“TASDIQLAYMAN”

“Agrobank” ATB

Boshqaruv raisi o'rinbosari v.b.



F.B.Nasriyev

2026 yil “16” noyabr

TEXNIK TOPSHIRIQ
“BLACKBOX” (QORA QUTI) YONDASHUVI ASOSIDA RED TEAMING XIZMATINI KO‘RSATISH UCHUN

Toshkent 2026

Umumiy qoidalar

Mazkur texnik topshiriq Buyurtmachining axborot tizimlari, xodimlari va xavfsizlik jarayonlarining real ilg‘or maqsadli kiberhujumlarga bardoshliligini “Blackbox” yondashuvi asosida amaliy baholash uchun talablarni belgilaydi.

Hujjat “Blackbox” (Qora quti) yondashuvi asosida Red Teaming xizmatini ko‘rsatish reglamenti mazmuni, amaldagi milliy qonunchilik hamda tan olingan xalqaro kiberxavfsizlik metodologiyalaridan kelib chiqib tuzilgan.

Buyurtmachi	Texnik topshiriqni tasdiqlovchi tashkilot
Ijrochi	Belgilangan tartibda tanlangan va xizmat ko‘rsatish shartnomasi tuzilgan tashkilot
Xizmat turi	“Blackbox” yondashuvi asosida Red Teaming
Bajarish muddati	Shartnomada va ish rejasida belgilanadi
Ish natijasi	Ekspert hisoboti, texnik dalillar, tavsiyalar va yakuniy taqdimot

Atamalar va qisqartmalar

Atama	Mazmuni
APT	Advanced Persistent Threat - ilg‘or va davomli maqsadli kiberhujum.
Blackbox	Ijrochiga ichki arxitektura, IP-manzillar, hisob ma’lumotlari va himoya vositalari haqida dastlabki texnik ma’lumot berilmaydigan sinov yondashuvi.
C2	Command and Control - sinov doirasidagi boshqaruv va aloqa infratuzilmasi.
Flag	Sinovda erishilishi yoki erishish imkoniyati tasdiqlanishi kerak bo‘lgan maqsadli natija.
OSINT	Open-Source Intelligence - ochiq manbalardan razvedka ma’lumotlarini yig‘ish va tahlil qilish.
PoC	Proof of Concept – ish jarayonidagi holatlar uchun xavfsiz shaklda berilgan amaliy tasdiqlangan dalil (isbot).
RoE	Rules of Engagement - sinov ko‘lami, cheklovlari, amalga oshirish vaqti (davri) va aloqa tartibini belgilovchi o‘zaro ta’sir qoidalari.
SOC / Blue Team	Kiberhodisalarni aniqlash, tahlil qilish va ularga javob choralarini muvofiqlashtiruvchi himoya jamoasi.
White Team	Buyurtmachi tomonidan tuziladigan, sinov to‘g‘risida to‘liq xabardor bo‘lgan cheklangan ishonchli vakillar guruhi; ko‘lam, tasdiqlash darvozalari va favqulodda to‘xtatish bo‘yicha qaror qabul qiladi.
Deconfliction	Sinov faoliyatini real kiberhujumdan ajratish maqsadida Ijrochining harakatlari va indikatorlarini oldindan hamda real vaqtda qayd etib borish tartibi.
Freeze window	Muzlatilgan davr - bank operatsiyalarining kritik davri; ushbu davrda faol sinov o‘tkazilmaydi.
Approval gate	Tasdiqlash darvozasi - yuqori tavakkalli harakatni bajarishdan oldin White Team ning yozma tasdig‘ini olish tartibi.
MTTD / MTTC	Hujumni aniqlashgacha (Mean Time to Detect) va uni cheklashgacha (Mean Time to Contain) ketgan o‘rtacha vaqt ko‘rsatkichlari.
Kill switch	Ijrochining barcha faol vositalari va implantlarini bitta buyruq bilan to‘xtatish mexanizmi.

Xizmatning maqsadi va vazifalari

1. Maqsad

Buyurtmachining muhim axborot tizimlariga ruxsatsiz kirish, ma’lumotlarning sizib chiqishi, kritik tizimlar faoliyatiga ta’sir ko‘rsatish hamda himoya jarayonlarini chetlab o‘tish ehtimolini real hujumga yaqin, boshqariladigan va xavfsiz sharoitda aniqlash va baholash.

2. Asosiy vazifalar

- tashqi hujum xavfini ochiq manbalar asosida aniqlash va tahlil qilish;
- tashqi himoya perimetri, ijtimoiy muhandislik va boshqa kelishilgan shartli hujum vektorlar orqali dastlabki kirish imkoniyatini sinash;
- ichki tarmoqqa kirish tasdiqlanganda tizimdagi huquqlarni oshirish va maqsadli tizimlar tomon yashirin harakatlanish imkoniyatini tekshirish;
- kelishilgan flaglarga erishish yoki ularga erishish mumkinligini zarar yetkazmaydigan PoC (dalillar) bilan tasdiqlash;
- SOC / Blue Team vositalari va jarayonlarining aniqlash, tahlil qilish, eskalatsiya va cheklash samaradorligini baholash;
- aniqlangan texnik va tashkiliy bo‘shliqlar bo‘yicha ustuvor, amaliy va tekshiriladigan tavsiyalar ishlab chiqish;
- hujum yo‘li, vaqt xronologiyasi va dalillarni Buyurtmachi uchun qayta tekshirish mumkin bo‘lgan shaklda hujjatlashtirish.
- mobil bank ilovasi va uning backend API si xavfsizligini ishlab chiqarish muhitidagi (build) asosida baholash;
- filial tarmog‘idan markaziy infratuzilmaga o‘tish imkoniyatini va tarmoq segmentatsiyasi samaradorligini tekshirish;
- zaxira nusxa infratuzilmasiga yetib borish imkoniyatini baholash orqali tashkilotning shifrlovchi zararli dasturlarga bardoshliligini aniqlash;
- himoya vositalarining har bir hujum bosqichidagi real samaradorligini aniqlash qamrovi matritsasi ko‘rinishida hujjatlashtirish;
- aniqlanmagan texnikalar bo‘yicha SOC bilan birgalikda aniqlash qoidalarini ishlab chiqish va topshirish.

Sinov obyekti va ko‘lami (ro‘yxati)

Sinovning aniq doirasi RoE (sinov qoidalari) va rasmiy ruxsat hujjatida belgilanadi. Ushbu hujjatlarda qaysi axborot tizimlari, serverlar, saytlar, domenlar va tashkilotlar tekshirilishi, sinov qaysi hududda va qaysi vaqt oralig‘ida o‘tkazilishi, shuningdek sinovdan chiqarib tashlangan obyektlar va taqiqlangan harakatlar ko‘rsatiladi.

Blackbox sinovi shartlarini saqlash maqsadida Ijrochiga tizim haqida batafsil ichki ma’lumotlar berilmaydi. Unga faqat sinovni qonuniy ravishda o‘tkazish, ruxsat etilgan chegaralarni aniq bilish va ushbu chegaralardan chiqib ketmaslik uchun zarur bo‘lgan ma’lumotlar taqdim etiladi.

№	Yo‘nalish	Holati	Aniqlashtirish / chegaralar
1	Tashqi tarmoq perimetri	RoEda belgilanadi	Domenlar va tashkilotga tegishli tashqi aktivlarni aniqlash hamda sinash.
2	Veb-ilovalar va API	RoEda belgilanadi	Ishlab turgan muhitlar, test muhitlari va istisnolar alohida ko‘rsatiladi.
3	Elektron pochta va identifikatsiya	RoEda belgilanadi	Pochta himoyasi, hisob (akkaunt) yozuvlari va autentifikatsiya jarayonlari.
4	Ijtimoiy muhandislik	RoEda belgilanadi	Fishing ssenariysi, nishonga olinuvchi guruhlar, jo‘natish limiti va kuzatiladigan ko‘rsatkichlar.

5	Ichki tarmoq	Shartli	Keyingi harakatlar faqat oldindan kelishilgan sinov usuli orqali tizimga ruxsat etilgan dastlabki kirish qo‘lga kiritilgandan so‘ng va RoEda belgilangan chegaralar doirasida amalga oshiriladi.
6	Fizik xavfsizlik	Alohida kelishuv	Faqat maxsus ssenariy, manzil, vaqt va taqiqlangan zonalar yozma tasdiqlanganda.
7	Uchinchi tomon aktivlari	Ko‘lamdan tashqari	Uchinchi tomonning alohida yozma ruxsatisiz sinovdan o‘tkazilmaydi.
8	Mobil ilova va backend API	RoEda belgilanadi	iOS va Android ilovalari OWASP MASVS/MASTG bo‘yicha, backend API OWASP API Security Top 10 bo‘yicha. Faqat sintetik test hisoblari bilan.
9	Masofaviy bank xizmatlari	RoEda belgilanadi	Internet-banking kabinetlari, autentifikatsiya va OTP mexanizmlari, to‘lov jarayonining biznes-mantiqi. Real tranzaksiya yakunlanmaydi.
10	Filial tarmog‘i	Shartli	Namuna sifatida tanlangan 3-5 ta filial: nazoratsiz ulanish nuqtalari, VLAN segmentatsiyasi, tarmoqqa kirish nazoratini chetlab o‘tish. Filialning real ish jarayoniga ta’sir taqiqlanadi.
11	Simsiz tarmoqlar	RoEda belgilanadi	Korporativ Wi-Fi autentifikatsiyasining chidamliligi, mehmon segmentining izolyatsiyasi, ruxsatsiz o‘rnatilgan kirish nuqtalari.
12	Bankomat va o‘z-o‘ziga xizmat qurilmalari segmenti	Alohida kelishuv	Faqat tarmoq darajasida. Naqd pul chiqarish, qurilma korpusini ochish va dasturiy ta’minotni o‘zgartirish taqiqlanadi.
13	Zaxira nusxa infratuzilmasi	Shartli	Yetib borish imkoniyati faqat imkoniyat darajasida tasdiqlanadi. Zaxiralarni o‘chirish, shifrlash va replikatsiyani buzish taqiqlanadi.
14	Ta’minot zanjiri va uchinchi tomon kirish kanallari	Alohida kelishuv	Pudratchilar uchun ochilgan VPN va masofadan boshqarish kanallari orqali bank tarmog‘iga kirish imkoniyati. Uchinchi tomon tizimlariga hujum qilinmaydi.

Agar sinov davomida aniqlangan, ammo oldindan tasdiqlangan ro‘yxat (ko‘lamga) kirmaydigan tizim, server, domen yoki boshqa aktivga nisbatan hech qanday faol harakat amalga oshirilmaydi. Bunday aktiv haqidagi ma’lumot dalil sifatida qayd etiladi va aloqa tartibida belgilangan vakolatli shaxsga xabar beriladi.

Buyurtmachi Blackbox shartini buzmagan holda, faqat identifikatorlar ro‘yxati ko‘rinishida beqaror, eskirgan yoki ishlab chiqaruvchi tomonidan qo‘llab-quvvatlanmaydigan tizimlarni «faqat passiv» belgisi bilan RoEga kiritadi. Bunday tizimlarga nisbatan faqat passiv aniqlash va banner tahlili ruxsat etiladi; ekspluatatsiya, lug‘atli hujum va yuklama beruvchi tekshiruvlar taqiqlanadi.

Ushbu ro‘yxat hujum vektori, arxitektura yoki himoya vositalari to‘g‘risida ma’lumot bermaydi va Blackbox yondashuvini buzmaydi; u faqat operatsion zararning oldini olish maqsadida taqdim etiladi.

Blackbox sharti va boshlang‘ich ma’lumotlar

Ijrochiga berilmaydigan ma’lumotlar

- ichki tarmoq topologiyasi va axborot tizimlari arxitekturasi;
- aktivlar va IP-manzillarning to‘liq ro‘yxati;

- foydalanuvchi hisoblari, parollar, kalitlar yoki sinov uchun tayyorlangan kirish huquqlari;
- joriy himoya vositalari, aniqlash qoidalari va SOC ishlash tartibi;
- xodimlar haqida ochiq manbalarda mavjud bo‘lmagan ma’lumotlar.

Sinov boshlanishidan oldin rasmiylashtiriladigan ma’lumotlar

- Buyurtmachining xizmatga buyurtma berish va sinovga ruxsat berish vakolatini tasdiqlovchi hujjat;
- RoE, shu jumladan ko‘lam, flag‘lar, taqiqlangan harakatlar, vaqt oynasi va emergency stop tartibi;
- maxfiylik va ma’lumotlarni oshkor qilmaslik kelishuvi (NDA);
- vakolatli kontaktlar hamda favqulodda aloqa kanallari;
- sinov dalillarini saqlash, uzatish va yakunda yo‘q qilish tartibi.
- muhim axborot infratuzilmasi subyekti sifatida vakolatli organni xabardor qilish to‘g‘risidagi hujjat nusxasi (qonunchilikda nazarda tutilgan hollarda);
- White Team tarkibini tasdiqlovchi bank buyrug‘i va 24/7 navbatchilik jadvali;
- muzlatilgan (taqiqlangan) davrlar kalendari;
- «faqat passiv» rejimidagi nozik tizimlar ro‘yxati;
- xavfsizlik parametrlari: hisobning bloklanish chegarasi va bloklanish oynasi qiymatlari;
- Ijrochi tomonidan taqdim etiladigan indikatorlar ro‘yxati: manba IP-manzillari, C2 va fishing domenlari, jo‘natuvchi manzillar, artefaktlarning xesh qiymatlari va unikal marker;
- fizik yoki joyida bajariladigan ishlar uchun har bir jamoa a’zosiga beriladigan avtorizatsiya xatining jismoniy nusxasi;
- ko‘lamdagi kritik tizimlar bo‘yicha zaxira nusxalarning mavjudligi va tiklanishi tekshirilganligi to‘g‘risidagi tasdiq;
- kasbiy javobgarlik sug‘urtasi polisi yoki shartnomada belgilangan javobgarlik limiti to‘g‘risidagi hujjat.

Yuqorida keltirilgan xavfsizlik parametrlari Ijrochiga tizim arxitekturasi yoki himoya vositalari haqida ma’lumot bermaydi va Blackbox shartini buzmaydi.

Blackbox va maqsadli xavfsizlik sinovlarini amalga oshirish

Red Teaming doirasidagi xavfsizlik sinovlari **ikki bosqichda** amalga oshirilishi kerak. Har bir bosqichning maqsadi, boshlang‘ich ma’lumotlari, bajariladigan ishlar va yakuniy natijalari alohida belgilanadi.

To‘liq Blackbox xavfsizlik sinovi

Birinchi bosqich **to‘liq Blackbox (Qora quti)** yondashuvi asosida amalga oshirilishi kerak.
Ushbu bosqich boshlanishidan oldin Ijrochiga Buyurtmachining ichki axborot tizimlari va infratuzilmasi to‘g‘risida batafsil texnik ma’lumotlar berilmasligi kerak. Xususan, imkon qadar quyidagi ma’lumotlar oldindan taqdim etilmasligi kerak:

- ichki tarmoq topologiyasi;
- ichki IP-manzillar va tarmoq diapazonlari;
- serverlar va ishchi stansiyalar ro‘yxati;
- ichki DNS yozuvlari;
- ichki domenlar va servislar;
- foydalanilayotgan operatsion tizimlar va ularning versiyalari;
- xavfsizlik vositalari va ularning konfiguratsiyasi;
- firewall, WAF, EDR, SIEM va boshqa himoya vositalari konfiguratsiyasi;

- foydalanuvchi hisoblari, login/parollar va autentifikatsiya ma’lumotlari;
- administrator hisoblari;
- API kalitlari, tokenlar va boshqa maxfiy ma’lumotlar;
- ichki xodimlar to‘g‘risidagi ommaviy bo‘lmagan ma’lumotlar.

Blackbox bosqichida Ijrochi Buyurtmachining **Internet tarmog‘idan tashqi tomondan ko‘rinadigan hujum yuzasini mustaqil ravishda aniqlashi** kerak.
Buning uchun quyidagi faoliyatlar amalga oshirilishi mumkin:

- Ochiq manbalardan ma’lumot yig‘ish va tahlil qilish (OSINT);
- Buyurtmachiga tegishli domenlar va subdomenlarni aniqlash;
- Internet tarmog‘ida ochiq bo‘lgan IP-manzillarni aniqlash;
- Ochiq tarmoq servislarini aniqlash;
- Internetga chiqarilgan web-ilovalar va APIlarni aniqlash;
- Elektron pochta infratuzilmasini tekshirish;
- Ochiq autentifikatsiya interfeyslarini aniqlash;
- Internetga chiqarilgan masofaviy kirish servislarini aniqlash;
- Tashkilot xodimlari va texnik infratuzilma to‘g‘risida OSINT orqali mavjud ma’lumotlarni tahlil qilish;
- Aniqlangan tashqi aktivlarda xavfsizlik zaifliklarini tekshirish;
- Aniqlangan zaifliklardan foydalanish imkoniyatini xavfsiz PoC orqali baholash;
- Tashqi hujumchi nuqtayi nazaridan ehtimoliy hujum yo‘llarini shakllantirish.

Birinchi bosqichning asosiy maqsadi — Buyurtmachining **tashqi hujum yuzasini va Internet orqali boshlanishi mumkin bo‘lgan real hujum ssenariylarini** aniqlashdan iborat.
Birinchi bosqichda Ijrochi tomonidan aniqlangan barcha aktivlar dastlabki aktivlar ro‘yxati sifatida qayd etilishi kerak. Har bir aniqlangan aktiv bo‘yicha kamida quyidagi ma’lumotlar qayd etiladi:

- aktiv nomi;
- domen yoki IP-manzil;
- aniqlangan servis;
- aniqlangan texnologiya;
- mavjud ochiq portlar;
- aniqlangan zaifliklar;
- zaiflikning xavf darajasi;
- foydalanish mumkin bo‘lgan hujum vektori;
- xavfsiz PoC/evidence;
- hujumning keyingi bosqichga olib kelishi mumkin bo‘lgan ta’siri.

Ushbu bosqichda Ijrochi **Buyurtmachining ichki infratuzilmasi to‘g‘risidagi oldindan berilmagan ma’lumotlardan foydalanmasdan**, tashqi hujumchi ega bo‘lishi mumkin bo‘lgan imkoniyatlar asosida test o‘tkazishi kerak.

1-bosqich yakunlari

Birinchi bosqich yakunida Ijrochi Buyurtmachiga kamida quyidagilarni taqdim etishi kerak:

- Internet orqali aniqlangan tashqi aktivlar ro‘yxati;
- aniqlangan domen va subdomenlar;
- aniqlangan IP-manzillar va servislar;

- web-ilovalar va APIlar ro‘yxati;
- aniqlangan zaifliklar;
- zaifliklarning xavf darajasi;
- tasdiqlangan hujum yo‘llari;
- PoC va texnik dalillar;
- tashqi hujum yuzasining umumiy bahosi;
- keyingi bosqichda maqsadli tekshirish uchun tavsiya etiladigan aktivlar ro‘yxati.

2-bosqich — Buyurtmachi taqdim etgan resurslar bo‘yicha maqsadli Penetration Testing

Birinchi bosqich yakunlanganidan va uning natijalari qayd etilganidan so‘ng, Buyurtmachi Ijrochiga **Penetration Testing uchun mo‘ljallangan o‘z axborot resurslarining to‘liq va kelishilgan ro‘yxatini** taqdim etishi kerak.

Ikkinchi bosqichni amalga oshirish uchun Buyurtmachi Ijrochiga Penetration Testing doirasida tekshirilishi lozim bo‘lgan o‘zining ichki va tashqi axborot resurslari, texnik infratuzilma obyektlari, IP-manzillari, domenlari, web-ilovalari, APIlari, serverlari, tarmoq segmentlari va boshqa tegishli resurslarning to‘liq va kelishilgan ro‘yxatini taqdim etadi.

Ijrochi Buyurtmachi tomonidan taqdim etilgan mazkur ichki va tashqi resurslarning barchasi bo‘yicha tasdiqlangan RoE doirasida maqsadli Penetration Testing o‘tkazishi, aniqlangan zaifliklarni baholashi, ekspluatatsiya qilish imkoniyatlarini xavfsiz PoC orqali tekshirishi hamda har bir resurs bo‘yicha test natijalarini yakuniy hisobotda aks ettirishi kerak.

Ro‘yxatga, zaruratga qarab, quyidagilar kiritilishi mumkin:

- tashqi IP-manzillar;
- ichki IP-manzillar;
- serverlar;
- web-ilovalar;
- APIlar;
- mobil ilovalar;
- mobil ilovalarning backend servislar;
- ma’lumotlar bazalari;
- autentifikatsiya servislar;
- Active Directory/domen infratuzilmasi;
- elektron pochta tizimlari;
- masofaviy kirish servislar;
- internet-banking servislar;
- muhim bank tizimlari;
- tarmoq segmentlari;
- xavfsizlik boshqaruv konsollari;
- boshqa Buyurtmachi tomonidan testga kiritilgan axborot resurslari.

Ikkinchi bosqichda Ijrochi Buyurtmachi tomonidan taqdim etilgan ro‘yxat asosida **maqsadli va chuqurlashtirilgan Penetration Testing** o‘tkazishi kerak.

Ikki bosqich o‘rtasidagi bog‘liqlik

Birinchi bosqichda aniqlangan tashqi aktivlar va hujum vektorlari ikkinchi bosqichda taqdim etilgan aktivlar ro‘yxati bilan solishtirilishi kerak.

Hisobotda kamida quyidagi holatlar ko‘rsatilishi kerak:

№	Tekshiruv	Natija
1	Blackbox orqali aniqlangan aktiv	Aniqlangan / aniqlanmagan
2	Buyurtmachi tomonidan taqdim etilgan aktiv	Ro‘yxatda mavjud / mavjud emas
3	Tashqi tomondan aniqlangan zaiflik	Ha / yo‘q
4	Maqsadli testda tasdiqlangan zaiflik	Ha / yo‘q
5	Hujum yo‘li shakllantirildi	Ha / yo‘q
6	PoC mavjud	Ha / yo‘q
7	Yakuniy xavf darajasi	Critical / High / Medium / Low

Metodologik asos

Sinov rejalashtirish, bajarish va hisobot tayyorlashda quyidagi metodologik manbalardan vazifaga mos qismlarda foydalaniladi:

- MITRE ATT&CK - tahdid taktikalari, texnikalari va protseduralarini rejalashtirish hamda natijalarni xaritalash uchun;
- TIBER-EU - moliya sektori va muhim funksiyalar uchun tahdid razvedkasiga asoslangan Red Team yondashuvini qo‘llash uchun;
- PTES - tayyorgarlik, razvedka, tahdidlarni modellashtirish, ekspluatatsiya, post-ekspluatatsiya va hisobot bosqichlarini izchil tashkil etish uchun;
- O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi va “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonunlari hamda muhim axborot infratuzilmasini himoya qilishga oid talablar.
- O‘zbekiston Respublikasi Markaziy bankining bank tizimida axborot xavfsizligini ta’minlash bo‘yicha normativ hujjatlari, shu jumladan masofaviy bank xizmatlari xavfsizligiga oid talablar;
- OWASP MASVS va MASTG - mobil ilovalar xavfsizligini baholash uchun;
- OWASP API Security Top 10 va OWASP ASVS - API va veb-ilovalarni baholash uchun;
- PCI DSS amaldagi versiyasining penetratsion sinov va segmentatsiyani tekshirishga oid talablari - karta ma’lumotlari muhiti ko‘lamga kiritilgan taqdirda.

Metodologiya Buyurtmachining tarmoq barqarorligi, ma’lumotlar toifasi va biznes jarayonlari xususiyatiga moslashtiriladi. Har bir faol texnika RoE doirasida, minimal ta’sir tamoyili asosida qo‘llaniladi.

Har bir topilma yakuniy hisobotda tegishli normativ hujjat bandi bilan bog‘lab ko‘rsatiladi. Bu esa hisobotdan muvofiqlikni tasdiqlovchi dalil sifatida foydalanish imkonini beradi.

Ishlarni bajarish bosqichlari

№	Bosqich	Asosiy ishlar	Natija
1	Tayyorgarlik va avtorizatsiya	Texnik topshiriq, RoE, NDA, kontaktlar, flag‘lar, vaqt oynasi va emergency stop mezonlarini kelishish.	Tasdiqlangan ish reja va RoE
2	Tahdid razvedkasi va OSINT	Ochiq manbalardan tashqi hujum yuzasi, xodimlar, texnologiyalar, domenlar va ehtimoliy vektorlarni aniqlash.	Razvedka xulosasi va hujum gipotezalari
3	Hujum infratuzilmasini tayyorlash	Ajratilgan C2, domenlar, sertifikatlar, kuzatuv va dalillarni xavfsiz qayd etish mexanizmlarini sozlash.	Sinovga tayyor infratuzilma
4	Tashqi razvedka va dastlabki kirish	Tashqi perimetr, ochiq xizmatlar, veb-resurslar va kelishilgan ijtimoiy muhandislik ssenariylarini sinash.	Dastlabki kirish holati va PoC

5	Ichki harakatlanish	Foothold olinganda huquqlarni oshirish, hisoblar va ishonch munosabatlarini tahlil qilish, maqsadli tizimlar tomon yashirin harakatlanish.	Hujum yo‘li va erishilgan imkoniyatlar
6	Maqsadli flaglarni tekshirish	Biznes-kritik tizimlarga ta’sir ko‘rsatish imkoniyatini xavfsiz PoC bilan tasdiqlash; real operatsiyalarni o‘zgartirmaslik.	Flag holati va dalillar
7	Aniqlash va javob jarayonini baholash	SOC / Blue Team telemetriyasi mavjud bo‘lganda ogohlantirish, triage, eskalatsiya va cheklash vaqtlarini Timeline bilan solishtirish.	Aniqlash qamrovi va vaqt ko‘rsatkichlari
8	Tozalash va yakunlash	Yaratilgan hisoblar, fayllar, implantlar va boshqa artefaktlarni kelishilgan tartibda olib tashlash.	Tozalash ro‘yxati
9	Hisobot va taqdimot	Rahbariyat va texnik jamoa uchun natijalar, dalillar, hujum yo‘llari va tavsiyalarni taqdim etish.	Yakuniy hujjatlar to‘plami
10	Qayta tekshirish (retest)	Kritik va yuqori darajadagi topilmalarning bartaraf etilganligini tekshirish.	Qayta tekshirish hisoboti

Maqsadli ssenariylar (flag‘lar)

Quyidagi ssenariylar Buyurtmachida tegishli tizim mavjud bo‘lganda va RoEda alohida tasdiqlanganda qo‘llanadi. Yakuniy flag‘lar biznesning kritik funksiyalari va tahdid modelidan kelib chiqib aniqlanadi.

ID	Ssenariy	Muvaffaqiyat mezoni	Amaliy cheklov
F-01	SWIFT yoki muhim to‘lov shlyuziga ruxsatsiz ulanish imkoniyati	Kirish darajasi va ehtimoliy operatsiyani PoC bilan tasdiqlash.	Real tranzaksiya yaratilmaydi, o‘zgartirilmaydi va yuborilmaydi.
F-02	Avtomatlashtirilgan bank tizimi (ABT / CBS) va ma’lumotlar bazasiga kirish	Ruxsat darajasi, ko‘rinadigan obyektlar va hujum yo‘li dalillar bilan qayd etiladi.	Yozuvlar o‘zgartirilmaydi yoki o‘chirilmaydi.
F-03	Shaxsiy yoki moliyaviy ma’lumotlarni tashqi tarmoqqa olib chiqish imkoniyati	Nazorat qilinadigan sintetik fayl yoki xesh/metadata orqali kanal tasdiqlanadi.	Real mijoz ma’lumotlari tashqariga olib chiqilmaydi.
F-04	Yuqori imtiyozli huquqlarni olish	Kelishilgan muhitda Domain Admin yoki unga teng huquqqa erishish yo‘li tasdiqlanadi.	Imtiyoz faqat dalil olish va xavfsiz tekshiruv uchun qo‘llanadi.
F-05	Buyurtmachiga xos flag		
F-06	Internet-banking va masofaviy bank xizmatlarining ma’muriy paneliga kirish	Ma’muriy interfeysga kirish darajasi va ko‘rinadigan funksiyalar dalil bilan qayd etiladi.	Hech qanday mijoz operatsiyasi bajarilmaydi va sozlama o‘zgartirilmaydi.
F-07	Mobil ilova backend API si orqali boshqa foydalanuvchi ma’lumotlariga kirish	Sintetik test hisobi orqali boshqa hisob obyektiga murojaat qilish imkoniyati tasdiqlanadi.	Faqat sintetik hisoblar; real mijoz ma’lumotiga murojaat taqiqlanadi.

F-08	Karta protsessing shlyuzi segmentiga tarmoq darajasida yetib borish	Segmentga ulanish va xizmatlarni aniqlash imkoniyati qayd etiladi.	Protsessing tizimiga faol ta’sir va tranzaksiya shakllantirish taqiqlanadi.
F-09	Bankomat tarmoq segmentiga kirish	Segmentga kirish va boshqaruv kanalining himoyalanganligi baholanadi.	Naqd pul chiqarish va qurilma dasturiy ta’minotini o‘zgartirish taqiqlanadi.
F-10	Zaxira nusxa infratuzilmasini boshqarish konsoliga kirish	Zaxiralarni o‘chirish yoki o‘zgartirish imkoniyati mavjudligi tasdiqlanadi.	Real o‘chirish, shifrlash va replikatsiyani buzish qat’iyan taqiqlanadi.
F-11	Imtiyozli kirishni boshqarish tizimi va parol seyfiga kirish	Seyfdagi hisob ma’lumotlariga kirish imkoniyati darajasi qayd etiladi.	Hisob ma’lumotlari nusxalanmaydi va Ijrochi tizimlariga ko‘chirilmaydi.
F-12	Xavfsizlik boshqaruv konsollariga kirish (SIEM, xavfsizlik devori, EDR)	Konsolga kirish va qoidalarni ko‘rish imkoniyati tasdiqlanadi.	Qoidalarni o‘zgartirish va jurnallarni tozalash taqiqlanadi.
F-13	Manba kodi repozitoriysi va CI/CD quvuriga kirish	Kodga va yig‘ish jarayoniga o‘zgartirish kiritish imkoniyati tasdiqlanadi.	Kodga real o‘zgartirish kiritilmaydi va reliz jarayoniga aralashilmaydi.
F-14	Kadrlar va ish haqi tizimi hamda rahbariyat pochtasiga kirish	Kirish darajasi va ko‘rinadigan ma’lumot toifasi qayd etiladi.	Xatlar o‘qilmaydi, yuborilmaydi va o‘chirilmaydi; faqat kirish fakti tasdiqlanadi.
F-15	Videokuzatuv va kirish nazorati tizimiga kirish	Tizimga kirish va boshqaruv imkoniyati darajasi qayd etiladi.	Eshiklarni ochish, yozuvlarni o‘chirish va kameralarni o‘chirish taqiqlanadi.
F-16	Filial tarmog‘idan markaziy ma’lumotlar markaziga yetib borish	Segmentatsiya nazoratini chetlab o‘tish va markaziy resursga ulanish tasdiqlanadi.	Filialning real ish jarayoniga ta’sir qiluvchi harakatlar taqiqlanadi.
F-17	Tier-0 aktivlarini (domen kontrolleri, sertifikat xizmati) nazorat qilish	Domen ma’muri yoki unga teng huquqqa erishish yo‘li tasdiqlanadi.	Katalog bazasi ko‘chirilmaydi, doimiy persistensiya qoldirilmaydi.

RoE va xavfsiz bajarish talablari

Taqiqlangan harakatlar

- DDoS / DoS yoki xizmatlarning mavjudligiga qasddan salbiy ta’sir ko‘rsatadigan boshqa yuklama hujumlari;
- real tranzaksiyalar, moliyaviy oqimlar, balanslar yoki to‘lov topshiriqlarini yaratish, o‘zgartirish yoki ko‘chirish;
- mijozlar va boshqa real subyektlarga tegishli ma’lumotlarni o‘zgartirish, o‘chirish yoki nazorat qilinmaydigan kanal orqali ko‘chirish;
- RoEga kirmaydigan aktivlarga faol ta’sir ko‘rsatish;
- uchinchi tomon infratuzilmasini alohida yozma ruxsatsiz sinash;

- Buyurtmachi tomonidan taqiqlangan eksploit, zararli kod, fizik kirish usuli yoki ijtimoiy muhandislik ssenariysidan foydalanish.
- hodisa jurnallarini o‘chirish, tozalash, o‘zgartirish yoki jurnalga yozish va audit sozlamalarini o‘chirish;
- antivirus, EDR va boshqa himoya agentlarini o‘chirish, olib tashlash yoki konfiguratsiyasini o‘zgartirish;
- xavfsizlik vositalari qoidalariga istisno qo‘shish yoki mavjud qoidalarni o‘zgartirish;
- tizim vaqtini yoki vaqt manbasini o‘zgartirish;
- barqarorligi tasdiqlanmagan, xotira buzilishiga asoslangan yoki xizmatning ishdan chiqishiga olib kelishi ma’lum bo‘lgan eksploitlardan tasdiqsiz foydalanish;
- o‘z-o‘zidan tarqaluvchi kod, chuvalchang xususiyatiga ega payload yoki real shifrlovchi zararli dasturdan foydalanish;
- zaxira nusxalarni o‘chirish, shifrlash, replikatsiyani buzish yoki yo‘q qilish;
- domen ma’muri yoki unga teng huquqni loyiha yakunidan keyin ham saqlab qoluvchi persistensiya o‘rnatish;
- real mijoz hisoblariga nisbatan autentifikatsiya, parolni tiklash yoki bir martalik parol so‘rash urinishlari;
- mijozlarga nisbatan har qanday ijtimoiy muhandislik harakati;
- davlat organlari, huquqni muhofaza qiluvchi organlar yoki regulyator nomidan ish yuritish;
- psixologik travma keltiruvchi bahonalardan (o‘lim, kasallik, ishdan bo‘shatish, oilaviy favqulodda holat) foydalanish;
- xodimlarning shaxsiy qurilmalari, shaxsiy pochtasi, shaxsiy moliyaviy ma’lumotlari va oila a’zolarini nishonga olish;
- haqiqiy parollarni ochiq matnda yig‘ish va saqlash; faqat hisob ma’lumoti kiritilgani fakti, vaqt tamg‘asi va parol uzunligi qayd etiladi;
- yong‘in signalizatsiyasi, videokuzatuv, kirish nazorati, elektr ta’minoti va muhandislik tizimlariga ta’sir ko‘rsatish;
- bankomat va o‘z-o‘ziga xizmat ko‘rsatish qurilmalarida naqd pul chiqarish yoki qurilma korpusini ochish;
- litsenziyasiz, noma’lum manbadan olingan yoki uchinchi tomonga telemetriya uzatuvchi vositalardan foydalanish;
- aniqlangan zaiflik yoki dalilni Buyurtmachining yozma roziligisiz uchinchi tomonga, jumladan mahsulot ishlab chiqaruvchisiga yoki jamoatchilikka oshkor qilish.

Yuklama, intensivlik va bosqichma-bosqich kengaytirish cheklovlari

- RoEda quyidagi limitlar raqamlar bilan belgilanadi: bitta nishon xostga so‘rovlar soni (sekundiga), bir vaqtda ochiladigan ulanishlar soni va bir vaqtda skanerlanadigan xostlar soni. Tavsiya etiladigan boshlang‘ich qiymatlar: bitta xostga 10 so‘rov/sekunddan ko‘p emas, 5 tadan ko‘p bo‘lmagan parallel ulanish, bir vaqtda 25 tadan ko‘p bo‘lmagan xost;
- skanerlash past intensivlikdan bosqichma-bosqich oshirish tamoyili bo‘yicha bajariladi; har bir oshirishdan keyin kamida 30 daqiqa davomida nishon tizimlarning holati kuzatiladi;
- skanerlash vositalari «xavfsiz tekshiruvlar» rejimida ishlaydi; xizmatni ishdan chiqarishi mumkin bo‘lgan tekshiruv modullari o‘chiriladi;
- sinov «avval past tavakkalli, keyin yuqori tavakkalli» tamoyili bo‘yicha bajariladi: passiv razvedka, cheklangan faol skanerlash, nazorat ostidagi ekspluatatsiya, ichki harakatlanish va kritik segmentlarga yaqinlashish. Har bir keyingi bosqichga o‘tish White Team ogohlantiriladi.

Hisoblarning ommaviy bloklanishining oldini olish

- parolni tanlash faqat quyidagi rejimda ruxsat etiladi: bitta hisob uchun bloklanish oynasi ichida ko‘pi bilan bitta urinish; urinishlar to‘lqinlari orasida kamida 60 daqiqa tanaffus;

xizmat, imtiyozli va ma’muriy hisoblar butunlay chiqarib tashlanadi; bir to‘lqinda nishonga olinadigan hisoblar soni RoEda belgilanadi;
- kirish urinishlari natijasida biror hisobning bloklanganligi aniqlansa, tegishli faoliyat darhol to‘xtatiladi va White Team xabardor qilinadi.

Yuqori tavakkalli harakatlarni tasdiqlash tartibi (approval gate)

Quyidagi harakatlar faqat White Team ning real vaqtdagi tasdig‘i bilan bajariladi:
- ishlab chiqarish muhitida barqarorligi tasdiqlanmagan yoki xotira buzilishiga asoslangan eksploitdan foydalanish;
- domen kontrolleri, imtiyozli kirishni boshqarish tizimi, SIEM, zaxira nusxa infratuzilmasi, kriptografik modul va to‘lov segmentiga har qanday faol ta’sir;
- persistensiya mexanizmini o‘rnatish;
- ma’lumot chiqarish (exfiltration) sinovini o‘tkazish;
- fizik kirish urinishi;
- ijtimoiy muhandislikning har bir yangi to‘lqinini boshlash;
- sinov davomida yangi aniqlangan aktivni ko‘lamga kiritish.

White listga kiritish taqiqi va himoya vositalarining daxlsizligi
- Ijrochining IP-manzillari, domenlari va artefaktlari xavfsizlik devori, veb-proksi, pochta himoyasi, EDR yoki boshqa nazorat vositalarida oq ro‘yxatga kiritilmaydi. Istisno faqat White Teamning roziligi asosida boshlang‘ich sinovlariga nisbatan, yozma tasdiq bilan va vaqt bilan chegaralangan holda qo‘llaniladi;
- himoya vositalarini chetlab o‘tish faqat ularni o‘chirmasdan, texnik usullar bilan bajariladi; har bir bunday holat yakuniy hisobotda alohida qayd etiladi.

Faol ish vaqti

Sinov boshlanishi	____ / ____ / 20____, soat ____:____
Sinov yakuni	____ / ____ / 20____, soat ____:____
Ruxsat etilgan kunlar	
Ruxsat etilgan soatlar	_____
Alohida cheklangan davrlar	
Vaqt zonasi	

Muzlatilgan (taqiqlangan) davrlar

Faol sinov quyidagi davrlarda o‘tkazilmaydi. Aniq sanalar Buyurtmachi tomonidan to‘ldiriladi va RoEga ilova qilinadi.

№	Davr yoki jarayon	Cheklov turi	Aniq sanalar / soatlar
1	Oylik hisobotni yopish va regulyatorga hisobot topshirish kunlari	To‘liq taqiq	
2	Choraklik va yillik hisobotni yopish davri	To‘liq taqiq	
3	Ish haqi, pensiya va nafaqalarni ommaviy to‘lash kunlari	To‘liq taqiq	
4	Soliq va majburiy to‘lovlarning oxirgi muddatlari	To‘liq taqiq	
5	Operatsion kunni yopish va tungi paketli qayta ishlash	Har kuni: __:__ - __:__	
6	Bayram kunlari va ulardan oldingi 2 ish kuni	To‘liq taqiq	
7	Rejalashtirilgan yirik o‘zgarishlar (yangilanish, migratsiya, reliz)	Kalendar bo‘yicha	
8	Regulyator yoki tashqi audit tekshiruvi davri	To‘liq taqiq	
9	Kassa operatsiyalarining cho‘qqi soatlari (fizik sinov uchun)	__:__ - __:__	
10	Inkassatsiya jarayoni (fizik sinov uchun)	To‘liq taqiq	

Yuqori tavakkalli harakatlar past yuklama davrida bajariladi. Shu bilan birga, aniqlash imkoniyatini real baholash uchun harakatlarning kamida 50 foizi ish vaqtida, real trafik fonida bajarilishi shart; taqsimot RoEda belgilanadi.

Faol sinov davri Buyurtmachining o‘zgarishlarni boshqarish jadvali bilan solishtiriladi va yirik o‘zgarishlar bilan bir vaqtga to‘g‘ri kelmasligi ta’minlanadi. Kelishilgan kalendar White Team tomonidan yuritiladi va yangilanadi.

Favqulodda to‘xtatish (emergency stop) tartibi

Quyidagi holatlardan biri kuzatilganda tegishli faoliyat vaqtincha to‘xtatiladi, dalillar xavfsiz holatda saqlanadi va vakolatli aloqa shaxsiga zudlik bilan xabar beriladi:

- mablag‘ yoki muhim ma’lumotlarni darhol egallash imkonini beruvchi kritik zaiflik aniqlanishi;
- xizmatning sekinlashishi, uzilishi yoki boshqa kutilmagan operatsion ta’sir alomatlari;
- real maxfiy ma’lumotlarning nazorat qilinmagan tarzda ochilishi;
- ko‘lamdan tashqari aktivga yoki uchinchi tomon tizimiga kirib qolish;
- Buyurtmachining vakolatli shaxsi tomonidan sinovni to‘xtatish ko‘rsatmasi berilishi.

Avtomatik to‘xtatish mezonlari

Faol sinov davrida Buyurtmachi ko‘lamdagi xizmatlar bo‘yicha kuchaytirilgan monitoringni yoqadi. Quyidagi chegaralardan biri oshib ketganda favqulodda to‘xtatish avtomatik ishga tushadi:

- xizmatning o‘rtacha javob vaqti odatdagi qiymatdan 50 foizdan ortiq oshishi;
- ko‘lamdagi har qanday xizmatning 60 soniyadan ortiq uzilishi;
- tarmoq uskunasi yoki server resurslaridan foydalanishning 90 foizdan oshishi;
- asosiy bank tizimida xatoliklar sonining keskin o‘sishi.

Aniq chegaraviy qiymatlar RoEda belgilanadi.

To‘xtatish tartibi va muddatlari

- to‘xtatish buyrug‘i berilgandan keyin barcha faol harakatlar 15 daqiqa ichida to‘xtatiladi;
- 30 daqiqa ichida Ijrochi bajarilgan harakatlar to‘g‘risida dastlabki hisobot, 3 soat ichida esa holat va tavakkalchilik bahosini taqdim etadi;
- ikkala tomonda 24/7 navbatchi va zaxira kontakt bo‘ladi; javob berish muddati - 15 daqiqa. Ijrochi bilan aloqa uzilgan taqdirda sinov avtomatik to‘xtatilgan hisoblanadi.

Real hujum bilan aralashib ketishning oldini olish

- sinov davrida haqiqiy kiberhujum yoki jiddiy insident aniqlansa, Ijrochining barcha faol harakatlari darhol to‘xtatiladi va faqat White Team qarori bilan qayta tiklanadi;
- Ijrochi sinov davomida oldindan mavjud bo‘lgan real buzilish alomatlarini aniqlasa, 1 soat ichida White Team ga xabar beradi, dalillarni o‘zgartirmasdan saqlaydi va Buyurtmachining kiberhodisalarga javob berish jarayoniga texnik ko‘mak beradi.

Kutilmagan operatsion ta’sir va tiklash tartibi

- Ijrochining harakati natijasida xizmat uzilishi yoki sekinlashuvi yuz berganda 15 daqiqa ichida White Team xabardor qilinadi;
- Ijrochi tiklash ishlariga texnik yordam beradi va zarur bo‘lgan barcha texnik ma’lumotni (bajarilgan buyruqlar, vaqt tamg‘alari, nishonlar) darhol taqdim etadi;
- 3 ish kuni ichida sabab tahlili rasmiylashtiriladi va holat yakuniy hisobotning alohida bo‘limida qayd etiladi;
- faol bosqich boshlanishidan oldin Buyurtmachi ko‘lamdagi kritik tizimlar bo‘yicha zaxira nusxalarning tekshirilganligini tasdiqlaydi va tiklash uchun mas’ul texnik guruhning navbatchiligini ta’minlaydi.

Tashkiliy hamkorlik va aloqa tartibi

Blackbox sinovining yashirinligini saqlash uchun loyiha haqida xabardor shaxslar soni zarur minimum bilan cheklanadi. Kontaktlar ro‘yxati alohida himoyalangan holda saqlanadi.

Rol	F.I.O.	Telefon / xavfsiz kanal	Mavjudlik
Buyurtmachi loyiha koordinatori			
Emergency stop vakili			24/7 /
Avtorizatsiya bo‘yicha vakil			
Ijrochi loyiha rahbari			
Ijrochi Incident Response vakili			24/7 / _
Texnik kuzatuvchi (deconfliction)			
Ma’lumotlar himoyasi mas’uli			
Ijrochi texnik rahbari			

Oddiy ishchi aloqa, kritik xabar, fayl almashinuvi va emergency stop uchun alohida kanallar RoEda belgilanadi. Maxfiy dalillar ochiq elektron pochta yoki ommaviy fayl almashish xizmatlari orqali yuborilmaydi.

White Team (ishonchli vakillar guruhi)

Buyurtmachi tomonidan bank buyrug‘i bilan 3-5 kishidan iborat White Team tuziladi. Guruh tarkibiga loyiha koordinatori, avtorizatsiya bo‘yicha vakil, favqulodda to‘xtatish vakili (24/7), texnik kuzatuvchi va ma’lumotlar himoyasi mas’uli kiradi. White Team RoEni to‘liq biladi, kundalik deconfliction ni yuritadi hamda tasdiqlash darvozalarida qaror qabul qiladi.

Maxfiylik rejimi

- loyiha hujjatlari cheklangan kirish rejimida saqlanadi; xarid va moliyaviy hujjatlarda sinovning mazmunini oshkor qiluvchi atamalardan foydalanishdan qochiladi;
- SOC / Blue Team, tizim va tarmoq ma’murlari hamda White Teamga kirmagan boshqa xodimlar xabardor qilinmaydi.

Xabar berish muddatlari

- kritik topilma - darhol, 4 soatdan kechiktirmay, dastlabki bartaraf etish tavsiyasi bilan birga;
- yuqori darajadagi topilma - 24 soat ichida;
- kutilmagan operatsion ta’sir - 15 daqiqa ichida;
- real buzilish alomati - 1 soat ichida;
- to‘lov, karta va mijoz autentifikatsiyasi bilan bog‘liq sinovlar White Team orqali bilan oldindan muvofiqlashtiriladi.

Ijro etuvchi jamoa va texnik imkoniyatlarga talablar

Jamoa tarkibi va tajriba

- jamoa kamida 4 nafar mutaxassisdan iborat bo‘lishi;
- loyiha rahbarining kiberxavfsizlik sohasida kamida 5 yil, bevosita Red Team amaliyotida kamida 2 yil tasdiqlangan tajribaga ega bo‘lishi;
- jamoada Network Exploitation, Reverse Engineering va Social Engineering bo‘yicha alohida kompetensiyalar mavjud bo‘lishi;
- jamoa a’zolarida amaliy kiberxavfsizlik bo‘yicha xalqaro miqyosda tan olingan sertifikatlar mavjud bo‘lishi;
- favqulodda kiberhodisa yuzaga kelganda Buyurtmachi hududiga yetib borish imkoniga ega lokal Incident Response guruhi mavjud bo‘lishi.

- jamoada hujumkor xavfsizlik bo‘yicha amaliy sertifikat (OSCP yoki ekvivalent) egasi kamida 2 nafar, Red Team yo‘nalishiga ixtisoslashgan sertifikat (OSEP, CRTO, CRTL, GXPN, CREST CCSAS/CCSAM yoki ekvivalent) egasi kamida 1 nafar bo‘lishi; sertifikat nusxalari va amal qilish muddati taklif bilan birga taqdim etilishi;
- Ijrochi so‘nggi 3 yil ichida bank yoki moliya tashkilotida bajarilgan kamida 2 ta shunga o‘xshash loyiha bo‘yicha ma’lumot va tavsiyanoma taqdim etishi;
- loyiha rahbari shaxsan kamida 2 ta yakunlangan Red Team loyihasida rahbar bo‘lganligi tasdiqlanishi.

Ruxsat va ishonchlilik talablari

- muhim axborot infratuzilmasi yoki davlat siri bilan bog‘liq ko‘lam mavjud bo‘lsa, jalb etiladigan xodimlarda tegishli ruxsatnomalar mavjud bo‘lishi;
- har bir jalb etilgan xodim Buyurtmachi tasdiqlagan NDA bilan tanishishi va uni imzolashi;
- subpudratchi yoki uchinchi tomon mutaxassisini jalb etish zarurati oldindan yozma kelishilishi;
- jamoa a’zolari va foydalaniladigan infratuzilma ro‘yxati loyiha boshlanishidan oldin tasdiqlanishi.
- xizmat turi qonunchilikda litsenziyalash yoki akkreditatsiya talab qiladigan bo‘lsa, Ijrochida tegishli hujjat mavjud bo‘lishi;
- har bir jalb etilgan xodim bo‘yicha shaxsni tasdiqlovchi hujjat nusxasi, sudlanganlik holati to‘g‘risidagi ma’lumot; jamoa tarkibiga o‘zgartirish faqat oldindan yozma kelishuv bilan kiritilishi;
- O‘zbekiston Respublikasi hududidan tashqarida joylashgan xodimlarning loyiha ma’lumotlariga, dalillarga va C2 infratuzilmasiga kirishi taqiqlanishi;
- fizik yoki joyida bajariladigan ishlar uchun har bir jamoa a’zosida Buyurtmachi tomonidan imzolangan xatining jismoniy nusxasi bo‘lishi; unda sinov muddati, ruxsat etilgan obyektlar va tasdiqlovchi mas’ul shaxsning 24/7 telefon raqami ko‘rsatilishi;

Texnik imkoniyatlar

- ajratilgan C2 infratuzilmasini mustaqil tashkil etish va kuzatish;
- zarur hollarda maqsadli muhitga mos maxsus implant yoki yordamchi dastur ishlab chiqish;
- harakatlarni aniq vaqt tamg‘asi (timestamp) bilan jurnalga yozish va dalillar zanjirini saqlash;
- sinov trafikini boshqarish, tezlikni cheklash va kill switch mexanizmidan foydalanish;
- dalillarni shifrlash, xavfsiz uzatish va qayta tiklab bo‘lmaydigan tarzda yo‘q qilish.
- C2 infratuzilmasi boshqa mijozlar bilan umumiy bo‘lmasligi, faqat kelishilgan IP diapazonlaridan ulanishni qabul qilishi va O‘zbekiston Respublikasi hududida joylashtirilishi;
- kill switch mexanizmi buyruq berilgandan keyin 15 daqiqa ichida barcha faol vositalarni to‘xtatishi;
- Ijrochining barcha ish stantsiyalari va serverlari to‘liq diskli shifrlash, ko‘p faktorli autentifikatsiya hamda himoya vositalari bilan ta’minlanishi; shaxsiy qurilmalardan foydalanish taqiqlanishi;
- bajarilgan barcha buyruqlar va harakatlar sessiya jurnali yoki ekran yozuvi ko‘rinishida qayd etilishi va Buyurtmachining talabi bilan taqdim etilishi.

Ma’lumotlarni himoya qilish va lokalizatsiya

- sinov natijalari, skanerlash ma’lumotlari, loglar, kredensiallar, ekran tasvirlari va hisobotlar faqat O‘zbekiston Respublikasi hududida joylashgan ajratilgan, himoyalangan tizimlarda qayta ishlanadi va saqlanadi;
- xorijiy bulutli saqlash, ommaviy kod repozitoriylari, ochiq messenjerlar va nazorat qilinmaydigan tashqi xizmatlardan foydalanilmaydi;
- ma’lumotlar saqlashda va uzatishda kuchli shifrlashdan foydalaniladi, kalitlar alohida kanal orqali boshqariladi;
- kirish huquqi loyiha uchun tasdiqlangan xodimlar bilan cheklanadi va kirish hodisalari jurnalga yoziladi;
- real ma’lumot nusxasini olish zarurati tug‘ilganda minimal hajm tamoyili qo‘llanadi; imkon qadar xesh, metadata yoki sintetik ma’lumot bilan PoC beriladi;
- yakuniy hisobot va dalillar Buyurtmachiga xavfsiz kanal orqali topshirilgach hamda qabul qilish-topshirish dalolatnomasi imzolangach, 3 ish kuni ichida Ijrochining serverlari, ishchi qurilmalari, vaqtinchalik xotiralari va C2 infratuzilmasidagi loyiha ma’lumotlari secure wipe usulida yo‘q qilinadi;
- ma’lumotlarni yo‘q qilish yakuni bo‘yicha Buyurtmachiga rasmiy kafolat xati taqdim etiladi.
- real shaxsga doir yoki bank siri tarkibidagi ma’lumotlarga duch kelinganda ular nusxalanmaydi; hisobotda barcha identifikatorlar (F.I.O., karta va hisob raqamlari, PINFL, telefon raqami) qisman yashiriladi;
- ijtimoiy muhandislik uchun xodimlar to‘g‘risidagi ma’lumotlar faqat ochiq manbalardan olinadi;
- Buyurtmachi loyiha davomida va uning yakunida Ijrochining ma’lumotlarni saqlash, qayta ishlash va yo‘q qilish jarayonlarini tekshirish huquqiga ega;
- uchinchi tomon mahsulotida aniqlangan zaiflik faqat Buyurtmachi bilan kelishilgan holda va kelishilgan muddatda ishlab chiqaruvchiga xabar qilinadi; yozma rozilikdan tashqari oshkor qilish, nashr etish yoki ro‘yxatlarga kiritish taqiqlanadi.

Mulk huquqi: Sinov doirasida aniqlangan zaifliklar, olingan dalillar, loglar, yozishmalar, oraliq materiallar va yakuniy hisobotlar Buyurtmachiga tegishli. Loyiha nomi yoki natijalaridan portfolio, reklama yoki keys sifatida foydalanish faqat Buyurtmachining oldindan yozma roziligi bilan mumkin.

Hisobot va topshiriladigan natijalar

Yakuniy hisobot tarkibi

- Executive Summary - rahbariyat uchun asosiy xavflar, biznesga ta’sir va erishilgan flag‘lar xulosasi;
- sinov ko‘lami, istisnolar, metodologiya, qo‘llangan taxminlar va cheklovlar;
- Timeline - barcha muhim harakatlarning sana, soat va daqiqagacha bo‘lgan xronologiyasi;
- hujum yo‘llari - dastlabki kirishdan maqsadli aktivgacha bo‘lgan ketma-ketlik, bog‘liqlik va pivot nuqtalari;
- MITRE ATT&CK xaritasi - qo‘llangan taktika va texnikalar, natija va kuzatilgan telemetriya;
- flag‘lar reyestri - bajarilgan, qisman bajarilgan yoki bajarilmagan holatlar va dalillar;
- texnik topilmalar - identifikator, aktiv, daraja, tavsif, shartlar, PoC, ta’sir, dalillar va bartaraf etish tavsiyasi;
- SOC / Blue Team bahosi - aniqlangan va aniqlanmagan harakatlar, birinchi signal, triage, eskalatsiya hamda cheklash vaqt ko‘rsatkichlari;
- Remediation rejasi - tezkor, o‘rta muddatli va arxitekturaviy takomillashtirishlar, ustuvorlik va qayta tekshirish mezonlari;

- tozalash reyestri - yaratilgan hisoblar, fayllar, implantlar, tokenlar, qoidalar va ularni olib tashlash holati;
- ilovalar - ekran tasvirlari, log parchalari, IoC ro‘yxati, diagrammalar va boshqa zarur dalillar.
- himoya vositalari samaradorligi kartasi - har bir vosita hujumning qaysi bosqichida ishlagani, qayerda chetlab o‘tilgani va konfiguratsiyani takomillashtirish bo‘yicha aniq tavsiya;
- har bir kritik va yuqori darajadagi topilma uchun biznes ssenariysi: qaysi biznes jarayon to‘xtaydi, taxminiy moliyaviy, reputatsion va regulyativ oqibat, tiklanish uchun zarur vaqt;
- normativ muvofiqlik xaritasi - topilmalarni tegishli normativ hujjat bandlariga bog‘lovchi jadval;
- bartaraf etish rejasida har bir chora uchun mas’ul bo‘linma turi, tavsiya etiladigan muddat, murakkablik darajasi va bartaraf etilganini tasdiqlovchi tekshirish mezoni ko‘rsatiladi; 1-2 hafta ichida minimal xarajat bilan qo‘llanadigan choralar «tez g‘alabalar» sifatida alohida ajratiladi.

Kritik topilmani darhol xabar qilish

Kritik darajadagi topilma aniqlanganda Ijrochi yakuniy hisobotni kutmasdan, 4 soat ichida qisqa xabarnoma taqdim etadi: topilmaning mohiyati, ta’sirlangan aktiv, ekspluatatsiya shartlari, tavakkalchilik bahosi va zudlik bilan qo‘llash mumkin bo‘lgan vaqtinchalik chora. Ijrochi bunday holatda Buyurtmachining bartaraf etish ishlariga texnik maslahat beradi.

Topilma kartasi uchun minimal maydonlar

Maydon	Talab
ID va nomi	Noyob identifikator va topilmaning aniq nomi.
Daraja	Kritik / yuqori / o‘rta / past / axborot darajasi va baholash asosi.
Ta’sirlangan aktiv	Domen, tizim, xizmat, komponent yoki jarayon.
Tavsif va shartlar	Topilmaning mohiyati, zarur old shartlar va kuzatilgan holat.
Hujum yo‘li	Topilmaga olib kelgan texnikalar va oldingi bosqichlar bilan bog‘liqlik.
Dalil / PoC	Zarar yetkazmaydigan, vaqt tamg‘ali va qayta tekshiriladigan amaliy tasdiq.
Ehtimoliy ta’sir	Maxfiylik, yaxlitlik, mavjudlik va biznes jarayoniga ta’sir.
Tavsiya	Aniq texnik, konfiguratsion yoki jarayoniy takomillashtirish.
Qayta tekshirish mezoni	Topilma bartaraf etilganini tasdiqlovchi kutiladigan holat.

Natijalarni taqdim etish formati

Natija	Format	Taqdim etish usuli
Yakuniy ekspert hisoboti	DOCX va PDF	Shifrlangan elektron fayl, xavfsiz kanal orqali
Texnik dalillar ilovasi	PDF / himoyalangan arxiv	Hisobotdan alohida, kirish nazorati bilan
IoC va tozalash ro‘yxati	XLSX / CSV yoki jadval	Buyurtmachi texnik jamoasiga
Rahbariyat taqdimoti	PPTX / PDF	Yopiq yakuniy uchrashuvda

Ma’lumotlarni yo‘q qilish xati	Imzolangan PDF yoki qog‘oz nusxa	Dalolatnomadan keyin 3 ish kuni ichida
Aniqlash qamrovi matritsasi	XLSX	Buyurtmachi texnik jamoasiga
Tahdid razvedkasi hisoboti	PDF	Shifrlangan elektron fayl, xavfsiz kanal orqali
Birlamchi ma’lumotlar (skanerlash natijalari, loglar)	Shifrlangan arxiv	Buyurtmachining talabiga ko‘ra
Qayta tekshirish hisoboti	DOCX va PDF	Retest yakunlangandan keyin

Yakuniy hisobot o‘zbek var rus tilida taqdim etiladi. Rahbariyat uchun qisqacha xulosa (Executive Summary) va yakuniy taqdimot o‘zbek va rus tillarida tayyorlanadi.

Qabul qilish mezonlari

Xizmat natijalari quyidagi mezonlar bo‘yicha ko‘rib chiqiladi:

- kelishilgan ko‘lam va flag‘larning har biri bo‘yicha holat va dalil mavjudligi;
- Timeline, hujum yo‘llari, topilmalar va tavsiyalar o‘rtasida izchil bog‘lanish mavjudligi;
- texnik dalillarda vaqt tamg‘asi, aktiv va bajarilgan harakatni aniqlash uchun yetarli kontekst mavjudligi;
- tavsiyalar aniq, ustuvorlashtirilgan va qayta tekshirish mezoniga ega bo‘lishi;
- SOC / Blue Team bahosi Buyurtmachi taqdim etgan telemetriya bilan solishtirilgan bo‘lishi;
- sinov artefaktlari bo‘yicha tozalash reyestri yakunlangan bo‘lishi;
- hisobot va ilovalar kelishilgan formatda ochilishi, o‘qilishi va tarkiban to‘liq bo‘lishi;
- yakuniy natijalar rahbariyat va texnik jamoaga alohida tushuntirilishi;
- qabul qilish-topshirish dalolatnomasi rasmiylashtirilishi.
- Aniqlangan topilmalarni qayta tekshirish ushbu xizmat doirasiga kiritilishi yoki alohida kelishuv asosida bajarilishi mumkin.
- aniqlash qamrovi matritsasi va aniqlash/javob berish vaqt ko‘rsatkichlari to‘liq keltirilgan bo‘lishi;
- himoya vositalari samaradorligi kartasi va normativ muvofiqlik xaritasi mavjud bo‘lishi;
- tozalash reyestri Ijrochi tomonidan bajarilib, Buyurtmachi tomonidan mustaqil ravishda tasdiqlangan bo‘lishi; tozalash to‘liq tasdiqlanmaguncha qabul qilish-topshirish dalolatnomasi imzolanmaydi;
- kritik va yuqori darajadagi topilmalar bo‘yicha qayta tekshirish xizmat narxiga kiritiladi va yakuniy hisobot topshirilgandan keyin 3 oy ichida kamida bir marta bepul o‘tkaziladi.

Javobgarlik va shartnoma shartlari

- Ijrochida kasbiy moliyaviy javobgarlik mavjud bo‘lishi yoki shartnomada javobgarlikning aniq moliyaviy limiti belgilanishi;
- Ijrochining RoEni buzishi yoki ehtiyotsizligi natijasida yuzaga kelgan xizmat uzilishi, ma’lumot yo‘qolishi yoki oshkor bo‘lishi uchun javobgarlik tartibi va jarima miqdori shartnomada belgilanishi;
- taqiqlangan harakat sodir etilgan yoki RoE jiddiy buzilgan taqdirda Buyurtmachi shartnomani bir tomonlama bekor qilish huquqiga ega bo‘lishi;
- hisobot topshirilgandan keyin 3 oy davomida Ijrochi topilmalar bo‘yicha savollarga va bartaraf etish choralari yuzasidan bepul maslahat berishi;
- taklif narxiga quyidagilar to‘liq kiritilishi va keyinchalik alohida to‘lov talab qilinmasligi: tahdid razvedkasi hisoboti va aniqlash qoidalarini topshirish, qayta tekshirish, rahbariyat va texnik jamoa uchun ikkita alohida taqdimot, hisobotning o‘zbek va rus tillaridagi versiyalari hamda ma’lumotlarni yo‘q qilish kafolat xati;

- RoEga kiritiladigan har qanday o‘zgartirish faqat imzolangan yozma qo‘shimcha kelishuv bilan kuchga kiradi; operativ vaziyatda og‘zaki berilgan ruxsat 24 soat ichida yozma rasmiylashtiriladi; RoEning har bir versiyasi raqamlanadi va yakuniy hisobotda qaysi versiya amal qilgani ko‘rsatiladi.

Ish reja va muddatlar

Aniq muddatlar sinov ko‘lami, flag‘lar soni, tizimlar murakkabligi va ish oynasidan kelib chiqib shartnomada hamda quyidagi kalendar rejada belgilanadi.

№	Bosqich	Boshlanish	Yakun	Davomiyligi
1	Tayyorgarlik va RoE	__/__/20__	__/__/20__	___ ish kuni
2	OSINT va tahdid modellashtirish	__/__/20__	__/__/20__	___ ish kuni
3	Hujum infratuzilmasini tayyorlash	__/__/20__	__/__/20__	___ ish kuni
4	Faol Red Team sinovi	__/__/20__	__/__/20__	___ ish kuni
5	Tozalash va dalillarni tizimlashtirish	__/__/20__	__/__/20__	___ ish kuni
6	Hisobot tayyorlash	__/__/20__	__/__/20__	___ ish kuni
7	Taqdimot va qabul qilish	__/__/20__	__/__/20__	___ ish kuni
8	Qayta tekshirish (retest)	__/__/20__	__/__/20__	___ ish kuni

Texnik topshiriqni kelishish

Tomon	Lavozimi	F.I.O.	Imzo	Sana
Buyurtmachi	_____	_____	_____	__/__/20__
Ijrochi	_____	_____	_____	__/__/20__

Ilova: RoE parametrlarini to‘ldirish varag‘i

Ruxsat etilgan domenlar / diapazonlar	
Tekshiruv doirasi (ko‘lamiga) kirmaydigan aktivlar	
Ruxsat etilgan ijtimoiy muhandislik	
Ruxsat etilgan ekspluatatsiya darajasi	
Ma’lumot olish limiti	
Tezlik / yuklama limiti	
Fizik kirish parametrlari	
Emergency stop kalit so‘zi	
Dalillarni uzatish kanali	
Qo‘shimcha cheklovlar	
Tezlik limitlarining raqamli qiymatlari (so‘rov/sekund, parallel ulanish, parallel xost)	

«Faqat passiv» rejimidagi tizimlar ro‘yxati	
Hisobning bloklanish chegarasi va bloklanish oynasi	
Muzlatilgan (taqiqlangan) davrlar	
Tasdiqlash talab qilinadigan yuqori tavakkalli harakatlar	
Ijtimoiy muhandislik vektorlari va jo‘natish limitlari	
Avtomatik to‘xtatish chegaraviy qiymatlari	
White Team tarkibi va navbatchilik jadvali	
Ish vaqti va ish vaqtidan tashqari harakatlar taqsimoti	

Ilova: Yakuniy natijalarni tekshirish ro‘yxati

№	Tekshiruv bandi	Holat	Izoh
1	Tasdiqlangan ko‘lam va flag‘lar reyestri kiritilgan.	☐	
2	Executive Summary va biznesga ta’sir xulosasi mavjud.	☐	
3	Daqiqagacha aniqlikdagi Timeline mavjud.	☐	
4	Hujum yo‘llari va MITRE ATT&CK xaritasi kiritilgan.	☐	
5	Har bir texnik topilma uchun PoC va tavsiya mavjud.	☐	
6	SOC / Blue Team aniqlash va javob ko‘rsatkichlari kiritilgan.	☐	
7	IoC, yaratilgan artefaktlar va tozalash reyestri mavjud.	☐	
8	Hisobot DOCX va PDF formatlarida topshirilgan.	☐	
9	Rahbariyat va texnik jamoa uchun yakuniy taqdimot o‘tkazilgan.	☐	
10	Ma’lumotlarni yo‘q qilish kafolat xati taqdim etilgan.	☐	
11	Aniqlash qamrovi matritsasi to‘liq to‘ldirilgan.	☐	
12	Aniqlash va javob berish vaqt ko‘rsatkichlari keltirilgan.	☐	
13	Himoya vositalari samaradorligi kartasi mavjud.	☐	
14	Normativ muvofiqlik xaritasi kiritilgan.	☐	
15	Aniqlash qoidalari va IoC mashinada o‘qiladigan formatda topshirilgan.	☐	
16	Tozalash Buyurtmachi tomonidan mustaqil ravishda tasdiqlangan.	☐	
17	Qayta tekshirish muddati kelishilgan va rejalashtirilgan.	☐	

Ilova: Yuqori tavakkalli harakatni tasdiqlash (approval gate) so‘rovi shakli

Ijrochi tomonidan to‘ldiriladi, White Team tomonidan tasdiqlanadi.

Maydon	Ma’lumot
So‘rov raqami va sanasi	

Harakat turi	
Nishon aktiv va uning toifasi	
Rejalashtirilgan texnika va vosita	
Kutilayotgan natija	
Operatsion ta’sir tavakkalchiligi bahosi (past / o‘rta / yuqori)	
Tavakkalchilikni kamaytirish choralari	
Rejalashtirilgan vaqt oynasi	
Orqaga qaytarish (rollback) rejasi	
White Team qarori: ruxsat berildi / rad etildi / shart bilan	
Qaror qabul qilgan shaxs, sana va vaqt	

Ilova: Ijrochi indikatorlarini oldindan ro‘yxatdan o‘tkazish shakli

Faol bosqichdan kamida 1 ish kuni oldin to‘ldiriladi va real vaqtda yangilab boriladi. Faqat White Team da saqlanadi.

Indikator turi	**Qiymatlar**
Manba IP-manzillari va tarmoq diapazonlari	
C2 domenlari va ularning IP-manzillari	
Foydalaniladigan TLS sertifikatlari (barmoq izi)	
Fishing uchun ro‘yxatdan o‘tkazilgan domenlar	
Jo‘natuvchi elektron pochta manzillari	
SMS va telefon qo‘ng‘iroqlari uchun raqamlar	
Unikal marker (HTTP sarlavhasi yoki User-Agent qatori)	
Sinov uchun yaratilgan hisob nomlari	
Ro‘yxat oxirgi yangilangan sana va vaqt	

Ilova: Aniqlash qamrovi matritsasi shakli

Ijrochi tomonidan yakuniy hisobotda majburiy element sifatida to‘ldiriladi. «Natija» ustunida to‘rt qiymatdan biri ko‘rsatiladi: oldi olindi / aniqlandi va ogohlantirildi / faqat jurnalga yozildi / telemetriya yo‘q.

Taktika	**Texnika (ID va nomi)**	**Vaqt**	**Natija**	**Vosita**	**Tavsiya**

Ilova: Faol bosqichdan oldingi tayyorgarlik tekshiruv ro‘yxati

Faol sinov faqat quyidagi barcha bandlar bajarilgandan keyin boshlanadi. Ro‘yxat White Team tomonidan to‘ldiriladi va ikkala tomon imzosi bilan tasdiqlanadi.

№	Tekshiruv bandi	Holat
1	RoE yakuniy versiyasi imzolangan va versiya raqami qayd etilgan.	☐
2	Avtorizatsiya hujjati va NDA barcha jamoa a’zolari tomonidan imzolangan.	☐
3	White Team bank buyrug‘i bilan rasmiylashtirilgan, 24/7 navbatchilik jadvali tasdiqlangan.	☐
4	Muzlatilgan davrlar kalendari tasdiqlangan va o‘zgarishlar jadvali bilan solishtirilgan.	☐
5	Yuklama va tezlik limitlari raqamlar bilan belgilangan.	☐
6	«Faqat passiv» rejimidagi nozik tizimlar ro‘yxati taqdim etilgan.	☐
7	Hisobning bloklanish chegarasi va oynasi xavfsizlik parametri sifatida oshkor qilingan.	☐
8	Kritik tizimlar bo‘yicha zaxira nusxalar mavjudligi va tiklanishi tekshirilgan.	☐
9	Ijrochi indikatorlari ro‘yxati olingan va White Team da saqlanmoqda.	☐
10	Mavjudlik monitoringi yoqilgan, avtomatik to‘xtatish chegaralari sozlangan.	☐
11	Emergency stop kalit so‘zi, callback tartibi va zaxira kontaktlar kelishilgan.	☐
12	Ijrochi jamoasi tarkibi, sertifikatlari va qurilmalari ro‘yxati tasdiqlangan.	☐
13	Foydalaniladigan vositalar ro‘yxati tasdiqlangan.	☐
14	Tiklash uchun mas’ul texnik guruhning navbatchilik jadvali tasdiqlangan.	☐
15	Firibgarlikka qarshi kurash bo‘linmasi bilan muvofiqlashtirish bajarilgan.	☐

Kelishildi:

Z.X.Mamajonov



S.R.Mamasiddikov



F.S.Abdukadirov

U.X.Beknazarov

