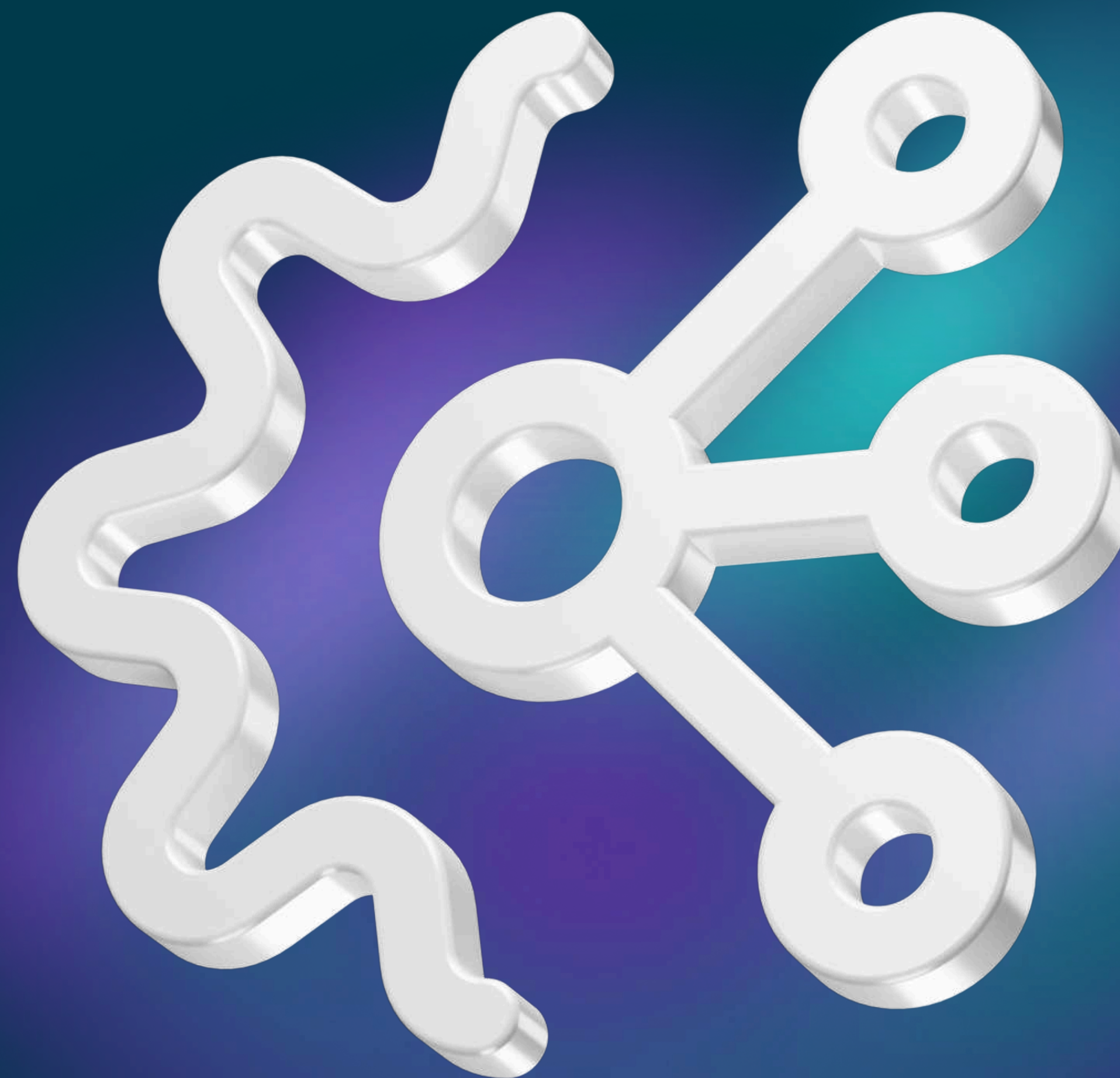


UDV DATAPK

Комплекс решений для мониторинга
состояния защищенности
и оперативного обнаружения
инцидентов ИБ в промышленных сетях



UDV Group – ведущий разработчик в области кибербезопасности

UDV Group предоставляет единый портфель решений для защиты технологических сетей, корпоративного сегмента и автоматизации в области объектовой безопасности:

- защита АСУ ТП и объектов КИИ
- мониторинг инфраструктуры
- реагирование на инциденты ИБ
- автоматизация работы SOC
- выполнение требований регуляторов

200+

Разработчиков в штате

Распределённая команда
со штаб-квартирой в Екатеринбурге

1000+

Инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей

10+

Патентов

Собственный исследовательский
центр в области кибербезопасности

10

Лет на рынке

Подтвержденный опыт интеграции
в крупных предприятиях
нефтегазовой отрасли, энергетики,
металлургии и других

UDV DATAPK Industrial Kit

UDV DATAPK Industrial Kit – это комплексное решение для обеспечения ИБ АСУ ТП.

Решение позволяет быстро начать реагировать на угрозы без негативного влияния на защищаемые системы. Обеспечивает видимость ландшафта АСУ ТП, выявляет инциденты на ранних этапах и помогает выполнить требования регуляторов.

UDV DATAPK Industrial Kit использует целостный подход в рамках единого решения, что позволяет оптимизировать расходы на защиту АСУ ТП.

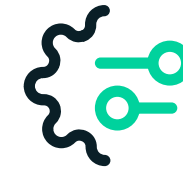
Возможности UDV DATAPK Industrial Kit



Industrial NTA + IDS

Анализ сетевого трафика и обнаружение вторжений

- Анализ копии сетевого трафика (SPAN)
- Выявление и инвентаризация активов
- Визуализация карты устройств в сети и сетевых соединений
- Обнаружение атак, нелегитимных узлов, несанкционированных сетевых соединений
- Более 20 000 правил обнаружения «из коробки»
- Обновление правил обнаружения без модификации программного кода
- Формирование инцидентов ИБ



Configuration Manager

Управление конфигурациями

- Контроль безопасных настроек и их неизменности, аудит изменений
- Анализ соответствия требованиям ИБ
- Работа без использования агентов
- Использование стандартных общедоступных протоколов компонентов АСУ ТП
- Формирование инцидентов ИБ

Возможности UDV DATAPK Industrial Kit



Vulnerability Manager Управление уязвимостями

- Неинвазивный аудит безопасности без использования агентов
- Проверка соответствия требованиям (Compliance)
- Технологии OVAL и «CPE to CVE»
- Поддержка различных БДУ, включая ФСТЭК России
- Формирование инцидентов ИБ



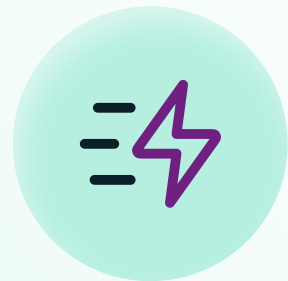
External Event Manager Управление внешними событиями

- Получение событий ИБ с различных источников
- Нормализация событий ИБ
- Корреляция событий ИБ
- Возможность настройки правил корреляции событий ИБ
- Отправка инцидентов ИБ в сторонние системы (syslog)
- Формирование инцидентов ИБ

UDV DATAPK Industrial Kit

Комплексное решение для мониторинга состояния
защищенности и оперативного обнаружения
инцидентов ИБ в промышленных сетях

Классы средств защиты информации к которым относится **UDV DATAPK Industrial Kit** в соответствии с Приказом №235 ФСТЭК России



Средство
управления
событиями



Система
обнаружения
вторжений



Средство
анализа
защищенности

Больше чем COB для АСУ ТП



Замена нескольких
разнородных решений
единым комплексом,
разработанным
для промышленных
предприятий



Выполнение
требований регулятора
и реализация мер
31 и 239 приказов
ФСТЭК России



Обладает
дополнительной
функциональностью
нескольких классов
решений



Оптимизирует
процессы управления
ИБ в организации

Режимы работы DATAPK Industrial Kit

Режим наблюдения

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

Режим запрос-ответ

- Взаимодействие с объектами защиты в режиме «запрос-ответ» с использованием штатных механизмов и протоколов
- Получение с объектов защиты данных о программном обеспечении, его версиях, патчах и конфигурациях
- 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 UDV DATAPK Industrial Kit

SUPERVISION

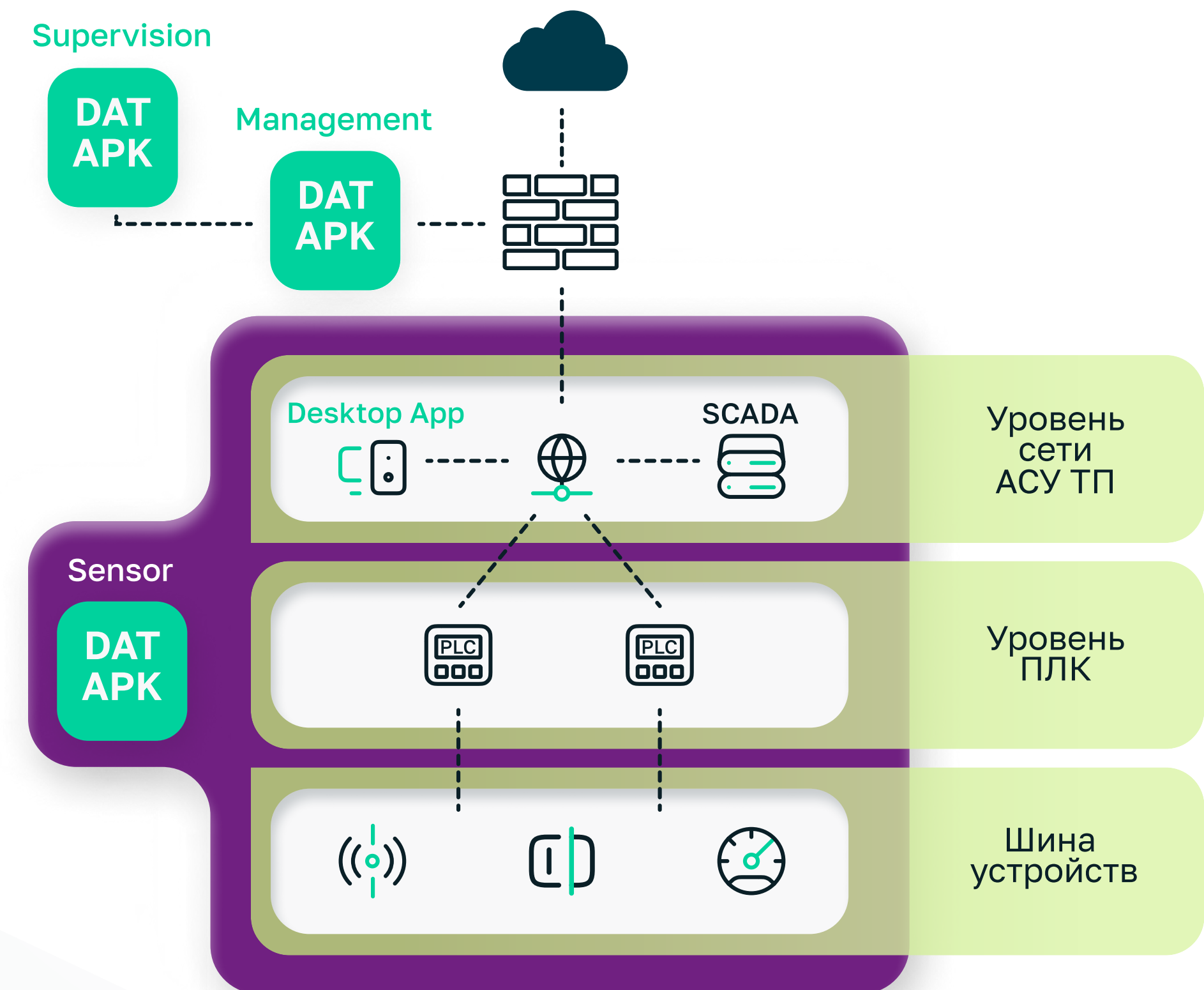
- Централизованная аналитика и отчетность для любой роли
- Централизованное управление всей системой

MANAGEMENT

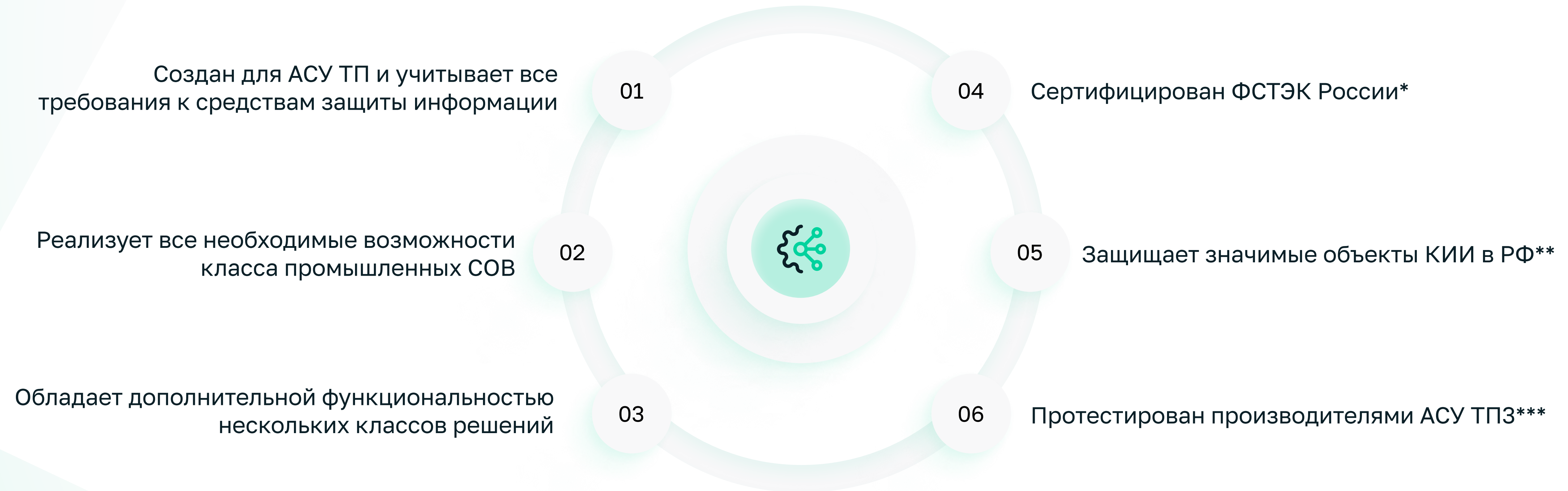
- Детализированное представление данных
- Базовые панели мониторинга и отчетность
- Конфигурация системы
- Управление сенсорами
- REST API для интеграции со сторонними системами

SENSOR

- Получение данных, полученных от компонентов АСУ ТП, и передача на уровень Management
- Пассивный анализ копии сетевого трафика
- Активный сбор данных о конфигурациях, уязвимостях, и т.д.
- Получение событий из внешних источников (syslog)



Преимущества UDV DATAPK Industrial Kit



*Сертификат №4451 от 27.09.2021 ФСТЭК России по требованиям профиля защиты COB уровня сети, уровням доверия в соответствии с Приказом №76 от 2 июня 2020 года

**«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

***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

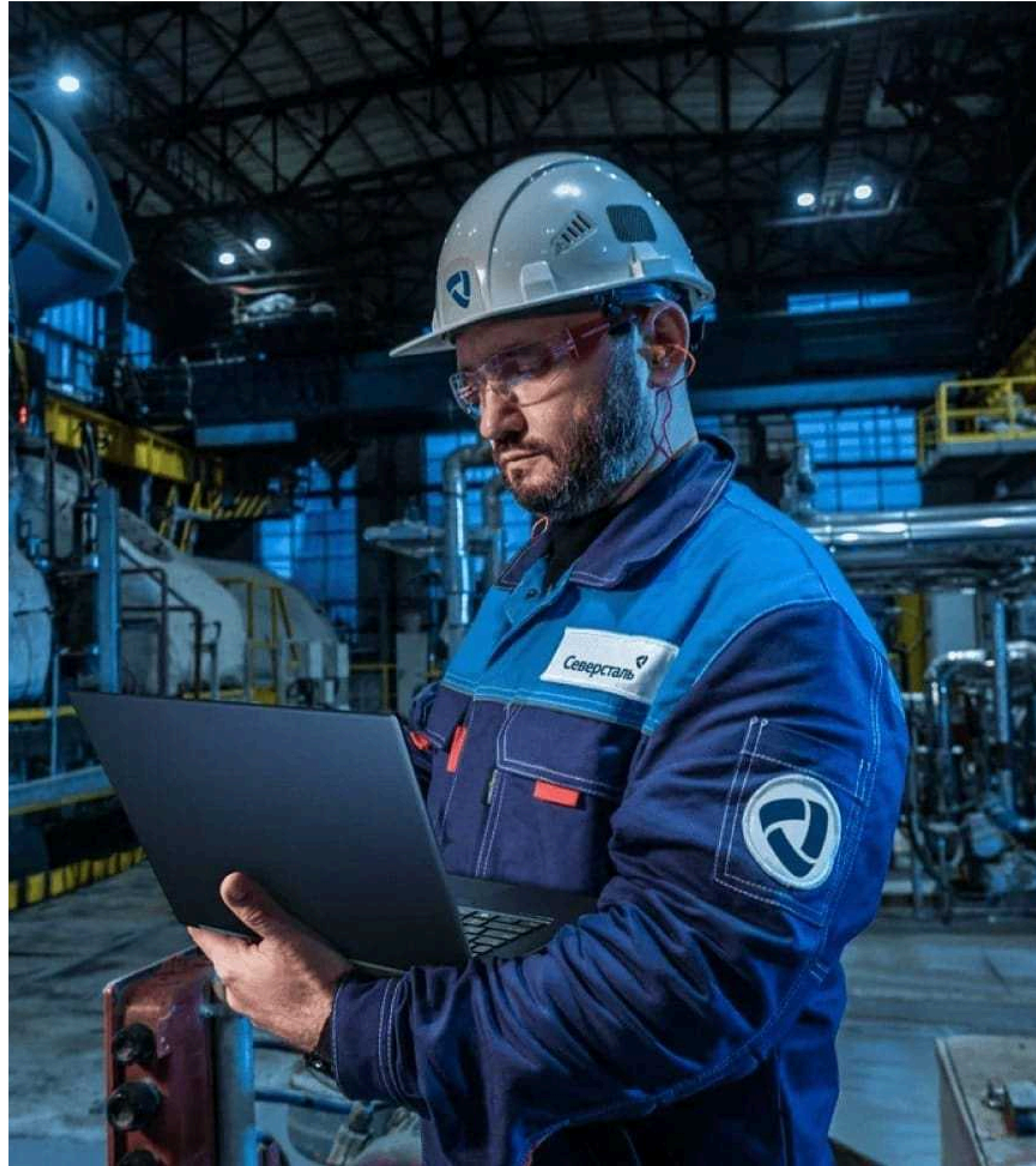
Кейсы внедрения

Кейс внедрения: 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.



Кейс внедрения: Северсталь

Цели и особенности проекта

Основной целью проекта являлось внедрение централизованной системы 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



Кейс внедрения: Северсталь

Результаты проекта

Используя DATARK

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



Спасибо!

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты

commercial@udv.group
8-800-511-65-51

Адрес

620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4

Сайт

udv.group

Telegram

@udv_group

