



Positive Technologies  
Industrial Security  
Incident Manager

# PT ISIM

ОПИСАНИЕ ПРОДУКТА



[ptsecurity.com](https://ptsecurity.com)

# Ключевые возможности и преимущества

## Области применения



- Автоматизированные системы управления технологическими процессами промышленных предприятий
- Системы управления городских инженерных инфраструктур
- Автоматизированные системы управления объектов критической инфраструктуры
- Системы управления инженерной инфраструктурой центров обработки данных, деловых и торговых центров
- Промышленные предприятия и производства с распределенной инфраструктурой
- **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.
- **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: верхнеуровневая и детализированная отчетность, передача отдельных событий и инцидентов на уровень SOC: в SIEM и другие системы, возможности для 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.
- **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.
- **Учет специфики предприятия.** С помощью PT ISIM можно контролировать угрозы и векторы атак, уникальные для промышленного объекта. Для настройки механизма контроля этих векторов используются данные, получаемые в результате анализа защищенности АСУ ТП предприятия.
- **Соответствие требованиям промышленной среды.** Физические условия эксплуатации в промышленности бывают крайне агрессивными. Промышленное исполнение компонентов PT ISIM подбирается с учетом специфики отрасли и защищаемого предприятия.

## 4000+

правил обнаружения  
промышленных угроз

## PT Industrial Security Threat Indicators

Для обнаружения фактов нарушения информационной безопасности PT ISIM использует собственную уникальную базу промышленных киберугроз — PT Industrial Security Threat Indicators (PT ISTI). Она позволяет PT ISIM 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 АСУ ТП (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 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.

Доставка обновлений в PT ISIM может осуществляться автоматически и вручную. База содержит несколько тысяч сигнатур и правил обнаружения различных атак на распространенные системы ABB, Emerson, Hirschman, Schneider Electric, Siemens, Yokogawa.

## Цели и задачи

PT ISIM предназначена для повышения уровня защищенности, доступности и поддержки непрерывности технологических процессов с помощью анализа сетевого трафика и превентивного обнаружения атак, направленных на АСУ ТП.

PT ISIM netView Sensor не требует от пользователей специальных навыков и знаний ни при внедрении, ни в эксплуатации

### Цели внедрения системы

- Непрерывный анализ киберзащищенности АСУ ТП
- Контроль действий персонала и подрядчиков
- Обнаружение нарушений ИБ и кибератак на АСУ ТП
- Своевременное выявление инцидентов и информирование ответственных лиц
- Создание доверенного источника данных для эффективного проведения расследований нарушений ИБ
- Анализ инцидентов, включая определение причин возникновения, а также оценку последствий
- Помощь в планировании мер по устранению и предотвращению инцидентов
- Обеспечение соответствия требованиям регулирующих организаций (в том числе — выполнение приказов ФСТЭК № 31, 239, норм закона о КИИ № 187-ФЗ и выстраивание взаимодействия с центрами ГосСОПКА)

## меньше 1 часа

занимают работы по пуску  
и автоматической настройке  
PT ISIM netView Sensor  
на действующем сегменте  
АСУ ТП

## Решение технических задач

- Непрерывная обработка копии трафика АСУ ТП, получаемого через однонаправленный шлюз (диод данных)
- Анализ событий на уровне различных коммуникационных протоколов, включая промышленные (Siemens S7, IEC104, DIGSI, GOOSE/MMS, Schneider Electric UMAS, CIP, Yokogawa, PROFINET DCP, SPA-Bus, EKRA, OPC, Modbus и другие)
- Автоматическая визуализация схемы сети АСУ ТП
- Выявление неавторизованных подключений к сети АСУ ТП
- 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)
- 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, 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

Решение на базе PT ISIM гибко масштабируется в зависимости от конкретных требований и задач. Внедрение компонентов PT ISIM может происходить поэтапно, не требуя крупных единовременных инвестиций. Базовая версия сетевого сенсора — PT ISIM netView Sensor — требует минимальных усилий по установке и идеально подходит как для пилотного внедрения, так и для ежедневной 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.

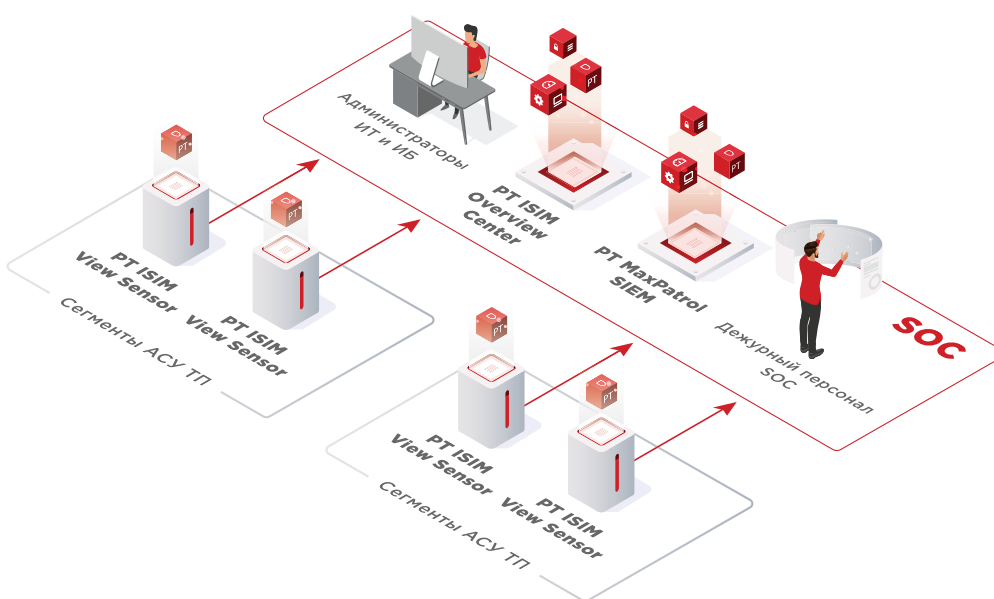
# Компоненты системы.

## Назначение и технические особенности

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

- На уровне защищаемого сетевого сегмента АСУ ТП (в котором расположены АРМ операторов, серверы SCADA и ПЛК) применяются серверы сбора и анализа трафика — полнофункциональные сенсоры PT ISIM View Sensor или безинтерфейсные PT ISIM Sensor. Они получают копию 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 (например, MaxPatrol SIEM).
- Все компоненты PT ISIM работают под управлением ОС Debian. Взаимодействие между компонентами происходит по протоколу HTTPS. Для установки и первоначальной настройки может требоваться доступ по протоколу SSH.

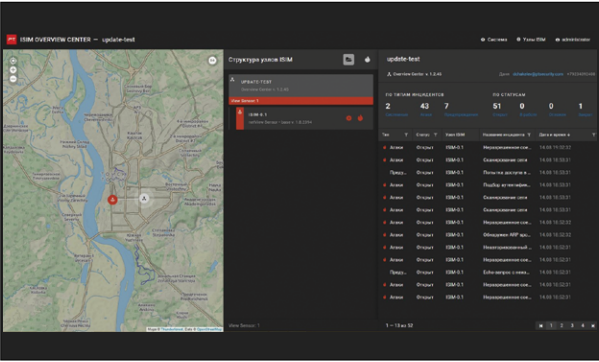
Г Комплексное решение на базе PT ISIM, PT MaxPatrol SIEM и MaxPatrol 8 идеально подходит для организации SOC промышленного предприятия



Пример архитектуры с применением сенсоров View Sensor и сервера управления Overview Center

# Компоненты PT ISIM системы

Компонент	Назначение и основные возможности
<b>PT ISIM View Sensor</b>	<ul style="list-style-type: none"><li>▪ Анализ копии трафика сегмента АСУ ТП</li><li>▪ Обработка событий в реальном времени</li><li>▪ Поддержка промышленных и IT-протоколов (DPI)</li><li>▪ Автоматическая идентификация узлов сети АСУ ТП (инвентаризация)</li><li>▪ Визуализация топологии промышленной сети</li><li>▪ Интеллектуальное обнаружение нарушений (неавторизованного управления компонентами АСУ ТП и эксплуатации уязвимостей)</li><li>▪ Анализ событий с учетом бизнес-логики техпроцесса</li><li>▪ Мощный ретроспективный анализ событий</li></ul>
<b>PT ISIM Overview Center</b>	<ul style="list-style-type: none"><li>▪ Централизованное управление сенсорами PT ISIM (обновление, диагностика, и так далее)</li><li>▪ Сводная информация по зафиксированным инцидентам ИБ</li></ul>
<b>PT ISIM View Point и PT ISIM Sensor</b>	<ul style="list-style-type: none"><li>▪ Анализ трафика и выявление инцидентов в распределенных, слабонагруженных системах АСУ ТП</li><li>▪ Первичный анализ трафика производится с помощью недорогих, низкопроизводительных сенсоров PT ISIM Sensor, размещенных на удаленных площадках</li><li>▪ Высокоуровневая обработка результатов анализа трафика и визуализация данных выполняется централизованно в консоли PT ISIM View Point</li></ul>



Экран управления сенсорами PT ISIM Overview Center



Экран сводной аналитики 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 со SPAN-порта коммутатора на сенсор PT ISIM;
- агрегирующее устройство, позволяющее уменьшить требуемое количество покупаемых 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

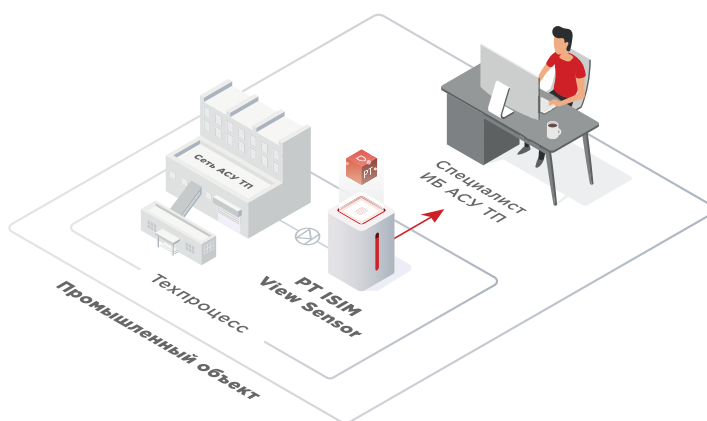
Возможность	PT ISIM Sensor	PT ISIM netView Sensor	PT ISIM proView Sensor
Безопасная и быстрая интеграция с сетью АСУ ТП	+	+	+
Пользовательский web-интерфейс управления инцидентами*	-	+	+
Автоматическое построение карты узлов сети АСУ ТП	+	+	+
Автоматическое построение карты сетевых коммуникаций АСУ ТП	+	+	+
Визуализация схемы сети АСУ ТП	+	+	+
Контроль подключений узлов к сети АСУ ТП в реальном времени	+	+	+
Поддержка промышленных протоколов (DPI)	+	+	+
Инструменты поиска и фильтрации событий	+	+	+
Обнаружение эксплуатации уязвимостей в ПО и оборудовании АСУ ТП	+	+	+
Контроль целостности сетевых коммуникаций	+	+	+
Визуализация инцидентов на схеме сети АСУ ТП	+	+	+
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	+	+	+
Режим автоматического обучения	+	+	+
Контроль критических параметров тех.процесса	-	-	+
Визуализация инцидентов на мнемосхеме техпроцесса	-	-	+
Инструменты для создания и настройки собственных правил анализа	-	-	+
Инструменты создания графических мнемосхем	-	-	+
Экспорт данных во внешние системы (например, в SIEM-систему)	+	+	+
Встроенная база знаний промышленных угроз PT ISTI	+	+	+
Подключение к PT ISIM Overview Center	+	+	+
Управление через консоль PT ISIM ViewPoint	до 30 сенсоров на одну консоль	-	-

\* PT ISIM Sensor не имеет пользовательского интерфейса. Для управления сенсорами данного типа и их обновления необходим отдельный компонент: PT ISIM View Point



## Примеры сценариев использования

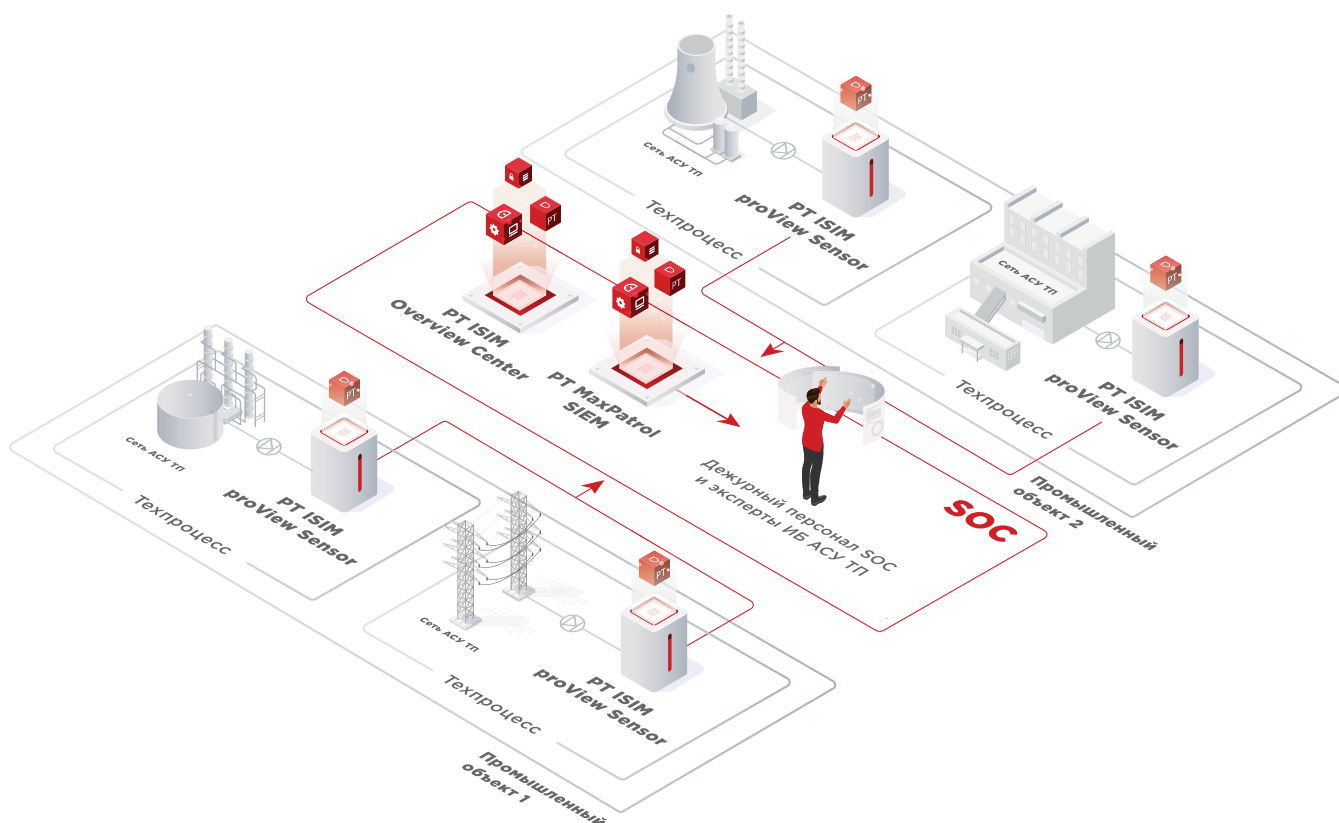
### Сценарий 1. Автономное управление и минимальные затраты



- 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 глубокого предварительного обследования сети АСУ ТП и технологического процесса.
- Каждый сенсор управляется отдельно.
- Минимальные усилия по развертыванию, не требует специальных знаний.
- Подходит для защиты небольших инфраструктур, а также для поэтапного масштабирования решения на больших предприятиях с распределенной инфраструктурой.

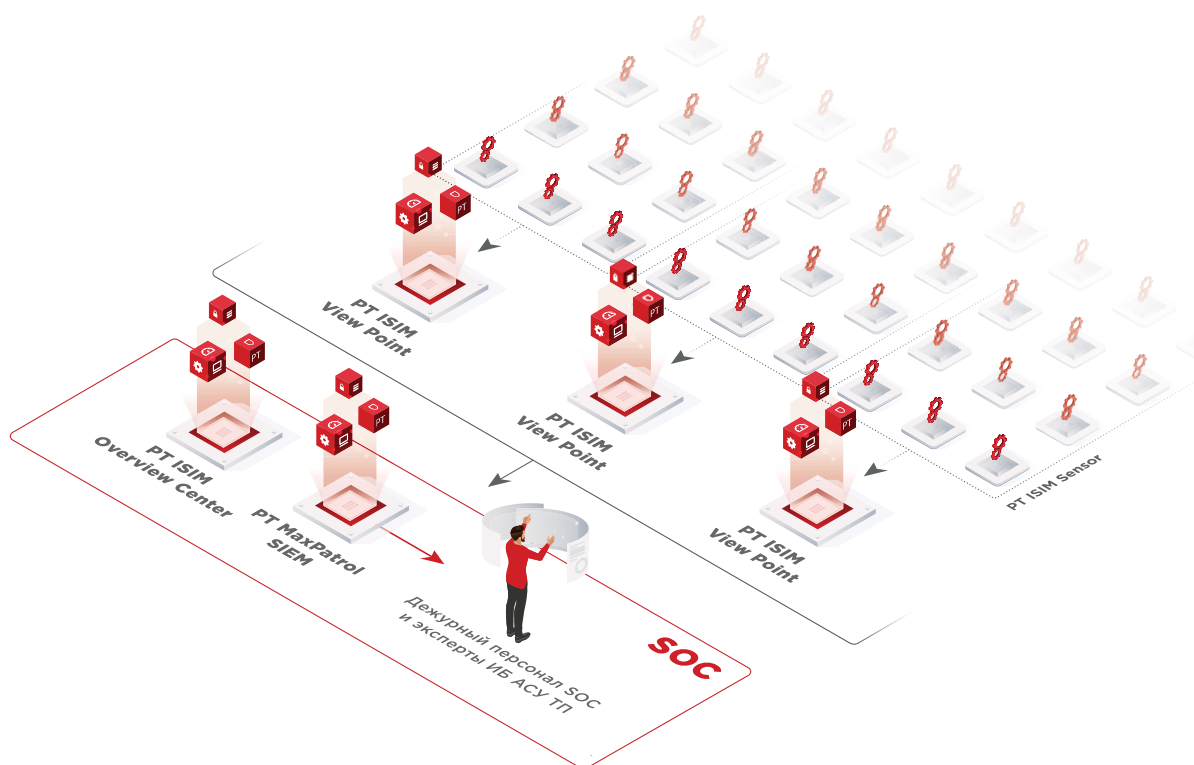


## Сценарий 2. Максимальная эффективность и централизованное управление



- Необходимо провести 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 конфигурировании 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 централизованно управляет всеми компонентами PT ISIM.
- Инциденты обрабатываются централизованно в SIEM-системе

### Сценарий 3. Распределенная инфраструктура с большим количеством слабонагруженных сегментов



- На удаленных и слабонагруженных сетях сегментов с АСУ ТП устанавливается недорогой, компактный PT ISIM Sensor без пользовательского интерфейса.
- В точках консолидации или в SOC устанавливаются серверы PT ISIM View Point, которые позволяют управлять сенсорами и получать доступ к результатам анализа трафика
- Инциденты обрабатываются централизованно в SIEM-системе

Для заметок

# Спецификация оборудования

	PT ISIM View Sensor	PT ISIM Overview Center	PT ISIM Sensor	PT ISIM View Point
Процессор	Intel Xeon E-2134 3.5GHz, 8M cache, 4C/8T	Intel Xeon E-2134 3.5GHz, 8M cache, 4C/8T	Intel Core™ i7-9700T, 2,0–4,3 GHz, 12M cache, 8C/8T	Intel Xeon E-2134 3.5GHz, 8M cache, 4C/8T
ОЗУ	2x16 Gb DDR4	2x16 Gb DDR4	16 Gb DDR4	2x16 Gb DDR4
Хранилище	2x480 GB SSD	2x480 GB SSD	1 TB M.2 SSD	2x480 GB SSD
Сетевые подключения	6x10/100/1000 Mbps, RJ45;	2x10/100/1000 Mbps, RJ45;	1 x 1Gb/s RJ-45  USB-Eth 1Gb/s внешний адаптер (дополнительное оборудование)	2x10/100/1000 Mbps, RJ45;
Питание	1x220V AC	1x220V AC	1x 220V AC	1x220V AC

## О компании

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/PositiveTechnologies  
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.