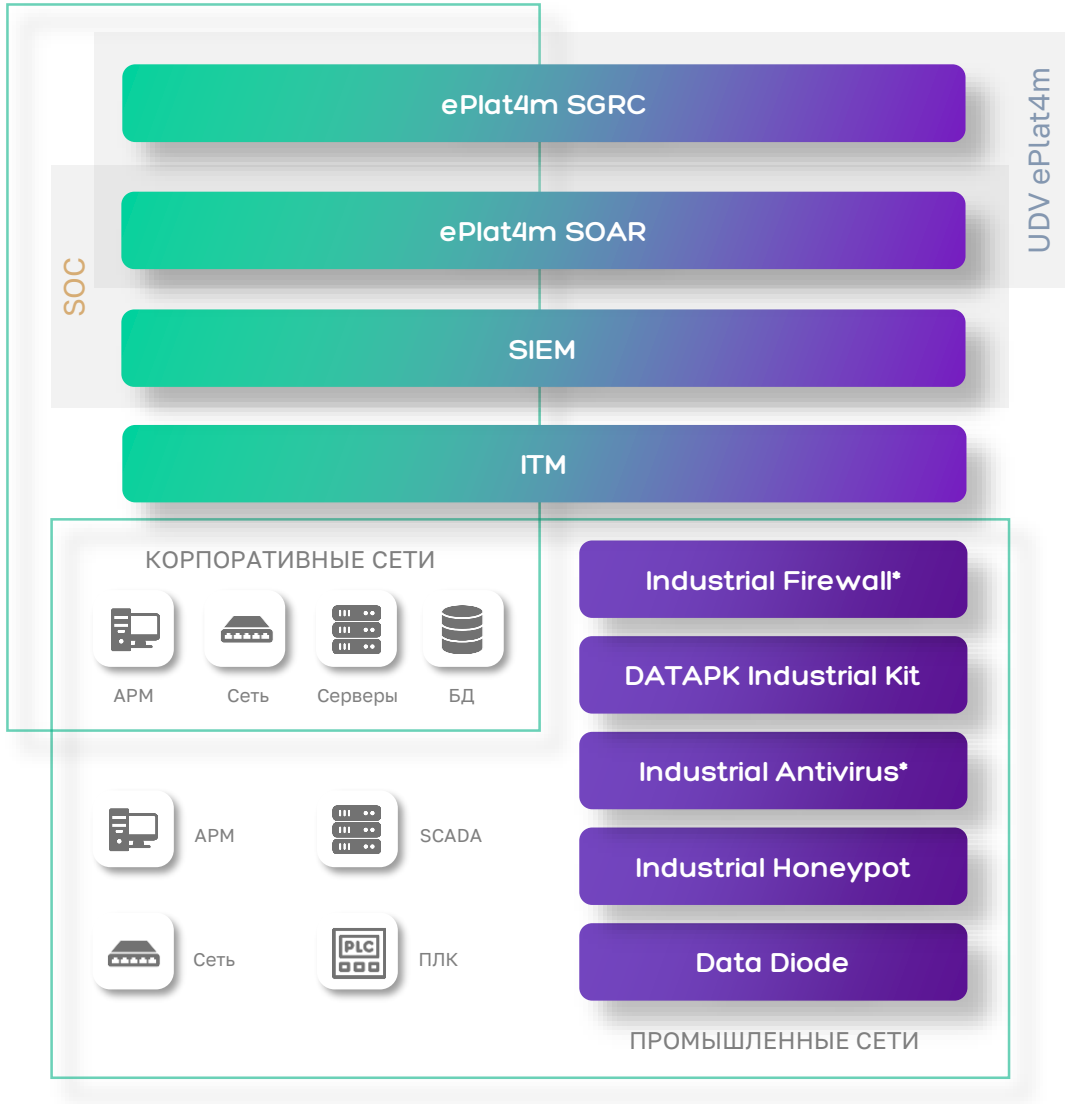
Экосистема решений UDV Group в области кибербезопасности

Валов Илья
Пресейл инженер
Техническая поддержка продаж
UDV Group

РОССИЙСКИЙ РАЗРАБОТЧИК В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ
ДЛЯ ПРОМЫШЛЕННЫХ И КОРПОРАТИВНЫХ СЕТЕЙ

Экосистема решений UDV Group



- Защита АСУ ТП и объектов КИИ
- Мониторинг ИБ и реагирование на инциденты
- Автоматизация бизнес-процессов

* Партнёрское решение.

udv|group

Типовые задачи в области кибербезопасности промышленных сетей

Насколько уязвим объект защиты? Правильно ли сконфигурированы узлы?

ИНВЕНТАРИЗАЦИЯ ПРОМЫШЛЕННОЙ СЕТИ

АНАЛИЗ НА НАЛИЧИЕ УЯЗВИМОСТЕЙ

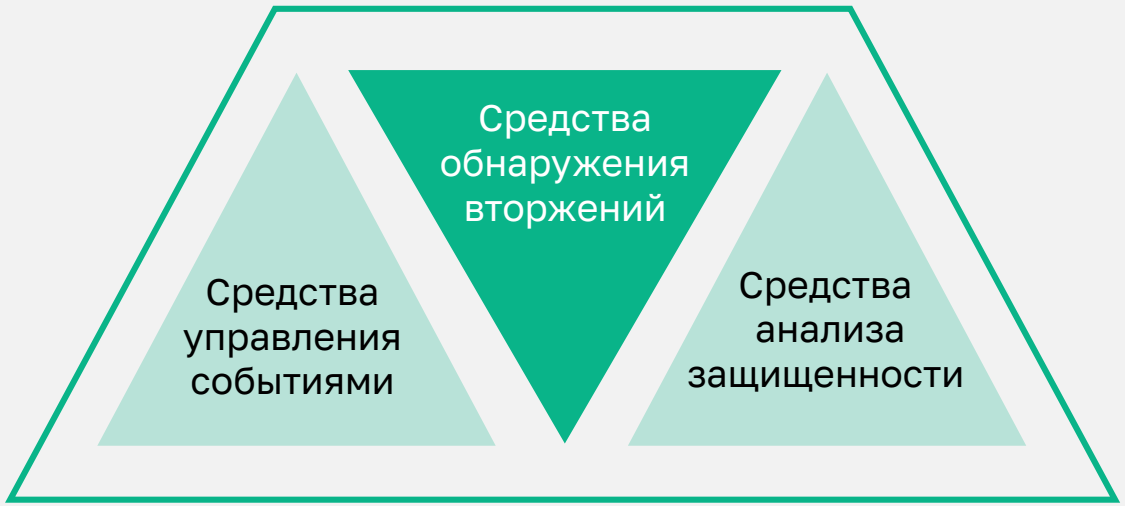
МОНИТОРИНГ

Что является объектом защиты? Из каких узлов состоит? Как они взаимодействуют?

- Фиксация и регистрация событий ИБ
- Анализ и корреляция событий ИБ
- Контроль конфигураций и соответствия настроек
- Поиск и контроль уязвимостей
- Контроль доступности оборудования, ресурсов и каналов

Оперативное обнаружение инцидентов ИБ в промышленных сетях

CyberLympha DATAPK → udv DATAPK Industrial Kit



Классы средств защиты информации в соответствии с Приказом №235 ФСТЭК России

- Создан для АСУ ТП и учитывает все требования к средствам защиты информации
- Реализует все необходимые возможности класса промышленных СОВ
- Обладает дополнительным функционалом нескольких классов решений
- Сертифицирован ФСТЭК России[1]
- Защищает значимые объекты КИИ в РФ[2]
- Протестирован производителями АСУ ТП[3]

1 – Сертификат №4451 от 27.09.2021 ФСТЭК России по требованиям профиля защиты СОВ уровня сети, уровням доверия в соответствии с Приказом №76 от 2 июня 2020 года.
2 – «Северсталь» и УЦСБ завершили один из этапов построения системы защиты https://www.severstal.com/rus/media/news/document22118.phtml, информация о внедрениях на других предприятиях является конфиденциальной.
3 – Schneider Electric и компания «СайберЛимфа» успешно завершили испытания совместимости программных комплексов https://www.se.com/ru/ru/about-us/newsroom/news/press-releases/, информация о тестировании с другими производителями предоставляется по запросу.

Архитектура DATAPK Industrial Kit

SUPERVISION

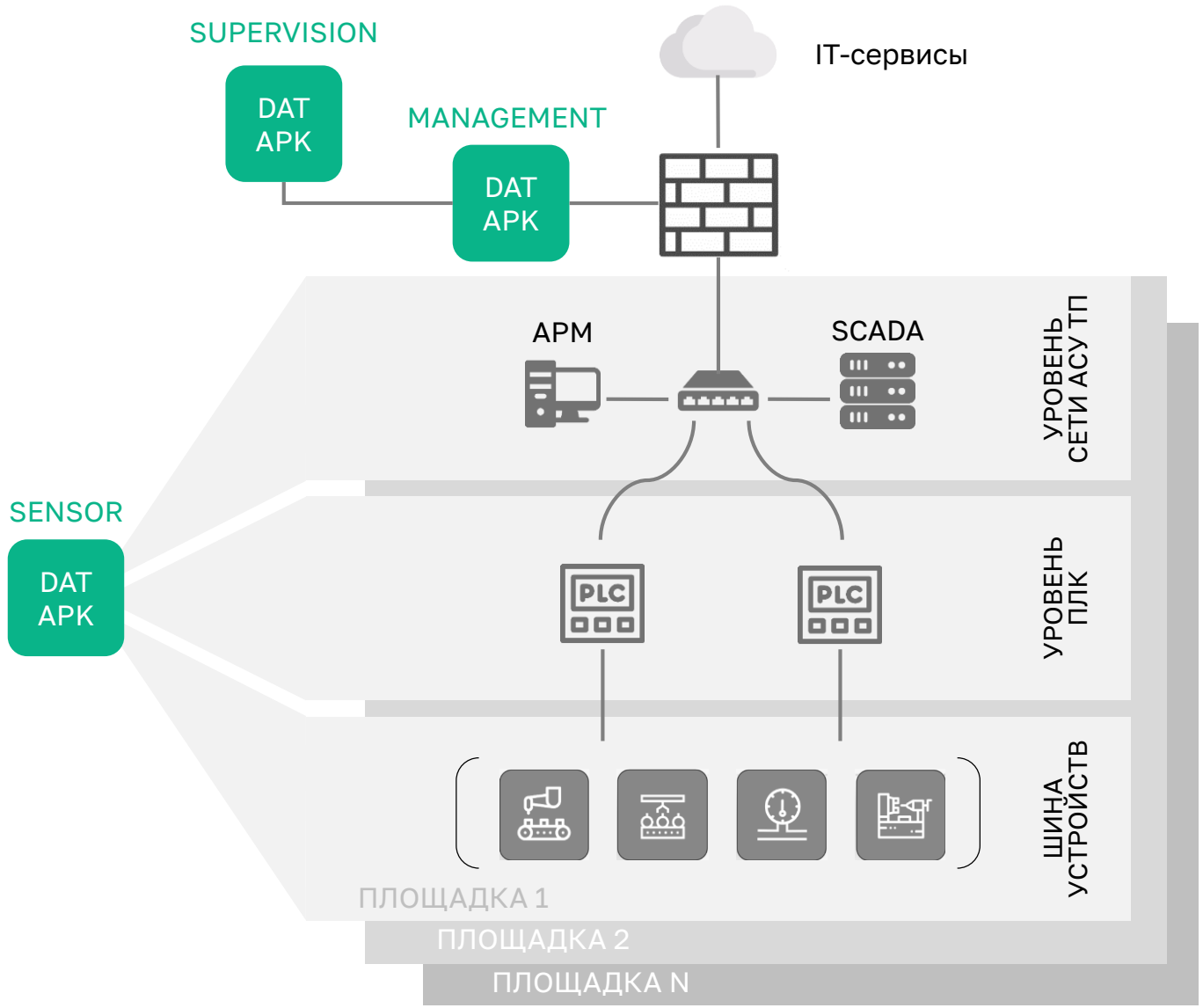
- Централизованное управление инфраструктурой DATAPK предприятия
- Формирование инцидентов и отображение панелей мониторинга

MANAGEMENT

- Нормализация и корреляция событий
- Формирование инцидентов и отображение панелей мониторинга
- Управление небольшой сетью сенсоров

SENSOR

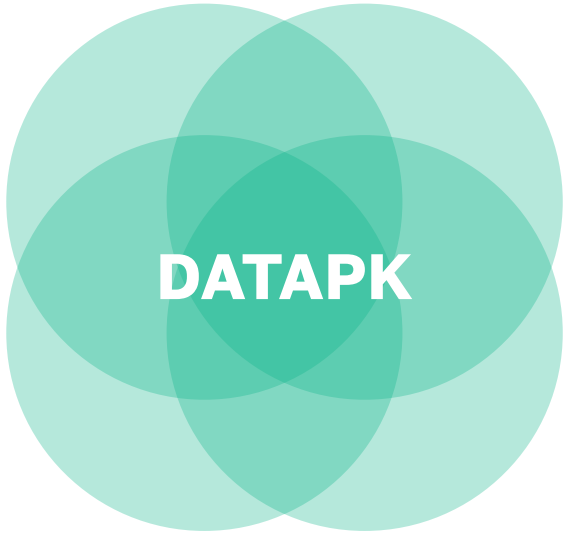
- Сбор и анализ трафика из сети АСУ ТП
- Взаимодействие с объектами защиты уровня ПЛК и выше



DATAPK Industrial Kit больше чем СОВ для АСУ ТП

АНАЛИЗ
СЕТЕВОГО ТРАФИКА

УПРАВЛЕНИЕ
КОНФИГУРАЦИЯМИ



ОБНАРУЖЕНИЕ
ИНЦИДЕНТОВ

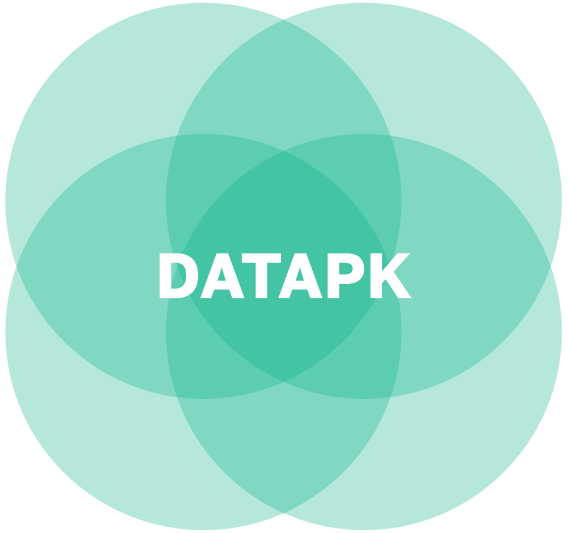
УПРАВЛЕНИЕ
УЯЗВИМОСТЯМИ

- 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

DATAPK Industrial Kit больше чем СОВ для АСУ ТП

УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ



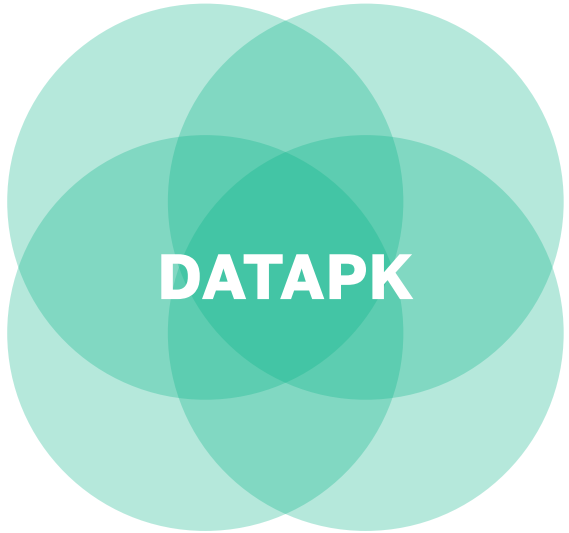
«Компьютерный червь Stuxnet, поразивший ядерные объекты Ирана, отбросил атомную программу страны на два года назад»

lenta.ru

«По словам эксперта, применение вредоносной программы оказалось по эффективности сравнимо с полноценной военной операцией»

lenta.ru

Набор решений для защиты АСУ ТП



- UDV DATAPK Industrial Agentless EDR
- UDV DATAPK Version Control
- UDV Data Diode
- UDV Industrial Honeypot
- UDV Industrial Firewall

Набор решений для защиты АСУ ТП

Безагентный EDR для поведенческого анализа и контроля ПЛК

- Работа в полностью пассивном режиме на копии трафика
- Глубокий анализ пакетов для выявления любой сетевой активности ПЛК
- Моделирование работы ПЛК и всех узлов сети, с которыми ПЛК взаимодействуют
- Выявление аномалий

UDV DATAPK Industrial Agentless EDR

UDV DATAPK Version Control

UDV Data Diode

UDV Industrial Honeypot

UDV Industrial Firewall

Набор решений для защиты АСУ ТП

Система контроля версий проектов ПЛК (Q4 2023)

- Резервное копирование исходного кода проектов ПЛК
- Контроль и отслеживание изменений между версиями
- Восстановление любой предыдущей версии программы
- Отчёты и уведомления об изменениях

UDV DATAPK Industrial Agentless EDR

UDV DATAPK Version Control

UDV Data Diode

UDV Industrial Honeypot

UDV Industrial Firewall

Набор решений для защиты АСУ ТП

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

- 100 Мбит/с
- 1 Гбит/с

- Односторонняя передача данных
- Ответвление и передача копии сетевого трафика в адрес средств анализа

UDV DATAPK Industrial Agentless EDR

UDV DATAPK Version Control

UDV Data Diode

UDV Industrial Honeypot

UDV Industrial Firewall

Набор решений для защиты АСУ ТП

Приманка для сбора информации о злоумышленнике: имитация сервисов и сетевого оборудования

- ☑ Встроенный Sniffer
- ☑ Обнаружение MiTM атак

- Имитация Linux-сервера
- Имитация рабочей станции Windows
- Имитация устройства Cisco
- Имитация ПЛК (в новой версии)

UDV DATAPK Industrial Agentless EDR

UDV DATAPK Version Control

UDV Data Diode

UDV Industrial Honeypot

UDV Industrial Firewall

Набор решений для защиты АСУ ТП

Индустриальный межсетевой экран для применения в промышленных сетях

Полностью свободная независимая аппаратная архитектура

- Соответствие требованиям российского законодательства
- Нет ограничений для приобретения
- Высокая скорость работы
- Горизонтальная масштабируемость

UDV DATAPK Industrial Agentless EDR

UDV DATAPK Version Control

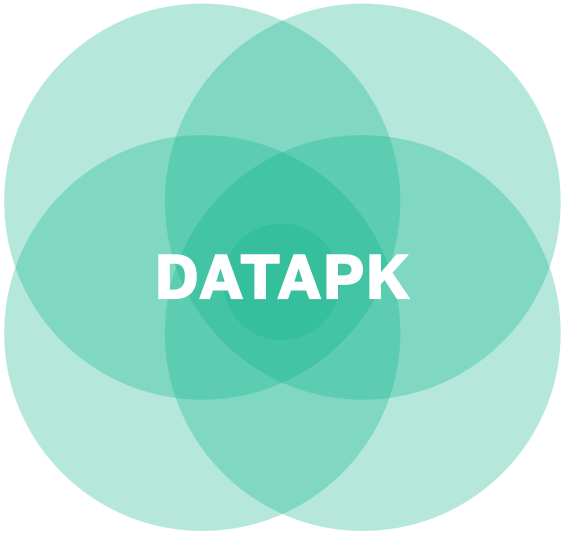
UDV Data Diode

UDV Industrial Honeypot

UDV Industrial Firewall

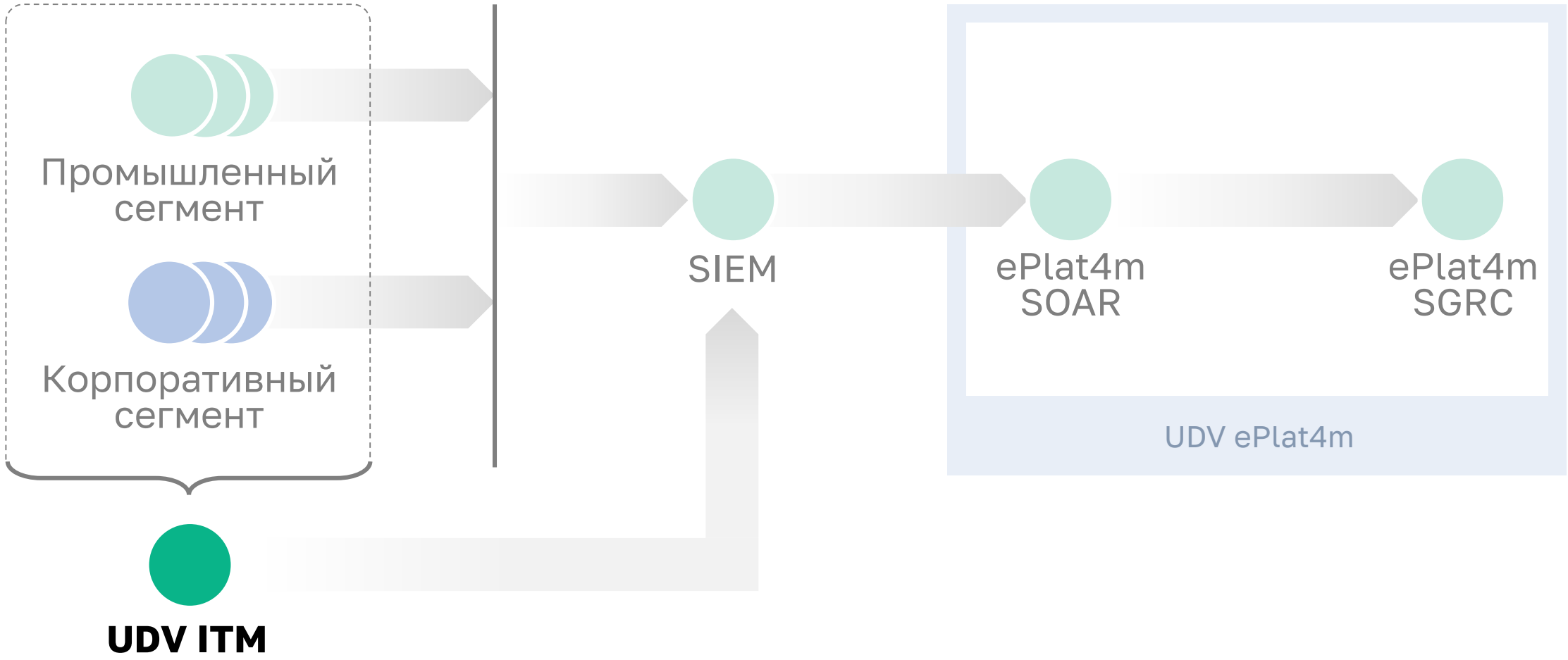
Доступность для пилотирования осенью 2023 г.

Набор решений для защиты АСУ ТП



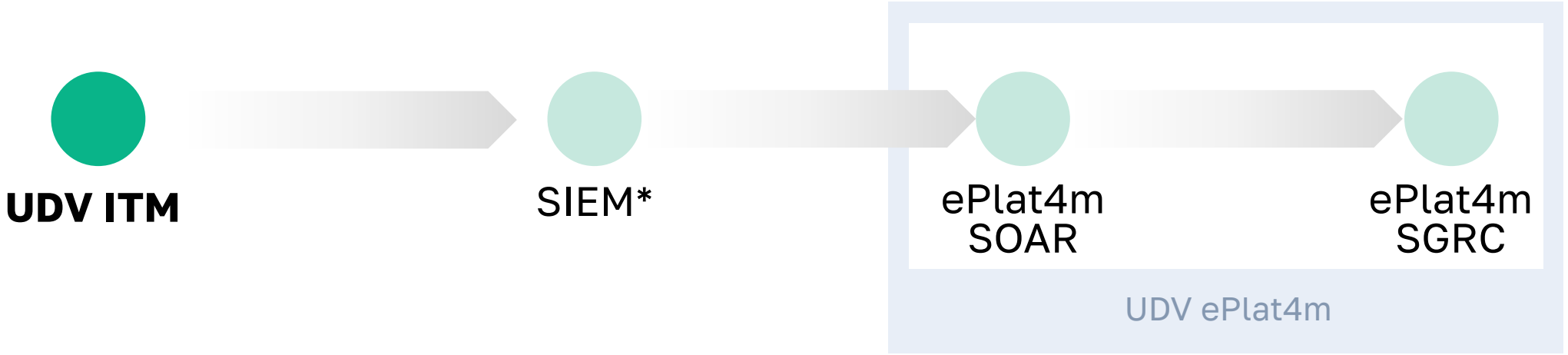
- UDV DATAPK Industrial Agentless EDR
- UDV DATAPK Version Control
- UDV Data Diode
- UDV Industrial Honeypot
- UDV Industrial Firewall

Интеграция решений UDV Group



Мониторинг доступности и производительности АСУ ТП, каналов связи и ИТ-ресурсов

Интеграция решений UDV для защиты промышленных сетей

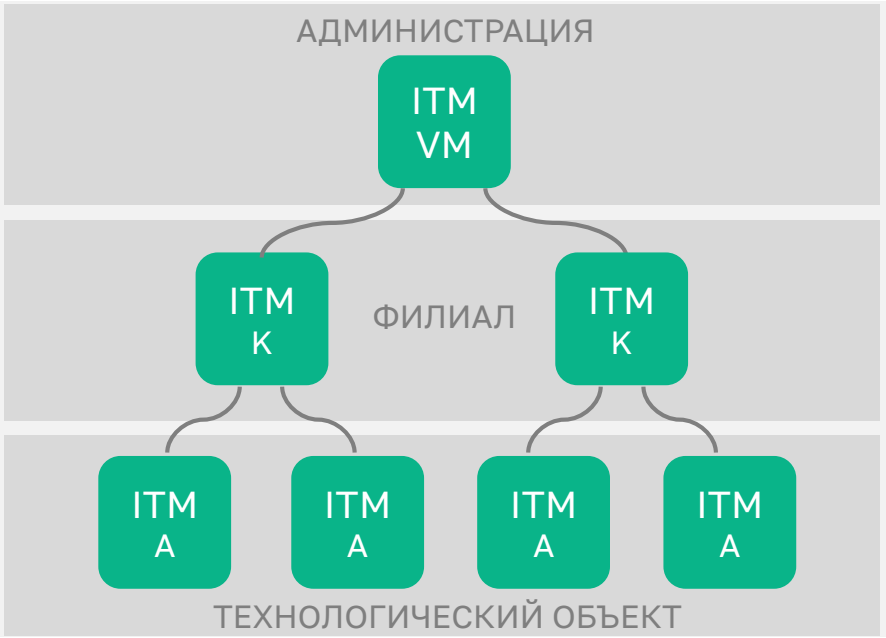


Мониторинг параметров функционирования:

- Агентный способ. (Windows, Linux, UNIX)
- Безагентный способ (SNMP, IPMI, WMI, ICMP)

Обнаружение отклонений и оповещения:

- Обнаружение отклонений нормального функционирования
- Оповещения (Email, SMS, Telegram и др.)



* Включено в дорожную карту развития продуктовой линейки на 2023 год

Интеграция решений UDV для защиты промышленных сетей

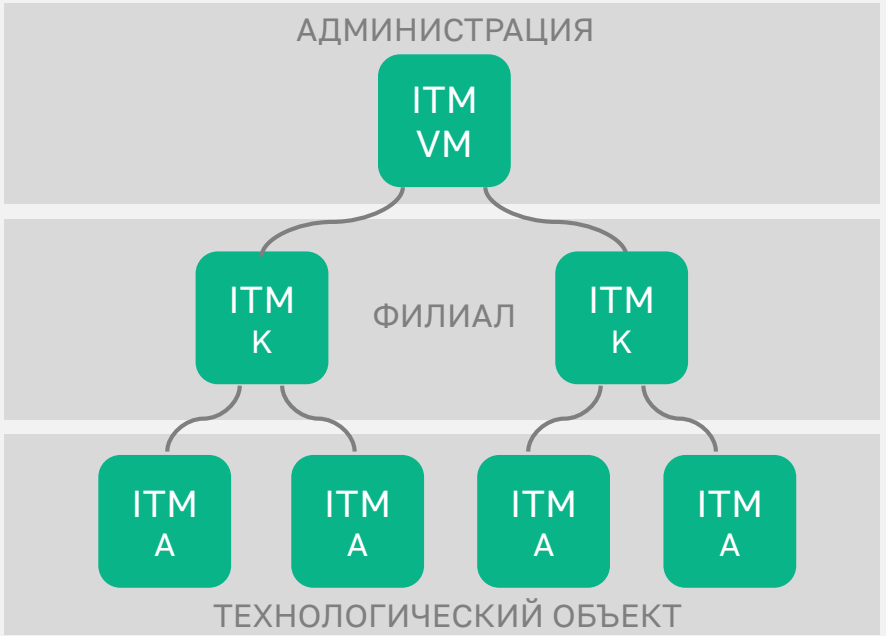
28.08.2023
Переполнение дискового пространства стало причиной остановки заводов Toyota в Японии

Мониторинг параметров функционирования:

- Агентный способ. (Windows, Linux, UNIX)
- Безагентный способ (SNMP, IPMI, WMI, ICMP)

Обнаружение отклонений и оповещения:

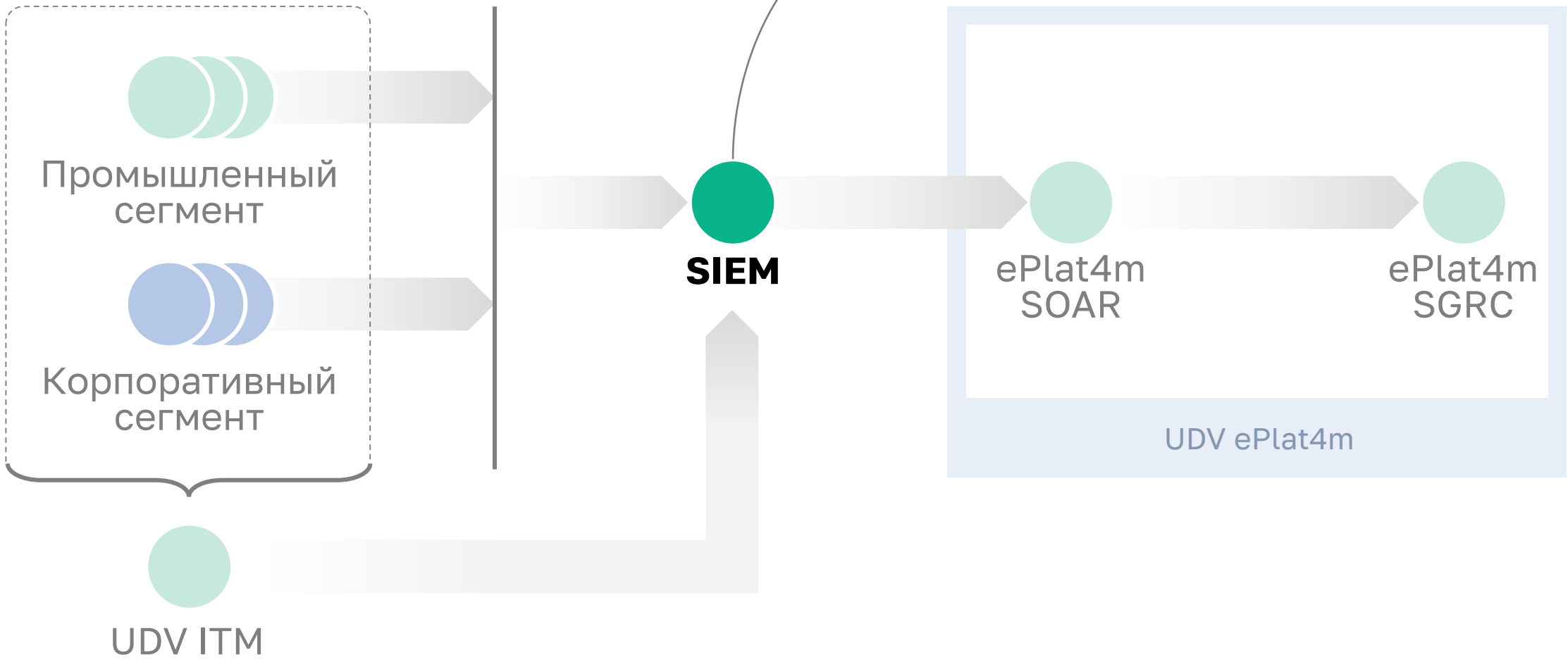
- Обнаружение отклонений нормального функционирования
- Оповещения (Email, SMS, Telegram и др.)



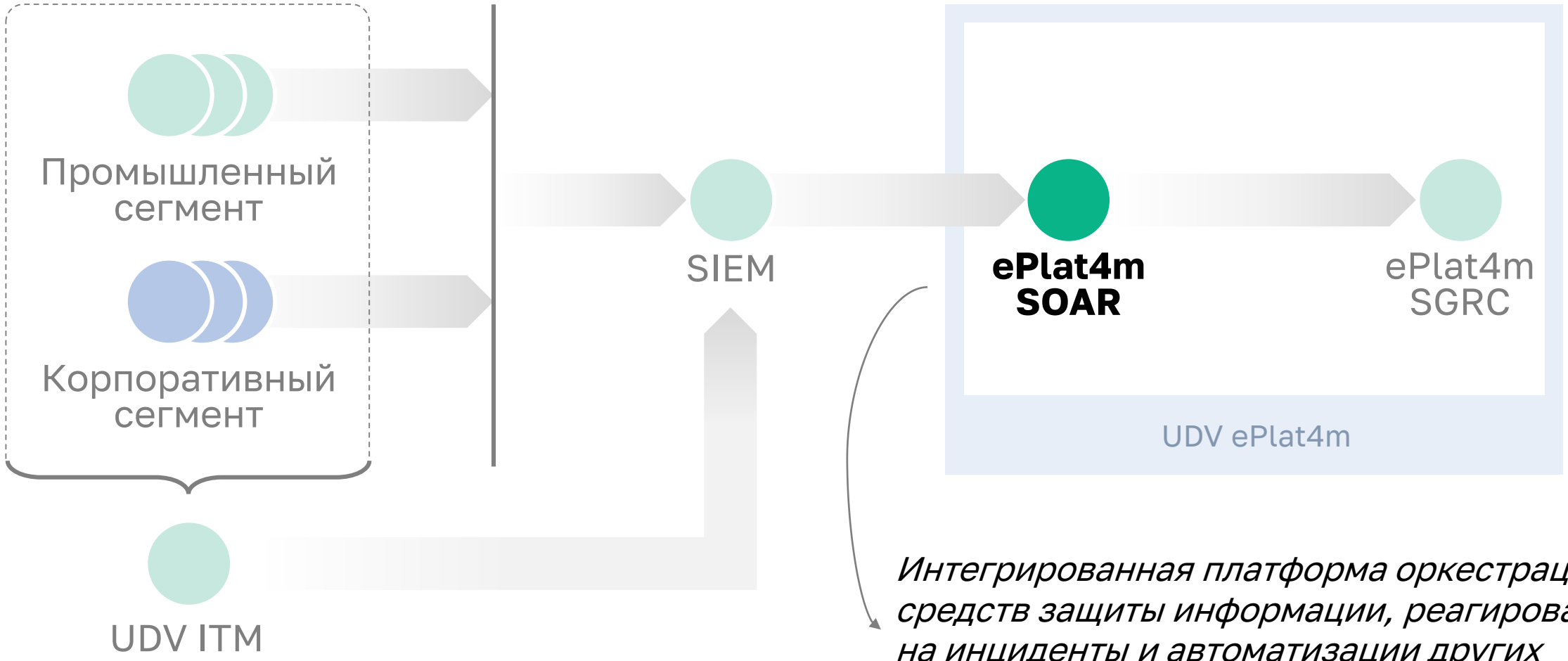
* Включено в дорожную карту развития продуктовой линейки на 2023 год

Интеграция решений UDV Group

Сбор и корреляция событий безопасности + пакет экспертизы для промышленных сетей

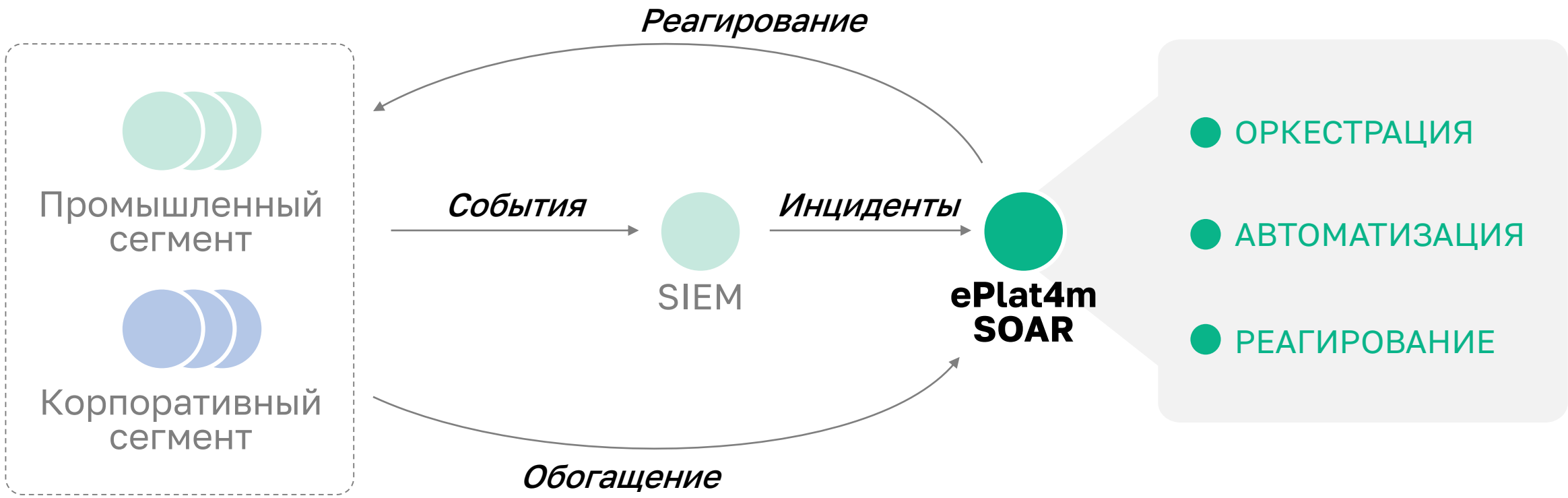


Интеграция решений UDV Group



Интегрированная платформа оркестрации средств защиты информации, реагирования на инциденты и автоматизации других функций ИБ

Интеграция решений UDV Group

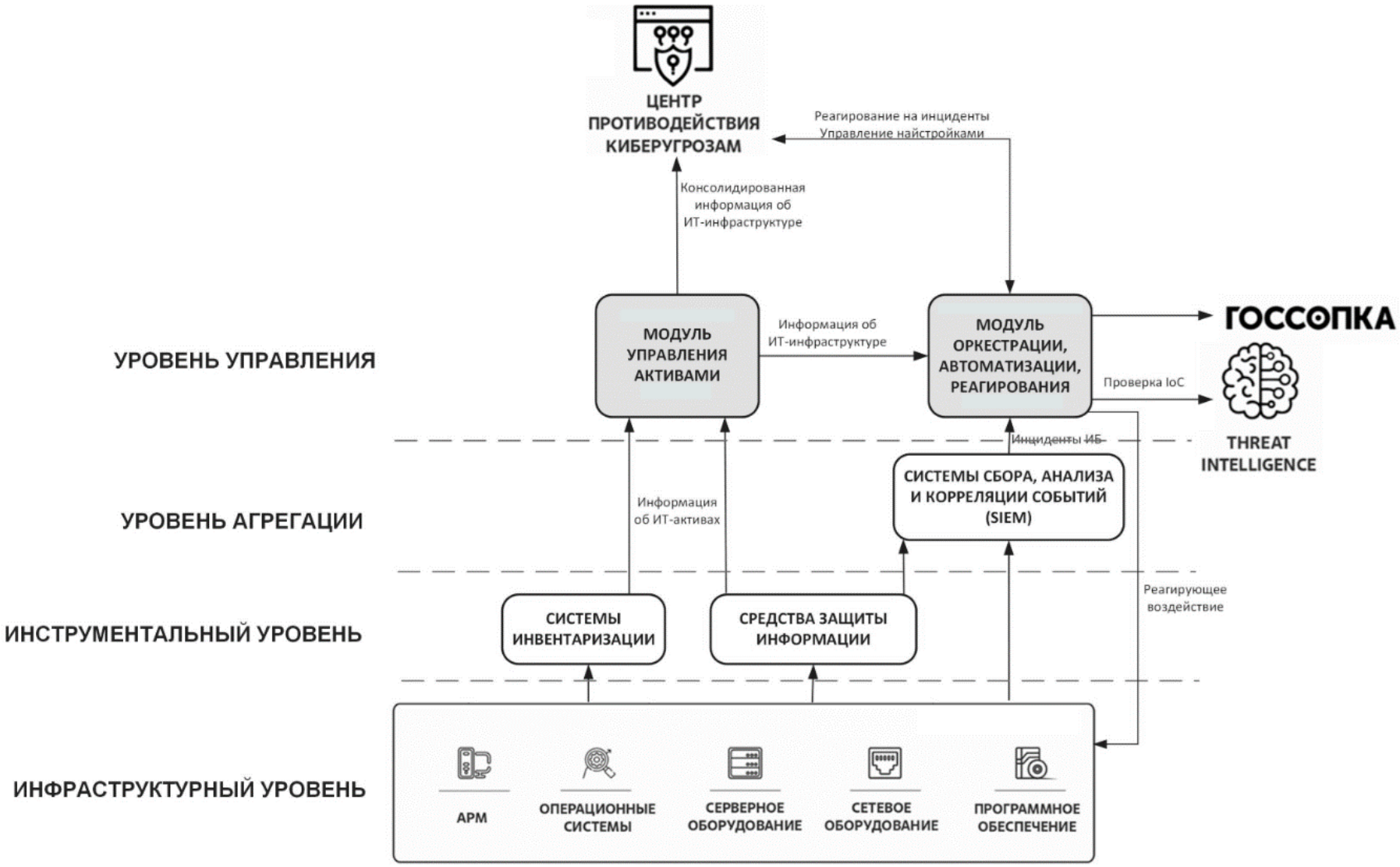


Уменьшение числа обрабатываемых «вручную» инцидентов с **10 000** до **500**

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

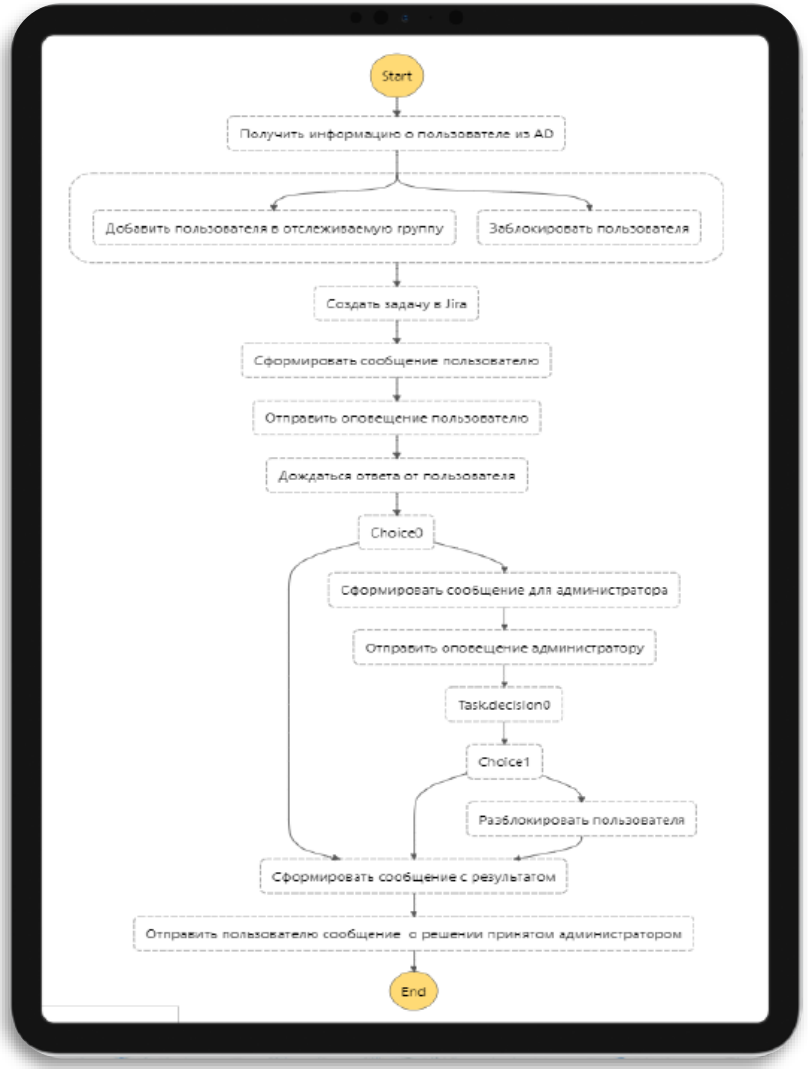
Автоматическая реакция для **30%** инцидентов

Схема функционирования UDV ePlat4m SOAR

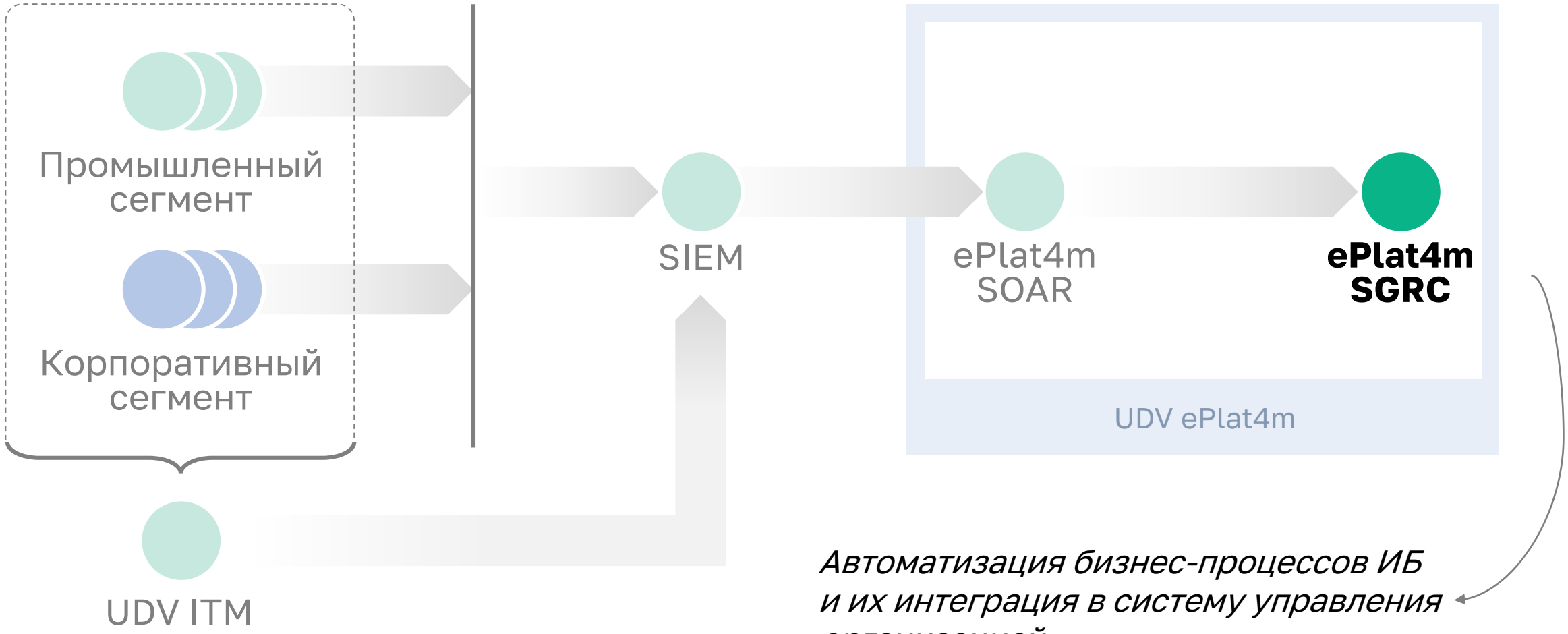


Модуль оркестрации, автоматизации и реагирования

- сбор инцидентов ИБ из внешних систем, формирование и ведение карточки инцидента ИБ
- автоматизация workflow алгоритма реагирования на инцидент ИБ
- разграничение прав доступа к инцидентам ИБ согласно ролевой модели, контроль выполнения SLA по инцидентам ИБ
- обогащение инцидентов ИБ информацией из внутренних систем;
- проверка атрибутов инцидента ИБ во внешних сервисах
- реализация реагирующего воздействия на инциденты ИБ в автоматическом режиме путем выполнения скриптов
- возможность самостоятельной разработки и отладки новых наборов скриптов автоматизации



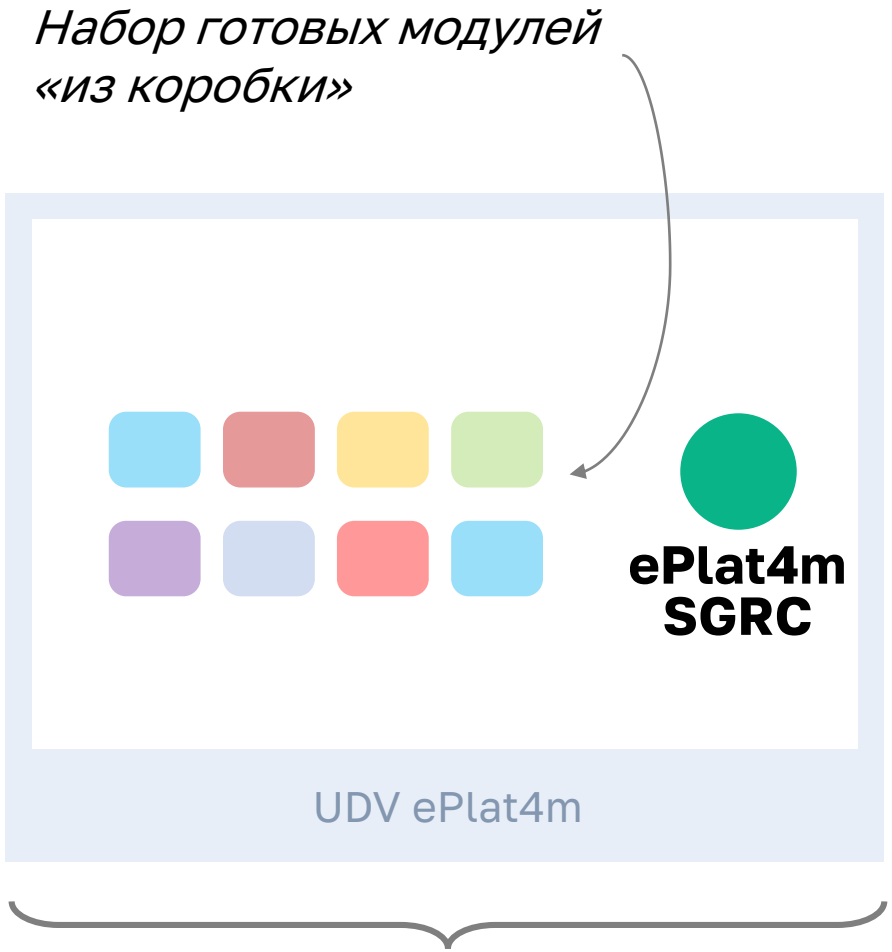
Интеграция решений UDV Group



Автоматизация бизнес-процессов ИБ и их интеграция в систему управления организацией

Интеграция решений UDV Group

- Централизованное управление и контроль процессов ИБ, используя принципы Security GRC
- Автоматизированный контроль выполнения требований регуляторов и лучших практик в области ИБ
- Интеграция и сбор данных со средств защиты информации
- Формирование отчетности, расчет метрик эффективности процессов ИБ



Low-code UDV ePlat4m

Low-code платформа для автоматизации бизнес-процессов и создания собственных приложений без навыков программирования

Некоторые модули UDV ePlat4m SGRC

udv|group

СПАСИБО ЗА ВНИМАНИЕ!

Закажите пилотный проект или персональную демонстрацию наших решений

ILIA.VALOV@UDV.GROUP

8-800-511-6551

udv.group