PT Industrial Security Incident Manager

Система глубокого анализа трафика в промышленных ИТ-инфраструктурах

ptsecurity.com

Области применения

- Автоматизированные системы управления технологическими процессами промышленных предприятий
- Автоматизированные системы управления субъектов КИИ
- Системы управления инженерной инфраструктурой городских и муниципальных служб, центров обработки данных, деловых и торговых центров
- Системы управления движением рельсового транспорта
- Промышленные предприятия и производства с распределенной инфраструктурой
- Промышленный интернет вещей (IIoT)
- DICOM-совместимые системы и сети медицинских учреждений

PT Industrial Security Incident Manager (PT ISIM) контролирует безопасность технологической сети, позволяет вовремя распознать угрозы кибербезопасности и предотвратить ущерб предприятию.

PT ISIM предоставляет следующие возможности:

1. Наблюдаемость и контроль изменений

Пользователь видит, из чего состоит технологическая сеть, контролирует изменения и получает возможность повысить киберустойчивость инфраструктуры.

2. Мониторинг безопасности

Пользователь видит события информационной безопасности и может предотвратить опасные технологические нарушения.

3. Обнаружение и анализ угроз

Пользователь знает об актуальных угрозах безопасности, получает возможность защищать от них сеть и поддерживать непрерывность технологических и бизнес-процессов.

PT ISIM работает с копией трафика, не влияет на функционирование технологического оборудования и контролируемых сетевых сегментов. Помогает соблюдать требования регулирующих органов, в том числе выполнение приказов ФСТЭК № 239 и № 31, норм закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Сценарии использования PT ISIM

Инвентаризация технологической сети и выявление новых узлов

Невозможно обеспечивать устойчивую работу АСУ ТП без четкого понимания состава и структуры технологической сети.

С PT ISIM сотрудники службы ИБ и эксплуатации АСУ ТП могут контролировать целостность сети, обнаруживать появление в сети новых узлов (рабочих станций, контроллеров или сетевых устройств), мгновенно выявлять попытки внешних подключений к компонентам АСУ ТП и выходы в интернет из технологической сети.

Выявление аномалий и угроз в технологическом трафике

Не весь технологический трафик проходит через межсетевой экран. Большой объем коммуникаций остается внутри технологической сети, и в этом трафике также важно выявлять угрозы.

Благодаря профилированию трафика, PT ISIM может в реальном времени обнаруживать нелегитимный удаленный доступ к компонентам АСУ ТП, активность ВПО (вирусы, трояны, шифровальщики), создание прокси-серверов и туннелей, использование слабых паролей и паролей по умолчанию.

Обнаружение эксплуатации уязвимостей и других техник злоумышленников

Даже в технологических сетях целью злоумышленников часто становятся элементы классической ИТ-инфраструктуры.

PT ISIM умеет определять атаки на Windows- и Linux-системы, на стандартное сетевое оборудование и промышленные устройства: более 8000 правил и индикаторов угроз доступны «из коробки». Для обнаружения актуальных угроз безопасности PT ISIM постоянно наполняется новой экспертизой.

Выявление опасных технологических команд

Технологические нарушения могут происходить из-за появления в сети опасных команд управления, отправляемых злоумышленниками, о которых служба эксплуатации АСУ ТП ничего не знает.

PT ISIM выявляет перепрошивку ПЛК, форсирование переменных, очистку памяти — легитимные, но редко происходящие в работающей АСУ ТП операции. Для того чтобы можно было видеть не только отдельные действия, но и контекст вокруг них, PT ISIM анализирует все аномальные события, которые обнаруживает в инфраструктуре, и объединяет их в цепочки.

Соблюдение требований регулирующих организаций

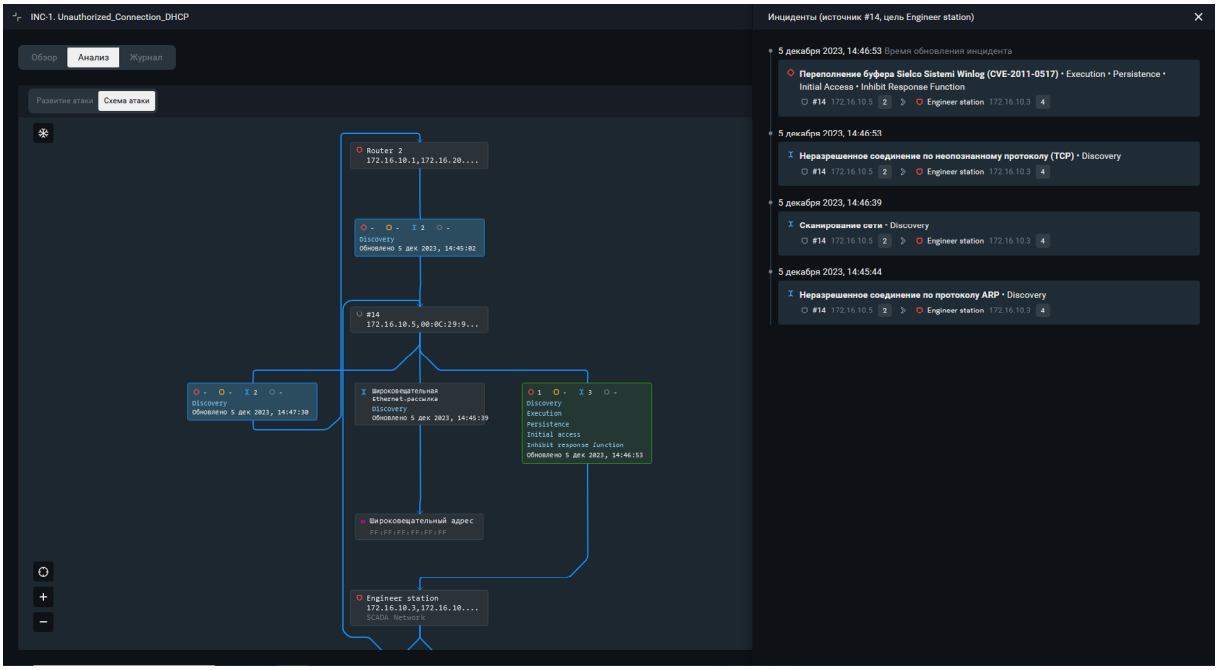
Субъекты критической инфраструктуры должны соответствовать требованиям регуляторов.

PT ISIM помогает обеспечить выполнение приказов ФСТЭК № 31, № 239, норм закона № 187-ФЗ о безопасности объектов критической информационной инфраструктуры, также помогает выстраивать взаимодействие с центрами ГосСОПКА.

Обнаружение ВПО в трафике и возможность отправлять подозрительные файлы на анализ

Передача по сети файлов может свидетельствовать о возможном заражении ВПО или преднамеренном изменении конфигурации системы злоумышленниками.

PT ISIM извлекает передаваемые по сети файлы для анализа в PT Sandbox, чтобы выявить нелегитимную передачу прошивок ПЛК, проектов SCADA или распространение ВПО, в том числе не обнаруживаемого классическими антивирусами.



8000

правил обнаружения промышленных угроз в сетевом трафике:

Siemens, Schneider Electric, Yokogawa, Emerson, Honeywell, ABB, Wonderware, GE, Allen-Bradley, МЭК 60870-5-104/101, МЭК-61850, Modbus TCP, OPC UA, «Прософт-Системы», ПТК «Квинт»

Полный список протоколов

- PT ISIM определяет угрозы в соответствии с матрицей MITRE ATT&CK и приказом ФСТЭК России № 239
- PT ISIM может обнаруживать актуальные угрозы АСУ ТП «из коробки» без кропотливой предварительной настройки

Промышленная экспертиза PT Industrial Security Threat Indicators

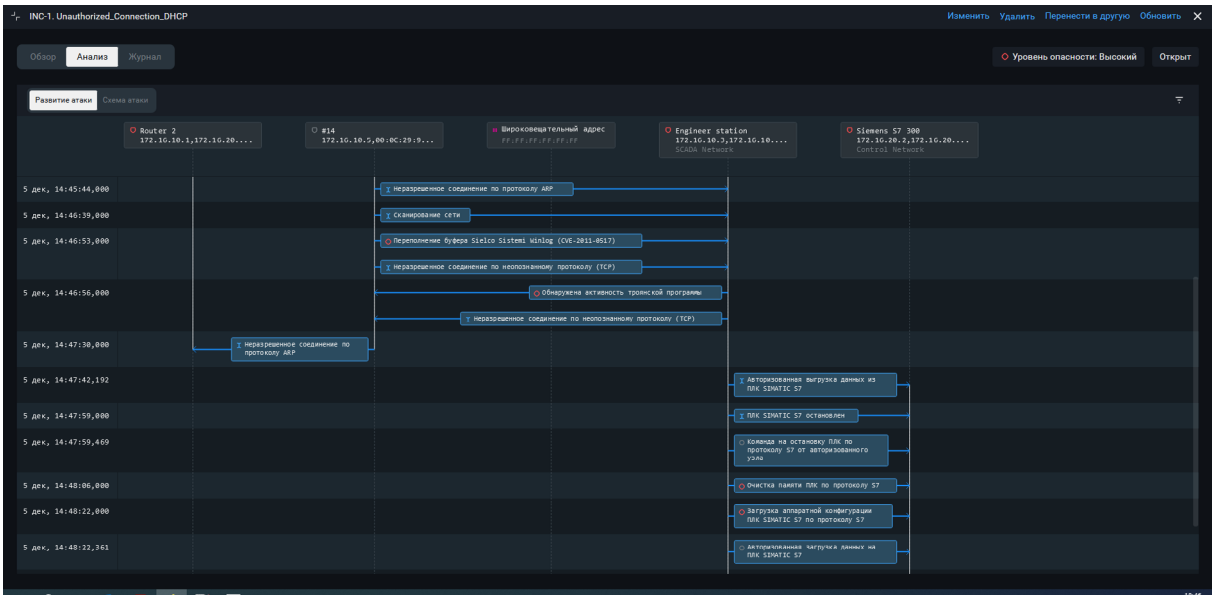
Для обнаружения нарушений информационной безопасности PT ISIM использует собственную уникальную базу киберугроз — PT Industrial Security Threat Indicators (PT ISTI).

PT ISTI позволяет на ранней стадии выявлять подготовку к кибератакам на ПО и оборудование АСУ ТП (сканирование узлов, эксплуатацию уязвимостей), находить недостатки в настройке систем (слабые пароли, отключенное шифрование), обнаруживать применение потенциально небезопасных средств сетевого взаимодействия (например, устаревшие и уязвимые версии протоколов) и использование недокументированных, в том числе небезопасных, команд управления оборудованием (ПЛК, промышленными коммутаторами и терминалами).

База угроз помогает PT ISIM превентивно выявлять уязвимости сети АСУ ТП, в том числе те, которые эксплуатируются вирусами-шифровальщиками (например, WannaCry, Petya) и другим вредоносным ПО (например, Trisis, Triton), а также идентифицировать в сети работу майнеров криптовалюты.

Эксперты Positive Technologies регулярно пополняют базу PT ISTI новыми сигнатурами и правилами обнаружения атакна промышленную и ИТ-инфраструктуру. База формируется на основе уязвимостей и типичных недостатков информационной безопасности АСУ ТП, найденных специалистами компании в ходе проектов по анализу защищенности, а также в рамках регулярных исследований новых угроз.

База содержит несколько тысяч индикаторов компрометации сети, сигнатур, правил обнаружения атак на распространенные системы. Доставка обновлений в PT ISIM осуществляется вручную или автоматически в виде пакетов экспертизы.



- PT ISIM гибко масштабируется в зависимости от конкретных требований и задач.
- Опции лицензирования PT ISIM позволяют расширять функциональность системы без замены оборудования.
- Итоговое количество компонентов PT ISIM в составе системы не ограничено.
- На начальных этапах развертывания система может использоваться только на критически важных площадках с последующим полным покрытием всех процессов в промышленной сети.

Компоненты PT ISIM

Сенсоры PT ISIM View Sensor

Сенсоры PT ISIM View Sensor применяются для анализа и хранения сетевого трафика, устанавливаются на уровне сегмента сети АСУ ТП, в котором расположены АРМ операторов, серверы SCADA и ПЛК.

PT ISIM Overview Center

Управляющая консоль Overview Center устанавливается на уровне ситуационного центра (SOC) или ЦОД и собирает события с подчиненных сенсоров, а также используется для их централизованной настройки и обновления. С помощью Overview Center можно разграничить доступ пользователей к разным сенсорам и реализовать сквозную авторизацию (SSO).

Сенсоры и управляющая консоль PT ISIM работают под управлением Astra Linux SE или Debian и взаимодействуют по защищенному протоколу HTTPS. Для установки и первоначальной настройки может требоваться доступ по протоколу SSH.

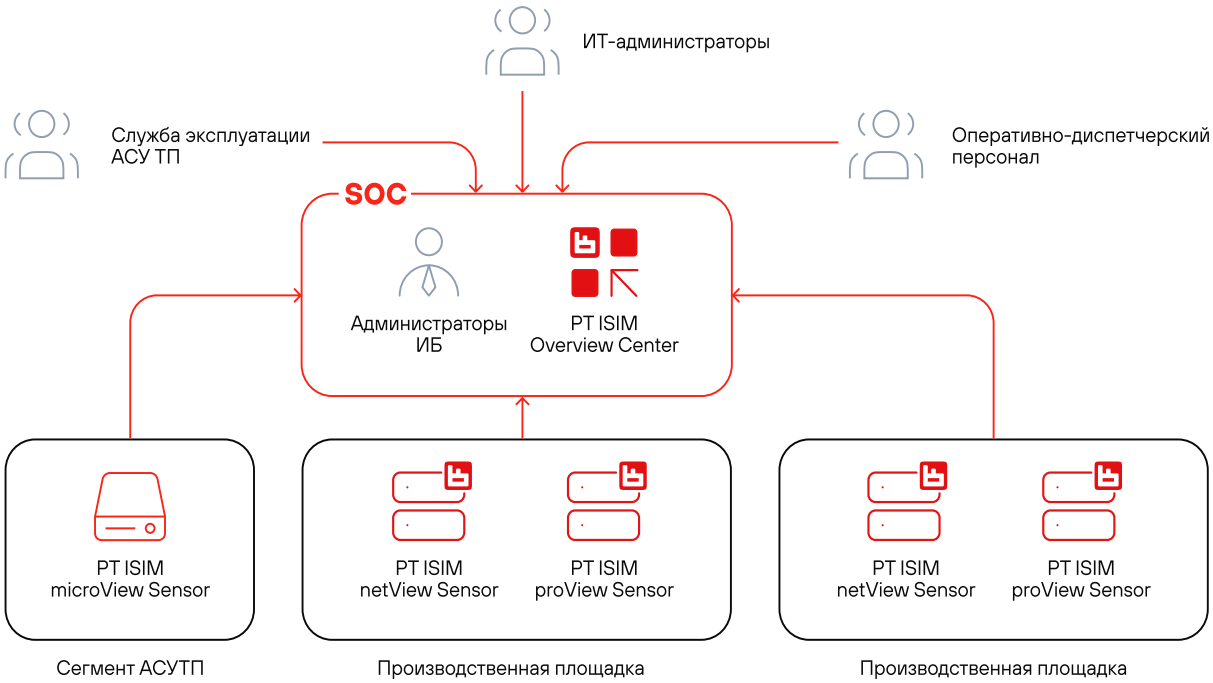


Схема № 1. Пример архитектуры с применением сенсоров PT ISIM microView Sensor, netView Sensor, proView Sensor и управляющей консоли PT ISIM Overview Center

Алгоритм обработки трафика

Сенсоры PT ISIM обрабатывают копию сетевого трафика и выявляют события информационной безопасности. В результате обработки трафика регистрируются события ИБ и производится инвентаризация сети: сохраняется информация об узлах, строится визуальная топология взаимодействия между ними — карта сети.

Сенсор собирает трафик со SPAN-порта коммутатора. Исходная копия трафика сохраняется на сервере в формате PCAP.

Нормализованные и отфильтрованные сообщения проверяются на соответствие правилам корреляции.

Если правило срабатывает, регистрируется событие ИБ.

Связанные события объединяются в цепочки, подготовленные для расследования.

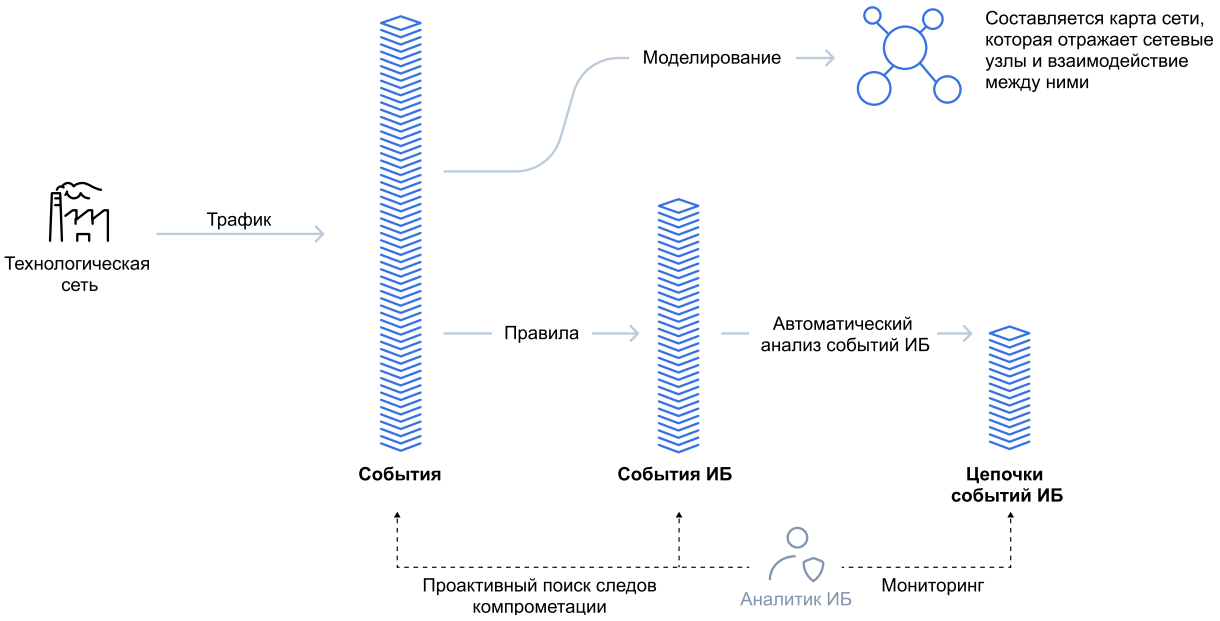


Схема № 2. Алгоритм обработки трафика

Сенсоры PT ISIM могут передавать информацию о событиях и инцидентах напрямую в SIEM-систему (например, MaxPatrol SIEM).

В PT ISIM View Sensor поступает копия трафика с порта зеркалирования коммутатора (SPAN), с TAP-устройства и брокера данных. Копию трафика можно направить в сенсор через диод данных — это обеспечит более высокий уровень защиты. Обратного трафика от PT ISIM в сторону технологической сети на порт SPAN не предусмотрено. Для работы сенсоров с Overview Center нужна двусторонняя связь по порту 443.

Опциональные компоненты

Для подключения сенсоров PT ISIM могут использоваться следующие дополнительные компоненты сторонних производителей.

- **Аппаратный диод данных**

Обеспечивает однонаправленную передачу данных со SPAN порта коммутатора на сенсор PT ISIM на физическом уровне

- **Агрегирующее устройство**

Позволяет уменьшить количество закупаемых сенсоров PT ISIM за счет агрегации трафика со SPAN-портов нескольких коммутаторов

- **Регенерирующее устройство**

Позволяет реплицировать трафик с одного SPAN-порта на несколько других портов для устройств мониторинга

- **TAP-устройство**

Служит для получения копии трафика при отсутствии SPAN-порта

Функциональные возможности

PT ISIM View Sensor	microView Sensor	netView Sensor	proView Sensor
Глубокий анализ технологического трафика ▪ Непрерывный анализ копии трафика в промышленной сети без влияния на работу технологического оборудования ▪ Глубокий разбор (DPI) коммуникационных протоколов, включая промышленные ▪ Запись, хранение и экспорт трафика сети АСУ ТП **Инвентаризация технологической инфраструктуры** ▪ Обнаружение узлов и сегментов сети АСУ ТП, контроль подключения новых узлов и целостности сетевых коммуникаций в реальном времени ▪ Автоматическое построение карты сетевых коммуникаций и узлов сети АСУ ТП ▪ Автоматическое формирование белых списков узлов сети и сетевых соединений, управление списками **Обнаружение и анализ угроз** ▪ Обнаружение неавторизованного изменения технологических параметров, контроль доступа к параметрам ПЛК по сети, обнаружение неавторизованного управления ПЛК ▪ Обнаружение эксплуатации уязвимостей в ПО и оборудовании АСУ ТП ▪ Обнаружение сетевых аномалий ▪ Создание и настройка собственных правил анализа и обнаружения угроз **Интеграция** ▪ Подключение к PT ISIM Overview Center ▪ Передача сообщений о событиях ИБ на syslog-сервер ▪ Отправка почтовых уведомлений об инцидентах	+	+	+
Регистрация, хранение, поиск и фильтрация событий	–	+	+
Извлечение файлов из трафика	–	+	+
Контроль критически важных параметров техпроцесса	–	–	+
Создание графических мнемосхем и визуализация инцидентов на мнемосхеме техпроцесса	–	–	+

PT ISIM Overview Center	
Предоставление сводной информации о зафиксированных инцидентах ИБ	+
Централизованное управление сенсорами (обновление, диагностика)	+
Обновление базы решающих правил на подключенные сенсоры PT ISIM	+
Управление доступом пользователей к сенсорам	+
Сквозная авторизация (SSO)	+

Требования к инфраструктуре

	microView Sensor	**netView Sensor**	**proView Sensor**	**Overview Center**
Количество активов в сети	До 100	До 1 тыс.		–
Объем обрабатываемого трафика	До 10 Мбит/с	До 100 Мбит/с		–
Пропускная способность внешнего канала связи	До 5 Мбит/с			

Аппаратные требования

	microView Sensor	**netView Sensor**	**proView Sensor**	**Overview Center**
Центральный процессор	Intel Core i5	Intel Xeon 3,5 ГГц, кэш 8 МБ, 4C/8T		
Память (ОЗУ)	16 ГБ DDR4 рекомендуется 32 ГБ	2 × 16 ГБ DDR4		
Дисковое пространство	SSD 256 ГБ	1 ТБ SSD или 1 ТБ SSD и 4 ТБ HDD*		1 ТБ SSD
Сетевой адаптер	2 x 10/100/1000 Мбит/с RJ-45	6 x 10/100/1000 Мбит/с RJ-45		2 x 10/100/1000 Мбит/с RJ-45
Операционные системы	Debian 10.12 Buster Astra Linux Special Edition 1.7.2 в режиме защищенности «Воронеж» или «Смоленск»			

Примеры использования PT ISIM

Локальная установка

Преимущества

Минимальные трудозатраты, не требуются специальные знания, глубокое предварительное исследование технологического процесса и сети АСУ ТП.

Подходит для небольших инфраструктур и для поэтапного масштабирования продукта на крупных предприятиях с распределенной инфраструктурой.

Особенности

На каждый промышленный объект устанавливается минимальный набор компонентов: PT ISIM View Sensor (любая редакция) и, если нужно, однонаправленный шлюз данных для мониторинга событий информационной безопасности силами специалистов клиента.

Каждый сенсор используется и управляется отдельно.

Области применения

Локальные системы управления.

Отдельные сегменты или объекты распределенных систем управления.

Отдельные автоматизированные производственные объекты, технологические установки, инженерные объекты исооружения.

* Дополнительный HDD используется для хранения PCAP-файлов, увеличения общего времени хранения событий, статистики и PCAP-файлов, а также повышения стабильности работы ОС.

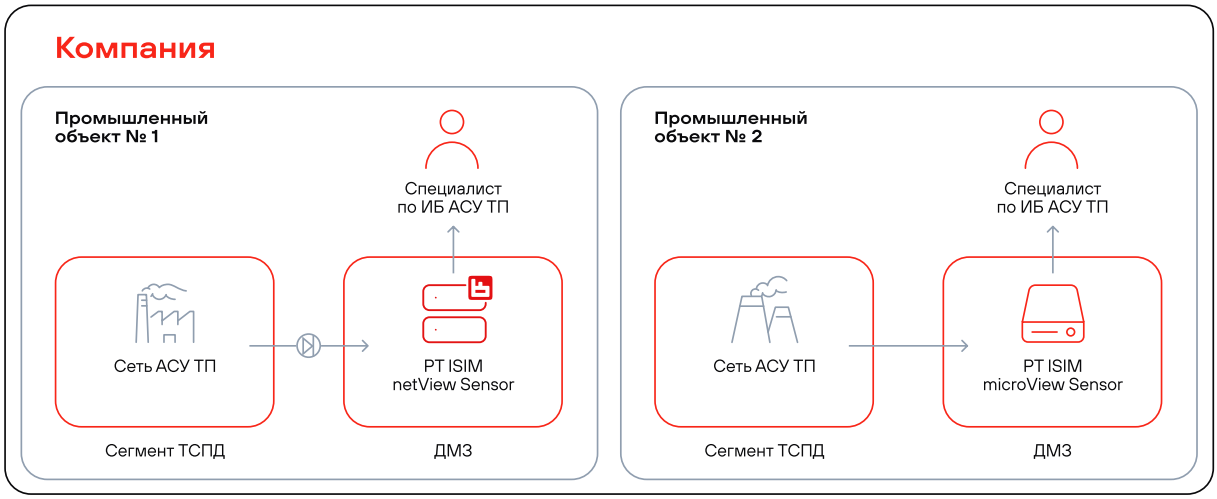


Схема № 3. Локальная установка

Распределенная установка

Преимущества

Централизованный мониторинг технологических сетей распределенных инфраструктур.

При использовании сенсоров PT ISIM proView Sensor векторы атак, найденные в ходе анализа защищенности, могут быть учтены в конфигурации системы мониторинга. Это позволяет оперативно реагировать на сложные кибератаки, специфичные для конкретной АСУ ТП, включая эксплуатацию уязвимостей нулевого дня.

Особенности

Организуется SOC (security operations center) — общий ситуационный центр для обработки инцидентов.

PT ISIM Overview Center управляет всеми компонентами PT ISIM.

Области применения

Распределенные системы управления.

Распределенные промышленные объекты.

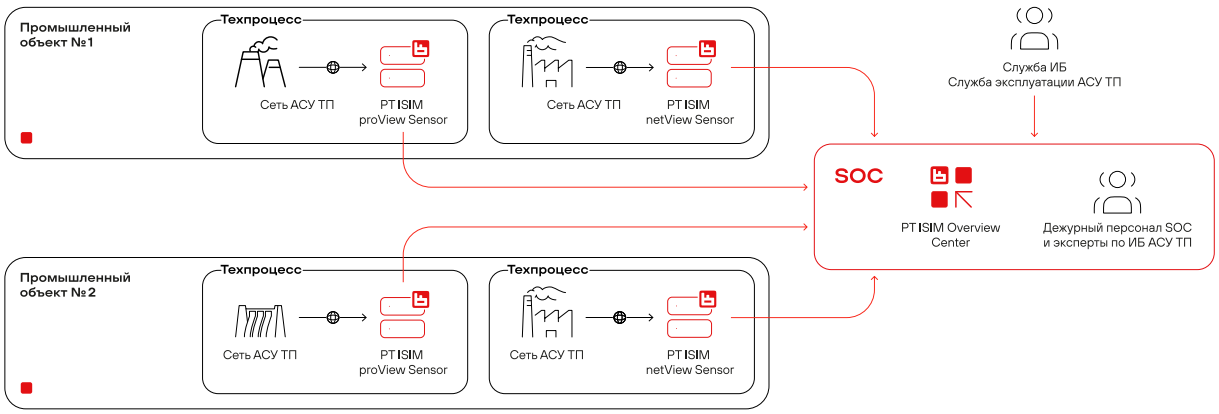


Схема № 4. Распределенная установка

Комплексная установка с использованием компонентов PT ICS

Преимущества

Комплексная защита промышленной ИТ-инфраструктуры компании: сетевых узлов, SCADA-серверов, ПЛК, рабочих станций.

Если в компании уже установлены продукты Positive Technologies для защиты корпоративной сети, достаточно расширить существующие лицензии, чтобы распространить их действие на технологический сегмент. При этом специалисты продолжат работу с привычными им инструментами.

Особенности

В состав PT ICS, кроме PT ISIM, входят MaxPatrol SIEM, MaxPatrol EDR, MaxPatrol VM и PT Sandbox с пакетами промышленной экспертизы.

MaxPatrol SIEM используется для сбора и анализа событий с прикладного уровня систем АСУ ТП: SCADA-серверов, инженерных рабочих станций или контроллеров.

MaxPatrol VM используется для выявления уязвимостей в промышленных системах.

В PT Sandbox выполняется поведенческий анализ файлов от PT ISIM (из сетевого трафика) или MaxPatrol EDR (с конечных устройств).

Инциденты централизованно обрабатываются в SIEM-системе.

Области применения

Обеспечение комплексной киберустойчивости промышленных предприятий.

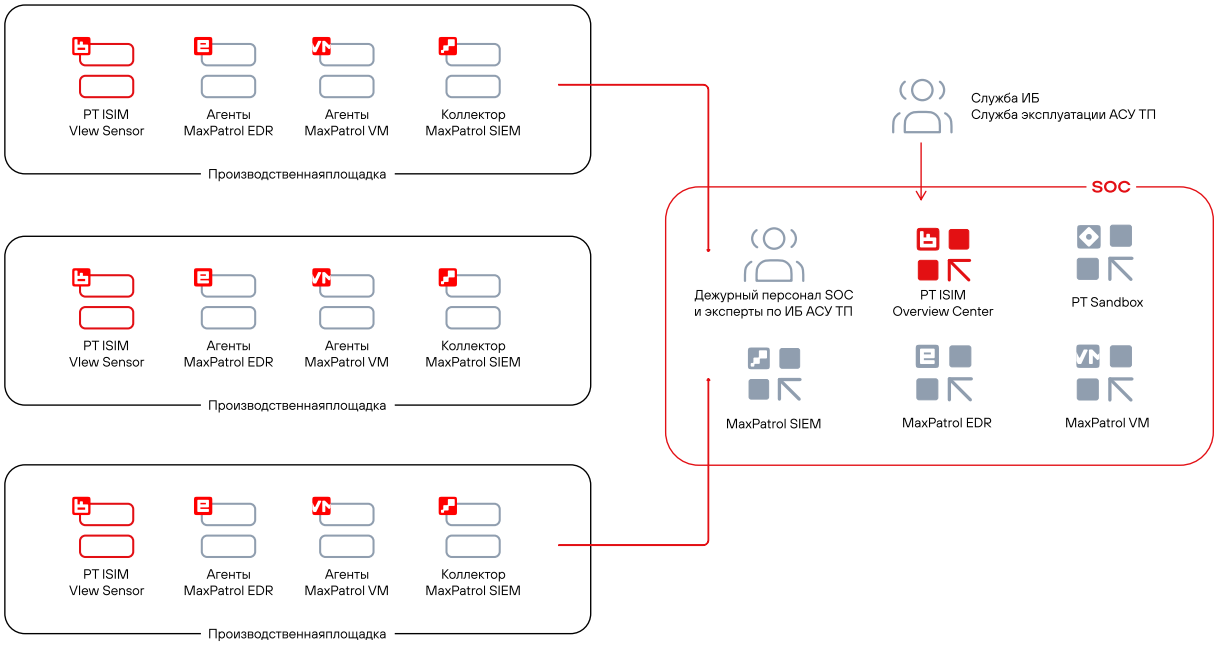


Схема № 5. Комплексная установка с использованием компонентов PT ICS

Реализация мер защиты объектов КИИ согласно приказу ФСТЭК № 239

PT ISIM помогает соблюдать требования регулирующих органов, в том числе выполнение приказов ФСТЭК № 239 и № 31, норм закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Обозначение и номер меры	Мера обеспечения безопасности	Категория значимости		
		3	2	1
I. Идентификация и аутентификация (ИАФ)				
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
V. Аудит безопасности (АУД)				
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.7	Мониторинг безопасности	+	+	+
VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+
СОВ.2	Обновление базы решающих правил		+	+
XII. Реагирование на компьютерные инциденты (ИНЦ)				
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+
XIII. Управление конфигурацией				
УКФ.4	Контроль действий по внесению изменений			

ptsecurity.com
pr@ptsecurity.com

PT ISIM_A4.RUS.0007.03.MAR.05.2024