Kaspersky Industrial Cybersecurity Conference 2023

KASPERSKY INDUSTRIAL CYBERSECURITY

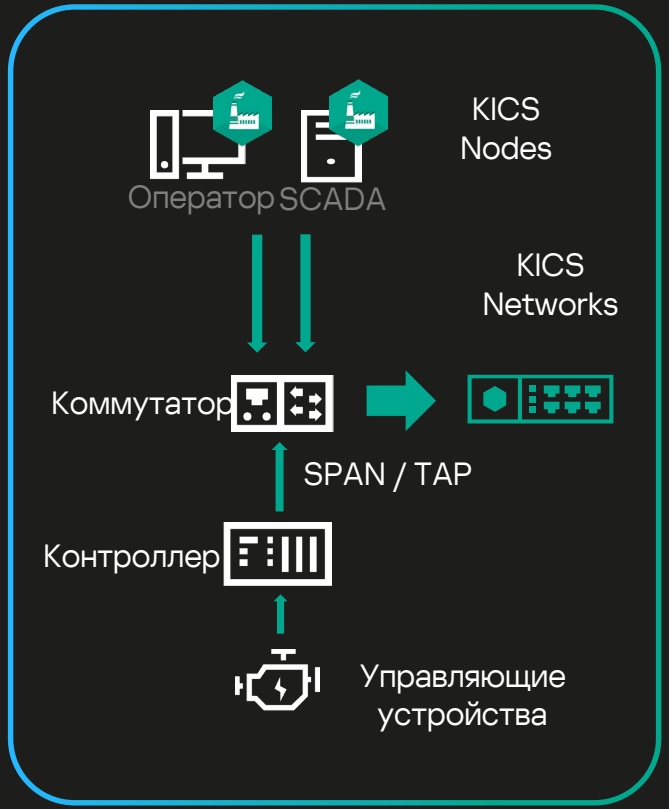
Объять необъятное – мониторинг телеметрии технологического процесса

Шмырев Денис Викторович

Заместитель директора
департамента информационной безопасности
Platformix

kaspersky

Функциональные модули KICS for Networks



AM **Asset and Vulnerability Management**
Инвентаризация активов и обнаружение уязвимостей промышленного оборудования

DPI **Deep Packet Inspection**
Контроль параметров технологических процессов в реальном времени

NIC **Network Integrity Control**
Контроль целостности сети

IDS **Intrusion Detection System**
Система обнаружения компьютерных атак

CC **Command Control**
Инспекция команд, передаваемых по промышленным протоколам

EXT **External Systems**
Получение событий из внешних источников внешние источники + корреляция событий

Контроль параметров технологического процесса

Сервера, диспетчерские и инженерные станции

Коммутатор

Контроллер

Управляющие устройства

Kaspersky Industrial CyberSecurity

kics-op...	OPC UA Bin...	Tag12	int32	int32	Нет	Tag12	48
kics-op...	OPC UA Bin...	Tag13	int64	int64	Нет	Tag13	84

TAG13
в рамках техпроцесса может быть от 50 до 100

50 — 100

если TAG13 100+

- Нарушение качества продукции
- Деструктивные воздействия
- Простой производства
- Повышенный износ механизмов

Сложности реализации

10+
производственных площадок

500+
систем автоматизации технологическим процессом

100 - 1000
тегов обрабатывается в рамках каждой АСУ ТП

Какие параметры необходимо контролировать?

контролируем **все доступные** параметры

! нереальные трудозатраты на реализацию и сопровождение

контролируем **только «важные»** параметры

? по каким критериям определить «важные» параметры

Выявление наиболее критичных систем автоматизации

Классификация и категорирование систем автоматизации

- Приказ ФСТЭК № 31
- Постановление Правительства РФ № 127
- Федеральный закон № 187

Список систем

Качественная и количественная оценка рисков

- ISO 27005
- ENISA
- NIST
- EBIOS Risk Manager

Список систем

ИТОГОВЫЙ СПИСОК
категорированных и/или классифицированных систем

Импорт проекта и профилирование

1 Импорт SCADA-проекта

- Импорт в (исходном) нативном формате
- Импорт через формат XML

2 Обучение системы

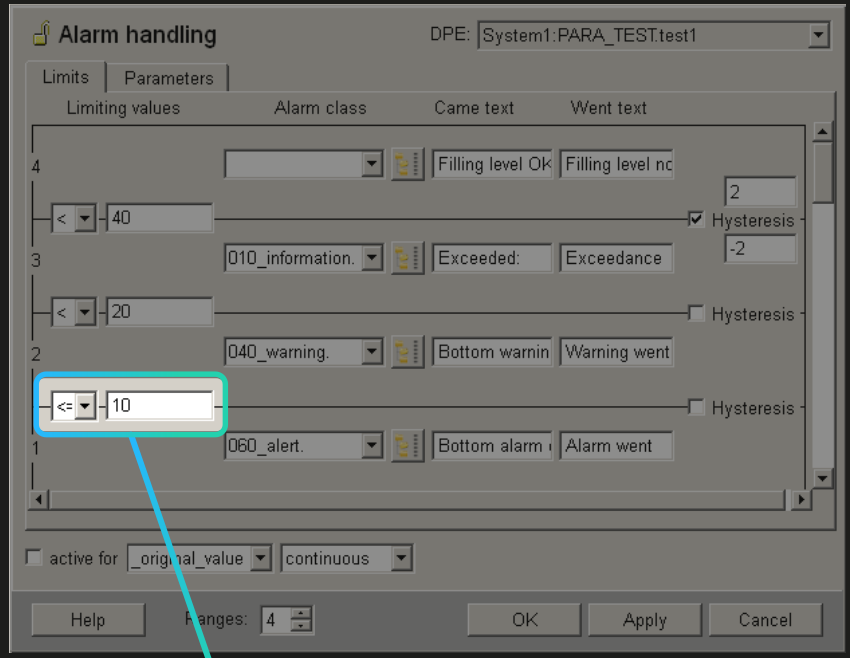
- Время обучения от нескольких часов до нескольких дней
- Автоматическое создание правил с диапазонами изменений

Анализ SCADA-проекта

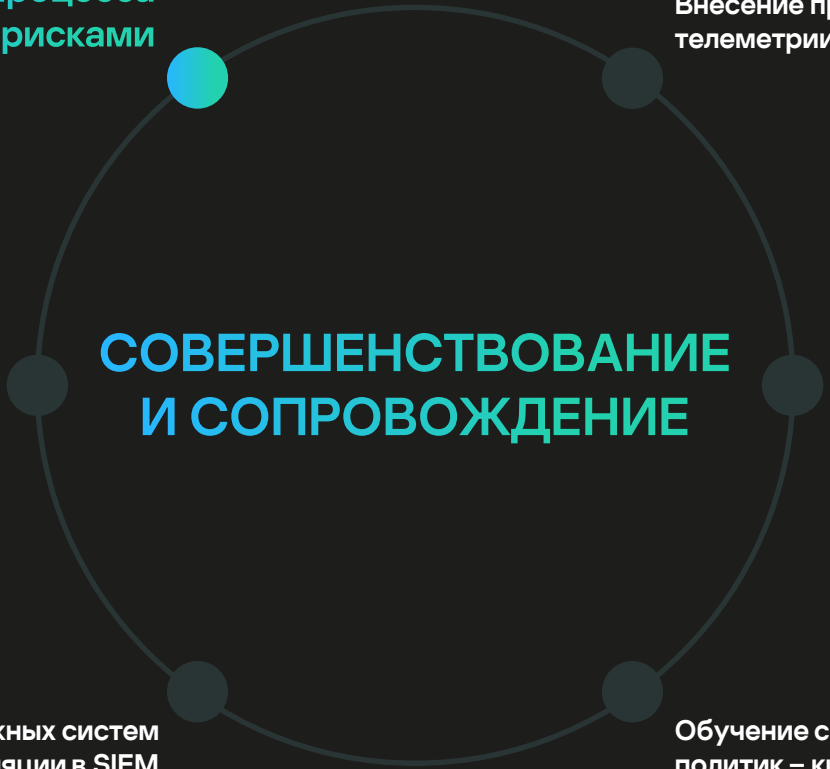
Карта уставок или параметры срабатывания автоматики безопасности

Значения ограничений закрепленные в SCADA проектах

Управляющие параметры или относительно параметра принимаются решения по корректировке работы процесса



значение для мониторинга



Пересмотр критичности в рамках процесса управления рисками

Внесение проработки мониторинга телеметрии в процесс проектного управления

Синхронизация изменений при обновлении SCADA проектов

Использование собственного инцидентного опыта

Адаптация смежных систем и правил корреляции в SIEM

Обучение специалистов и тестирование политик – киберучения и исследования на цифровых двойниках

СОВЕРШЕНСТВОВАНИЕ И СОПРОВОЖДЕНИЕ

Пересмотр критичности в рамках процесса управления рисками

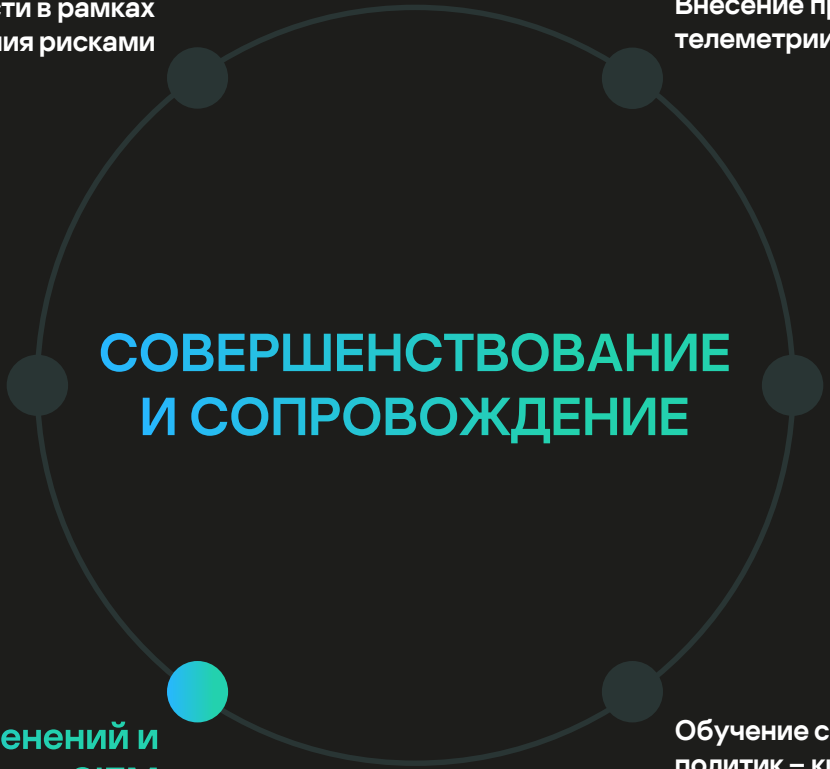
Внесение проработки мониторинга телеметрии в процесс проектного управления

Синхронизация изменений при обновлении SCADA проектов

Использование собственного инцидентного опыта

Адаптация изменений и правил корреляции в SIEM

Обучение специалистов и тестирование политик – киберучения и исследования на цифровых двойниках



Пересмотр критичности в рамках процесса управления рисками

Внесение проработки мониторинга телеметрии в процесс проектного управления

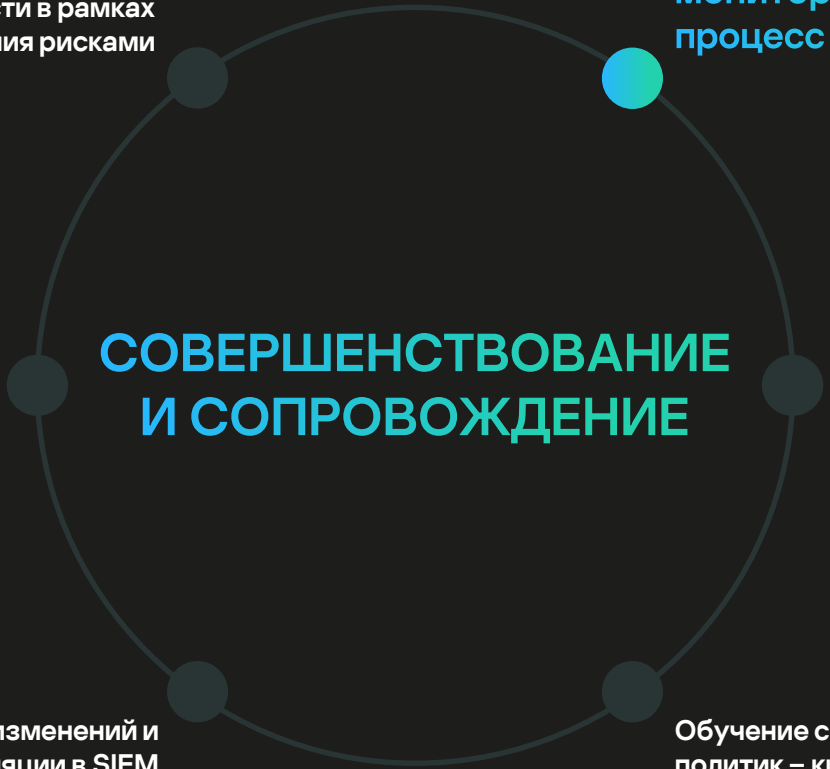
Синхронизация изменений при обновлении SCADA проектов

Использование собственного инцидентного опыта

Адаптация изменений и правил корреляции в SIEM

Обучение специалистов и тестирование политик – киберучения и исследования на цифровых двойниках

СОВЕРШЕНСТВОВАНИЕ И СОПРОВОЖДЕНИЕ



Внесение проработки мониторинга телеметрии в процесс проектного управления

Использование собственного инцидентного опыта

Обучение специалистов и тестирование политик – киберучения и исследования на цифровых двойниках

Адаптация изменений и правил корреляции в SIEM

Синхронизация изменений при обновлении SCADA проектов

Пересмотр критичности в рамках процесса управления рисками

СОВЕРШЕНСТВОВАНИЕ И СОПРОВОЖДЕНИЕ

Пересмотр критичности в рамках процесса управления рисками

Внесение проработки мониторинга телеметрии в процесс проектного управления

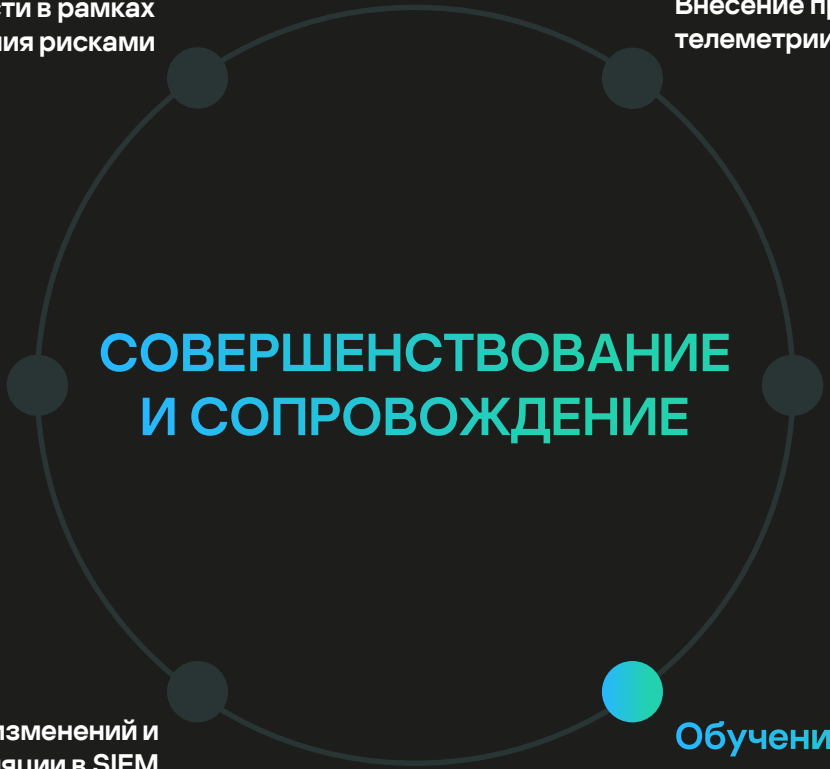
Синхронизация изменений при обновлении SCADA проектов

Использование собственного инцидентного опыта

Адаптация изменений и правил корреляции в SIEM

Обучение специалистов и тестирование политик – киберучения и исследования на цифровых двойниках

СОВЕРШЕНСТВОВАНИЕ И СОПРОВОЖДЕНИЕ



Пересмотр критичности в рамках процесса управления рисками

Внесение проработки мониторинга телеметрии в процесс проектного управления

Синхронизация изменений при обновлении SCADA проектов

Использование собственного инцидентного опыта

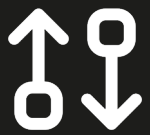
Адаптация изменений и правил корреляции в SIEM

Обучение специалистов и тестирование политик – киберучения и исследования на цифровых двойниках

ВАЖНО ВОВРЕМЯ

ОСТАНОВИТЬСЯ

Противоаварийная защита и карта аварийных уставок

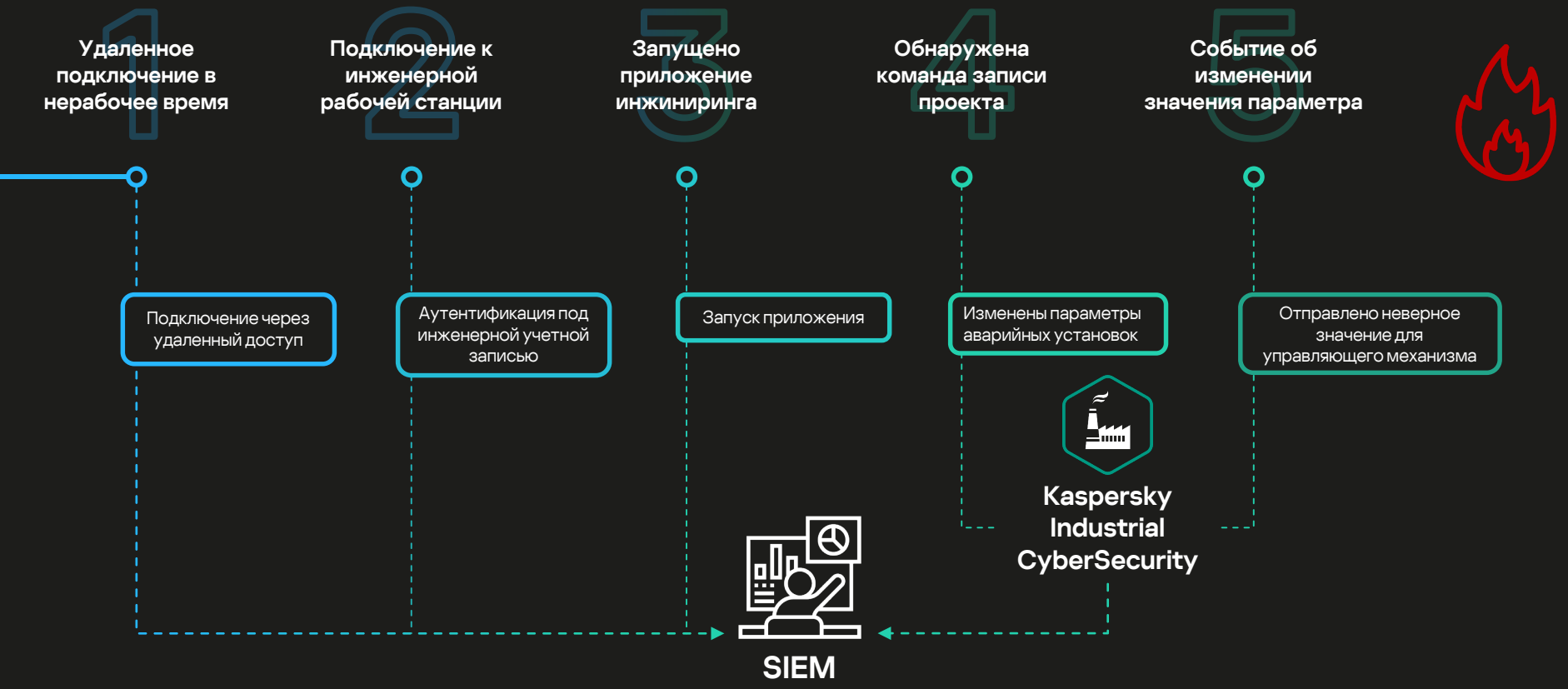


Параметры изменили несанкционированно

Параметры изменили случайно

Ошибка или сбой в работе системы

Моделирование сценария атаки



Специфика рисков в технологическом сегменте

сложность реализации

высокая

вероятность реализации

минимальная

ущерб от реализации

колоссальный

Вероятный ущерб

- Нарушение качества продукции
- Деструктивные воздействия
- Простой производства
- Повышенный износ механизмов

Прогнозирование событий

Сервера, диспетчерские и инженерные станции

Коммутатор

Контроллер

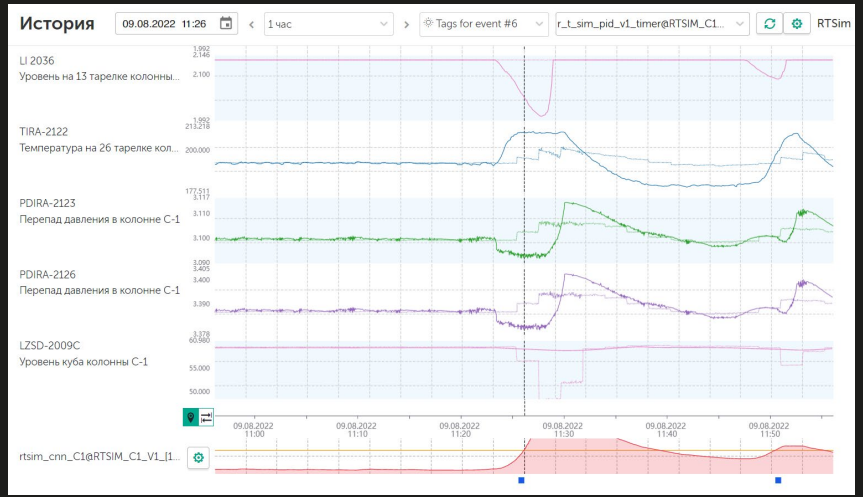
Управляющие устройства

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Industrial CyberSecurity

Детектор аномалий на основе искусственного интеллекта

- Ранее обнаружение отклонений и оповещение оператора
- Защита против специализированных атак и ошибок персонала
- Предотвращение сбоев и аварий, вызванных отказом оборудования
- Пассивный детектор: смотрим – находим – извещаем



Подведение итогов

Выявление наиболее критичных систем и определение ландшафта угроз

Профилирование взаимодействий и использование встроенных средств автоматизации

Анализ SCADA проектов выявление критичных параметров

ГК «БАЗОВЫЕ РЕШЕНИЯ»

Предлагает полный спектр решений и услуг в области построения надежных санкционно устойчивых корпоративных ИТ-инфраструктур

Platformix

Системный интегратор

Создание, защита и развитие
ИТ-инфраструктур заказчиков с 1992 года

СИЛА

Вендор

Производство корпоративного
ИТ-оборудования, разработка ПО

Нам доверяют:

Альфа-Банк, Unilever, Volvo, ФОСАГРО, СОВКОМБАНК, КАНОНФАРМА продакшн, М.видео, TELE2, Почта России, DECATHLON, Лукойл-Гарант, Негосударственный пенсионный фонд, ОИЯИ, РЖД, ОДК | Пермские моторы, beko, PHILIPS, ОСТАНКИНО, СИБУР, МТТ, открытие, Ford, Ренессанс Банк, AMGEN, Kellogg's, ГЛАВСТРОЙ, РОСБАНК

и еще более 2400 компаний

Platformix

Контактная информация


8 495 967 80 50 для звонков из Москвы


8 800 600 33 55 для звонков по России


info@platformix.ru

platformix.ru
127018, г. Москва, ул. Складочная, д. 3, стр. 1