



КИБЕРСИГУРНОСТ НА ВИК СИСТЕМИТЕ

Полският опит

BULAQUA 2026 • Старосел, 15 октомври 2026

КОИ СМЕ НИЕ?

ПОЛСКИ ПРОИЗВОДИТЕЛ НА СИСТЕМА ЗА
КИБЕРСИГУРНОСТ НА ОТ
за защита на критичната инфраструктура



С участие на държавата
акционер: група ORLEN



100% полска технология
собствен хардуер и софтуер



Само киберсигурност
единствена специализация от 2018 г.

КЛЮЧОВИ СЕКТОРИ



ВиК



Енергетика



Горива



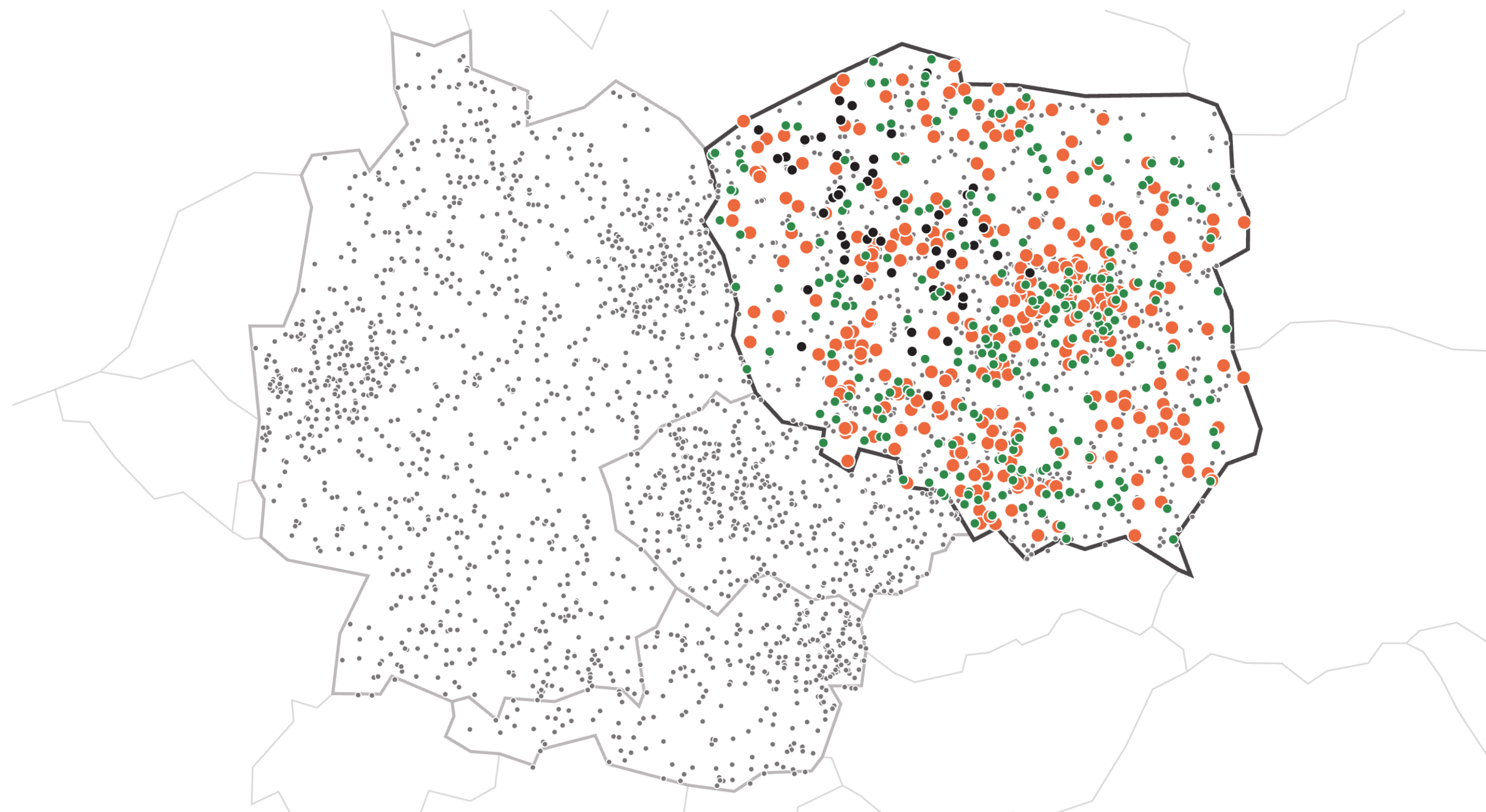
Топлофикация



Промисленост

НАШИТЕ ВНЕДРЯВАНИЯ И ПЛАНОВЕ

- ВиК обекти
- една от четирите най-големи енергийни групи в Полша
- нефтогазови обекти в Полша
- всички нефтогазови обекти – до 2027 г.



250+

ВиК обекти

380

подстанции в Северозападна
Полша

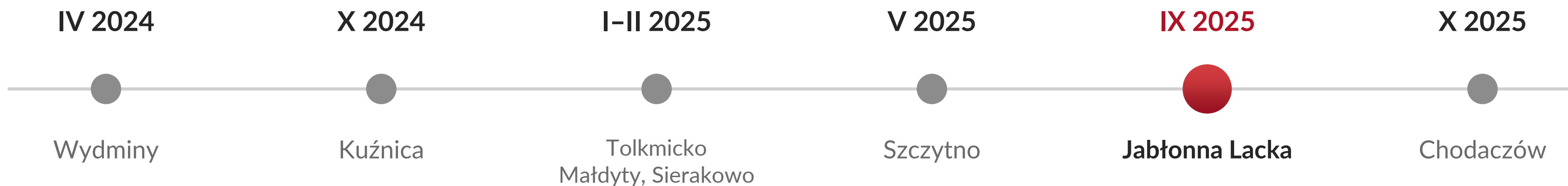
250+

наблюдавани бензиностанции в
Полша · голяма международна
нефтегазова компания

2 500+

станции в четири държави ·
предстоящи (Полша, Чехия,
Германия и Австрия)

2024–2025: АТАКИ СРЕЩУ ПОЛСКИТЕ ВИК



60 часа

без вода за 2 500 жители
Jabłonna Lacka, септември 2025

>50%

опита за атака спрени
(Министерство на цифровизацията)

ПРИЧИНА

Контролни панели, достъпни
от интернет, и прости
пароли.

КАК ОТГОВОРИ ПОЛША?



ЗАКОН

Закон за киберсигурност
(NIS2)
от 3 април 2026 (KSC)

Всяко общинско ВиК в
системата



ИНСТИТУЦИИ

Надзор: Министерство
на инфраструктурата
Инциденти: CSIRT NASK

Един канал: система S46



ПАРИ

Програма
„Киберсигурни
водопроводи“

100% от нетните разходи



ДОСТАВЧИЦИ

Оценка на риска от
доставчици
извън ЕС и НАТО

в закона

4 стълба на киберсигурността по Закона за KSC

ЗАКОН ЗА KSC · NIS2

1



Одити

Проверка на съответствието
и нивото на защита

2



Обучения

Ръководство
и служители

3



Мониторинг и защита на ИТ

Офис мрежи
и информационни системи

4



Мониторинг и защита на ОТ

SCADA, контролери
и индустриални мрежи



Инцидентите се докладват на CSIRT NASK | система S46

ПРОГРАМА „КИБЕРСИГУРНИ ВОДОПРОВОДИ“

627,7

млн. злоти (ок. 147 млн.
евро)

100%

от нетните разходи

896

заявления – 2,5 пъти над
бюджета

733

подписани договора

Допълнителни точки (+50%) за защита на ОТ мрежата:



сегментация на
мрежата



мониторинг на ОТ



сигурен отдалечен
достъп



SOC 24/7

ВИК СЕКТОРЪТ И ICSEC

СЕКТОРЪТ В ПОЛША

~2 700

ВиК дружества, предимно общински

733

ВиК дружества с финансиране

ICSEC В СЕКТОРА

250+

клиенти
във ВиК

150+

теста и одита
на ОТ мрежи

1.000+

обекта
под наблюдение

Внедрявания в малки общини и големи градове – в цяла Полша.

NIS2 – НОВИ ЗАДЪЛЖЕНИЯ НА РЪКОВОДСТВОТО

Ръководството отговаря за киберриска и за надзора над ОТ. Трябва да може да докаже, че:



рисковете се
идентифицират



инцидентите могат
да бъдат открити



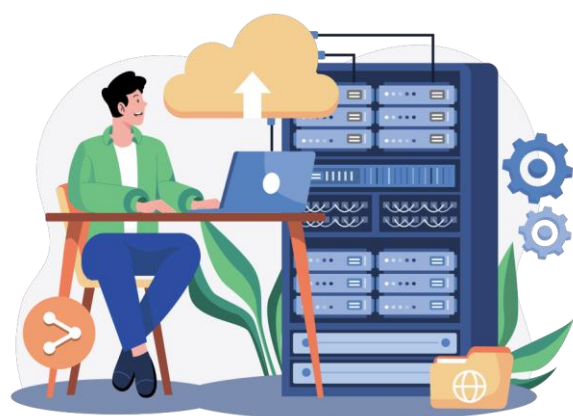
има мерки за
ограничаване на
последиците



сигурността
постоянно се подобрява

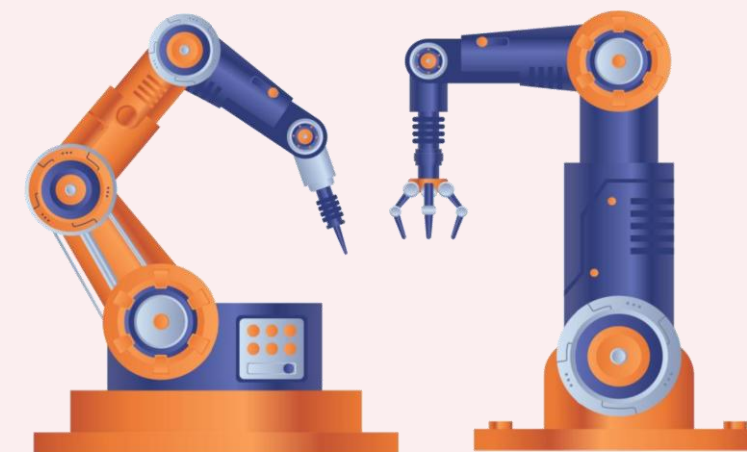
Днес въпросът не е дали имаме система за мониторинг, а дали можем да докажем, че знаем какво се случва в ОТ.

ИТ И ОТ – КАКВО ОЗНАЧАВА, ЧЕ СМЕ В ОТ



ИТ

компютри, поща, данни
приоритет: поверителност на данните
подмяна на 3–5 години



ОТ

помпи, кранове, хлор, пречистване
приоритет: водата трябва да тече
контролерите работят 20–30 години

ICsec защитава ОТ – там, където тече водата.

КАК ГО РАЗБИРАМЕ И КЪДЕ Е ICSEC



ИДЕНТИФИКАЦИЯ

В ОТ ТОВА ОЗНАЧАВА:

знаем какви устройства работят в мрежата



ОТКРИВАНЕ

В ОТ ТОВА ОЗНАЧАВА:

виждаме промяната, преди да се промени параметърът на водата



РЕАКЦИЯ

В ОТ ТОВА ОЗНАЧАВА:

бързо изолираме проблема и докладваме инцидента



ПОДОБРЯВАНЕ

В ОТ ТОВА ОЗНАЧАВА:

мрежата става все по-защитена – и това се вижда

ICSEC

автоматична
инвентаризация на OT

ICSEC

мониторинг 24/7, вкл.
нови атаки (ИИ)

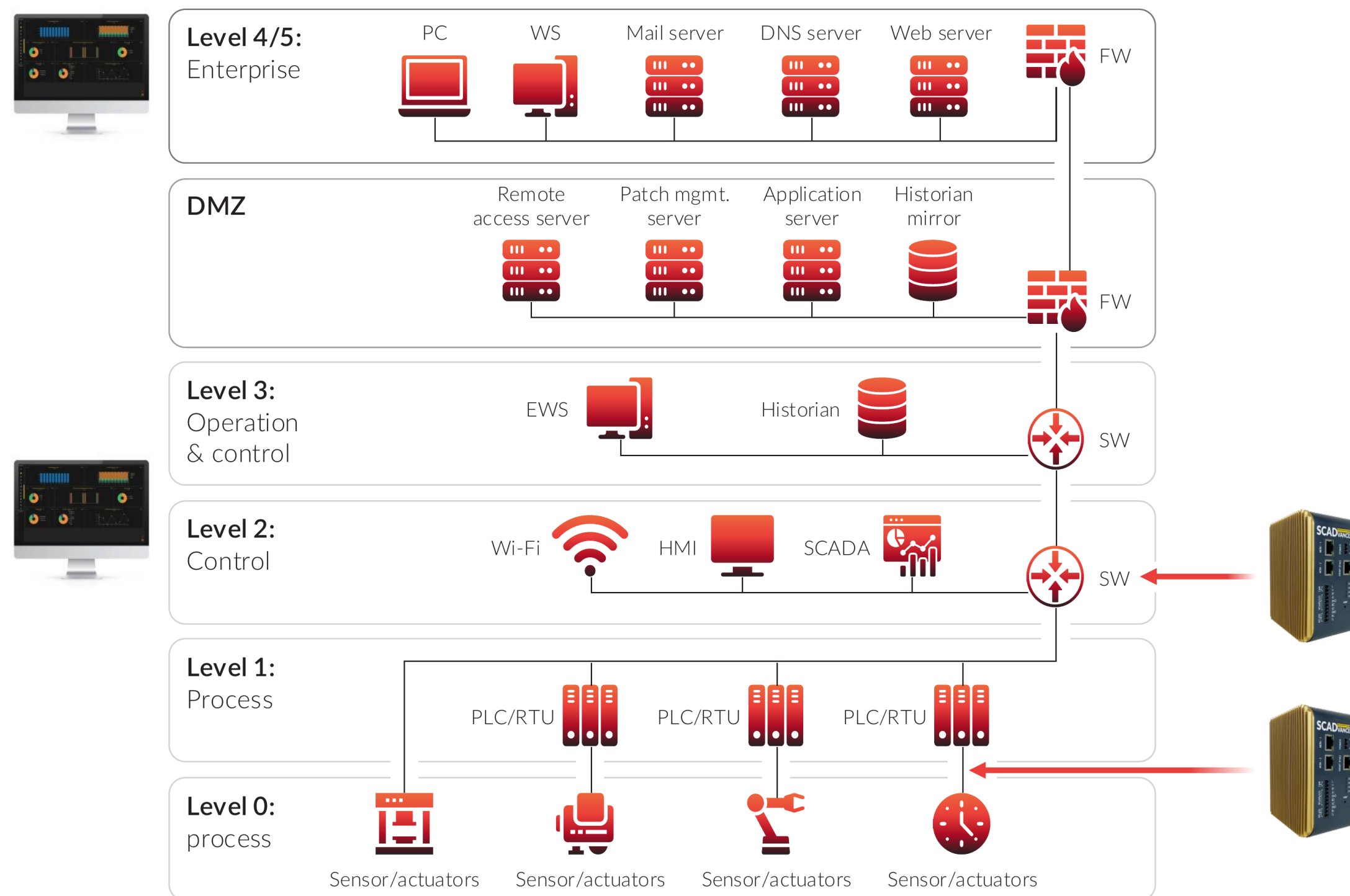
ICSEC

данни за доклад

ICSEC

отчети за
ръководството и
одитора

КЪДЕ В МРЕЖАТА РАБОТИ ICSEC



Офис (ИТ)

защитават го защитна стена и антивирус



Процес (ОТ)

контролери, HMI, SCADA – тук работи ICsec



Сондата само слуша

копие на трафика, 100% пасивно, без влияние върху процеса

НАШИЯТ ПРОДУКТ: ХАРДУЕР + СОФТУЕР



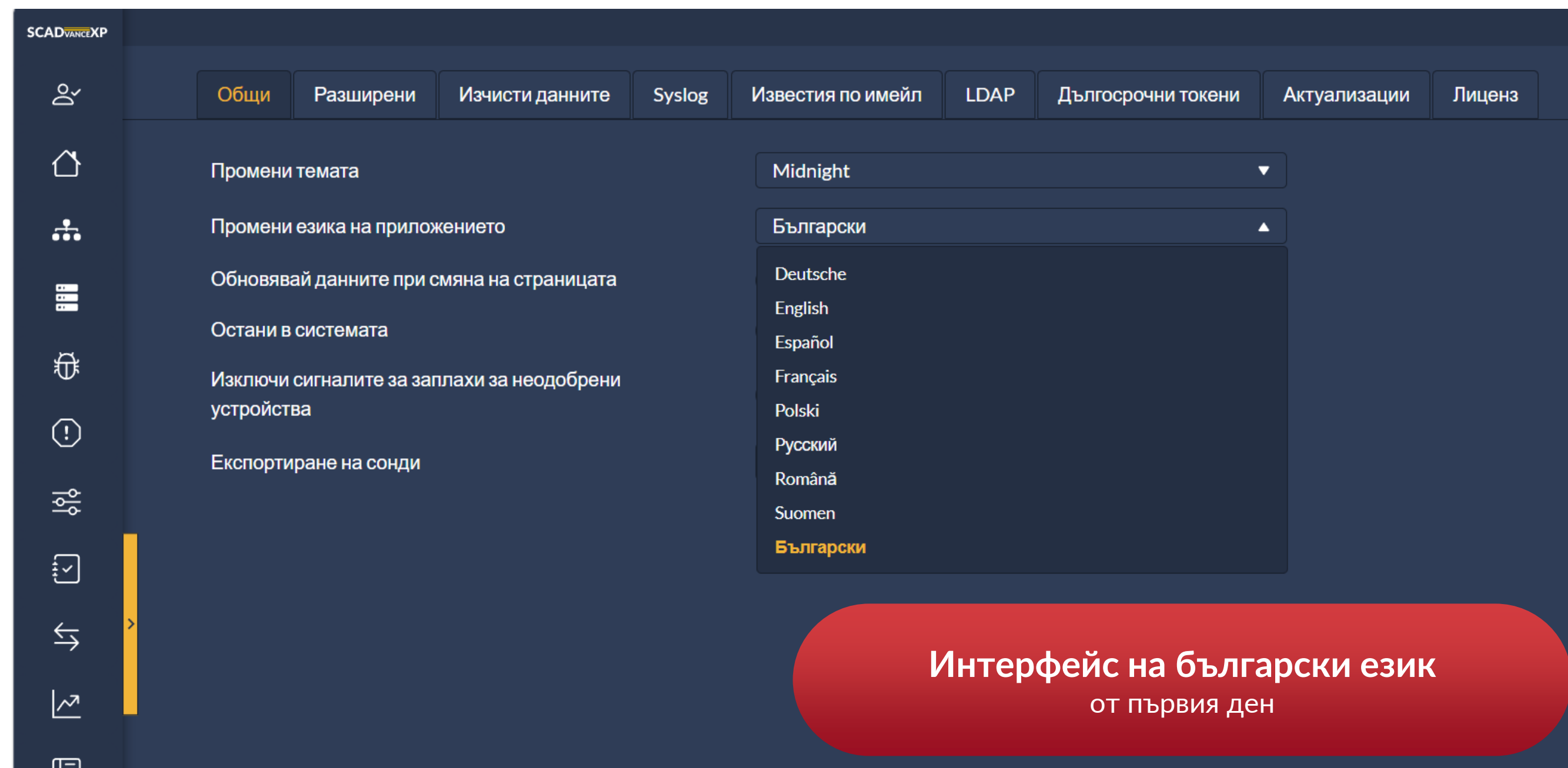
Сонда X1

хардуер, проектиран
и произведен в Полша

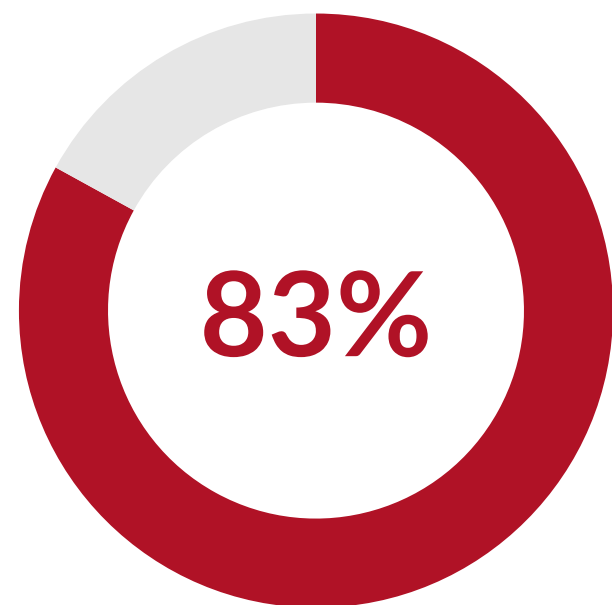


Аналитична система

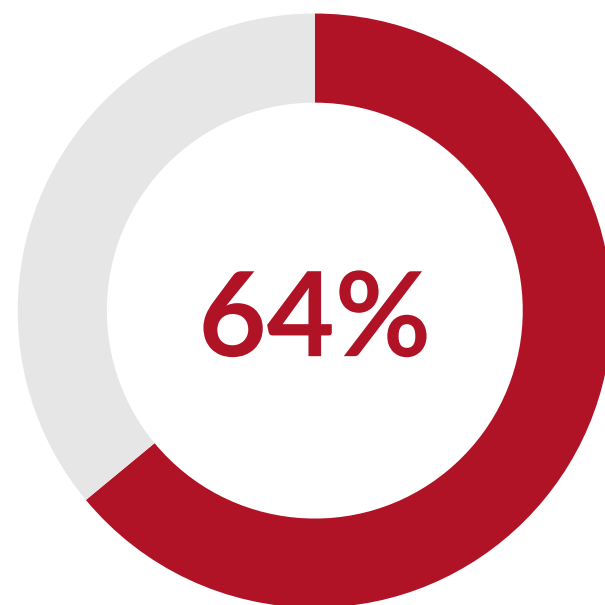
софтуер, работи в
сървърното на клиента



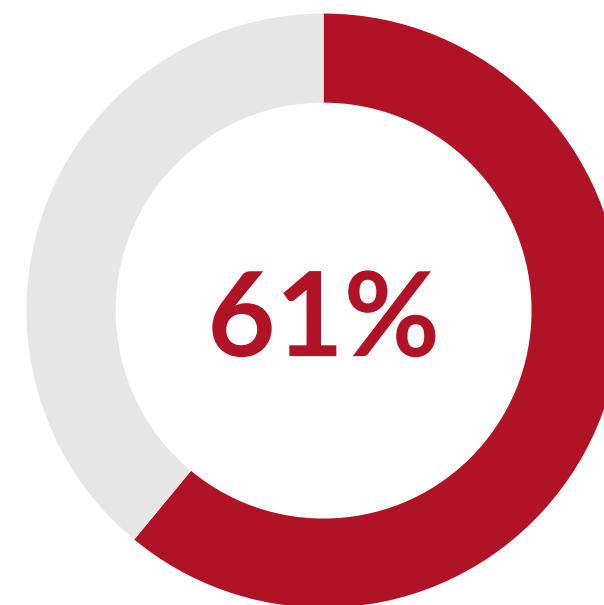
КАКВО ОТКРИВАМЕ В ОТ МРЕЖИТЕ



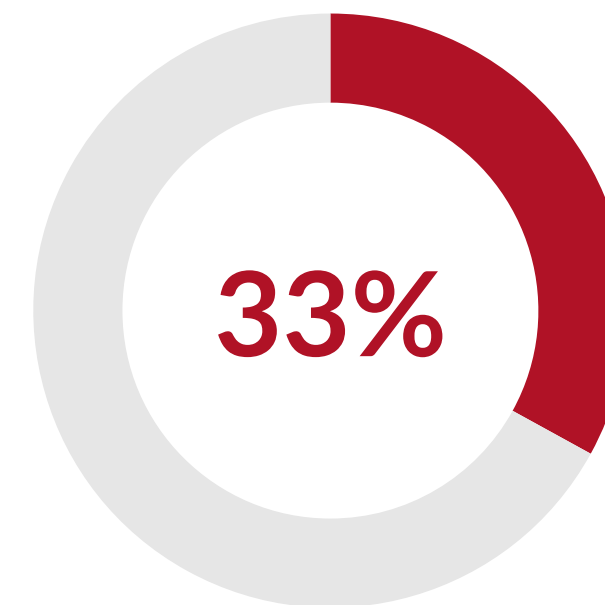
уязвими
устройства



OT устройства, достъпни
от интернет



UPnP – устройствата
сами отварят портове



камери за видеонаблюдение
в мрежата на контролерите

Операторът обикновено не знае за това – никой досега не е гледал тази мрежа.

Източник: анонимизирани резултати от тестове на OT мрежи, извършени от ICsec в Полша, 2021–2025 г.

ЕДНИ И СЪЩИ ЗАПЛАХИ, РАЗЛИЧЕН МАЩАБ

	<div> МАЛЪК напр. общинско ВиК</div>	<div> СРЕДЕН регионален оператор</div>	<div> ГОЛЯМ група с много обекти</div>
Размер	до 50 души, една община	50–1000 души, цял регион	1000+ души, няколко държави
Начална точка	„от нищо към нещо“	NIS2 е първата формална стъпка	пълен режим по NIS2, собствен SOC
Хора	един човек за ИТ и ОТ	компетенции, разпръснати по регионите	специализирани екипи
Решения	ръководството, доверие и цена	формални тестове	пилот и внедряване на етапи

ВНЕДРЯВАНЕТО НА ПРАКТИКА

	 МАЛЪК напр. общинско ВиК	 СРЕДЕН регионален оператор	 ГОЛЯМ група с много обекти
Познаване на мрежата	до 50% повече устройства от очакваното	регистрите на централата и регионите се различават	подредена инвентаризация
Мащаб	няколко обекта, до 1 000 устройства	стотици обекти, 10–20 хил. устройства	хиляди обекти, 100–300 хил. устройства
Внедряване	често едно посещение	съгласуване в регионите	отделен проект, на вълни
Цел на клиента	да види цялата мрежа	да види цялата мрежа в голям мащаб	да открие най-важните събития

Благодарим!
Dziękujemy!

Jan Markowski
+48 501 607 067
jan.markowski@icsec.pl

Paweł Tomala
+48 734 700 998
pawel.tomala@icsec.pl

ICsec Spółka Akcyjna
www.icsec.pl

