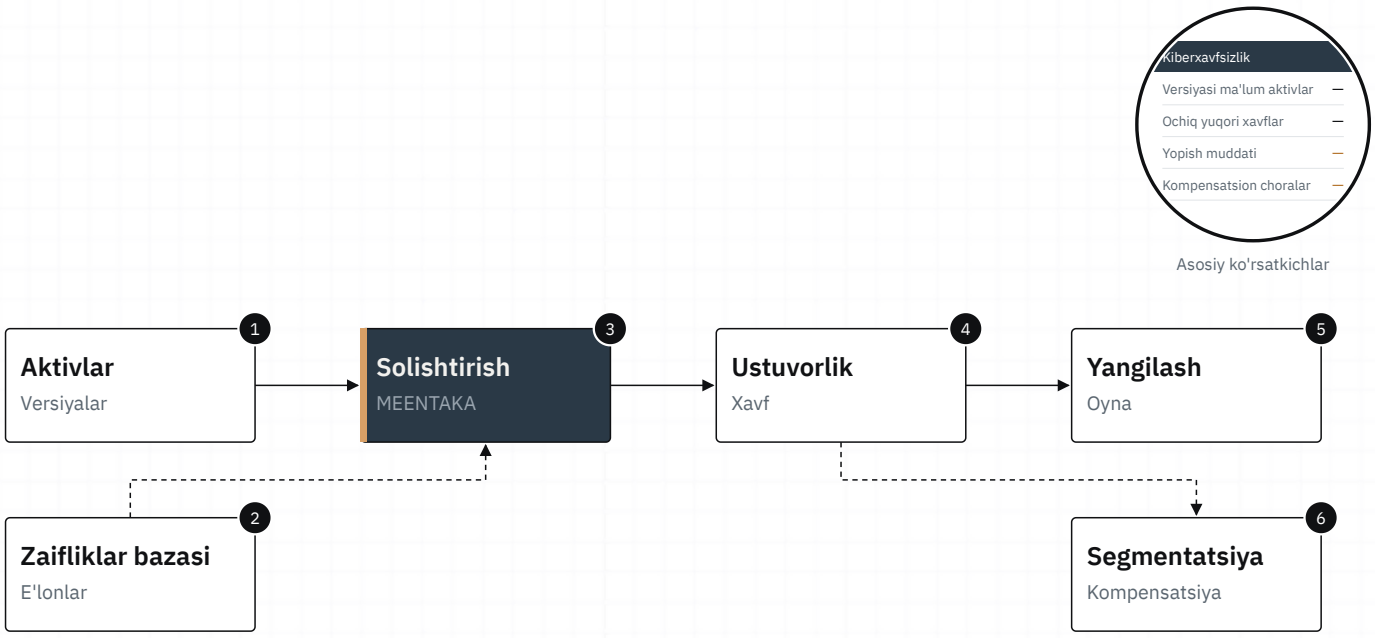
KIBERXAVFSIZLIK · KIBERXAVFSIZLIK · ZAIFLIKLAR

Zaifliklar va yangilanishlar: zavodda "hammasini yangila" ishlamaydi

Ishlab chiqarish tizimini har kuni yangilab bo'lmaydi. Shuning uchun qaysi zaiflik haqiqatda xavfli ekanini bilish va ustuvorlik berish kerak.



Hujjat turi	Kod	Til	Holat
Yechim hujjati	KX-10	O'zbekcha	Noyabr 2026

01 — Qisqacha

Zaiflik e'lon qilindi. Bizda shu uskuna bormi?

Dragos ma'lumotiga ko'ra zaiflik oshkor qilinganidan uning qurollangan eksploiti paydo bo'lguncha mediana 24 kun. PF–38 farmoni DXX ga mustaqil ekspertlar ishtirokida milliy axborot tizimlaridagi zaifliklarni topish tanlovlarini maxsus platformada o'tkazishni yukladi. Korxona uchun asosiy savol — qaysi zaiflik bizda bor va qaysi biri birinchi.

MAQSAD

Zaiflik e'lon qilindi. Bizda shu uskuna bormi?

YECHIM

Aktivlar va dastur versiyalari ro'yxatini ma'lum zaifliklar bazalari bilan solishtirish, ekspluatatsiya qilinish va jarayon ahamiyati bo'yicha ustuvorlik, rejalashtirilgan oynada yangilash yoki tarmoq segmentatsiyasi kabi kompensatsion choralar.

NATIJA

O'lchanadigan ko'rsatkichlar: versiyasi ma'lum aktivlar, ochiq yuqori xavflar, yopish muddati, kompensatsion choralar.

Kimlar uchun

Bosh muhandis
Uskuna.

IT/xavfsizlik
Zaifliklar.

Ishlab chiqarish
To'xtash oynasi.

Yetkazib beruvchi
Yangilanish.

> Hammasini yangilab bo'lmaydi — eng xavflisini bilish kerak.

QISQA FAKTLAR

24 kun
Oshkor qilishdan qurollangan eksploitgacha mediana (Dragos).[1]

Tanlovlar
DXX zaiflik topish tanlovlari (PF–38).[2]

O'zMSt 838–841
2026 milliy kiberxavfsizlik standartlari.[3]

Manbalar — oxirgi betda.

02 — Kontekst

Dunyoda va O'zbekistonda nima ma'lum

Xalqaro tahlil va rasmiy manbalar.

Fakt	Manba
Oshkor qilishdan qurollangan eksploitgacha mediana 24 kun.[1]	Dragos 2026 (controleng.com)
DXX mustaqil ekspertlar ishtirokida zaifliklarni topish tanlovlarini maxsus onlayn platformada o'tkazadi.[2]	PF–38 (spot.uz)
Milliy standartlar O'zMSt 838–841:2026.[3]	Kiberxavfsizlik markazi (csec.uz)

Bu raqamlarni qanday o'qish kerak

Zaifliklarni faol skanerlash ishlab chiqarish jarayoniga ta'sir qilishi mumkin — OT da faqat passiv usul yoki kelishilgan oynada. O'zbekiston korxonalari bo'yicha bu ko'rsatkich ochiq manbalarda topilmadi — dastlabki baholashda o'lchanadi.

Faktlar manbada qanday berilgan bo'lsa, shunday keltirilgan. Yetkazib beruvchi ma'lumotlari shunday belgilangan va boshqa korxonada kafolatlanmaydi.

03 — Muammo

Nima ishlamaydi

Odatdagi bo'shliqlar:

01
Ro'yxat
Qaysi versiyalar o'rnatilgani noma'lum.

02
Ustuvorlik
Hamma zaiflik bir xil muhim deb ko'riladi.

03
Oyna
Yangilash uchun to'xtash rejalashtirilmaydi.

04
Muqobil
Yangilab bo'lmaganda boshqa himoya yo'q.

Yo'qotishni qanday hisoblash mumkin

Ekspluatatsiya	`hodisa zarari`
Rejasiz to'xtash	`favqulodda yangilash`
Resurs	`muhim bo'lmaganga sarf`
Muvofiqlik	`talablar`

Formulalar namunaviy; aniq qiymat auditda o'lchanadi.

Rahbar o'ziga beradigan savollar

Uskunalar va dasturlar versiyalari ma'lummi?

Yangi zaiflik e'lonlari kuzatiladimi?

Ustuvorlik qoidasi bormi?

04 — Yechim arxitekturasi

Versiyalar ro'yxati → mos zaifliklar → ustuvorlik → yangilash yoki kompensatsiya

Aktivlar va dastur versiyalari ro'yxatini ma'lum zaifliklar bazalari bilan solishtirish, ekspluatatsiya qilinish va jarayon ahamiyati bo'yicha ustuvorlik, rejalashtirilgan oynada yangilash yoki tarmoq segmentatsiyasi kabi kompensatsion choralar.

Foydalanuvchilar	Bosh muhandis · IT/xavfsizlik · Ishlab chiqarish · Yetkazib beruvchi
Ro'yxat	Aktivlar · Versiyalar · Proshivka
Solishtirish	**Zaifliklar bazasi** · **Yetkazib beruvchi** · **Ogohlantirish**
Ustuvorlik	**Ekspluatatsiya** · **Jarayon** · **Ochiqlik**
Choralar	Yangilash · Segmentatsiya · Monitoring
Integratsiya	1C · ESF / EDO · Datchik va PLC · Telegram ogohlantirish

Boshqaruv paneli

Aktivlar bo'yicha zaifliklar, ustuvorliklar, yangilash rejasi

Qora qatorlar — MEENTAKA qatlami. Mavjud uskuna va tizimlar saqlanadi; ma'lumot ulardan yig'iladi.

05 — Modullar katalogi

Nima o'rnatiladi

Har bir modul alohida ishga tushadi; paket korxona ehtiyojiga qarab yig'iladi.

Modul	Vazifa	Tayyorlik
Versiyalar inventarizatsiyasi	Passiv/hujjat	◐ **Muhandislik imkoniyati**
Zaifliklar bilan solishtirish	Muntazam	◐ **Muhandislik imkoniyati**
Ustuvorlik va oyna rejasi	Ishlab chiqarish bilan	◐ **Muhandislik imkoniyati**
Mustaqil xavfsizlik sinovi	Ruxsat etilgan hamkor	○ **Ishlab chiqilmoqda**

● Tijoriy mavjud ◐ Muhandislik imkoniyati ○ Ishlab chiqilmoqda

Korxona tomonidan kerak

- Bosh muhandis
- Aktivlar ro'yxati
- Yetkazib beruvchilar kontaktlari
- To'xtash jadvali

Va'da qilinmaydi

- Sertifikatlash, attestatsiya yoki MAI obyektini rasmiy baholash (vakolatli organlar va akkreditatsiyalangan tashkilotlar vazifasi)
- Penetratsion test yoki xakerlik xizmatlari (faqat ruxsat etilgan hamkorlar orqali)
- "100% himoya" yoki hujum bo'lmasligi kafolati
- Yuridik maslahat

06 — Joriy qilish

Kichikdan boshlaymiz, o'lchab kengaytiramiz

Audit → pilot → kengaytirish → obuna. Har bosqich oldingisining o'lchangan natijasiga tayanadi.

1–2 hafta
Ro'yxat
Aktivlar va jarayonlar.

Natija: xavflar xaritasi.

30 kun
Pilot (1 sex)
Bitta sex yoki tizim, 30 kun.

Natija: birinchi natijalar.

2–3 oy
Butun zavod
Butun korxona.

Natija: doimiy jarayon.

Doimiy
Qo'llab-quvvatlash
Oylik hisobot.

Natija: ochiq yuqori xavflar.

Muddatlar taxminiy; auditdan keyin aniqlanadi.

O'lchanadigan ko'rsatkichlar

Ko'rsatkich	Birlik	Manba
Versiyasi ma'lum aktivlar	%	Ro'yxat
Ochiq yuqori xavflar	Soni	Panel
Yopish muddati	Kun	Reja
Kompensatsion choralar	%	Reja

07 — Keyingi qadam

Zaifliklaringizni boshqarasizmi

O'n savol. "Yo'q" javoblari — auditda birinchi ko'riladigan joylar.

01 Uskunalar va dasturlar versiyalari ma'lummi?

02 Yangi zaiflik e'lonlari kuzatiladimi?

03 Ustuvorlik qoidasi bormi?

04 Yangilash oynalari rejalashtiriladimi?

05 Yangilab bo'lmaganda kompensatsion chora bormi?

06 Yetkazib beruvchidan ogohlantirish olinadimi?

07 OT da faol skanerlash cheklanganmi?

08 Ochiq xavflar rahbariyatga ma'lummi?

09 Kiberxavfsizlik uchun mas'ul shaxs tayinlanganmi?

Zaifliklar ro'yxati

Bitta sex uskunalari va dasturlari bo'yicha ma'lum zaifliklar ro'yxatini tayyorlab, ustuvorlikni belgilaymiz.

meentaka.uz · info@meentaka.uz · +998 99 321 47 77

Natijada olasiz

- Aktivlar va xavflar xaritasi
- Ustuvor choralar rejasi
- Loyiha va oylik qo'llab-quvvatlash

Manbalar

1. Dragos 2026 OT/ICS Cybersecurity Year in Review (17.02.2026): 2025-yilda 119 ransomware guruhi 3 300 sanoat tashkilotiga ta'sir qilgan; sanoatga ransomware hujumlari +64%; qurbonlarning uchdan ikki qismidan ko'prog'i ishlab chiqarish; OT da ransomware o'rtacha 42 kun aniqlanmay qolgan, to'liq OT ko'rinishiga ega tashkilotlarda — 5 kun; oshkor qilishdan qurollangan eksploitgacha mediana 24 kun (controleng.com).
2. Farmon PF–38 (10.03.2026; spot.uz, norma.uz): 2026–2030 yillarga Kiberxavfsizlik strategiyasi va yo'l xaritasi; 01.04.2026 dan davlat organlari va tashkilotlari kiberxavfsizlikka mablag' ajratishi shart; Adliya, Energetika vazirliklari va Soliq qo'mitasida kiberxavfsizlik bo'limlari; DXX mustaqil ekspertlar ishtirokida zaifliklarni topish tanlovlarini maxsus platformada o'tkazadi.
3. Kiberxavfsizlik markazi (csec.uz): 2026-yilda O'zMSt 838–841:2026 milliy standartlari ishlab chiqilgan (bostirib kirishlarni aniqlash, zararli dasturlardan himoya, axborotni muhofaza qilish vositalari, amaliy dasturiy ta'minot talablari).

Hujjat 2026-yil noyabr holatiga ochiq manbalar asosida tayyorlangan. Ma'lumotlar manbada qanday berilgan bo'lsa, shunday keltirilgan. Hujjat huquqiy yoki moliyaviy maslahat emas; rasmiy matnlarni lex.uz va soliq.uz da tekshiring.

MEENTAKA

Nashr etuvchi

© 2026 MEENTAKA. «The Endurance Industrial Technologies» MChJ

Hujjat raqami
MT-KX-10-UZ · 11.2026

Aloqa
meentaka.uz · info@meentaka.uz · +998 99 321 47 77