarish paytida shifrlash/joylash;
- Tizim qoliplari;
- Time Bomb;
- Foydalanuvchi fayllarini tekshirish;
- Foydalanuvchi bilan o'zaro aloqani tekshirish;
- Virtual mashinalar va sandboxlarni aniqlash;
- Qayta chaqiruvlarni aniqlashni qo'llab-quvvatlash;
- Zararli URL manzillarga kirish, C&C botnet bilan aloqa va faollashtirilgan zararli DTdan tajovuzkorlar trafigi.
- Yuklab olinadigan qo'lga kiritilgan paketlar, trassirovka jurnallari va skrinshotlar.
- To'plangan ko'rsatkichlar va natijalardan foydalangan holda sun'iy intellektga asoslangan tahdidlar xulosasining mavjudligi.
- Ulanish va xizmatlar, litsenziya holati, skanerlash unumdorligi, tizim resurslari uchun panelda vidjetlarning mavjudligi.
- Foydalanish tarixini kuzatish uchun skanerlash unumdorligi sahifasining mavjudligi.
- Real vaqt rejimida monitoring vidjetlarining mavjudligi. Skanerlash natijalari statistikasi, Skanerlash faolligi (ma'lum vaqt davomida), Top target hostlar, Top zararli dasturlar, Top zararlangan URL manzillar, Top teskari chaqiruv domenlari.
- Hodisalarni ochib ko'rish vositasining mavjudligi. Harakatlar, zararli dastur nomi, reytingi, turi, manbasi, manzili, aniqlangan vaqti va yuklab olish yo'lidan iborat dinamik jadval.
- Hisobotlar va jurnallarni qo'llab-quvvatlash. Grafik interfeys, PDF yuklash va qayta ishlanmagan jurnal fayli.

- Topshiriqning bajarilishi haqida batafsil hisobot tuzish imkoniyati.
- Tizim holati, unumdorligi, skanerlash statistikasi va tizim resurslaridan foydalanishning davriy jurnallarini yaratish imkoniyati.
- MITRE ATT&CK v11 qo'llab-quvvatlash.
- Trassirovka jurnallari, PCAP va indikatorlarni STIX 2.0 formatida yuklash imkoniyati.
- Zararli fayl aniqlanganda elektron pochta orqali bildirishnomalar yuborish imkoniyati.
- Global elektron pochta ro'yxatlari va administratorlar uchun haftalik hisobotlar yaratish imkoniyati.
- Tizim konfiguratsiyasi va holati to'g'risida to'liq ma'lumot olish uchun TAC-hisobot yaratish imkoniyati.
- Grafik interfeys va CLI orqali sozlash imkoniyati.
- To'liq kirish yoki faqat ko'rish ruxsatini qo'llab-quvvatlaydigan bir nechta administrator hisoblarini qo'llab-quvvatlash.
- Administratorlar uchun Radius autentifikatsiyasini qo'llab-quvvatlash.
- Tizimga yagona kirish uchun SAML'ni qo'llab-quvvatlash.
- Konfiguratsiyalar, ulanishlar va xizmatlarni o'z-o'zini tekshirish vidjetining mavjudligi.
- HA va klaster tugunlarini boshqarish uchun klasterni boshqarish sahifasining mavjudligi.
- Administratorlarga individual qidiruv shartlarini yaratish imkonini beruvchi markazlashtirilgan qidiruv sahifasining mavjudligi.
- Istalgan litsenziyani bitta qulay sahifadan yuklab olish imkoniyati.
- Virtual mashinalar holatini monitoring qilish.
- Dvijok va signaturalarni avtomatik yangilash imkoniyati.
- Virtual mashinaning yangi obrazi mavjudligini avtomatik tekshirish imkoniyati.
- Tizimning ishlash qobiliyatini tekshirish haqida xabar berish tizimining mavjudligi.
- Zaxiralash, tiklash va tizim konfiguratsiyasini tekshirishni qo'llab-quvvatlash.
- Nosozliklarni aniqlash va bartaraf etish uchun birlashtirilgan CLI mavjudligi.
- Ustuvorlikni aniqlash va fayllarni keyingi skanerlash uchun uchinchi tomon skanerlash qurilmasiga yuborish uchun tarmoq diskrlarini skanerlash rejimida opsiya mavjudligi.

5.2.3 Fayl turlarini qo'llab-quvvatlash

- Windows ijro 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, .xlsm, .xlsx, .xlt, .xltn, .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-fayllari: .asp, .hta, .htm, .html, .lnk, .js, .lnk, .url, WEblink.
- Fayllarni siqing: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .udf, .upx, .xz, .z, .zip.
- Foydalanuvchi tomonidan belgilanadigan kengaytmalar.

5.2.3 Emulyatsiya uchun OTni qo'llab-quvvatlash

Quyidagi turdagi OTlarni majburiy qo'llab-quvvatlash:

- Windows (bir nechta versiya, jumladan, muhimlari);
- Linux (Redhat, OEL, Ubuntu, CentOS);
- 32/64-bit qo'llab-quvvatlash;

- virtual obrazlarni moslashtirish imkoniyati.

5.3 Integratsion talablar

5.3.1 Buyurtmachining tarmoq infratuzilmasi bilan integratsiyalashuv

Tizim quyidagilar bilan integratsiyani qo'llab-quvvatlashi kerak:

- fayervollar (NGFW);
- elektron pochta shlyuzi (Email Gateway);
- SIEM tizimi (Buyurtmachi tomonidan joriy etilgandan so'ng).

Ma'lumotlar almashinuvi quyidagilarni qo'llab-quvvatlashi kerak:

- REST API;
- STIX standarti;
- Syslog.

5.4 Tizim unumdorligi

5.4.1 Qurilmadagi lokal virtual mashinalar soni bo'yicha unumdorlik: 14 tadan kam emas.

5.4.2 Sandboxning samarali o'tkazish qobiliyati: soatiga kamida 10 000 ta fayl.

5.4.3 Obyektlarni dastlabki filtrlash (statistik tahlil) orqali tekshirish unumdorligi: soatiga kamida 20 000 ta fayl.

5.4.4 Virtual muhitda emulyatsiya (dinamik tahlil) orqali obyektlarni tekshirish unumdorligi: soatiga kamida 500 ta fayl.

5.4.5 Pochtani himoya qilish yechimi bilan integratsiyalashgandagi samaradorlik: soatiga 100 000 ta xat.

5.4.6 MTA Adapter orqali obyektlarni tekshirish unumdorligi soatiga 25 000 ta xat.

5.4.7 Snifer rejimidagi unumdorlik: kamida 500 Mbit/s.

5.5 APKning texnik xususiyatlari va sig'imi:

- Saqlanadigan ma'lumotlarning umumiy hajmi: kamida 960 GB;
- Tarmoq interfeyslari: kamida 4 ta port 1Gbit/s RJ-45 ulagichi;
- Ta'minot bloki: 100-240V AC, 60-50 Hz;
- TPM mavjudligi.

5.6 Tizimni boshqarish va ma'murlashtirish

- Boshqaruvning WEB-interfeysi;
- Rollarni ajratish (rollar modeli);
- Administratorlar harakatlarini qayd etish jurnali;
- AD/LDAP bilan integratsiya;
- Tizim administratorlari uchun ikki faktorli autentifikatsiyani qo'llab-quvvatlash.

5.7. Tizim hisobotlari

Yechim quyidagilarni taqdim etishi lozim:

- xatti-harakatlar bo'yicha batafsil hisobot:
 - fayllardagi faollik,
 - reyestrda o'zgarishlar,
 - tarmoqqa ulanishlar,
 - jarayonlar,
- kiberhujum bosqichlarining boshidan oxirigacha bo'lgan grafik tasvirini vizualizatsiya qilish,
- komprometatsiya belgilarini (hash, IP, URL, domen) shakllantirish,
- hisobotlarni PDF formatida eksport qilish.

5.8. Tizimni litsenziyalash

- "Pesochitsa" dvijogiga obuna muddati: kamida 3 yil.
- VM soni – kamida 4 dona (qo'shimcha litsenziyani faollashtirish orqali keyinchalik 14 donagacha kengaytirish imkoniyati bilan).

- Dasturiy ta'minotga obuna muddati – 3 yil.
- Texnik qo'llab-quvvatlash muddati – kamida 3 yil.

5.9. Qo'shimcha talablar

- Ishlab chiqaruvchining shaxsiy tadqiqot markazlari tomonidan qo'llab-quvvatlanishi;
- XDR sinfidagi platformalar bilan integratsiyalashuvi.

5.10. Tizimning ishlash rejimlariga qo'yiladigan talablar

Tizimning asosiy ishlash rejimi – administrator boshqaruvi ostidagi avtomatlashtirilgan rejimdir.

Tizim quyidagi rejimlarda ishlash imkoniyatini ta'minlashi kerak:

- shtat rejimi – shubhali fayl va obyektlarni kechayu kunduz uzluksiz detonatsiya qilish va tahlil etish;
- avtonom rejim – Sandbox komponentlari o'rtasida yoki tashqi tarmoqlar bilan aloqa bo'lmaganda, konfiguratsiya ma'lumotlariga va avval o'tkazilgan tahlil natijalariga kirish uchun.

Ijrochining xodimlari soni va malakasiga qo'yiladigan talablar.

Dasturiy majmuani yetkazib berish va Tizimning ish faoliyatini yo'lga qo'yishni ta'minlash uchun Ijrochining xodimlari tarkibida kamida bitta texnik qo'llab-quvvatlash muhandisi shtat birligi bo'lishi shart.

Texnik qo'llab-quvvatlash muhandisi Buyurtmachida Tizimga muntazam texnik va avariya xizmatini ko'rsatish uchun zarur bo'lgan hajmdagi bilimlarga ega bo'lishi shart.

5.12. Audit, monitoring va hisobotga qo'yiladigan talablar

- Tizim foydalanuvchilar va ma'murlarning xatti-harakatlari auditini, xavfsizlik hodisalari va Sandbox ekspluatatsiyasini qayd etishni, shuningdek, virtual appayans tarkibiy qismlarining holati va mavjudligini kuzatishni ta'minlashi lozim.
- Shubhali faoliyat yoki Sandbox ishlashidagi xatolar aniqlanganda ogohlantirishlar yuborish imkoniyati bilan real vaqt rejimida auditni qo'llab-quvvatlash kerak.
- Barcha hodisalar sana va vaqtni, hodisa manbasini, tahlil qilinayotgan obyekt turini va tahlil natijasini ko'rsatgan holda qayd etilishi lozim.
- Jurnallar ruxsatsiz o'zgartirish yoki o'chirishdan himoyalangan bo'lishi kerak.
- Tahlil natijalari va tizim holati to'g'risidagi hisobotlar so'rov bo'yicha va/yoki jadval asosida, standart formatlarga (PDF, CSV) eksport qilish imkoniyati bilan mavjud bo'lishi kerak.
- Auditorlik va monitoring ma'lumotlarini (loglarini) saqlash muddati - kamida 12 oy.

6. Ijrochiga qo'yiladigan talablar

6.1. Ijrochiga qo'yiladigan umumiy talablar

Ijrochi quyidagi talablarga javob berishi kerak:

- belgilangan xizmatlarni ko'rsatish (dasturiy ta'minotni yetkazib berish) bo'yicha kamida 3 yillik tasdiqlangan ish tajribasi;

- vakolatli hamkor bo'lishi, shuningdek, amalga oshirilayotgan/joriy etilayotgan dasturiy ta'minotdan foydalanish va joriy etish huquqlarini yakuniy foydalanuvchilarga tarqatish uchun hujjatli tasdiqqa ega bo'lishi;

- to'lovga qobiliyatsiz yoki bankrot hisoblanmasligi, tugatish jarayonida bo'lmasligi, Ijrochining iqtisodiy faoliyati to'xtatilmaligi, xatlanmasligi kerak;

- o'z tarkibida ushbu dasturiy ta'minotni o'rnatish, sozlash, foydalanish va texnik qo'llab-quvvatlash bo'yicha malakasini tasdiqlovchi sertifikatlariga ega bo'lgan kamida 2 (ikki) nafar mutaxassisga ega bo'lishi;

- Ijrochi ekspertizadan o'tish niyati to'g'risidagi kafolat xatini yoki "Kiberxavfsizlik markazi" DUKdan olingan axborot va kiberxavfsizlikni ta'minlash talablariga muvofiqlik yuzasidan ekspertizadan o'tganlik to'g'risidagi sertifikatni taqdim etish majburiyatini oladi.

Ijrochi O'zbekiston Respublikasining amaldagi qonunchiligida maxfiy axborotni 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'lib qolgan maxfiy axborotni oshkor etmasligi shart.

6.2. Ijrochi taklif tarkibiga uning yuqorida ko'rsatilgan talablarga muvofiqligini tasdiqlovchi quyidagi hujjatlarni kiritishi lozim:

- ishlab chiqaruvchi kompaniya bilan hamkorlik maqomi mavjudligi to'g'risidagi vakolatli xat nusxasi;

- ishlab chiqaruvchi kompaniyaning kamida 2 ta muhandislik sertifikatini nusxalari.

- oxirgi 3 yilda amalga oshirilgan IT-loyihalar ro'yxati.

6.3. Ishlab chiqaruvchiga qo'yiladigan talablar

Vender kompaniya bozorda kamida 5 yil faoliyat yuritishi va O'zbekiston bozorida vakolatli hamkorlarga ega bo'lishi kerak.

7. Ishlarni bajarish va xizmatlar ko'rsatish uchun xavfsizlik talablari

Ishlarni bajarishda xavfsizlik bo'yicha quyidagi talablar qo'yiladi:

7.1. Dasturiy majmuani o'rnatish, sozlash va ishga tushirish bo'yicha barcha ishlar elektr xavfsizligi talablariga, shuningdek amaldagi ichki me'yoriy hujjatlarga muvofiq bajarilishi shart.

7.2. Ijrochi ishlarni bajarish jarayonida axborot xavfsizligi talablariga rioya etilishi uchun to'liq javobgardir.

7.3. Ishlarni faqat Buyurtmachi tomonidan tasdiqlangan kelishilgan muddatlar va vaqt oralig'ida bajarishga ruxsat beriladi.

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

Tizimni joriy etish va sanoatda foydalanishga topshirish tugallangandan so'ng Ijrochi Tizimning amalda amalga oshirilgan holatini aks ettiruvchi ishchi (ijro) hujjatlarini tayyorlashi shart.

Hujjatlar quyidagilarga taqdim etiladi:

- qog'ozda 2 (ikki) nusxada;
- elektron shaklda (formatlar: DOCX va PDF).

Hujjatlarning majburiy tarkibi:

- Tizimning umumiy tavsifi;
- arxitektura va tarmoq sxemalari;
- dasturiy komponentlar ro'yxati va konfiguratsiyasi;
- buyurtmachining infratuzilmasi bilan integratsiyalashuv tavsifi;
- tarmoq manzili (IP, portlar, protokollar);
- qisqa ekspluatatsiya hujjatlari;
- axborot xavfsizligi bo'yicha amalga oshirilgan chora-tadbirlar tavsifi.

Hujjatlar dolzarb, to'liq va Tizimning amalda qo'llanilishiga mos kelishi, shuningdek, Ijro etuvchini jalb qilmasdan undan foydalanish uchun yetarli bo'lishi kerak.

9. Buyurtmachining xodimlarini o'qitishga talablar

Mazkur Texnik topshiriq doirasida Ijrochi quyidagi o'quv dasturlarini ta'minlaydi:

a) Buyurtmachining axborot xavfsizligi bo'yicha ikki nafar mutaxassisini ushbu majmuani boshqarishga sertifikatlangan holda o'qitish.

Tinglovchilar soni: 2 kishi.

Formati: kunduzgi / onlayn, amaliy mashg'ulotlar bilan.

O'qitish tili: rus / ingliz.

Materiallar: taqdimotlar, yo'riqnomalar, laboratoriya ishlari.

O'qitish yakunlariga ko'ra Ijrochi quyidagilarni taqdim etadi:

- o'quv materiallarini;

- mashg'ulotlar yozuvlarini;
 - o'qishdan o'tganlikni tasdiqlovchi hujjatlarni (sertifikatlarni).
- b) tizim foydalanuvchilarini o'qitish.

Tinglovchilar soni: 10 kishigacha.

Formati: namoyish + amaliy.

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

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

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

10. Kafolat majburiyatlari

Ijrochi ishlab chiqaruvchi tomonidan hujjatlarda belgilangan dasturiy ta'minotdan foydalanish qoidalariga rioya qilish va o'rnatilgan dasturiy ta'minot ishiga ruxsatsiz aralashmaslik sharti bilan bajarilgan ish sifati Buyurtmachi tomonidan ko'rsatilgan texnik topshiriq va talablarga muvofiq bo'lishini kafolatlashi kerak.

Tizimni joriy etish bo'yicha bajarilgan ishlar uchun kafolat muddati **36 (o'ttiz olti)** oyni tashkil etishi kerak va Tomonlar ishlarni topshirish-qabul qilish dalolatnomasini imzolagan kundan boshlab hisoblanadi.

Dasturiy ta'minot obunasining amal qilish muddati - **36 (o'ttiz olti) oy**.

Tajribaviy foydalanish davri 1 (bir) oyni tashkil etishi kerak va Tomonlar ishlarni topshirish-qabul qilish dalolatnomasini imzolagan kundan boshlab hisoblanadi.

11. Servis va texnik qo'llab-quvvatlash shartlari

Ishlab chiqaruvchining xizmat ko'rsatish muddati - DT joriy etilgan paytdan boshlab **36 (o'ttiz olti) oy**. Dasturiy ta'minot komponentlariga xizmat ko'rsatish ham ishlab chiqaruvchi, ham Ijrochi tomonidan amalga oshirilishi kerak.

Ijrochi hujjatlarni, yangilanishlarni, relizlarni mustaqil ravishda yuklab olish uchun dasturiy ta'minotni ishlab chiqaruvchi kompaniyaning axborot resurslari to'g'risidagi ma'lumotlarni taqdim etishi shart.

Ijrochi Dasturiy ta'minotning identifikatsiya ma'lumotlarini Buyurtmachining kabinetida, Ishlab chiqaruvchining veb-saytida bog'laydi.

Dasturiy ta'minotga xizmat ko'rsatish ishlari quyidagilarni o'z ichiga olishi kerak:

a) Sandbox tizimi dasturiy qismining uzluksiz ishlashini ta'minlash:

- Buyurtmachining apparat (server) resurslaridan foydalanishni optimallashtirish uchun Tizim parametrlarini sozlash;

- xavfsizlik siyosatini boshqarish uchun Tizim parametrlarini sozlash;

- yangilashlar amalga oshirilgandan keyin Tizimning normal rejimda ishlashini sinovdan o'tkazish.

b) Buyurtmachining mavjud boshqaruv va monitoring tizimlari bilan integratsiyalashuvi.

c) Tizimni masshtablash bo'yicha maslahatlar.

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

e) Tizim yangilangan taqdirda Tizimning 2 ta ma'muri bilan yo'riqnoma o'tkazish.

f) Tizim faoliyati bilan bog'liq yuzaga kelgan muammolarni hal etish, maslahatlar berish uchun "UMS" MChJ talabiga ko'ra mutaxassisni VPN orqali ulash.

g) Tizimning ishlash qobiliyatini tiklash:

- dasturiy vositalar ishdan chiqqandan keyin 2 ish kunidan kechikmay Tizimning ish qobiliyatini shtat rejimida tiklash;

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

- tiklash ishlarini amalga oshirish uchun Tizimni nosozlik vaqtida o'chirish imkoniyati (baypas

rejimi);

- dasturiy ta'minotdagi uzilishlar, quvvatning yo'qolishi va hokazolardan so'ng Tizim faolligining tiklanishi;

- zaxira nusxalardan ma'lumotlarni tiklash amallari.
- bajarilgan ishlar to'g'risida hisobotlar taqdim etish.

12. Apparat kompleksining texnik qo'llab-quvvatlanishiga qo'yiladigan talablar

12.1 Ijrochi yetkazib beriladigan apparat majmuasini shartnomaning butun amal qilish muddati davomida texnik qo'llab-quvvatlashni ta'minlashi shart.

12.2 Qo'llab-quvvatlash uskuna ishlab chiqaruvchisi yoki ishlab chiqaruvchining vakolatli xizmat ko'rsatuvchi hamkori tomonidan amalga oshirilishi lozim.

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

12.4. Qo'llab-quvvatlash quyidagilarga tatbiq etilishi lozim:

- apparat qismi (hardware);
 - o'rnatilgan dasturiy ta'minot (firmware, BIOS, kontrollerlar).
- 12.5. Qo'llab-quvvatlash quyidagi tartibda amalga oshirilishi lozim:

- 24x7x365 - muhim komponentlar uchun;
- 8x5 dan past bo'lmazligi kerak - muhim bo'lmaganlari uchun (Buyurtmachi bilan kelishilgan holda).

12.6 Hodisalarga javob berish 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 chetlab o'tish) vaqti:

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

12.8 Nosoz komponentlarni almashtirish texnik xizmat ko'rsatish doirasida, lekin 1 oydan ko'p bo'lmagan muddatda amalga oshirilishi lozim:

12.9 Barcha almashtiriladigan komponentlar quyidagi xususiyatlarga ega bo'lishi shart:

- original (OEM);
- yangi (tiklanmagan).

12.10 Ijrochiga TQga arizalarni ro'yxatga olishning yagona kanali taqdim etilishi lozim:

- Service Desk (portal);
- ishonch telefoni;
- e-mail

13. Ishlar, xizmatlar va ularni taqdim etish shartlariga qo'yiladigan boshqa talablar

13.1 Litsenziyalar/dasturiy ta'minot tomonlarning vakillari ishtirokida dasturiy ta'minotning jismoniy inventarizatsiyasi va ishlash qobiliyati o'tkazilgandan va tuzilgan shartnomaga muvofiq Qabul qilish-topshirish dalolatnomasi imzolangandan so'ng qabul qilingan hisoblanadi. Mazkur TTda va uning ilovalarida ko'rsatilmagan boshqa shartlar shartnomada ko'rsatiladi.

13.2 Xizmat ko'rsatishning majburiy sharti Buyurtmachining amaldagi ichki tartib-qoidalari, nazorat-o'tkazish rejimi, ichki nizomlar, yo'riqnomalar va talablarga rioya qilish bo'lib, ular haqida Buyurtmachi Ijrochiga xabar beradi. Buyurtmachi Ijrochiga dasturiy ta'minotga obunani faollashtirish bilan bog'liq bildirilgan muammolarni hal qilish uchun Ijrochi bilan bog'lanish huquqiga ega bo'lgan xodimlarning ro'yxati va aloqa ma'lumotlarini taqdim etadi.

13.3. Komplektlash talablari

Tizim joriy texnik topshiriq doirasida taklif etilayotgan yechimning to'liq ishlashi uchun to'liq komplektatsiyaga ega bo'lishi kerak. Dasturiy ta'minotning narxi to'liq komplektatsiyadan kelib chiqqan holda shakllantirilishi kerak.

13.4. Integratsiyaga talab

Integratsiya Buyurtmachi infratuzilmasining ishlash xususiyatlarini hisobga olishi kerak.

13.5. Yangilik haqida ma'lumot

Yetkazib beriladigan dasturiy ta'minot mahsulot va uning tarkibiy qismlari uchun zarur bo'lgan barcha litsenziyalar bilan eng so'nggi versiyada bo'lishi kerak.

13.6. Sug'urta

Talablar qo'yilmaydi.

13.7. Xizmat ko'rsatishda javobgarlikni taqsimlash matrisasi

Texnik xizmat ko'rsatish	Ijrochi	Buyurtmachi
Tizimning mavjudligi		
Muammoni aniqlash, uning ustuvorligini tasniflash va yechim uchun Huquq egasiga so'rov yuborish	A	R
Buyurtmachining DTni so'rov bo'yicha sozlash	A	R
Hisobot davri uchun muammolarni hal qilish statistikasini taqdim etish	R	A
Huquq egasi portalida barcha so'rovlarni ro'yxatdan o'tkazish	R	A
Dasturiy ta'minotni yangilash, tuzatish va sozlash		
Tartib-taomil usulini taqdim etish	R	A
O'rnatish vaqtini belgilash	A	R
APK, 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 (om angl. Responsible) – bevosita ijrochi;

A (om angl. Accountable) – ijrochining ishini boshqaradigan mas'ul shaxs;

C (om angl. Consulted) – maslahatchi (mutaxassis yoxud aniq qarorlar qabul qilingunga qadar mas'ul shaxs yordamga murojaat qiladigan soha bo'yicha ekspert);

I (om angl. Informed) – kuzatuvchi, xabardor qilinadigan shaxs (vazifa bajarilishining borishi (yoki natijalari) to'g'risida xabardor qilinishi lozim bo'lgan shaxs)

14. Qo'llaniladigan atamalar va qisqartmalar

№	Atama / Qisqartma	Rasshifrovka	Ta'rif
1	Sandbox	–	Nazorat qilinadigan virtual muhitda shubhali obyektlarni izolyatsiyalangan tahlil qilish tizimi
2	Zararli DT (ZDT)	–	Axborot tizimlariga zarar yetkazish uchun mo'ljallangan dasturiy ta'minot
3	Zero-day	–	Ilgari himoya vositalari ishlab chiqaruvchilariga ma'lum bo'lmagan zaiflik yoki zararli DT
4	IOC	Indicator of Compromise	Shikastlanish indikatori - zararli faoliyat mavjudligining texnik belgisi
5	APT	Advanced Persistent Threat	Infratuzilmada uzoq vaqt yashirin mavjudlik bilan maqsadli murakkab hujum
6	SIEM	Security Information and Event Management	Hodisalar va axborot xavfsizligini boshqarish tizimi
7	EDR	Endpoint Detection and Response	Yakuniy qurilmalarda hodisalarni aniqlash va ularga javob berish tizimi
8	XDR	Extended Detection and Response	Turli manbalardan olingan ma'lumotlarni birlashtiruvchi kengaytirilgan aniqlash va javob berish platformasi
9	NGFW	Next-Generation Firewall	DPI va ilova tahlili funksiyalariga ega yangi avlod tarmoqlararo ekrani
10	ICAP	Internet Content Adaptation Protocol	Trafikni tahlil qilish va o'zgartirish uchun integratsiya protokoli
11	API	Application Programming Interface	Tizimlar o'rtasidagi dasturiy o'zaro ta'sir interfeysi
12	VM	Virtual Machine	Izolyatsiyalangan tahlil uchun foydalaniladigan virtual mashina
13	Dinamik tahlil	–	Obyektning bajarilish jarayonidagi xatti-harakatlarini tahlil qilish
14	Statik tahlil	–	Faylni ishga tushirmasdan tahlil qilish
15	Hatti-harakat tahlili	–	Dastur harakatlarini tahlil qilish asosida tahdidlarni aniqlash usuli
16	PCAP	Packet Capture	Tarmoq trafiginini qamrab olish fayli
17	SLA	Service Level Agreement	Xizmatning qulaylik darajasi va sifati to'g'risidagi kelishuv
18	SOC	Security Operations Center	Axborot xavfsizligi hodisalarini kuzatish va ularga javob berish markazi
19	TI	Threat Intelligence	Kibertahdidlar va komprometatsiya indikatorlari haqidagi ma'lumotlar
20	On-premises	–	Buyurtmachining infratuzilmasida yechimni joylashtirish
21	Cloud Sandbox	–	Izolyatsiyalangan tahlil tizimini bulutli amalga oshirish

15. Ilovalar ro'yxati

1-ilova - Axborotlashtirish obyektining tavsifi.

2- ilova - Texnik muvofiqlik shakli.

TTni ishlab chiqdi:

AXvaRD Axborot xavfsizligi
bo'limi boshlig'i

AXvaRD direktori



R.A. Abdulvaat



B.A. Omatov

Axborotlashtirish obyektining tavsifi

“UMS” MChJ - 2014-yil 1-dekabrda boshlab O‘zbekiston Respublikasining butun hududida mobil aloqa xizmatlarini ko‘rsatuvchi telekommunikatsiya kompaniyasi.

“UMS” MChJ O‘zbekiston Respublikasi Vazirlar Mahkamasining 2014-yil 31-iyuldagi “Mobil aloqa xizmatlarini ko‘rsatish bo‘yicha “Universal Mobile Systems” qo‘shma korxonasini tashkil etish to‘g‘risida”gi 208-sonli qarori asosida tashkil etilgan bo‘lib, O‘zbekiston Respublikasining yetakchi mobil 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” MChJ ning ta‘sischisi hisoblanadi.

Kompaniyaning shtatdagi xodimlari soni 1800 kishi.

Sandbox’da axborot jamlanadigan serverlar va virtual mashinalarning umumiy soni: 200;

Sandbox bilan bog‘langan tarmoqning umumiy o‘tkazish qobiliyati: 10 Gbit/s;

Sandbox’da tahlil qilinadigan trafik yoki fayllarning taxminiy hajmi: kuniga 100 ta fayl;

Sandbox uchun ma’lumotlar manbalarining turlari: E-mail, WEB, Endpoints, fayllar.

Texnik muvofiqlik shakli

Talab raqami	Talab nomi/texnik tavsiflar
1	Yechim Sandbox sinfiga oid bo'lishi kerak.
2	Tizimni yoyish: On-Premise (dasturiy-apparat majmuasi)
3	APK tarkibidagi dasturiy ta'minot texnik yordamni o'z ichiga olgan holda, obuna shaklida 3 yil muddatga yetkazib berilishi kerak.
4	Yechim tahdidlarni tahlil qilishning quyidagi usullarini qo'llab-quvvatlaydi: <ul style="list-style-type: none"> • Real vaqt rejimida nolinchinchi kun fishing saytlarini, shu jumladan spam va zararli dasturlarni o'z ichiga olgan saytlarni 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.
5	<ul style="list-style-type: none"> • Fayl kengaytmalarining majburiy turlari: • Windows ijro 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, .xlsm, .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-fayllari: .asp, .hta, .htm, .html, .lnk, .js, .lnk, .url, WEblink. • Fayllarni siqing: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .udf, .upx, .xz, .z, .zip.
6	Emulyatsiya uchun quyidagi OT turlarini qo'llab-quvvatlash: <ul style="list-style-type: none"> • Windows (bir nechta versiya, jumladan, muhimlari); • Linux (Redhat, OEL, Ubuntu, CentOS); • 32/64-bit qo'llab-quvvatlash; • virtual obrazlarni moslashtirish imkoniyati.
7	Tizim quyidagilar bilan integratsiyani qo'llab-quvvatlashi kerak: <ul style="list-style-type: none"> • fayervollar (NGFW); • elektron pochta shlyuzi (Email Gateway); • Web Gateway; • antivirus (Endpoint Protection) • системой EDR / XDR tizimi • SIEM tizimi (kelgusida).
8	Ma'lumotlar almashinuvi quyidagilarni qo'llab-quvvatlashi kerak: <ul style="list-style-type: none"> • REST API; • STIX/ standarti; • Syslog.
9	Tizimni endpoint yechimlari (antivirus) bilan integratsiyalash <ul style="list-style-type: none"> • 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).

10	<p>Tizimning ish unumdorligi:</p> <ul style="list-style-type: none"> • Qurilmadagi lokal virtual mashinalar soni bo'yicha unumdorlik: 14 tadan kam emas. • Bulutda 80 tagacha virtual mashinaga kengaytirish imkoniyati; • Sandboxning 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 (dinamik tahlil) orqali obyektlarni tekshirish unumdorligi: soatiga kamida 500 ta fayl. • Pochtani himoyalash yechimi bilan integratsiya qilingandagi unumdorlik: soatiga 100 000 ta xat. • MTA Adapter orqali obyektlarni tekshirish unumdorligi: soatiga 25 000 ta xat; • Snifer rejimidagi unumdorlik: kamida 500 Mbit/s.
11	<p>Tizimni boshqarish va ma'murlashtirish</p> <ul style="list-style-type: none"> • Boshqaruvning WEB-interfeysi; • Rollarni ajratish (rollar modeli); • Administratorlar harakatlarini qayd etish jurnali; • AD/LDAP bilan integratsiya; • Tizim administratorlari uchun ikki faktorli autentifikatsiyani qo'llab-quvvatlash.
12	<p>Yechim quyidagi hisobotlarni taqdim etadi:</p> <ul style="list-style-type: none"> • xatti-harakatlar bo'yicha batafsil hisobot: <ul style="list-style-type: none"> – fayllardagi faollik, – reyestrda o'zgarishlar, – tarmoqqa ulanishlar, – jarayonlar, • kiberhujum bosqichlarining boshidan oxirigacha bo'lgan grafik tasvirini vizualizatsiya qilish, • komprometatsiya belgilarini (hash, IP, URL, domen) shakllantirish, • hisobotlarni PDF formatida eksport qilish.
13	<p>Tizimni litsenziyalash</p> <ul style="list-style-type: none"> • litsenziya quyidagilarni o'z ichiga olishi kerak: <ul style="list-style-type: none"> – tahlil qilinadigan obyektlar soni, – integratsiya qilinadigan qurilmalar soni, – signaturalar va dvijoklarni yangilash. • VM soni – kamida 4 dona (qo'shimcha litsenziyani faollashtirish orqali keyinchalik kengaytirish imkoniyati bilan). • Dasturiy ta'minotga obuna muddati – 3 yil. • Texnik qo'llab-quvvatlash muddati – kamida 3 yil.
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
15	Loyihaga o'rnatish ishlari kiritilgan.
16	Loyihaga loyihalash kiritilgan
17	Loyihaga Buyurtmachining 2 nafar mutaxassisini o'qitish kiritilgan.
18	Loyihaga MTBda DT/APKni sertifikatlash kiritilgan.
19	Interfeys tili - rus/ingliz
20	Ijrochida MAF mavjudligi