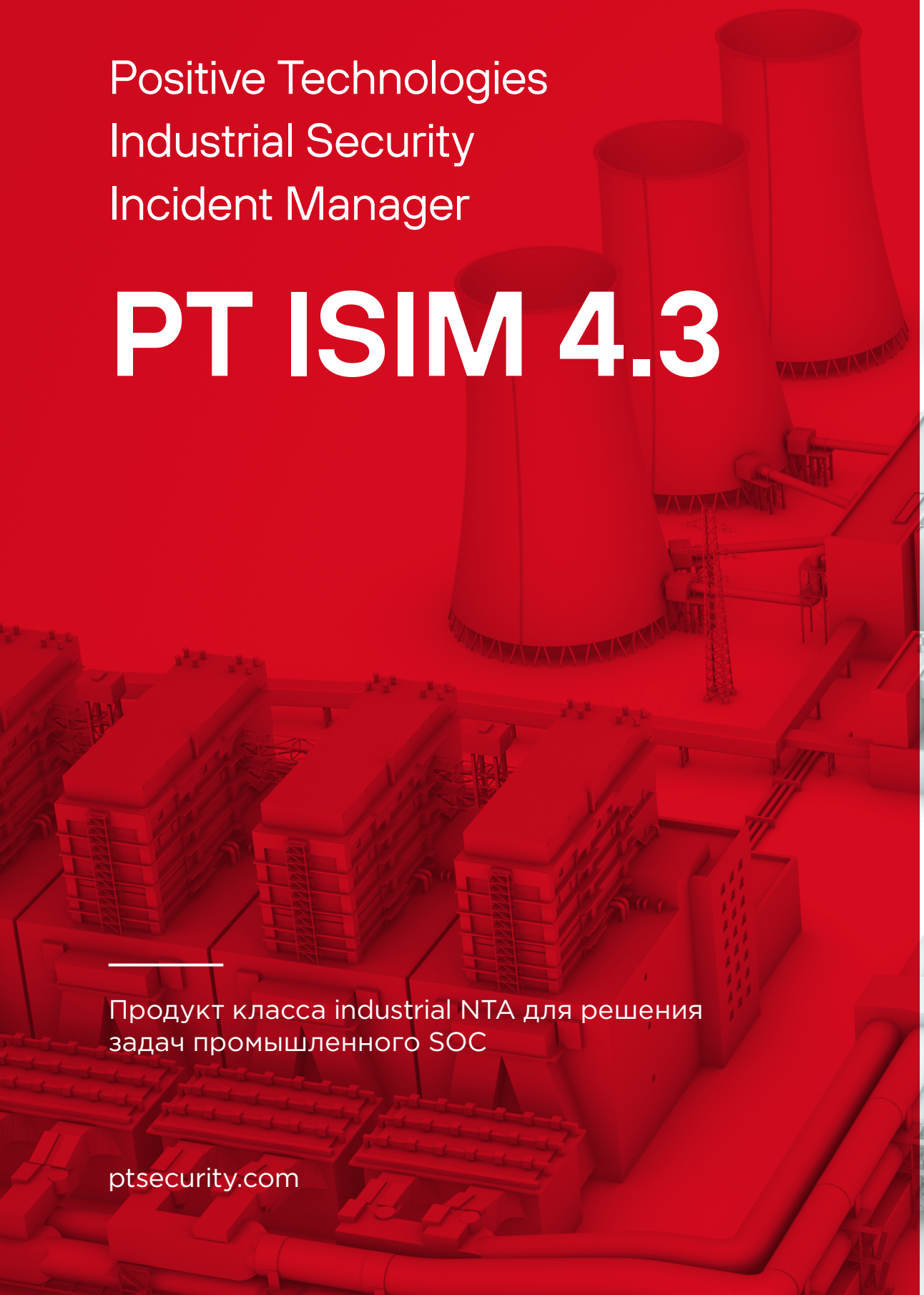
ОПИСАНИЕ ПРОДУКТА

Positive Technologies
Industrial Security
Incident Manager

PT ISIM 4.3



Продукт класса industrial NTA для решения задач промышленного SOC

ptsecurity.com

Ключевые возможности и преимущества

PT Industrial Security Incident Manager — это эффективный инструмент непрерывного анализа трафика технологических сетей предприятий. Является профессиональным продуктом класса NTA (network traffic analysis) для промышленных центров реагирования на инциденты информационной безопасности (SOC). Предоставляет специалистам SOC возможность контролировать работу АСУ ТП с точки зрения информационной безопасности.

Области применения

- Автоматизированные системы управления технологическими процессами промышленных предприятий
- Системы управления городской инженерной инфраструктурой
- Автоматизированные системы управления объектов критической инфраструктуры
- Системы управления инженерной инфраструктурой центров обработки данных, деловых и торговых центров
- Промышленные предприятия и производства с распределенной инфраструктурой

- **Компонент платформы PT ICS.** Обнаруживает сетевые угрозы, нарушения регламентов ИБ и аномалии в технологическом трафике. С помощью PT ISIM единый SOC получает сетевые контекстные данные о взаимодействии компонентов АСУ ТП и может определить источник угрозы, масштабы атак и выбрать правильный способ реагирования на инцидент.
- **Быстрое внедрение и повышение защищенности.** Архитектура пассивного мониторинга и режим автоматического обучения PT ISIM позволяют в кратчайшие сроки подключить систему к действующей сети АСУ ТП и получить первые результаты внедрения.
- **Цепочки инцидентов.** На основе выявленных событий автоматически строится граф развития атаки. PT ISIM определяет, насколько она опасна, с учетом важности затронутых злоумышленником ресурсов и характера его действий.
- **Визуализация инцидентов.** За счет удобных средств графического отображения элементов сетевой топологии и технологического процесса (мнемосхем) можно визуализировать инциденты информационной безопасности, в том числе на уровне бизнес-логики.
- **Обнаружение нарушений политик ИБ.** Система позволяет вовремя выявлять нарушения политик информационной безопасности и установленных предприятием технологических регламентов.
- **Легкая интеграция в существующие процессы ИБ.** PT ISIM располагает всеми необходимыми механизмами для встраивания в существующие процессы ИБ предприятия и их расширения: верхнеуровневой и детализированной отчетностью, передачей отдельных событий и инцидентов на уровень SOC в SIEM- и другие системы, возможностью расследования инцидентов и так далее.
- **Инвентаризация и контроль целостности сети АСУ ТП.** PT ISIM автоматически инвентаризирует элементы сети, включая компоненты промышленной системы управления, и непрерывно контролирует целостность технологической сети.
- **Учет специфики предприятия.** С помощью PT ISIM можно отслеживать угрозы и векторы атак, уникальные для промышленного объекта. Для этого используются данные, получаемые в результате анализа защищенности АСУ ТП предприятия.

6300
правил обнаружения промышленных угроз

- **Минимальное количество ложноположительных срабатываний.** За счет настраиваемых правил обнаружения угроз PT ISIM помогает сосредоточиться на действительно важных событиях ИБ.

- **Соответствие требованиям промышленной среды.** Физические условия эксплуатации в промышленности бывают крайне агрессивными. Исполнение компонентов PT ISIM подбирается с учетом специфики отрасли и защищаемого предприятия.

- **Определение сегментов сети.** PT ISIM автоматически определяет сегменты технологической сети, обнаруживая маршрутизаторы и подсети. За счет визуализации накопленных данных можно контролировать выполнение требований к сегментированию.

PT Industrial Security Threat Indicators

Для обнаружения нарушений информационной безопасности PT ISIM использует собственную уникальную базу промышленных киберугроз — PT Industrial Security Threat Indicators (PT ISTI). Она позволяет на ранней стадии выявлять подготовку к кибератакам на ПО и оборудование АСУ ТП (сканирование узлов сети АСУ ТП, эксплуатацию уязвимостей), находить недостатки в настройке систем (слабые пароли, отключенное шифрование), обнаруживать применение потенциально небезопасных средств сетевого взаимодействия (например, устаревшие 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, что 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 PT ISTI сигнатурами и правилами обнаружения атак на промышленное оборудование и программное обеспечение. 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 (ABB, Emerson, Hirschmann, Schneider Electric, Siemens, Yokogawa и так далее). Доставка обновлений в PT ISIM осуществляется вручную или автоматически с помощью пакетов экспертизы.

PT ISIM netView Sensor не требует от пользователей специальных навыков ни во внедрении, ни в эксплуатации

PT ISIM определяет угрозы в соответствии с матрицей MITRE ATT&CK и приказом ФСТЭК России № 239

Цели и задачи

PT ISIM предназначена для поддержки непрерывности и для повышения уровня защищенности, доступности технологических процессов с помощью анализа сетевого трафика и превентивного поиска угроз (threat hunting), направленных на АСУ ТП.

Цели внедрения системы

- Непрерывный анализ киберзащищенности АСУ ТП
- Контроль действий персонала и подрядчиков
- Обнаружение нарушений ИБ и кибератак на АСУ ТП

Меньше
1 часа

занимают пуск
и автоматическая настройка
PT ISIM netView Sensor
на действующем сегменте
АСУ ТП

- Своевременное выявление инцидентов и информирование ответственных лиц
- Создание доверенного источника данных для эффективного расследования нарушений ИБ
- Анализ инцидентов, включая определение причин возникновения, а также оценку последствий
- Планирование мер по устранению и предотвращению инцидентов
- Обеспечение соответствия требованиям регулирующих организаций (в том числе выполнение приказов ФСТЭК № 31, 239, норм закона о безопасности КИИ № 187-ФЗ и выстраивание взаимодействия с центрами ГосСОПКА).

Решение технических задач

- Непрерывная обработка копии трафика АСУ ТП, получаемого через однонаправленный шлюз (диод данных)
- Анализ событий на уровне коммуникационных протоколов, включая промышленные (CIP, DIGSI, GOOSE, IEC104, MMS, Modbus, OPC, PROFINET DCP, Schneider Electric UMAS, Siemens S7, SPA-Bus, протоколы устройств Yokogawa, компании «ЭКРА» и другие)
- Автоматическое построение графа развития атаки
- Автоматическая визуализация сети АСУ ТП
- Выявление неавторизованных подключений к сети АСУ ТП
- Соблюдение требований к сегментации промышленной сети
- Детектирование потенциальных угроз и прямых попыток эксплуатации известных уязвимостей
- Обнаружение неавторизованного изменения технологических параметров
- Контроль доступа к параметрам ПЛК по сети (чтение и изменение микропрограмм и проектов ПЛК)
- Обнаружение неавторизованного управления ПЛК по сети
- Выявление сложных, распределенных во времени атак на АСУ ТП (цепочки атак)
- Извлечение и передача файлов из технологического трафика во внешние системы
- Генерация инцидентов ИБ с учетом логики технологического процесса
- Визуализация мнемосхемы техпроцесса и индикация компонентов, работа которых нарушена в результате инцидентов ИБ
- Формирование и отправка отчетов об инцидентах и состоянии защищенности АСУ ТП во внешние системы (SIEM-систему, ГосСОПКА).

80%

актуальных угроз АСУ ТП может
быть обнаружено сенсором
PT ISIM netView Sensor
«из коробки» — без кропотливой
предварительной настройки,
характерной для других
решений

Возможности масштабирования

PT ISIM, как и комплексное решение на его базе, гибко масштабируется в зависимости от конкретных требований и задач. Внедрение компонентов продукта может происходить поэтапно, и для этого не нужны крупные единовременные инвестиции. Базовая версия сетевого сенсора — PT ISIM netView Sensor — требует минимальных усилий по установке и идеально подходит как для пилотного внедрения, так и для каждодневной эксплуатации. В дальнейшем 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.

Комплексное решение на базе PT ISIM, MaxPatrol SIEM и MaxPatrol VM идеально подходит для организации SOC промышленного предприятия

Компоненты системы. Назначение и технические особенности

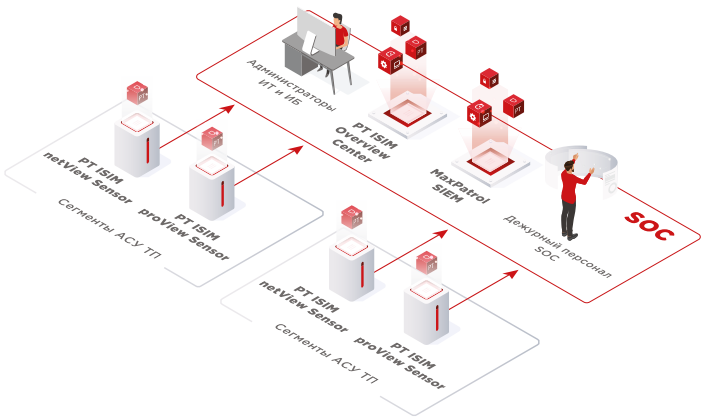
PT ISIM — программно-аппаратный комплекс, включающий серверы анализа сетевого трафика (сенсоры), серверы бизнес-аналитики и управления уровня ситуационного центра (SOC), предназначенный для индикации и квитирования критически опасных инцидентов персоналом промышленных объектов.

Глубокий анализ потока технологического трафика со скоростью **до 300 Мбит/с**

- На уровне защищаемого сетевого сегмента АСУ ТП (в котором расположены АРМ операторов, серверы SCADA и ПЛК) применяется сервер сбора и анализа трафика — PT ISIM View Sensor. В него поступает копия трафика с порта зеркалирования коммутатора (Mirror, SPAN) или TAP-устройства.

- Для централизации процесса управления сенсорами используется компонент PT ISIM Overview Center. Он предоставляет сводную информацию о зарегистрированных инцидентах, обеспечивает централизованную настройку и обновление компонентов на подключенных к нему сенсорах. Кроме того, сенсоры PT ISIM могут поставлять информацию о событиях и инцидентах напрямую в SIEM-систему (например, MaxPatrol SIEM).

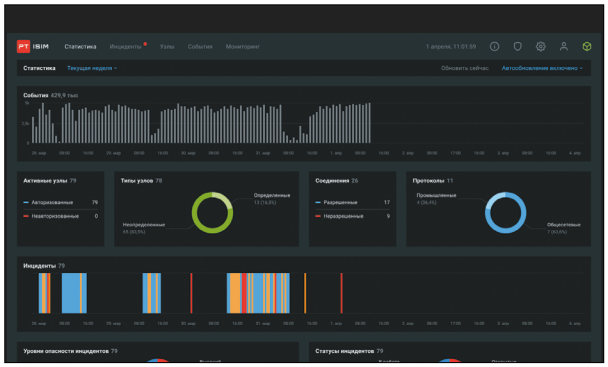
- Все компоненты PT ISIM работают под управлением Astra Linux и Debian. Взаимодействие компонентов происходит по протоколу HTTPS. Для установки и первоначальной настройки может требоваться доступ по протоколу SSH.



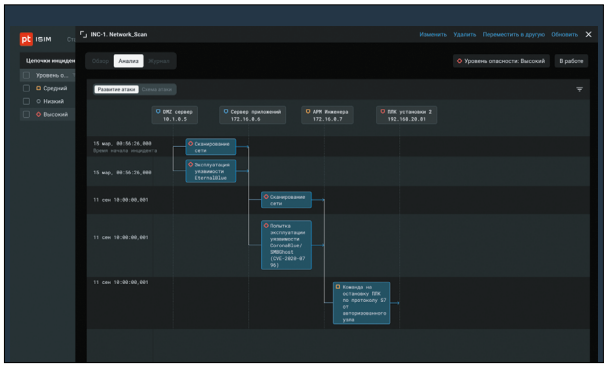
Пример архитектуры с применением PT ISIM View Sensor обеих версий и сервера управления PT ISIM Overview Center

Компоненты PT ISIM

Компонент	Назначение и основные возможности
PT ISIM View Sensor обеих версий	▪ Анализ копии трафика сегмента АСУ ТП ▪ Обработка событий в реальном времени ▪ Поддержка промышленных и IT-протоколов (DPI) ▪ Автоматическая идентификация узлов сети АСУ ТП (инвентаризация) ▪ Наличие редактора пользовательских правил ▪ Автоматическое построение графа развития атаки ▪ Визуализация топологии промышленной сети ▪ Извлечение файлов из трафика в индустриальных сетях ▪ Интеллектуальное обнаружение нарушений (неавторизованного управления компонентами АСУ ТП и эксплуатации уязвимостей) ▪ Определение сегментов сети ▪ Анализ событий с учетом бизнес-логики техпроцесса ▪ Мощный ретроспективный анализ событий
PT ISIM Overview Center	▪ Централизованное управление сенсорами PT ISIM (обновление, диагностика и т. д.) ▪ Предоставление сводной информации о зафиксированных инцидентах ИБ



Страница со сводной аналитикой в PT ISIM netView Sensor



Граф развития атаки, построенный PT ISIM netView Sensor

Дополнительные внешние компоненты

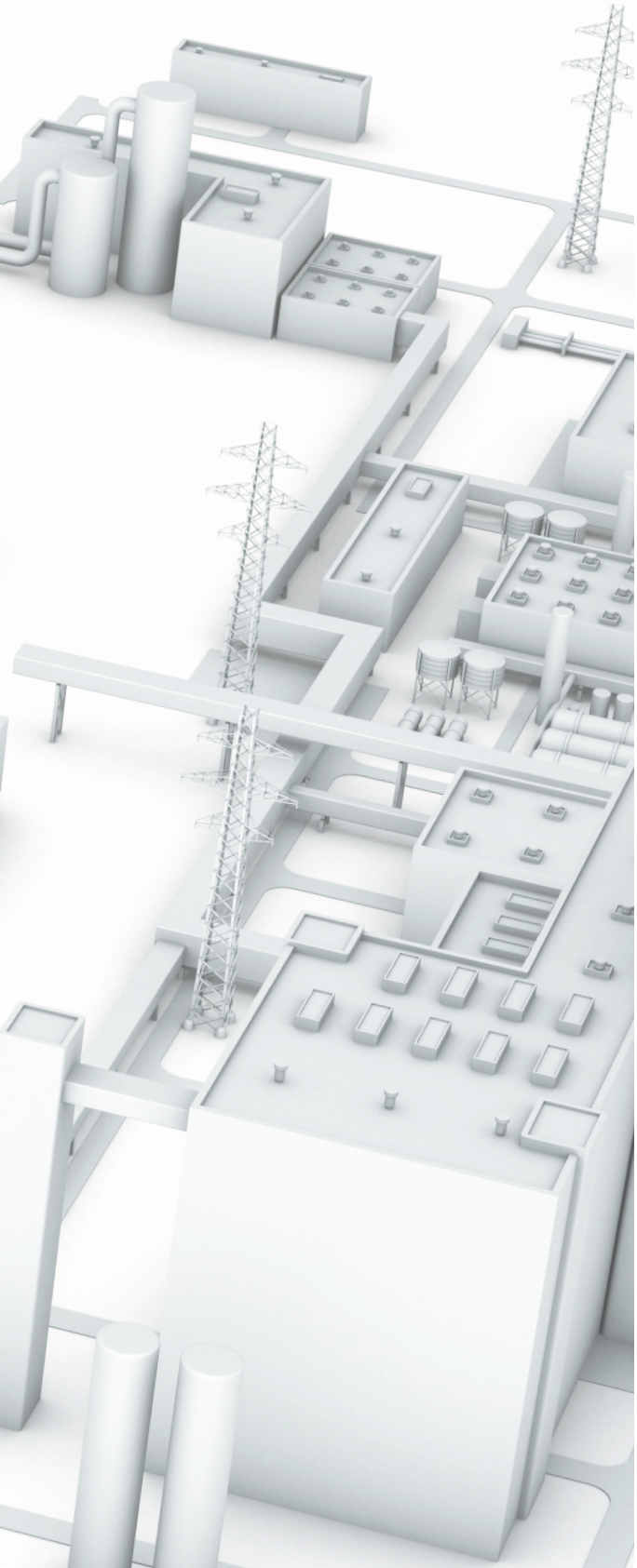
Для подключения сенсоров PT ISIM могут использоваться следующие дополнительные компоненты:

- Аппаратный диод, обеспечивающий на физическом уровне однонаправленную передачу данных со SPAN-порта коммутатора на сенсор PT ISIM
- Агрегирующее устройство, позволяющее уменьшить требуемое количество закупаемых сенсоров PT ISIM за счет агрегации трафика с нескольких SPAN-портов коммутаторов
- Регенерирующее устройство, позволяющее реплицировать трафик с одного SPAN-порта на несколько других портов для устройств мониторинга
- TAP-устройство для получения копии трафика при отсутствии SPAN-порта

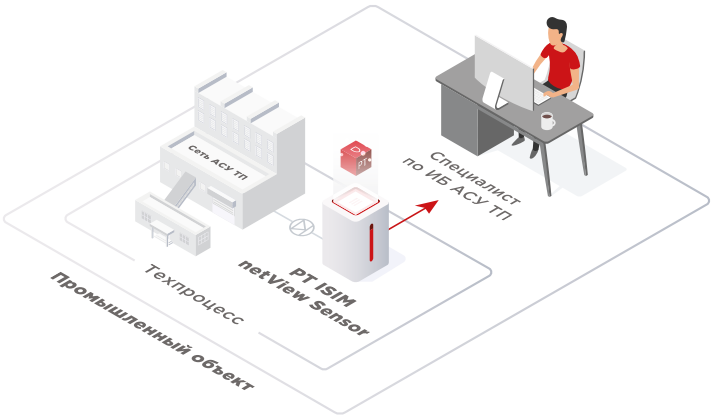
Версии сенсора

Возможность	PT ISIM netView Sensor	PT ISIM proView Sensor
Безопасная и быстрая интеграция с сетью АСУ ТП	+	+
Пользовательский веб-интерфейс управления инцидентами	+	+
Автоматическое построение графа развития атаки	+	+
Визуализация инцидентов на схеме сети АСУ ТП	+	+
Автоматическое построение карты узлов сети АСУ ТП	+	+
Автоматическое построение карты сетевых коммуникаций АСУ ТП	+	+
Визуализация схемы сети АСУ ТП	+	+
Контроль подключений узлов к сети АСУ ТП в реальном времени	+	+
Поддержка промышленных протоколов (DPI)	+	+
Извлечение файлов из трафика в индустриальных сетях	+	+
Поиск и фильтрация событий	+	+
Обнаружение эксплуатации уязвимостей в ПО и оборудовании АСУ ТП	+	+
Контроль целостности сетевых коммуникаций	+	+
Обнаружение сетевых сегментов	+	+
Автоматическое формирование белых списков сетевых соединений	+	+
Автоматическое формирование белых списков узлов сети	+	+
Управление белыми списками сетевых соединений	+	+
Управление белыми списками узлов сети АСУ ТП	+	+
Запись и хранение трафика сети АСУ ТП	+	+
Экспорт трафика и информации об инцидентах	+	+
Инвентаризация узлов сети АСУ ТП	+	+
Ретроспективный анализ событий	+	+
Обнаружение сетевых аномалий	+	+
Наличие режима автоматического обучения	+	+
Контроль критически важных параметров техпроцесса	–	+
Визуализация инцидентов на мнемосхеме техпроцесса	–	+
Редактор правил	+	+
Создание графических мнемосхем	–	+
Экспорт данных во внешние системы (например, в SIEM-систему)	+	+
Наличие базы знаний промышленных угроз (PT ISTI)	+	+
Подключение к PT ISIM Overview Center	+	+

Примеры сценариев использования

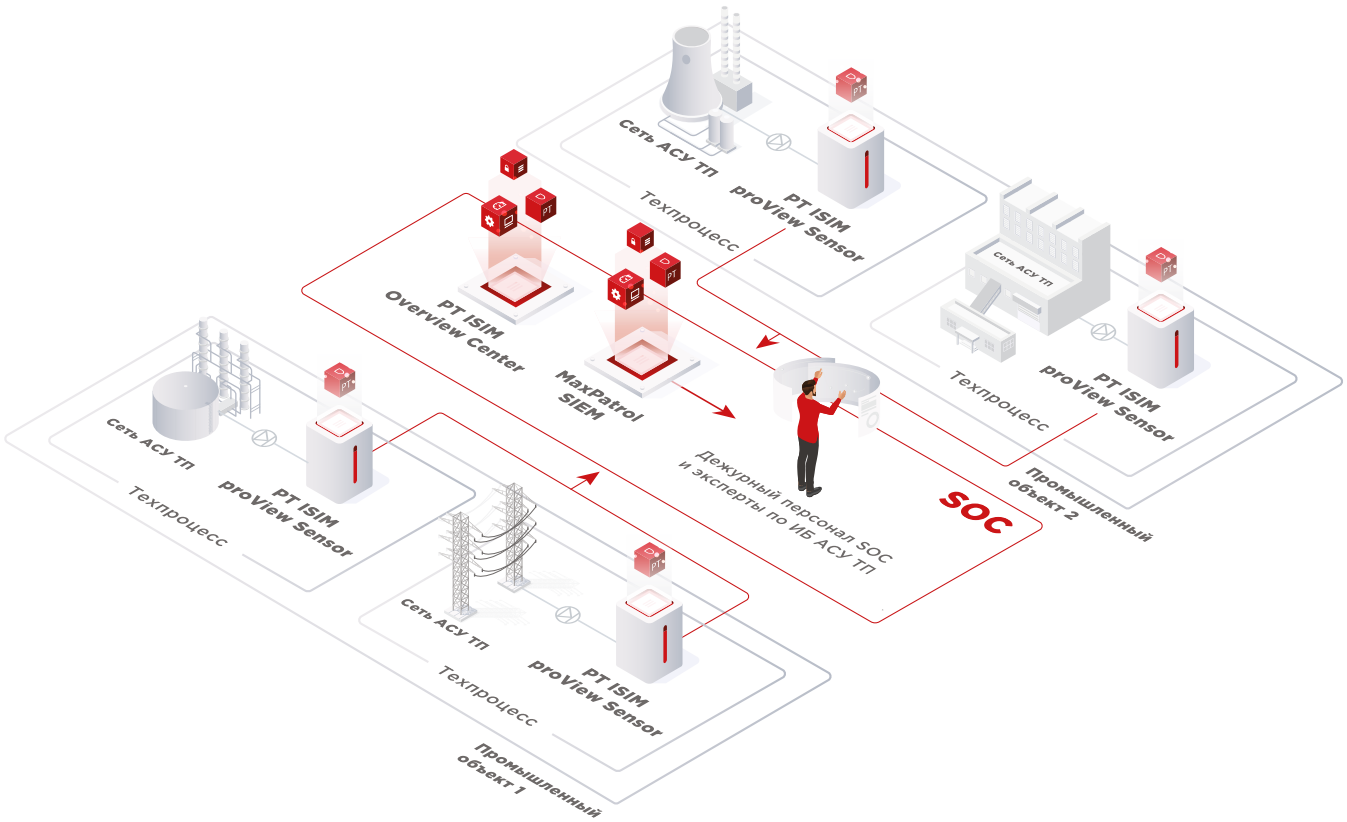


Сценарий 1. Автономное управление и минимальные затраты



- На каждую из защищаемых площадок устанавливается минимальный набор компонентов (сенсор PT ISIM netView Sensor и при необходимости однонаправленный шлюз данных) для мониторинга информационной безопасности силами специалистов заказчика.
- Не требует глубокое предварительное исследование технологического процесса и сети АСУ ТП.
- Каждый сенсор управляется отдельно.
- Для развертывания нужны минимальные усилия, специальные знания не требуются.
- Подходит для защиты небольших инфраструктур, а также для поэтапного масштабирования решения на больших предприятиях с распределенной инфраструктурой.

Сценарий 2. Максимальная эффективность и централизованное управление



- Проводится анализ защищенности технологических сегментов и компонентов АСУ ТП для достижения максимальной эффективности системы мониторинга.
- При использовании сенсоров PT ISIM proView Sensor векторы атак, найденные в ходе анализа защищенности, могут быть учтены в конфигурации системы мониторинга. Это дает возможность оперативно реагировать на сложные кибератаки, специфичные для конкретной АСУ ТП, включая эксплуатацию уязвимостей нулевого дня.
- Организуется общий ситуационный центр для обработки инцидентов.
- PT ISIM Overview Center управляет всеми компонентами PT ISIM.
- Инциденты обрабатываются централизованно в SIEM-системе.

Для заметок

Спецификация оборудования

	PT ISIM View Sensor обеих версий	**PT ISIM Overview Center**
Процессор	Intel Xeon E-2134 3,5 ГГц, кэш 8M, 4C/8T	Intel Xeon E-2134 3,5 ГГц, кэш 8M, 4C/8T
ОЗУ	2 × 16 ГБ DDR4	2 × 16 ГБ DDR4
Хранилище	2 x 480 ГБ SSD	2 x 480 ГБ SSD
Сетевые подключения	6 x 10/100/1000 Мбит/с, RJ-45;	2 x 10/100/1000 Мбит/с, RJ-45
Питание	220 В, AC (переменный ток)	220 В, AC (переменный ток)

ptsecurity.com
pr@ptsecurity.com

PT ISIM DS_A4.RUS.0015.07.APR.11.2023