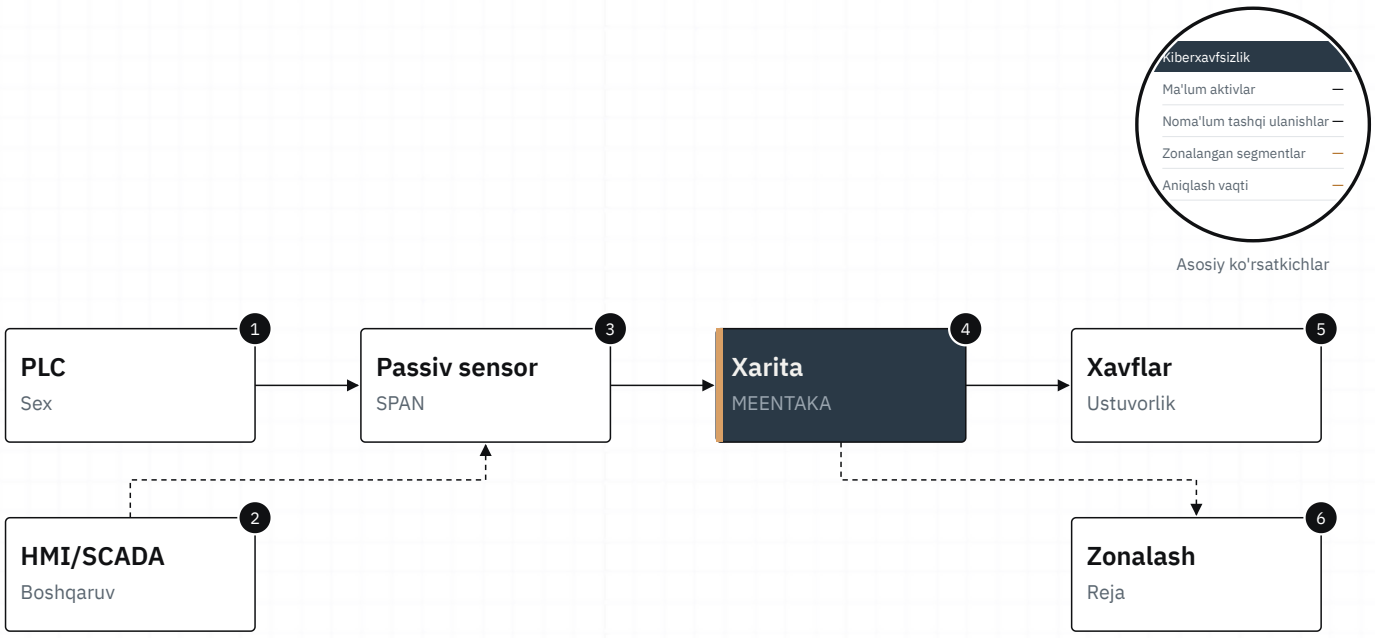
KIBERXAVFSIZLIK · KIBERXAVFSIZLIK · OT KO'RINISH

Zavod tarmog'ida nima bor: OT aktivlari va aloqalar xaritasi

Ko'rinmaydigan narsani himoya qilib bo'lmaydi. Sanoat tarmog'idagi PLC, SCADA, muhandis kompyuterlari va masofaviy ulanishlar ro'yxati — kiberxavfsizlikning birinchi qadami.



Hujjat turi	Kod	Til	Holat
Yechim hujjati	KX-01	O'zbekcha	Noyabr 2026

01 — Qisqacha

Sexda nechta qurilma tarmoqqa ulangan? Aniq javob kam.

Dragos 2026 hisobotiga ko'ra, to'liq OT ko'rinishiga ega tashkilotlar sanoat tarmog'idagi ransomware hodisalarini o'rtacha 5 kunda aniqlab cheklagan, umumiy o'rtacha esa 42 kun. Farq texnologiyada emas — tarmoqda nima borligini va u qanday gaplashayotganini bilishda.

MAQSAD

Sexda nechta qurilma tarmoqqa ulangan? Aniq javob kam.

YECHIM

Sanoat tarmog'iga passiv sensor ulanadi (jarayonga ta'sir qilmasdan), aktivlar va protokollar avtomatik aniqlanadi, aloqalar xaritasi tuziladi, eng xavfli bo'shliqlar ustuvorlik bo'yicha ro'yxatlanadi.

NATIJA

O'lchanadigan ko'rsatkichlar: ma'lum aktivlar, noma'lum tashqi ulanishlar, zonalangan segmentlar, aniqlash vaqti.

Kimlar uchun

Zavod direktori
Uzluksizlik.

Bosh muhandis / ASU TP
Tizimlar.

IT bo'limi
Tarmoq.

Kiberxavfsizlik mas'uli
Xavf.

> Ko'rinmaydigan aktivni himoya qilib bo'lmaydi.

QISQA FAKTLAR

5 / 42 kun

OT ko'rinishi bor va umumiy o'rtacha: ransomware aniqlash vaqti (Dragos).[1]

3 300

2025-yilda ransomware ta'sir qilgan sanoat tashkilotlari.[1]

2/3+

Qurbonlar orasida ishlab chiqarish korxonalari ulushi.[1]

Manbalar — oxirgi betda.

02 — Kontekst

Sohada va dunyoda nima ma'lum

Xalqaro tahlil va rasmiy manbalar.

Fakt	Manba
119 ransomware guruhi 3 300 sanoat tashkilotiga ta'sir qilgan; OT da o'rtacha 42 kun aniqlanmay qolgan; to'liq OT ko'rinishi bilan — 5 kun.[1]	Dragos 2026 Year in Review
Ko'p ransomware holatlari "IT hodisasi" deb tasniflanadi, garchi muhandis stansiyalari, SCADA va virtualizatsiya platformalari zararlangan bo'lsa ham.[1]	Dragos blog (OT Threat Landscape 2026)
MAI — avtomatlashtirilgan boshqaruv tizimlari va texnologik jarayonlar resurslarini ham o'z ichiga oladi.[2]	O'RQ–764 (lex.uz)

Bu raqamlarni qanday o'qish kerak

O'zbekiston sanoat korxonalarida OT ko'rinishi darajasi bo'yicha ochiq ma'lumot 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

Odatda nima topiladi

Xalqaro amaliyotda tez-tez uchraydigan bo'shliqlar:

01
Ro'yxat yo'q
PLC va panellar ro'yxati qog'ozda yoki umuman yo'q.

02
Tekis tarmoq
Ofis va sex bitta tarmoqda.

03
Noma'lum ulanish
Kim va qayerdan ulanayotgani ko'rinmaydi.

04
Eski tizimlar
Yangilanmaydigan operatsion tizimlar.

Yo'qotishni qanday hisoblash mumkin

To'xtash	`soat × ishlab chiqarish marjasi`
Tiklash	`kunlar × xarajat`
Uskuna	`noto'g'ri buyruq oqibati`
Javobgarlik	`MAI talablari`

Formulalar namunaviy; aniq qiymat auditda o'lchanadi.

Rahbar o'ziga beradigan savollar

> PLC va HMI ro'yxati bormi?

> Ofis va sex tarmoqlari ajratilganmi?

> Tashqi ulanishlar ro'yxati bormi?

04 — Yechim arxitekturasi

Passiv tinglash → aktivlar ro'yxati → aloqalar xaritasi → xavf ro'yxati

Sanoat tarmog'iga passiv sensor ulanadi (jarayonga ta'sir qilmasdan), aktivlar va protokollar avtomatik aniqlanadi, aloqalar xaritasi tuziladi, eng xavfli bo'shliqlar ustuvorlik bo'yicha ro'yxatlanadi.

Foydalanuvchilar	Zavod direktori · Bosh muhandis / ASU TP · IT bo'limi · Kiberxavfsizlik mas'uli
Sensor	SPAN/TAP · Passiv · Jarayonga ta'sirsiz
Aktivlar	**PLC** · **HMI/SCADA** · **Muhandis PC**
Aloqalar	**Protokollar** · **Zonalar** · **Tashqi ulanish**
Xavf	Ustuvorlik · Reja · Hisobot
Integratsiya	1C · ESF / EDO · Datchik va PLC · Telegram ogohlantirish

Boshqaruv paneli

OT aktivlari, aloqalar xaritasi, xavfli ulanishlar

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
Aktivlar inventarizatsiyasi	Passiv sensor	○ **Ishlab chiqilmoqda**
Aloqalar xaritasi va zonalash rejasi	Muhandislik	◐ **Muhandislik imkoniyati**
Xavflar ro'yxati	Ustuvorlik	◐ **Muhandislik imkoniyati**
OT monitoring platformasi	Hamkor	○ **Ishlab chiqilmoqda**

● Tijoriy mavjud ◐ Muhandislik imkoniyati ○ Ishlab chiqilmoqda

Korxona tomonidan kerak

- Bosh muhandis
- Tarmoq sxemasi (bo'lsa)
- Sexga kirish ruxsati
- Texnologik oyna (to'xtashsiz ulash)

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
OT baholash
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: yangi aktivlar va ulanishlar.

Muddatlar taxminiy; auditdan keyin aniqlanadi.

O'lchanadigan ko'rsatkichlar

Ko'rsatkich	Birlik	Manba
Ma'lum aktivlar	% jami	Sensor
Noma'lum tashqi ulanishlar	Soni	Sensor
Zonalangan segmentlar	%	Reja
Aniqlash vaqti	Kun	Monitoring

07 — Keyingi qadam

Zavod tarmog'ingizni bilasizmi

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

01 PLC va HMI ro'yxati bormi?

02 Ofis va sex tarmoqlari ajratilganmi?

03 Tashqi ulanishlar ro'yxati bormi?

04 Muhandis kompyuterlari nazoratdami?

05 Qaysi protokollar ishlatilishi ma'lummi?

06 Yangi qurilma ulanganda bilinadimi?

07 MAI toifasiga kirish-kirmasligi aniqlanganmi?

08 Tarmoq sxemasi dolzarbmi?

09 Kiberxavfsizlik uchun mas'ul shaxs tayinlanganmi?

OT ko'rinish baholash

Bitta sexning sanoat tarmog'ini passiv tinglab, aktivlar ro'yxati va aloqalar xaritasini tuzamiz.

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. "Kiberxavfsizlik to'g'risida"gi Qonun O'RQ–764 (15.04.2022, lex.uz): muhim axborot infratuzilmasi (MAI) — strategik va ijtimoiy-iqtisodiy ahamiyatga ega avtomatlashtirilgan boshqaruv tizimlari, axborot tizimlari, tarmoq va texnologik jarayonlar resurslari majmui; MAI subyektlari — bunday obyektlarga egalik qiluvchi davlat organlari va yuridik shaxslar; DXX MAI obyektlarining yagona reyestrini yuritadi (kun.uz).

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-01-UZ · 11.2026

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