Промышленная кибербезопасность

Fast Start

с Positive Technologies

ptsecurity.com

Недопустимые события

Отрасли и
Предприятия

Что такое недопустимые события

Всегда есть события, которые недопустимы для предприятия, отрасли, государства

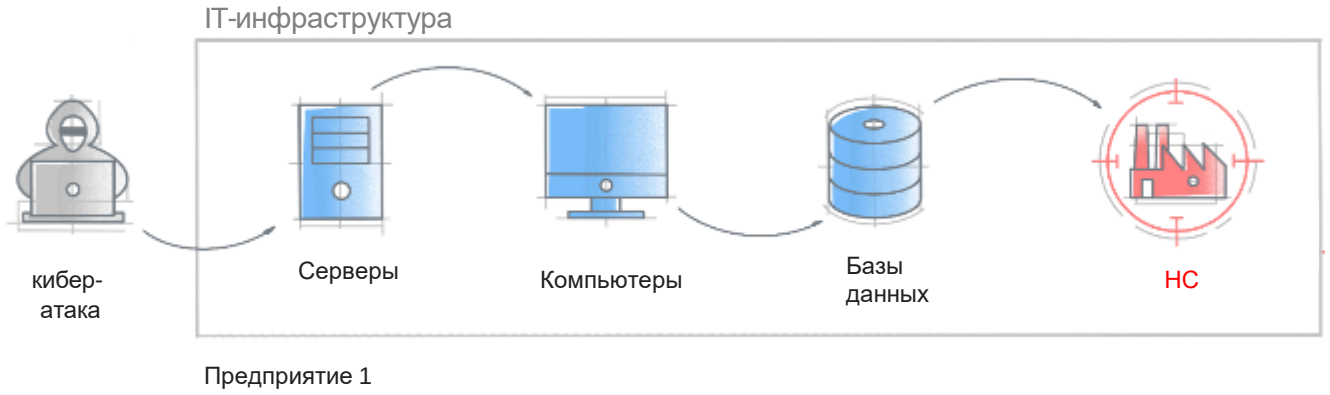
делающие **невозможным достижение** операционных и стратегических **целей** или приводящие к **длительному нарушению** основной **деятельности, в том числе в результате**

Выполняет все свои функции	Выполняет свои функции частично	Не выполняет свои функции
допустимый ущерб	ущерб ниже порогового значения	ущерб выше порогового значения

- крупные финансовые потери
- потеря доли рынка
- остановка производственных процессов
- публичные судебные разбирательства
- срыв контрактных обязательств

Недопустимое событие предприятия

Реализуется на уровне корпоративной или технологической ИТ-инфраструктуры организации/предприятия **в результате кибератаки**



Примеры НС

- Остановка/блокирование производства
- Запроектные режимы и аварии
- Кража денег со счетов организации
- Кража конфиденциальной информации
- Срыв контрактных обязательств

НС – недопустимое событие предприятия / организации

«Быстрый старт»

Текущая проблематика

- Есть критичные промышленные объекты
- Требуется результативная защита от киберугроз
- Есть стандартный подход реализации проектов

- Стандартный подход это всегда долго
- Длительность ИБ проекта обратно пропорциональна эффективности защиты
- Нужны быстрые, подтверждённые на практике результаты

- В текущих условиях результативная кибербезопасность критичных производственных активов – жизненно важный аспект устойчивости бизнеса любой промышленной компании.
- Киберустойчивость системообразующих отраслевых предприятий– это всегда про устойчивость отрасли и государства в целом

Что такое «Быстрый старт»

- Методология оперативного внедрения Центра Противодействия Киберугрозам (ЦПК) технологического сегмента ИТ инфраструктуры предприятия или организации в базовом объеме
- Фокус на промышленных предприятиях
- Итерационный подход к масштабированию защиты от недопустимых событий отдельного производственного участка(ЭЛОУ, АВТ, Крекинг), предприятия, филиала или компании целиком

Включает 3 основных этапа:

- Консалтинг по недопустимым событиям
- Создание Центра Противодействия Киберугрозам
- Киберучения

Суть Методологии «Быстрый старт»

- Минимальный объем документации, требуемый для внедрения.
- Итерационный характер внедрения позволяет учесть изменения в инфраструктуре.
- Фокус защиты направлен на целевые системы и связанные с ними недопустимые события.
- Эффект наблюдается сразу и усиливается ежегодно
- Выводы об эффективности внедренных средств защиты подтверждаются на основании практических испытаний.

Консалтинг. 1 этап

Состав работ:

- Определение НС и негативных последствий, сценарный анализ
- Практическая верификация НС и их последствий
- Формирование плана трансформации

Источники данных:

Киберугрозы

Акты категорирования

Модели угроз

Структура производства

Планы установок

Карты процессов

Инфраструктура АСУ

Паспорта

Проектная документация

Критичные события

Реестр рисков

Декларация безопасности

Получаемые данные:

- Актуальные угрозы кибербезопасности
- Профили настроек и конфигурации оборудования
- Уязвимости СПО и ППО сетевых узлов
- Политики и роли пользователей
- Сетевая связность
- Критичные производственные участки
- Наиболее критичные технологические и производственные процессы
- Опасные производственные объекты
- Наиболее критичные типы ущербов и риски
- Наиболее опасные для предприятия типы аварий и инцидентов

Результат этапа →

Реестр НС, целевых систем АСУ, ключевых систем технологической инфраструктуры, типы и размер ущерба

Модель ИБ Производства с планом трансформации

!!! Возможность реализации недопустимых событий и наличие хакеров в инфраструктуре проверены практическим путем

Карта НС предприятия(пример)

Нарушение режимов функционирования может привести к остановке предприятия.

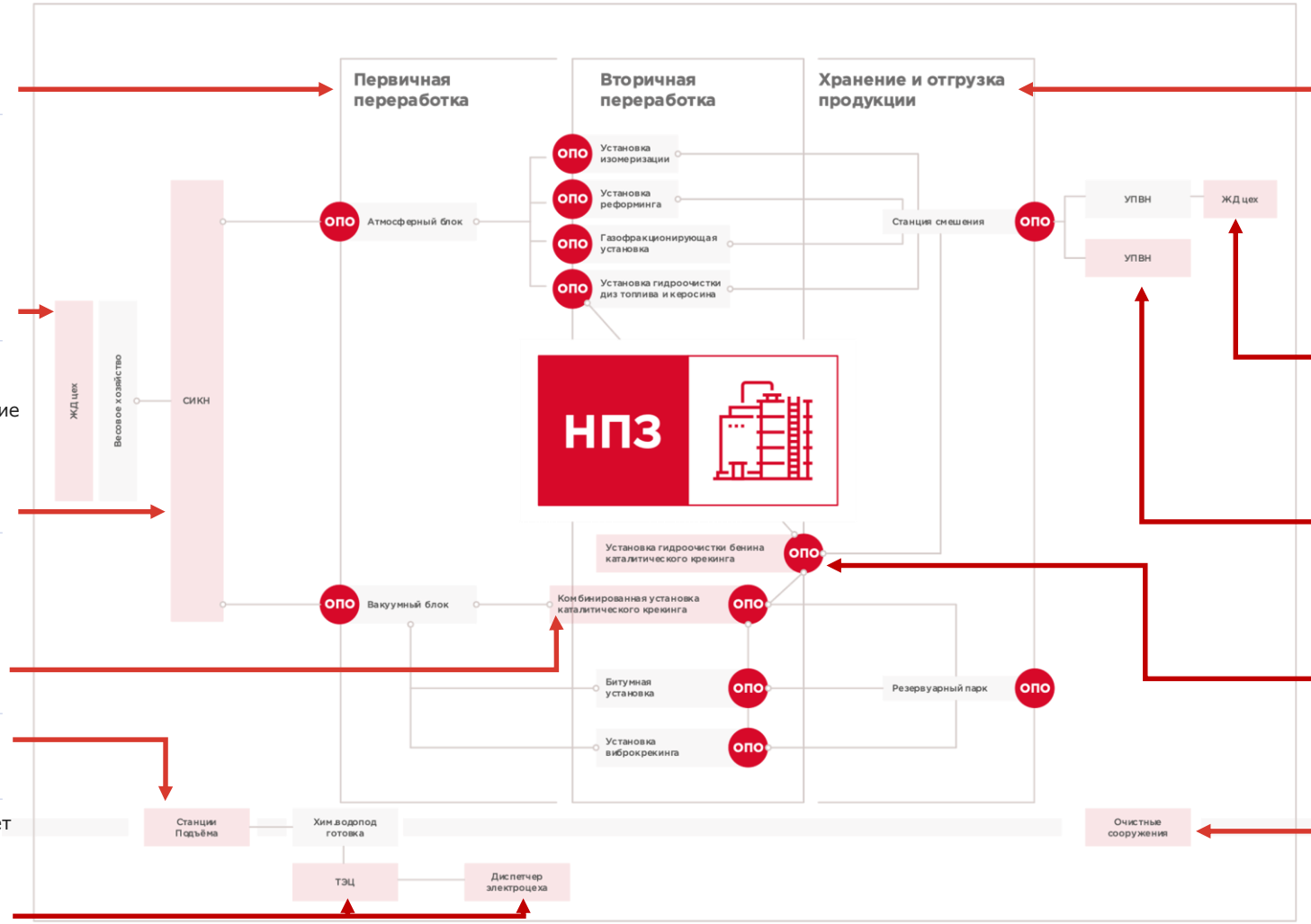
Нарушения работы систем управления движением составов (стрелки, семафоры, шлагбаумы на переездах) могут привести к сбоям в перемещении составов, аварийным столкновениям или схождению вагонов с опасными грузами с путей.

Вмешательство в работу СИКН позволяет реализовать мошеннические схемы с получением неучтённых объёмов для последующего незаконного сбыта.

Нарушение режимов функционирования может привести к авариям с повреждением оборудования, пожарами, уничтожением запасов сырья и продукции, остановке основной части предприятия

Остановка водоснабжения может привести к остановке производства.

Нарушение функционирования может привести к остановке подачи пара/ конденсата и остановке основного производства, остановке тепло/ водо/электроснабжения



Нарушение режимов функционирования может привести к авариям с разливом и выбросами опасных химических веществ, пожарами, уничтожением запасов сырья и готовой продукции, остановкой основного производства

Нарушения работы систем централизации управления движением составов (стрелки, семафоры, шлагбаумы на переездах) могут привести к сбоям в перемещении составов, аварийным столкновениям или схождению вагонов с опасными грузами с путей

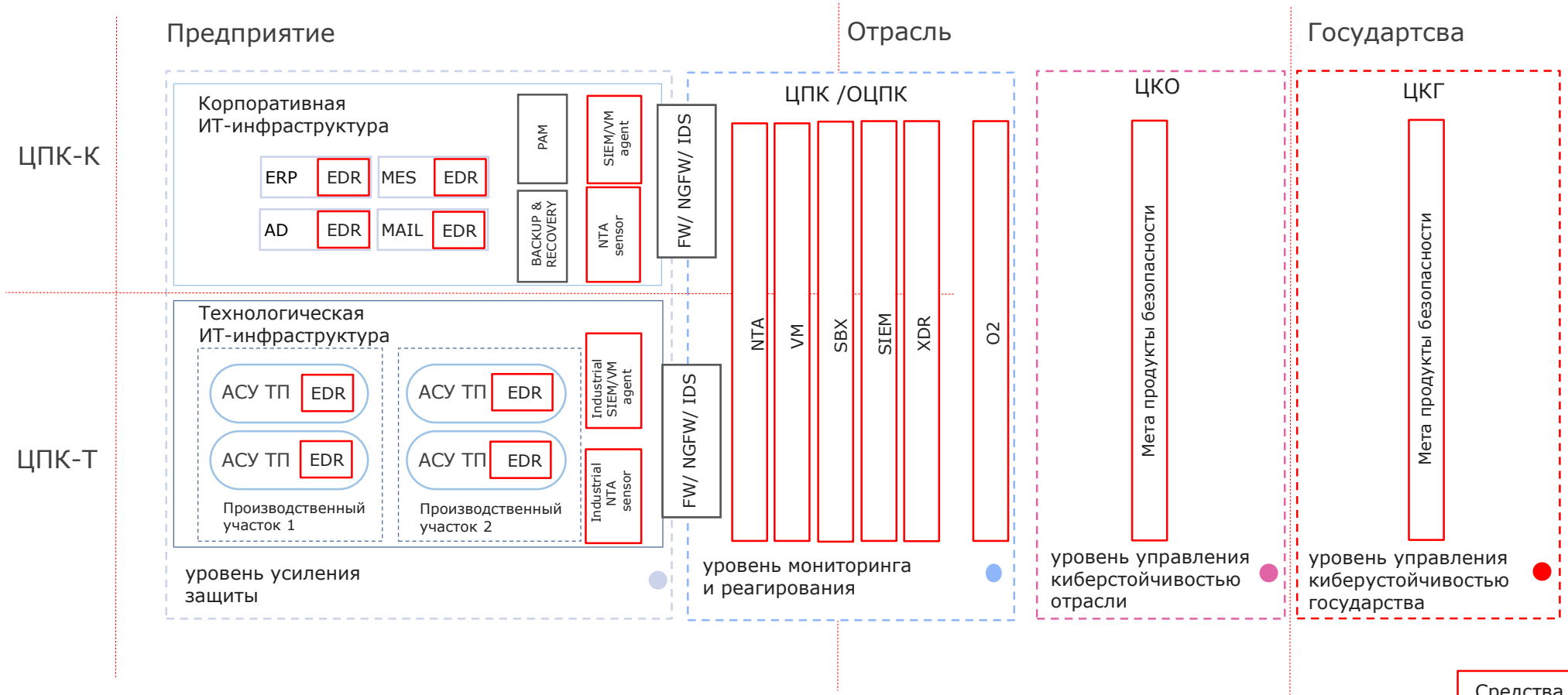
Вмешательство в работу УПВН реализовать мошеннические схемы с получением неучтённых объёмов для последующего незаконного сбыта.

Нарушение режимов функционирования может привести к авариям с повреждением оборудования, пожарами, уничтожением запасов сырья и продукции, остановке основной части предприятия

Нарушение работы очистных сооружений может привести к остановке водоснабжения предприятия, сбросу не очищенной воды

Финансово-экономический ущерб **Материальный ущерб** **Экологический ущерб** **Пострадавший персонал**

Архитектура систем безопасности (пример)



Создание ЦПК. 2 этап

Состав работ этапа:

- Построение первой очереди центра противодействия киберугрозам (ЦПК-Т)
- Разработка моделей процессов
- Разработка пользовательских пакетов выявления кибератак

Разработка проекта:

Основные технические решения

Карточки процессов кибербезопасности (4)

Стандарты MBSS

Решения по контенту

Правила нормализации и корреляции в ЭН

Кросс-продуктовые правила

Технические решения:

Первая очередь ЦПК-Т на базе комплексной платформы промышленной кибербезопасности

PT Industrial Cybersecurity Suite – PT ICS

Результат этапа → Минимальный объем технической документации, необходимой для внедрения

Установленный и введённый в эксплуатацию на площадке ЦПК-Т первой очереди

Киберучения. 3 этап

Сокращенный формат киберучений без влияния на Производство

Возможность приглашения внешней команды атакующих

Помощь команде защитников со стороны Исполнителя

Комплект методологии проведения киберучений

Комплект ТЗ на киберучения

Методика проведения

Регламент киберучений

Все необходимые формы отчетности

Результат этапа → Киберучения подтвердили эффективность Комплекса ЦПК-Т

Календарный план

Этап 1. Консалтинг

- Определение НС
- Определение целевых ИС
- Аудит и проектирование
- Подготовка ПАК ЦПК-Т
- Верификация НС

2 месяца

Этап 2. Создание ЦПК

- Внедрение сенсоров ЦПК-Т
- Наполнение базы активов пилотного сегмента
- Подключение источников и нормализация событий
- Настройка правил обнаружения и реагирования (ESC)
- Настройка безопасной конфигурации ИТ-инфраструктуры (харденинг)

3 месяца

Этап 3. Киберучения

- Предварительные учения (PT)
- Мониторинг и обнаружение атак (ЦПК-Т) → Отчет
- Боевые учения (Third Party) → Отчет

1 месяц

PT Industrial Cybersecurity Suite

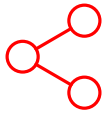
Единое решение для всей ИТ инфраструктуры предприятия

PT Industrial Cybersecurity Suite

PT ICS — комплексная платформа промышленной кибербезопасности

- **Продукты** с industrial агентами, пакетами экспертизы и спец лицензиями для использования в промышленных средах
- **Сервисы** по анализу защищенности и расследованию инцидентов в промышленных системах
- **Консалтинг** по эффективной трансформации архитектуры и процессов ИБ на промышленных предприятиях

Для всех отраслей: энергетика, транспорт, металлургия, машиностроение, судоходные компании, медицина, ЖКХ



Легко масштабируется от одной производственной площадки до размеров промышленного холдинга и отрасли

Единая экосистема продуктов для работы с корпоративной и технологической инфраструктурой предприятия

PT Industrial Cybersecurity Suite

PT ICS

Продукты

- ПТ ВЦ
- MP SIEM
- MP VM
- PT ISIM
- PT EDR
- PT SB

Сервисы ESC

- Анализ защищённости промышленных систем
- Ретроспективный анализ событий
- Расследование инцидентов
- Разработка пользовательского контента

Консалтинг ИБ2.0

- Консалтинг по недопустимым событиям
- Создание ЦПК
- Кибер учения

- Крупнейший в мире стек технологий и сервисов кибербезопасности для OT/IT инфраструктур промышленных предприятий
- Единый продуктовый портфель для корпоративных и технологических ИТ-инфраструктур
- Возможности продуктов, которыми уже пользуются Заказчики в корпоративных сегментах, теперь можно полноценно использовать и в сегментах OT/ICS

PT ICS. Продукты

Все продукты, входящие в PT ICS, «дружат» с АСУ ТП и позволяют обнаружить и остановить злоумышленника до того, как он успеет нанести ущерб.

IM	**ПТ ВЦ** Для промышленных систем	Взаимодействие специалистов отдельных служб при информировании, реагировании, и расследовании. Взаимодействие с НКЦКИ
SIEM	**MaxPatrol SIEM** Для промышленных систем	Обнаружение и управление инцидентами безопасности в промышленной инфраструктуре
VM	**MaxPatrol VM** Для промышленных систем	Управление уязвимостями, патч-менеджмент
NTA	**PT ISIM** Для промышленных систем	Глубокий анализ трафика технологических сетей, выявление атак и аномалий, Threat Hunting
SBX	**PT Sandbox** Для промышленных систем	Обнаружение и анализ вредоносного контента, инструментов APT
EDR	**PT XDR** Для промышленных систем	Обнаружение целевых и сложных угроз на конечных точках, реагирование

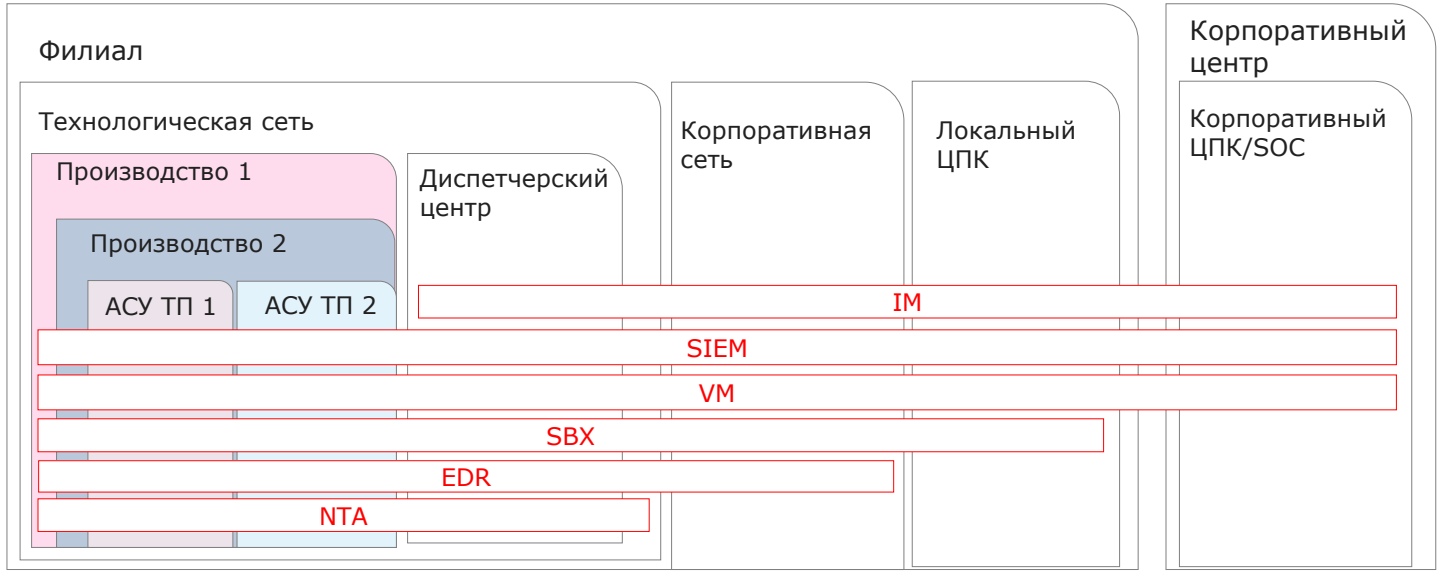
PT ICS. Продукты

Все продукты, входящие в PT ICS постоянно «накачиваются» кросс-продуктовой экспертизой с фокусом на платформы автоматизации и продукты конкретных производителей компонентов АСУ ТП

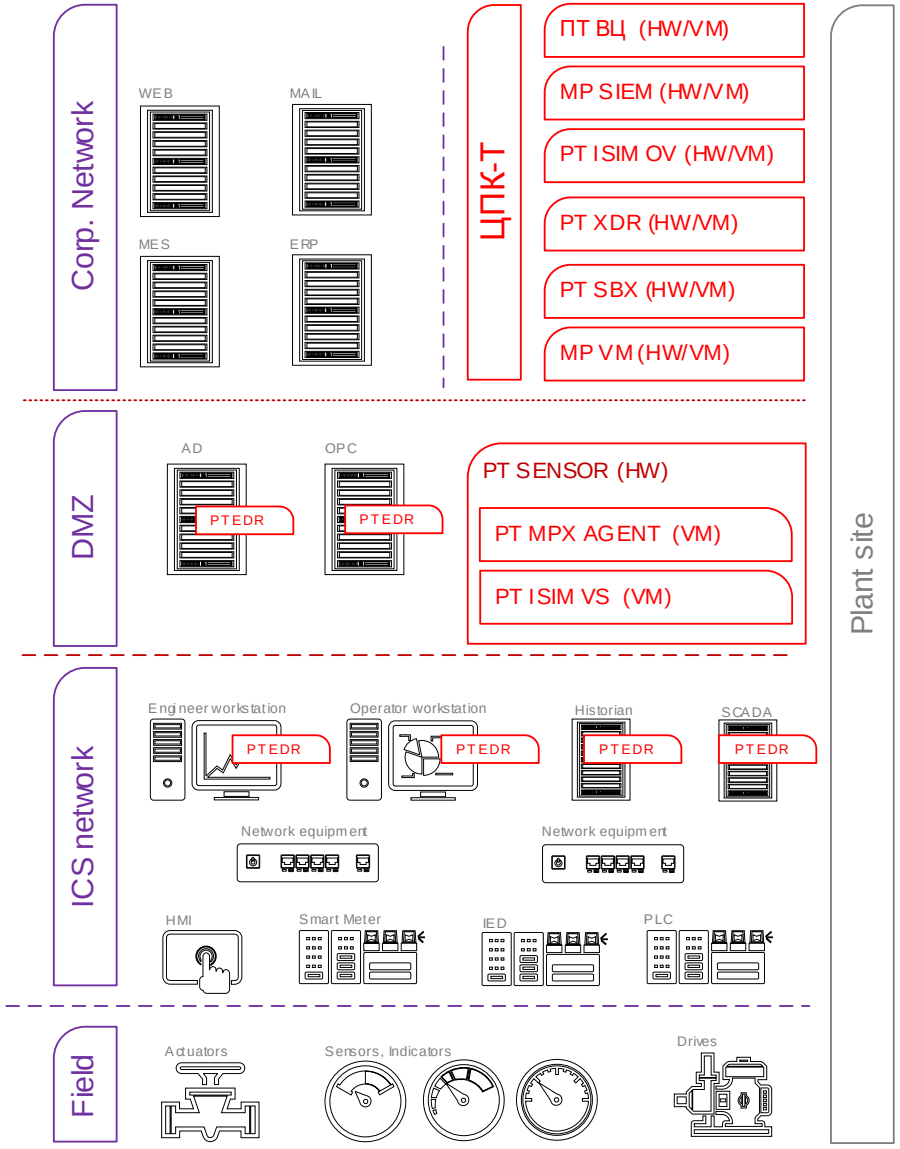
		Siemens Win CC PCS 7	Aveva Wonderware	Адастра Trace Mode	x ICS вендор
MP VM	Сканеры SCADA, Firmware Роботы поиска уязвимостей	✓	✓	✓	✓
MP SIEM	Транспорты к проприетарному Software и Firmware Нормализации событий SCADA, Firmware Кейс-ориентированные корреляции	✓	✓	✓	✓
PT ISIM	Поддержка промышленных сетевых протоколов Цепочки инцидентов в технологическом трафике	✓	✓	✓	✓
PT SBX	Эмуляция технологических сред Обнаружение SCADA / Firmware-специфичной malware	✓	✓	✓	✓
PT EDR	Совместимость со SCADA software	✓	✓	✓	✓

- Прозрачный Roadmap пакетов экспертизы
- По заявкам от партнёров и заказчиков Roadmap может быть изменён

PT ICS. Базовая архитектура



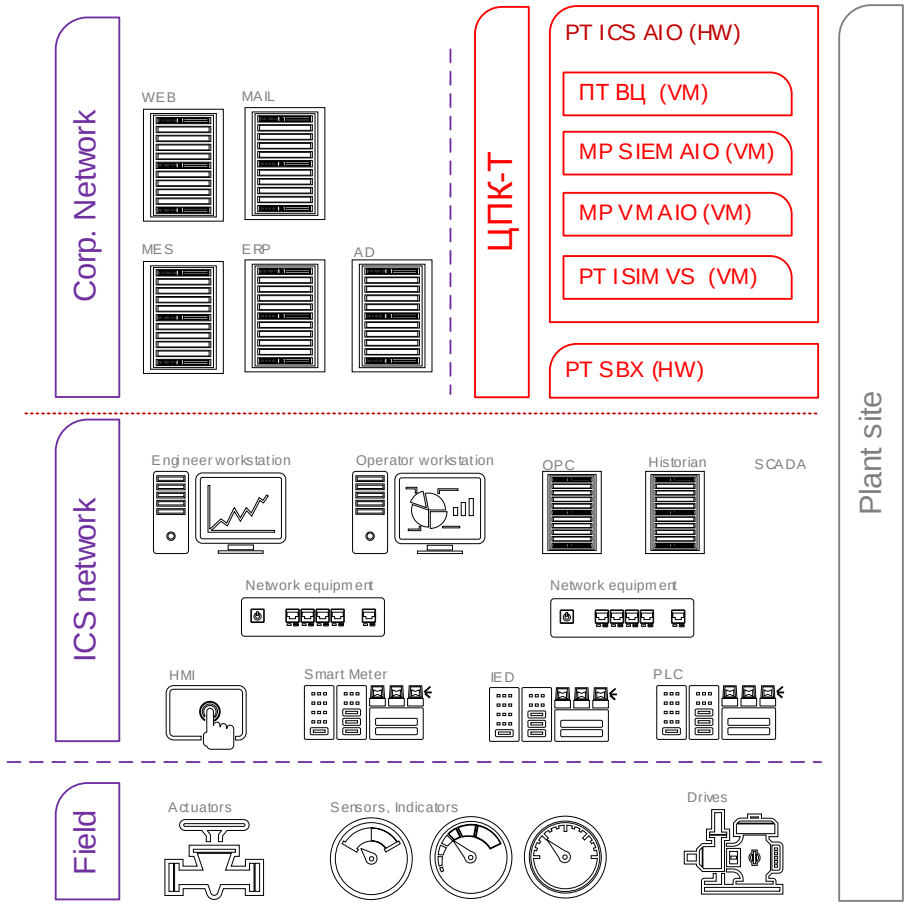
- Сквозные процессы управления безопасностью во всей компании – от ТОП менеджера до инженера наладки и диспетчера
- Единый для всей компании результат- отсутствие недопустимых событий во всей инфраструктуре и бизнес-процессах компании
- Максимальная автоматизация процессов и операций управления безопасностью в масштабе компании
- Централизация всех функций управления безопасностью.



Варианты решений

- Максимальное покрытие инфраструктуры средствами мониторинга безопасности, управления уязвимостями, обнаружения и реагирования на инциденты безопасности
- Возможность поэтапного масштабирования решения на уровне ОГ
- Централизация основных функций и процессов управления безопасностью за счёт возможности подключения имеющихся стандартных (СЗИ сторонних разработчиков – антивирусы, МЭ,) источников событий и не стандартных (Серверы исторических данных, проприетарные серверы логирования SCADA, ПЛК, Проприетарное прикладное ПО)
- Обеспечение взаимодействия специалистов служб ИБ, эксплуатации АСУ, Оперативно диспетчерских служб, служб ИТ в рамках базовых процессов управления безопасностью
- Бесшовная интеграция ЦПК-Т с Корпоративным SOC на базе решений Positive Technologies

Варианты решений



- Оптимальный объем и максимально сжатые сроки покрытия инфраструктуры небольших производственных площадок средствами мониторинга безопасности, управления уязвимостями, обнаружения и реагирования на инциденты безопасности
- Неинвазивность решения – все компоненты ЦПК-Т находятся за периметром технологических сетей
- Централизация основных функций и процессов управления безопасностью за счёт возможности подключения имеющихся стандартных (СЗИ сторонних разработчиков – антивирусы, МЭ,) источников событий и не стандартных (Серверы исторических данных, проприетарные серверы логирования SCADA, ПЛК, Проприетарное прикладное ПО)
- Обеспечение взаимодействия специалистов служб ИБ, эксплуатации АСУ, Оперативно диспетчерских служб, служб ИТ в рамках базовых процессов управления безопасностью
- Бесшовная интеграция ЦПК-Т с Корпоративным SOC на базе решений Positive Technologies

Спасибо
за внимание