DATAPK Industrial Kit на страже промышленного сегмента

CyberLympha®

ePlat4m

udv|group

РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ДЛЯ КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

udv|group

РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ДЛЯ КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

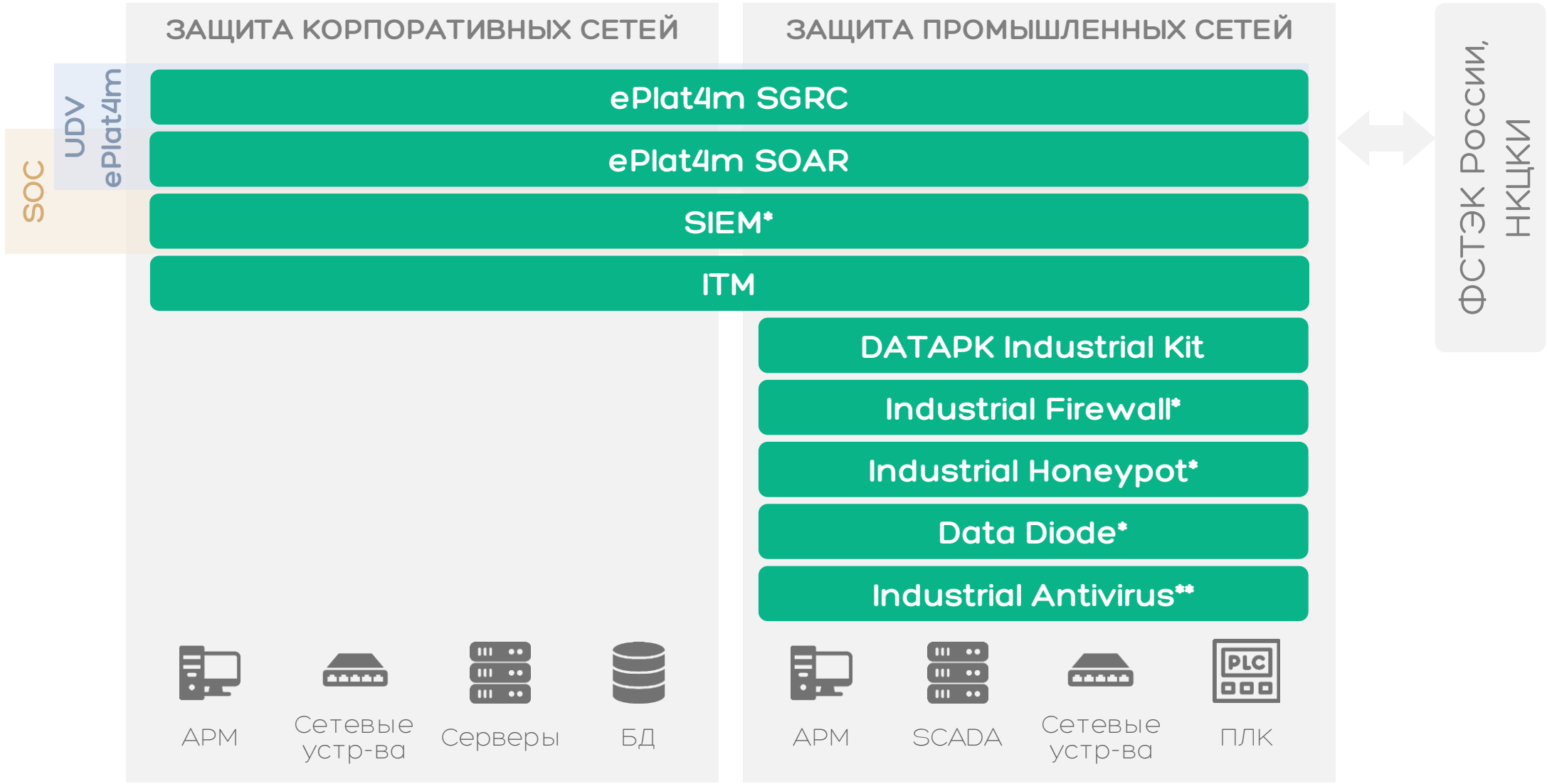
УНИВЕРСАЛЬНАЯ КОМПЛЕКСНАЯ СИСТЕМА КИБЕРФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

ЭКСПЕРТЫ ПО ИТ-БЕЗОПАСНОСТИ

СОБСТВЕННАЯ ЛАБОРАТОРИЯ R&D ЦЕНТР СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ОБРАБОТКИ ДАННЫХ И КИБЕРБЕЗОПАСНОСТИ

ПАРТНЁРСКАЯ СЕТЬ, ВКЛЮЧАЮЩАЯ ДЕЛОВЫХ И ТЕХНОЛОГИЧЕСКИХ ПАРТНЁРОВ

Экосистема решений UDV Group



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

Оперативное обнаружение инцидентов ИБ в промышленных сетях

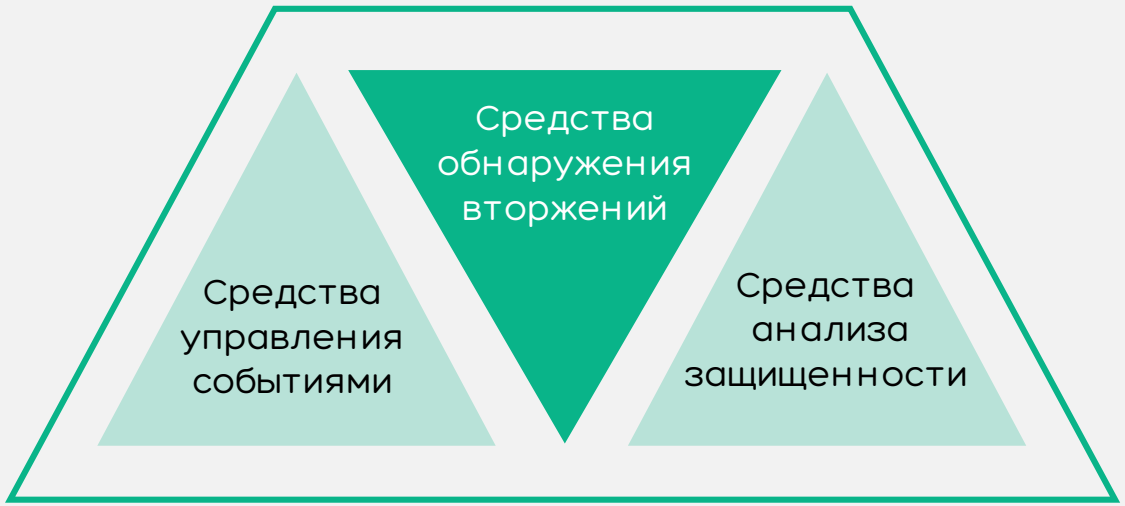
UDV ePlat4m

- 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

Оперативное обнаружение инцидентов ИБ в промышленных сетях

CyberLympha DATAPK → udv DATAPK Industrial Kit

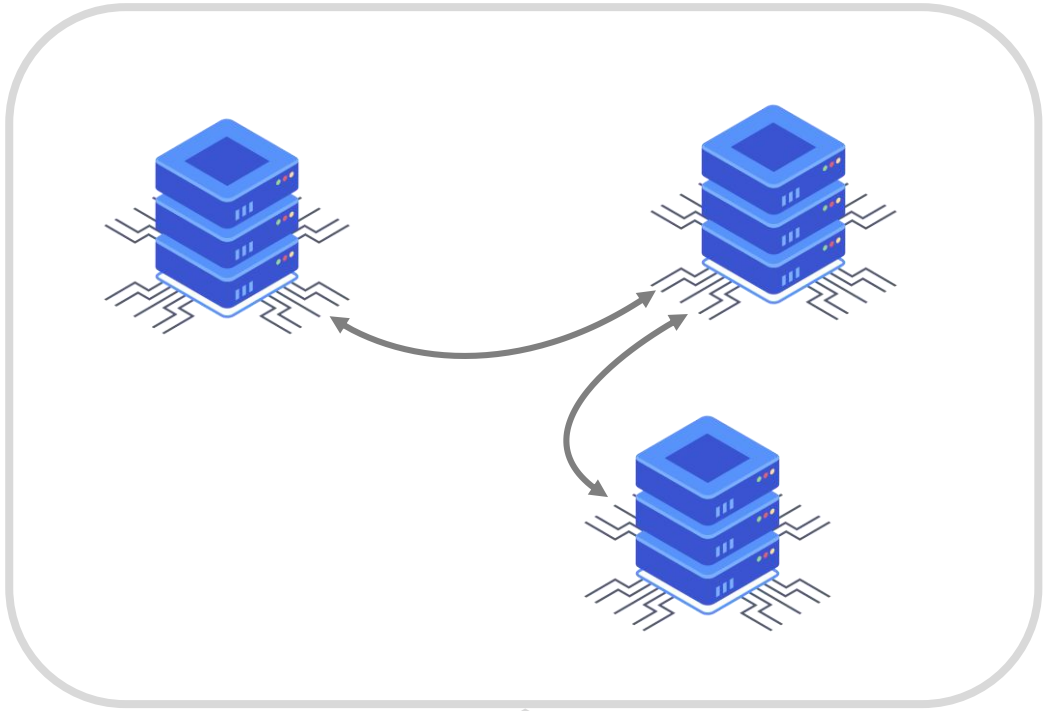


Классы средств защиты информации в соответствии с Приказом №235 ФСТЭК России

- 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

Оперативное обнаружение инцидентов ИБ в промышленных сетях

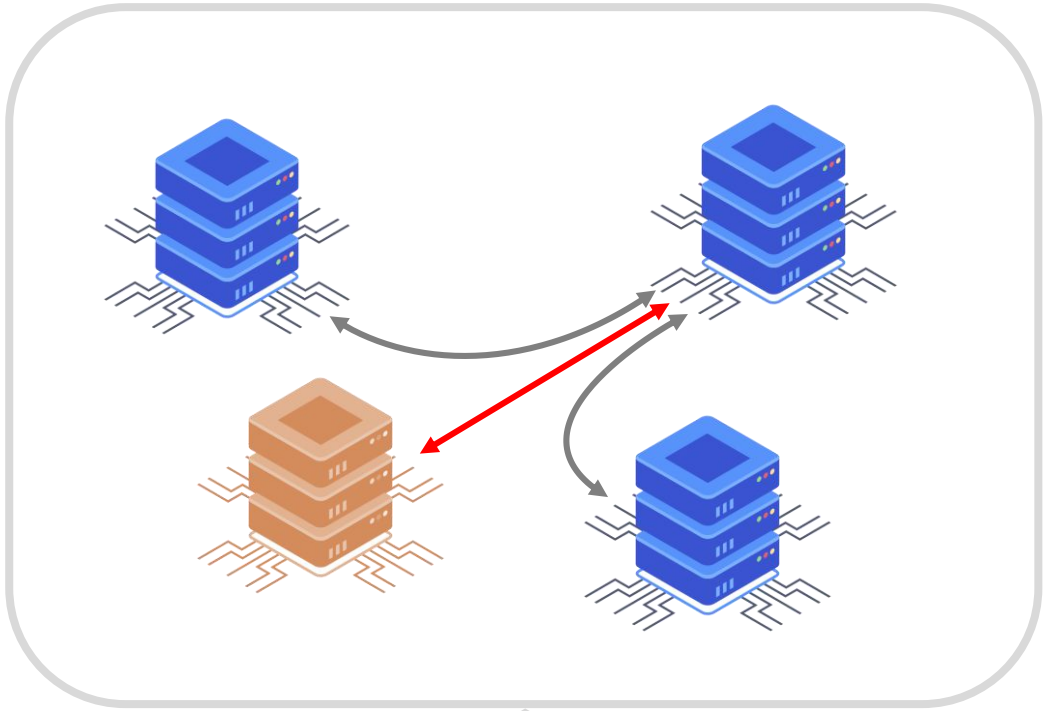


udv DATAPK Industrial Kit

Анализ сетевого трафика

- Пассивное получение данных посредством SPAN портов сетевого оборудования
- Визуализация карты сети и потоков
- Выявление и инвентаризация узлов

Оперативное обнаружение инцидентов ИБ в промышленных сетях

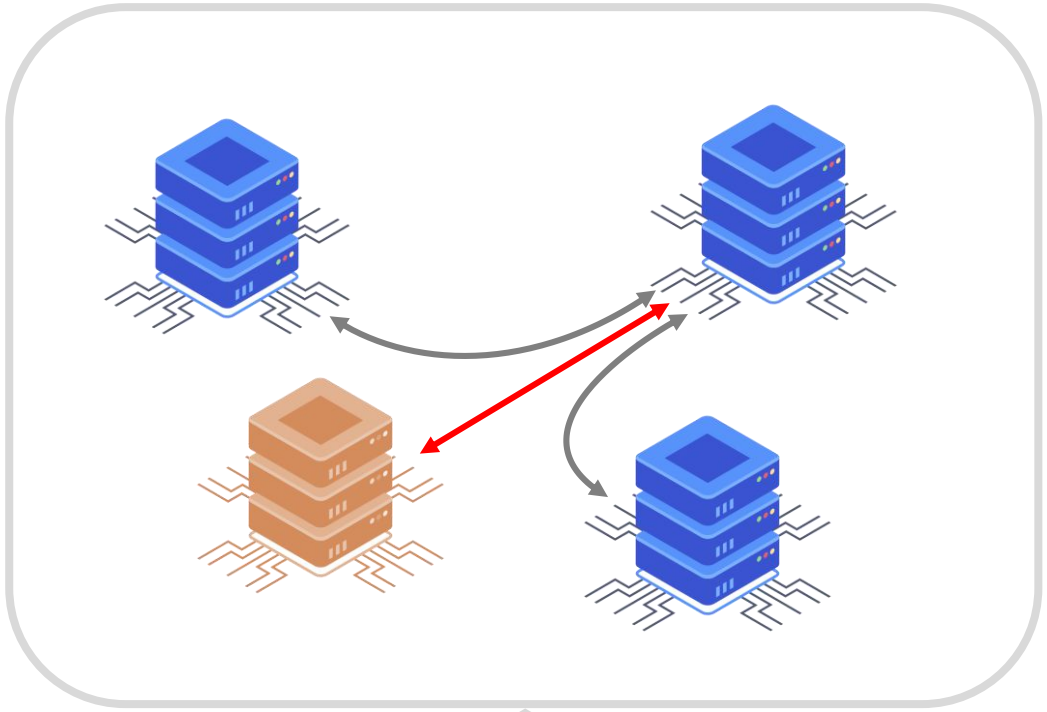


udv DATAPK Industrial Kit

Анализ сетевого трафика

- Пассивное получение данных посредством SPAN портов сетевого оборудования
- Визуализация карты сети и потоков
- Выявление и инвентаризация узлов
- Обнаружение несанкционированных подключений и потоков данных

Оперативное обнаружение инцидентов ИБ в промышленных сетях



udv DATAPK Industrial Kit

Машинное обучение

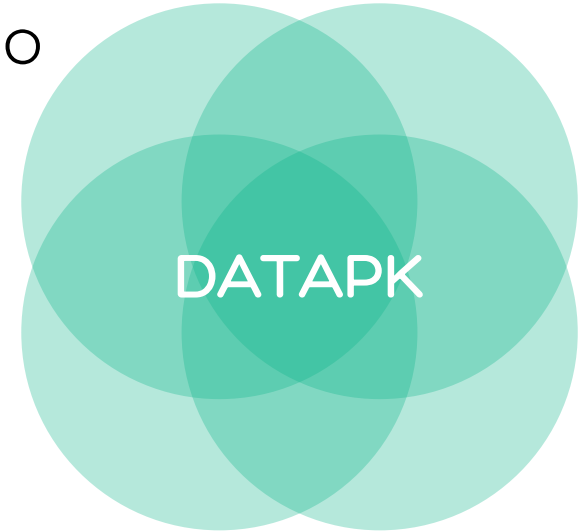
- Восстановление структуры закрытых промышленных протоколов
- Мониторинг отклонений от эталонных моделей и обнаружение несанкционированных изменений в АСУ ТП

? ? ? ? ? ? ?

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	✗ ✓	✓

Архитектура DATAPK Industrial Kit

SUPERVISION

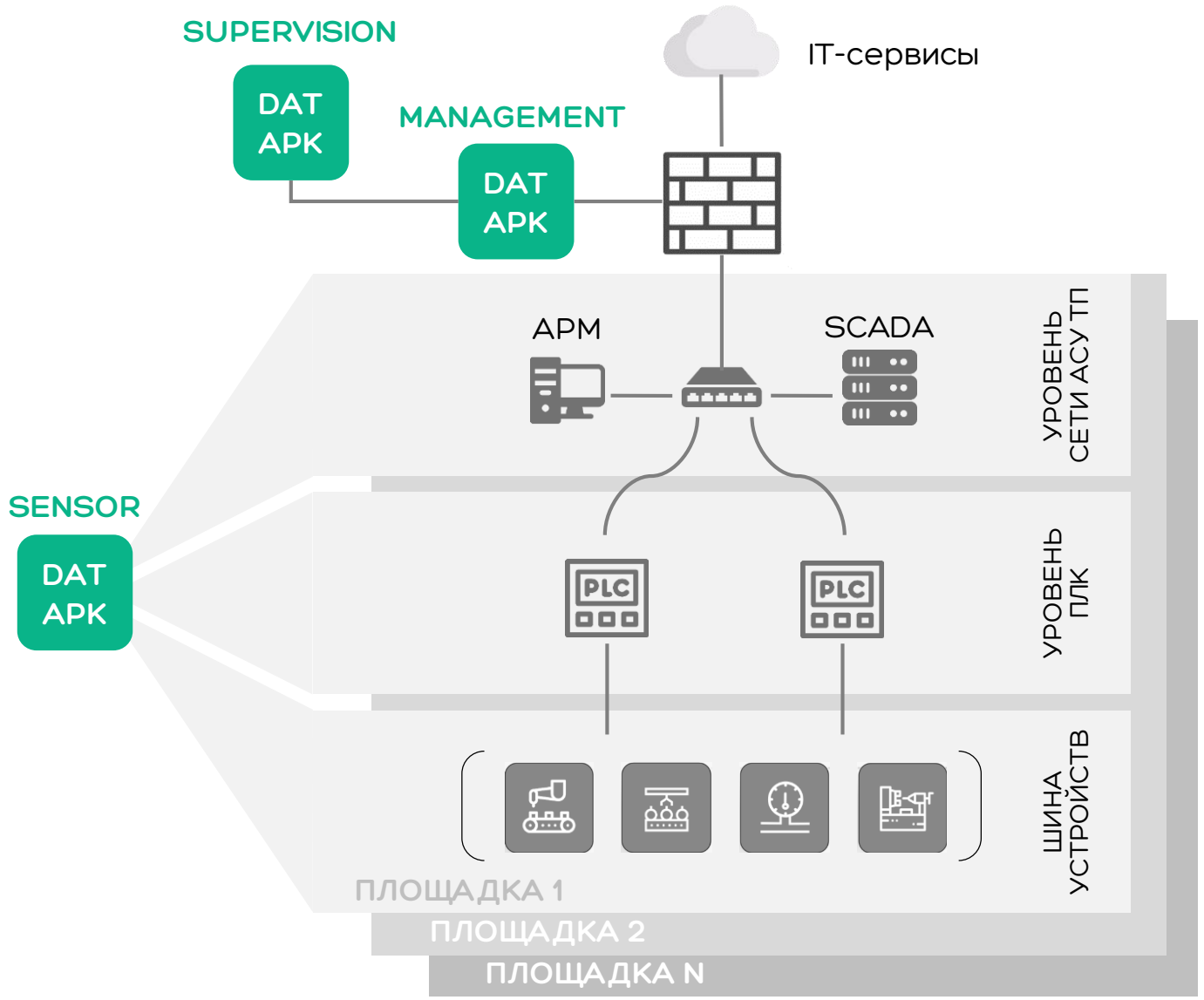
- Централизованное управление инфраструктурой DATAPK предприятия
- Формирование инцидентов и отображение панелей мониторинга

MANAGEMENT

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

SENSOR

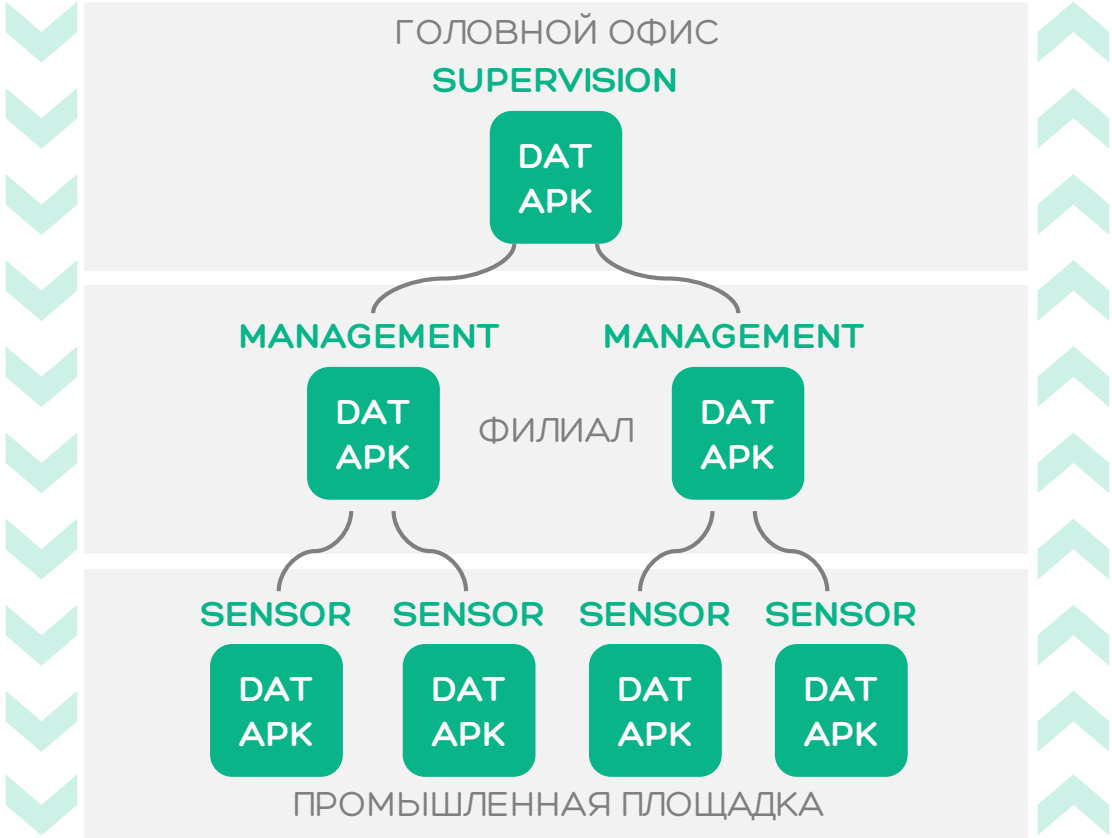
- Сбор и анализ трафика из сети АСУ ТП
- Взаимодействие с объектами защиты уровня ПЛК и выше



Иерархия DATAPK Industrial Kit

НИСХОДЯЩИЙ ПОТОК

- Команды управления
- Группы и тэги
- Политики сбора данных
- Правила нормализации событий
- Правила корреляции событий
- Правила обнаружения вторжений
- Определения OVAL



ВОСХОДЯЩИЙ ПОТОК

- Каталог объектов защиты
- Каталог сетевых взаимодействий
- Карты сети
- Конфигурации объектов
- События ИБ
- Инциденты ИБ
- Результаты проверки OVAL

- Минимальная нагрузка на каналы связи
- Защита инфраструктуры любого масштаба
- Обмен данными по расписанию
- Низкие требования к качеству каналов связи

Один из кейсов - СЕВЕРСТАЛЬ

ПРОФИЛЬ ЗАКАЗЧИКА

Одна из самых эффективных горно-металлургических компаний в мире, создающая продукты и комплексные решения из стали вместе с клиентами и партнерами. Основные активы холдинга находятся в России.

ЦЕЛЬ ПРОЕКТА

Внедрить централизованную систему мониторинга ИБ АСУ ТП.

ОСОБЕННОСТИ ПРОЕКТА

- Распределенная организационная структура Заказчика
- Необходимость реализации как локального, так и централизованного управления системой
- Необходимость интеграции с собственным SOC Заказчика

РЕЗУЛЬТАТЫ ПРОЕКТА

Используя DATAPK, специалисты Заказчика смогли обнаружить и устранить реальные угрозы ИБ АСУ ТП в инфраструктуре предприятия

Благодаря автоматизации процесса контроля соответствия требованиям надзорных органов, ресурсы квалифицированных специалистов ИБ перенаправлены на реальное повышение защищенности инфраструктуры

Реализован механизм автоматической инвентаризации сетевой инфраструктуры и оборудования промышленных сегментов для повышения осведомленности сотрудников SOC о состоянии ИБ АСУ ТП

udv|group

Спасибо!

Закажите пилотный проект или персональную демонстрацию наших решений для своих Заказчиков

commercial@udv.group

udv.group