udv|group

Экосистема решений UDV Group для обеспечения кибербезопасности промышленных предприятий

Алексей Шанин
Директор ООО «СайберЛимфа»
UDV Group

CyberLympha®

ePlat4m

udv|group

РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ДЛЯ КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

udv|group

РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ДЛЯ КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

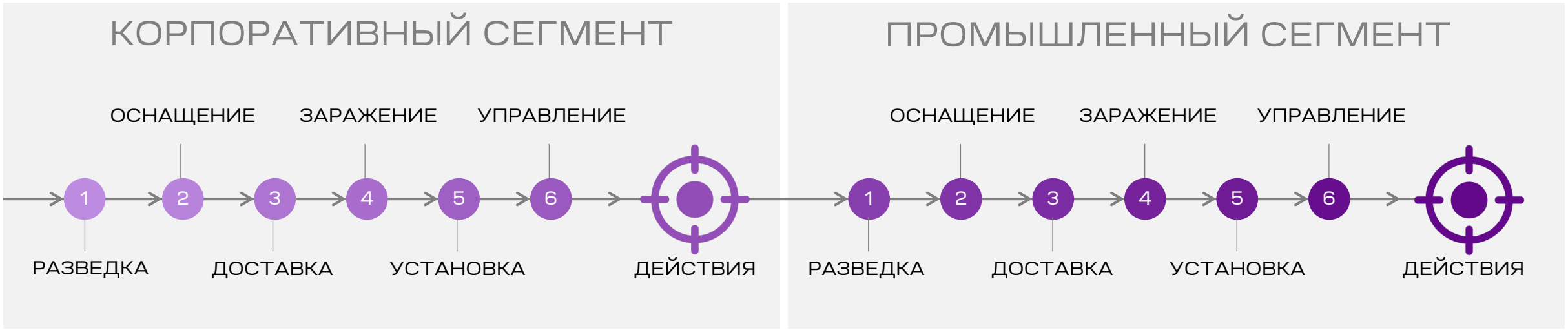
БОЛЕЕ 10 ЛЕТ ЭКСПЕРТИЗЫ ИБ АСУ ТП

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

СОБСТВЕННЫЙ R&D И ЛАБОРАТОРИЯ КИБЕРБЕЗОПАСНОСТИ

ДЕЛОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ ПАРТНЁРЫ

Множество способов реализации угроз на каждом этапе цепочки

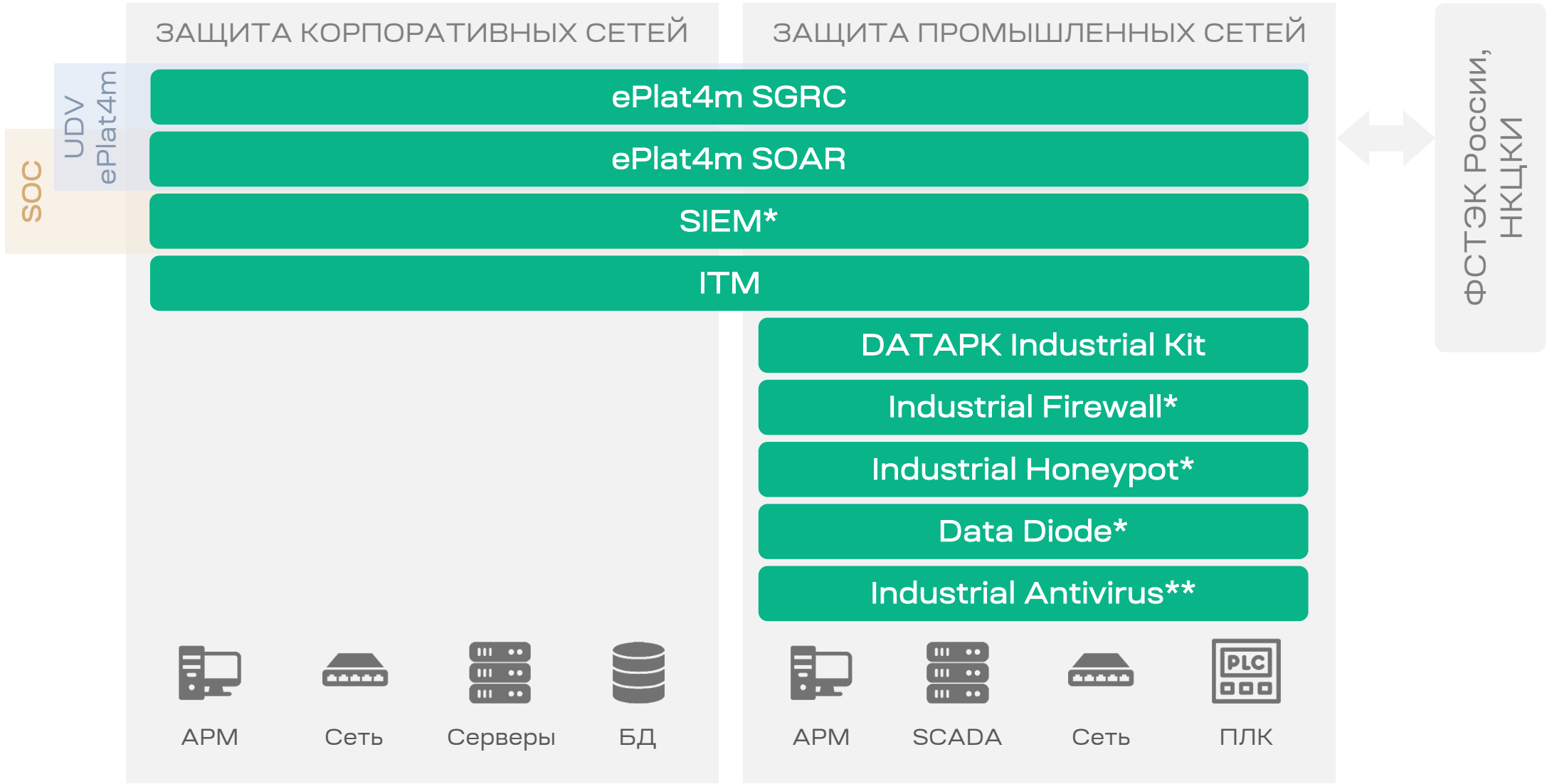


- Использование рабочих станций в личных целях
- Удалённый доступ персонала
- Использование беспроводных сетей
- Инсайдеры
- Социальный инжиниринг
- . . .

- Подключение устройств из закрытого сегмента к интернету
- Подключение съемных носителей
- Удаленный доступ подрядчиков
- Внесение изменений в настройки безопасности
- . . .

ДЛЯ ЗАЩИТЫ ПРОМЫШЛЕННЫХ СЕГМЕНТОВ ТРЕБУЕТСЯ МНОЖЕСТВО ИНСТРУМЕНТОВ, РАБОТАЮЩИХ ВМЕСТЕ

Экосистема решений UDV Group



* Включено в дорожную карту развития продуктовой линейки на 2023 год. ** Партнёрское решение.

Оперативное обнаружение инцидентов ИБ в промышленных сетях

UDV ePlat4m

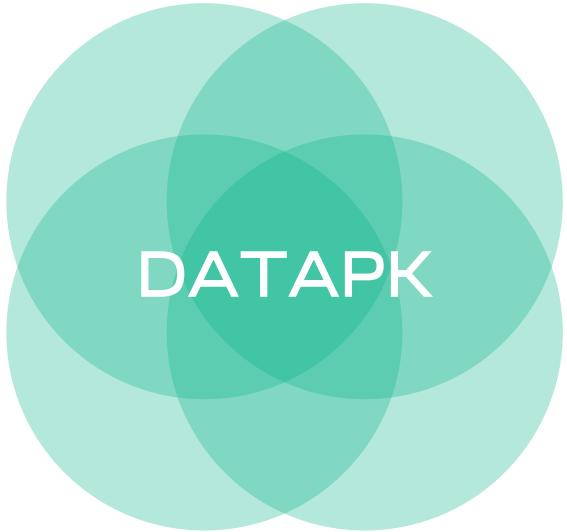
- ePlat4m SGRC — Менеджмент ИБ-процессов организации и управление соответствием требованиям
- ePlat4m SOAR — Оркестрация СЗИ, реагирование на инциденты и автоматизация функций ИБ
- SIEM* — Мониторинг функционирования ИТ-инфраструктуры, выявление инцидентов
- ITM
- DATAPK Industrial Kit — Выявление и инвентаризация узлов, обнаружение инцидентов, управление конфигурациями и уязвимостями

* Включено в дорожную карту развития продуктовой линейки на 2023 год

DATAPK Industrial Kit больше чем СОВ для АСУ ТП

АНАЛИЗ
СЕТЕВОГО ТРАФИКА

УПРАВЛЕНИЕ
КОНФИГУРАЦИЯМИ



ОБНАРУЖЕНИЕ
ИНЦИДЕНТОВ

УПРАВЛЕНИЕ
УЯЗВИМОСТЯМИ

- Замена нескольких разнородных решений единым комплексом, разработанным для промышленных предприятий
- Снижение общей стоимости приобретения и владения
- Выполнение требований регулятора и реализация мер 31 и 239 приказов ФСТЭК России
- Оптимизация процессов управления ИБ в организации

Режимы работы DATAPK Industrial Kit

РЕЖИМ НАБЛЮДЕНИЯ

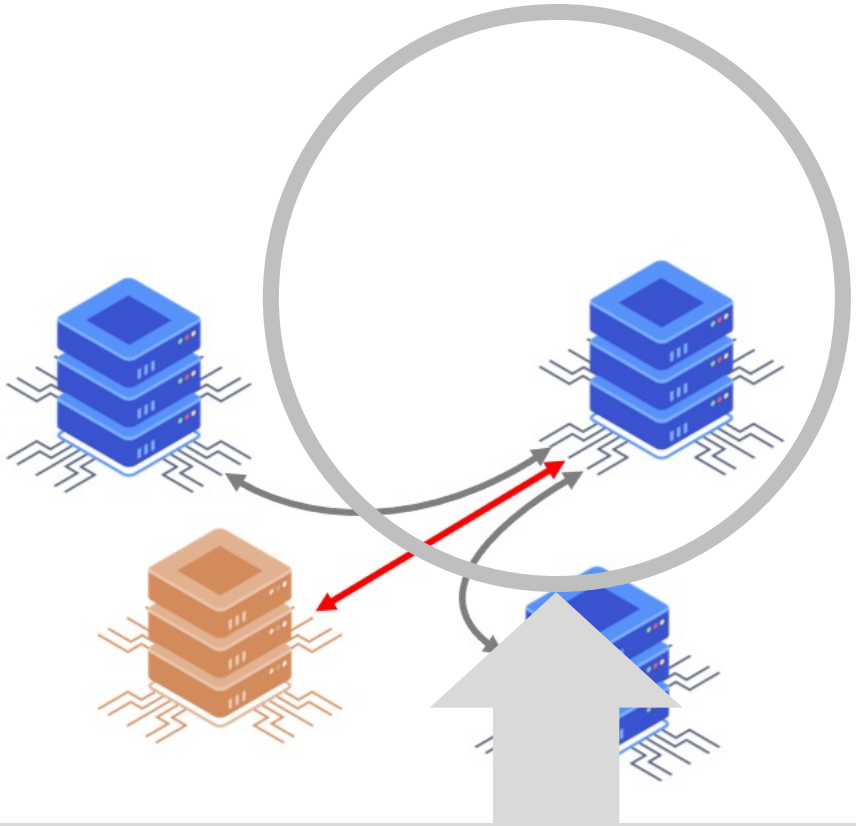
- Однонаправленное получение данных
- Прослушивание трафика и прием событий
- Возможно подключение через диод данных, для гарантии отсутствия влияния на объекты защиты

РЕЖИМ ЗАПРОС - ОТВЕТ

- Получение конфигураций и событий
- Взаимодействие с объектами защиты в режиме «запрос-ответ» с использованием штатных механизмов и протоколов
- Выявление уязвимостей и проверки на соответствие требованиям ИБ

ФУНКЦИИ	РЕЖИМ НАБЛЮДЕНИЯ	РЕЖИМ ОПРОСА
Сбор событий ИБ	✗✓	✓
Обнаружение атак	✓	✓
Выявление сетевых аномалий	✓	✓
Сбор конфигураций	✗	✓
Определение текущего состава ОЗ	✓	✓
Выявление изменений в составе ОЗ	✓	✓
Проверка ОЗ на наличие уязвимостей	✗✓	✓

Оперативное обнаружение инцидентов ИБ в промышленных сетях



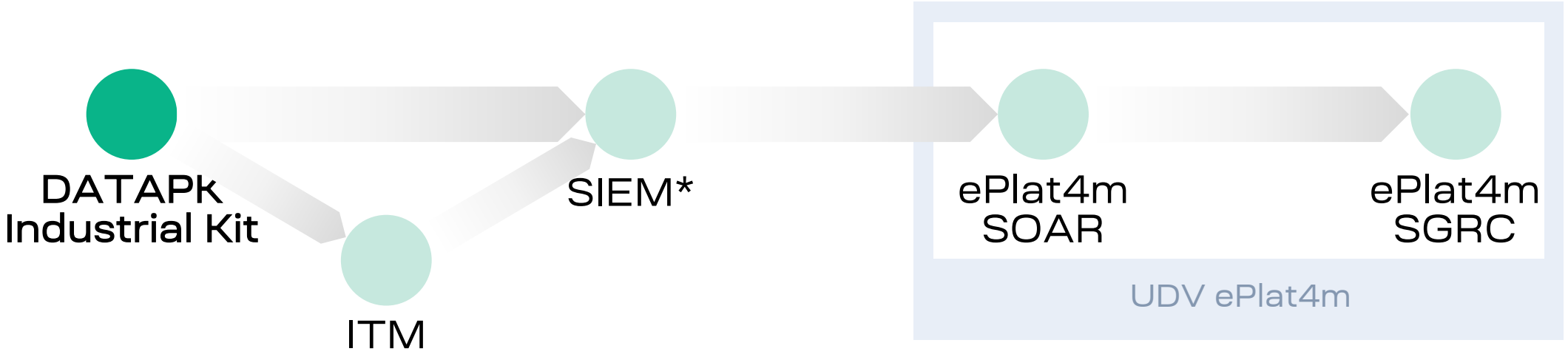
udv DATAPK Industrial Kit

Машинное обучение

- Восстановление структуры закрытых промышленных протоколов
- Мониторинг отклонений от эталонных моделей и обнаружение несанкционированных изменений в АСУ ТП

? ? ? ? ? ? ?

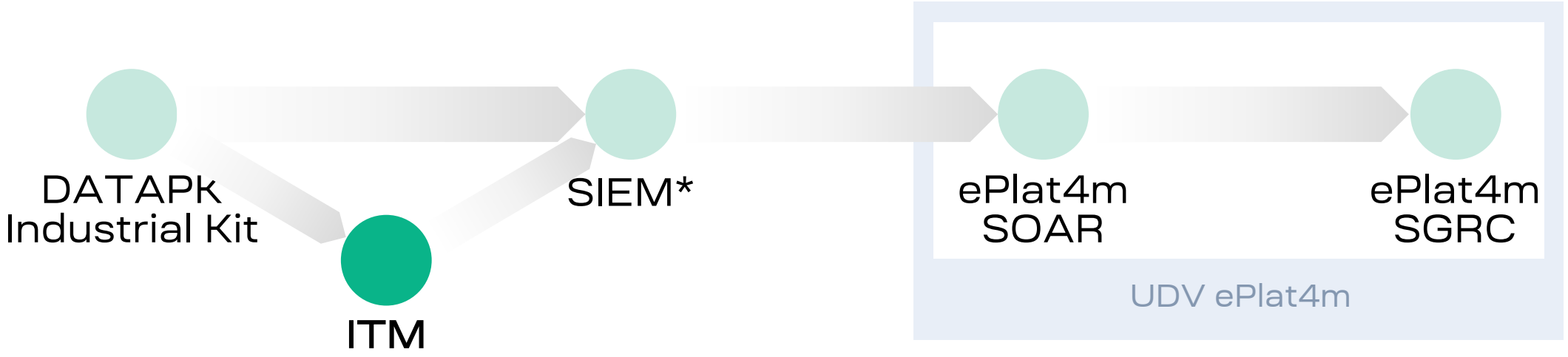
Интеграция решений UDV для защиты промышленных сетей



- CL DATAPK 2.0: новая архитектура, интерфейс и механизмы поиска уязвимостей
- Облегченная редакция CL DATAPK Lite
- Интеграция с модулями выявления аномалий

* Включено в дорожную карту развития продуктовой линейки на 2023 год

Интеграция решений UDV для защиты промышленных сетей



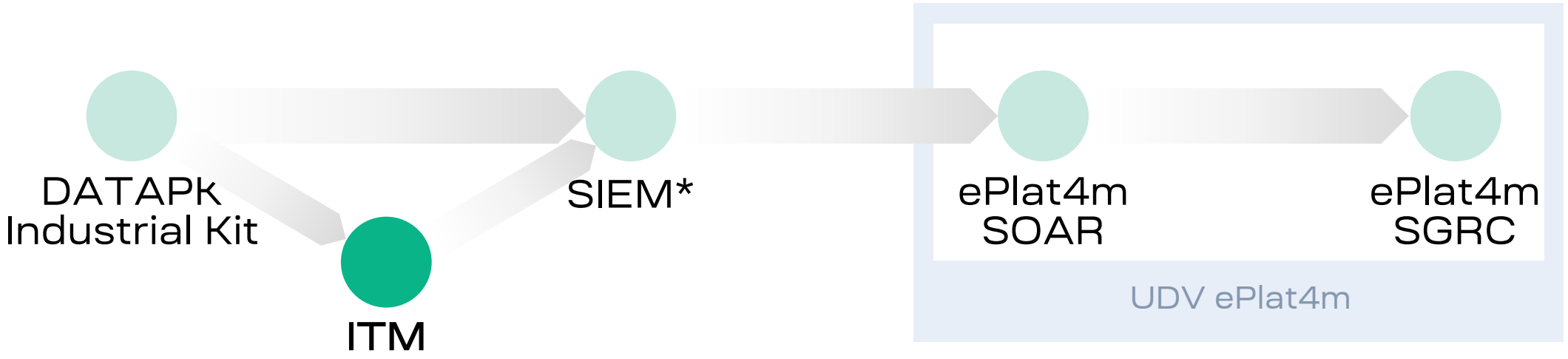
Единое решение для мониторинга удалённых площадок и филиалов

Расширяет и адаптирует функции существующих систем мониторинга

Включено в Реестр российских программ и БД, сертифицировано ФСТЭК России

* Включено в дорожную карту развития продуктовой линейки на 2023 год

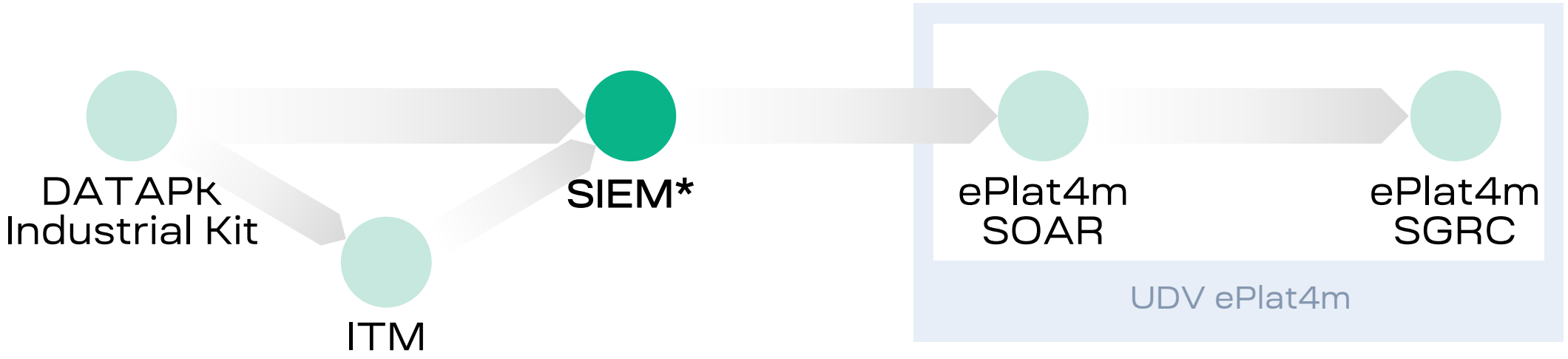
Интеграция решений UDV для защиты промышленных сетей



- Облачный сервис мониторинга состояния оборудования в условиях невозможности поддержки зарубежными вендорами
- Выявление инцидентов ИБ на основе аномальных показателей нагрузки на средства вычислительной техники

* Включено в дорожную карту развития продуктовой линейки на 2023 год

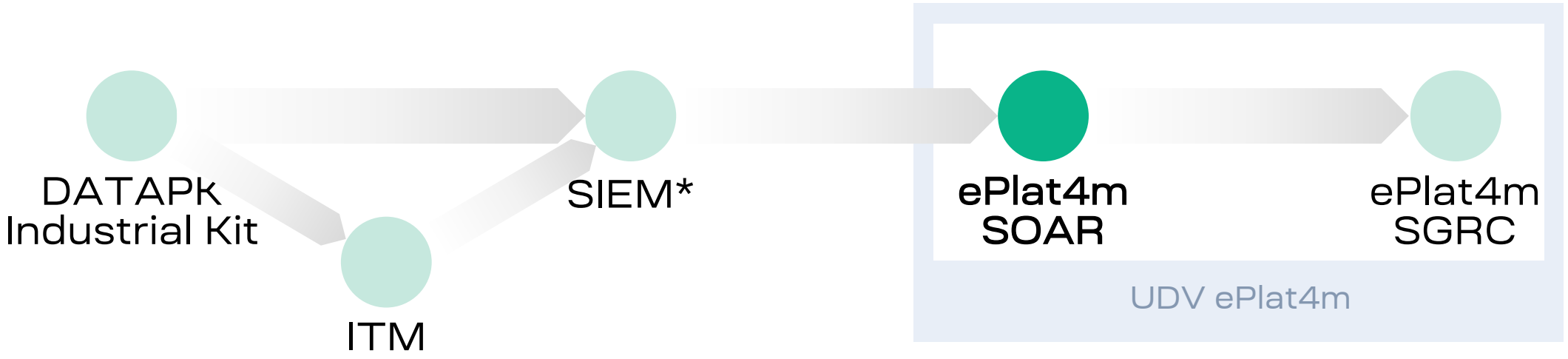
Интеграция решений UDV для защиты промышленных сетей



Осуществляет мониторинг и управление событиями ИБ в режиме реального времени. Реализует сбор и корреляцию событий безопасности, отображение и поиск данных. Является источником данных о возможных инцидентах для UDV SOAR. Обеспечивает долгосрочное хранение событий для ретроспективного анализа.

* Включено в дорожную карту развития продуктовой линейки на 2023 год

Интеграция решений UDV для защиты промышленных сетей



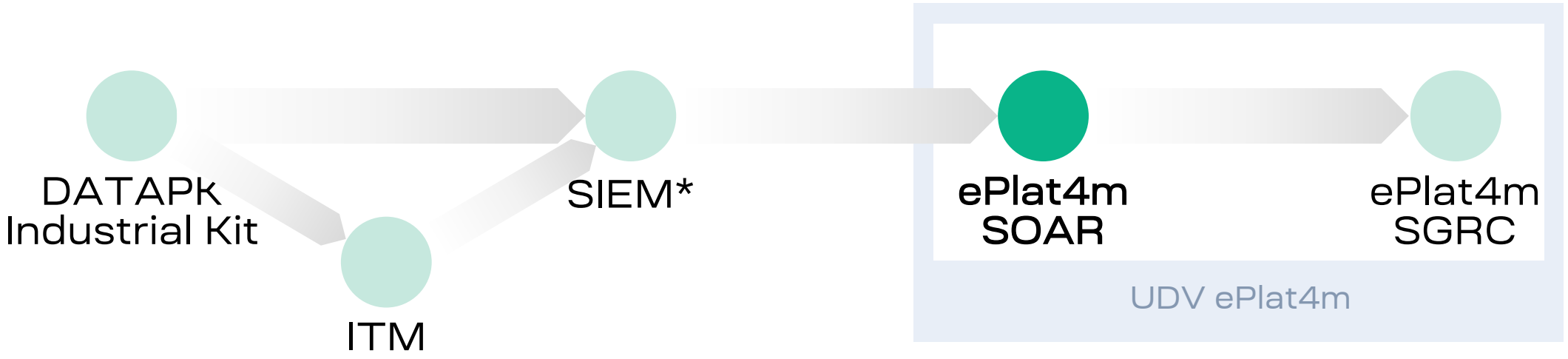
Уменьшение числа обрабатываемых «вручную» инцидентов с **10 000** до **500**

Снижение времени реагирования на инцидент с **3 дней** до **25 минут**

Автоматическая реакция для **30%** инцидентов

* Включено в дорожную карту развития продуктовой линейки на 2023 год

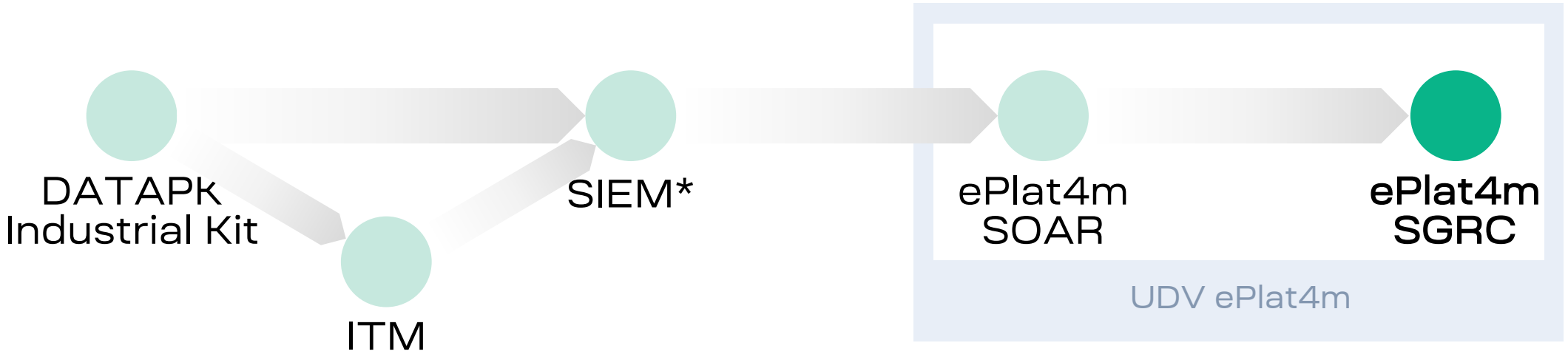
Интеграция решений UDV для защиты промышленных сетей



- Обогащение данными и сопоставление с индикаторами компрометации
- Реализация процесса реагирования и интеграция со смежными системами
- Оценка последствий инцидентов
- База знаний и рекомендации по реагированию
- Контроль SLA и отчетность

* Включено в дорожную карту развития продуктовой линейки на 2023 год

Интеграция решений UDV для защиты промышленных сетей



Управление категорированием объектов КИИ	Учет и классификация объектов защиты	Управление инцидентами по ИБ	Управление угрозами и уязвимостями ИБ	Управления контролем состояния безопасности	Управление мероприятиями по обеспечению ИБ
Моделирование угроз безопасности	Работа с персоналом и третьими лицами по вопросам ИБ	Управление рисками	Взаимодействие с НКЦКИ	Управление требованиями (документами) по ИБ	Управление обработкой персональных данных

* Включено в дорожную карту развития продуктовой линейки на 2023 год

Перспективные решения для защиты промышленных сетей

UDV Industrial Firewall*

Межсетевой экран типа «Д» на базе архитектуры RISK-V с аппаратным ускорением обработки трафика

UDV Data Diode*

Комбинация диода данных и ответвителя трафика (TAP) с аппаратным байпасом

UDV Industrial Honeypot*

Расширение возможностей системы мониторинга состояния защищенности АСУ ТП

UDV Industrial Antivirus**

Партнерское решение.
Coming soon :)

* Включено в дорожную карту развития продуктовой линейки на 2023 год. ** Партнёрское решение.

udv|group


АУДИТ
ПИЛОТИРОВАНИЕ
ИСПЫТАНИЯ
КОНСАЛТИНГ
ПРОЕКТИРОВАНИЕ
ВНЕДРЕНИЕ
ПОДДЕРЖКА

udv|group

СПАСИБО ЗА ВНИМАНИЕ!

Закажите пилотный проект или персональную демонстрацию наших решений

commercial@udv.group

udv.group

Присоединитесь к сообществу «Кибербезопасность АСУ ТП» / RUSCADASEC

RUSCADASEC

Независимая некоммерческая инициатива по развитию открытого русскоязычного международного сообщества специалистов
по промышленной кибербезопасности / кибербезопасности АСУ ТП

Целями инициативы являются повышение осведомлённости и квалификации специалистов по безопасности и промышленной автоматизации, развитие профессиональных связей между специалистами и организациями, содействие развитию рынка, развитие связей с профильными международными сообществами, и в итоге повышение уровня безопасности на промышленных предприятиях

www.ruscadasec.ru

Группа Telegram
«Кибербезопасность АСУ ТП»

https://t.me/RUSCADASEC