POSITIVE TECHNOLOGIES

PT ISIM 2.0

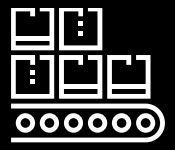
Защита технологических сетей промышленных предприятий

ptsecurity.com

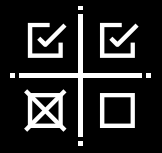
Коммерческие риски

Цифровизация ставит технологические процессы в зависимость от корректной работы информационных систем

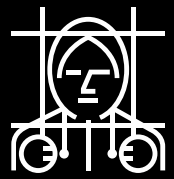
Умышленное нарушение технологического процесса компьютерными средствами – реальная угроза бизнесу



Остановка производства



Брак



Мошенничество и саботаж

Техногенная катастрофа

Кража технологических секретов

Источники угроз

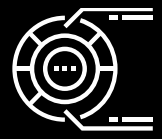
Источник угрозы	Примеры, цели, задачи
Случайные атаки	▪ Проникновение в сеть АСУ ТП вредоносного ПО (трояны, шифровальщики и так далее) ▪ Организация несанкционированного доступа с целью его перепродажи ▪ Шантаж, получение выкупа
Конкуренты	▪ Целевые атаки, как средство конкурентной борьбы ▪ Нарушение работы бизнеса, ущерб деловой репутации, кража технологических секретов
Структуры иностранных государств	▪ Целевые атаки спецслужб, как следствие международной конфронтации
Подрядчики и персонал	▪ Имеют полный доступ к АСУ ТП, в том числе удаленный ▪ Могут быть мотивированы к мошенничеству и саботажу

АСУ ТП – полуслепая зона для службы ИБ

Базовые средства ИБ, такие как антивирусное ПО, межсетевые экраны и контроль доступа на периметре, являются необходимыми, но недостаточным элементами кибербезопасности АСУ ТП крупного промышленного предприятия.

Специалистам SOC необходимо контролировать некоторые технологические аспекты функционирования АСУ ТП с точки зрения ИБ

Несанкционированный доступ к элементам АСУ ТП



Нарушение функциональных характеристик процесса

PT ISIM - первый в СНГ

1 Безагентный, неинвазивный режим:

Анализ трафика и профилирование сетевого взаимодействия

2 Инвентаризация активов:

Автоматизированное определение и профилирование сетевых активов

3 Мониторинг пром. протоколов:

Мониторинг и визуализация критичных изменений технологических параметров, процессов, сетевого окружения

4 Детектирование инцидентов :

Автоматическое выявление инцидентов безопасности и кибератак в трафике промышленных сетей

Выявление неавторизованного управления системами и технологическими процессами

5 Ретроспективный анализ:

Поддержка процессов реагирования и расследования инцидентов ИБ

Экспорт сохраненного трафика, данных инвентаризации, событий, инцидентов

6 Соответствие Законодательству:

Обеспечение соответствия требованиям регуляторов и законодательства

PT ISIM Sensor

Сбор, предобработка трафика

PT ISIM View Sensor, PT ISIM View Point

Анализ трафика

PT ISIM Overview Center

Централизованное управление

PT ISIM – это анализ трафика технологических сетей

Система анализа трафика АСУ ТП
PT ISIM View Sensor

- Поддерживает более 20 промышленных протоколов
- Передает инциденты и выбранные технологические события в SIEM
- Работает «из коробки» за счет автоматического обучения
- Содержит более 4200 правил обнаружения нарушений ИБ «из коробки»
- Подробные отчеты о состоянии защищенности АСУ ТП
- Хранит копию трафика сети АСУ ТП для расследования инцидентов
- Настройка правил анализа под модель угроз конкретного предприятия
- Визуализация нарушений тех. процесса на мнемосхеме

Система централизованного управления
PT ISIM Overview Center

- Обеспечивает централизованное управление сенсорами PT ISIM
- Предоставляет сводную информацию по зафиксированным инцидентам ИБ

Для распределенных АСУ ТП

Компактная система анализа трафика АСУ ТП – PT ISIM Sensor

- Подходит для контроля слабонагруженных и распределенных АСУ ТП
- Не имеет пользовательского интерфейса
- Поддерживает более 20 промышленных протоколов
- Работает «из коробки» за счет автоматического обучения
- Выявляет нарушения ИБ благодаря постоянно пополняемой базе правил PT ISTI
- Хранит копию трафика сети АСУ ТП для целей ретроспективного анализа и расследований

Консоль управления PT ISIM View Point

- Агрегирует информацию со всех подключенных сенсоров PT ISIM Sensor
- Позволяет работать с инцидентами и событиями на подключенных сенсорах PT ISIM Sensor
- Дашборды и отчеты для оперативного анализа ситуации

Расширение поля зрения SOC-инженеров

Чтение конфигураций и проектов ПЛК

Изменение режима работы ПЛК

Изменение проектов ПЛК

PT ISIM

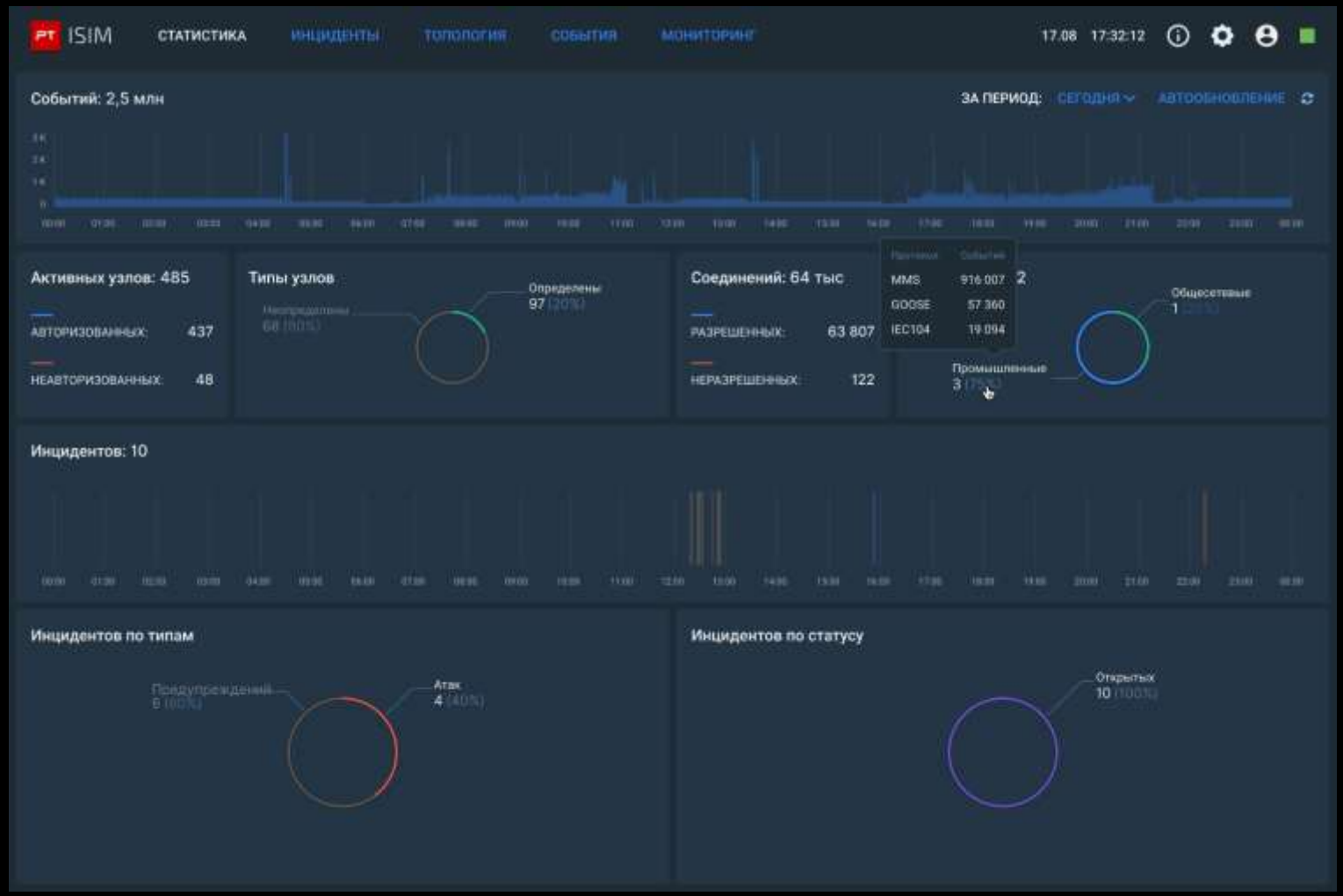
Помогает выявлять

Изменение уставок тех. процесса

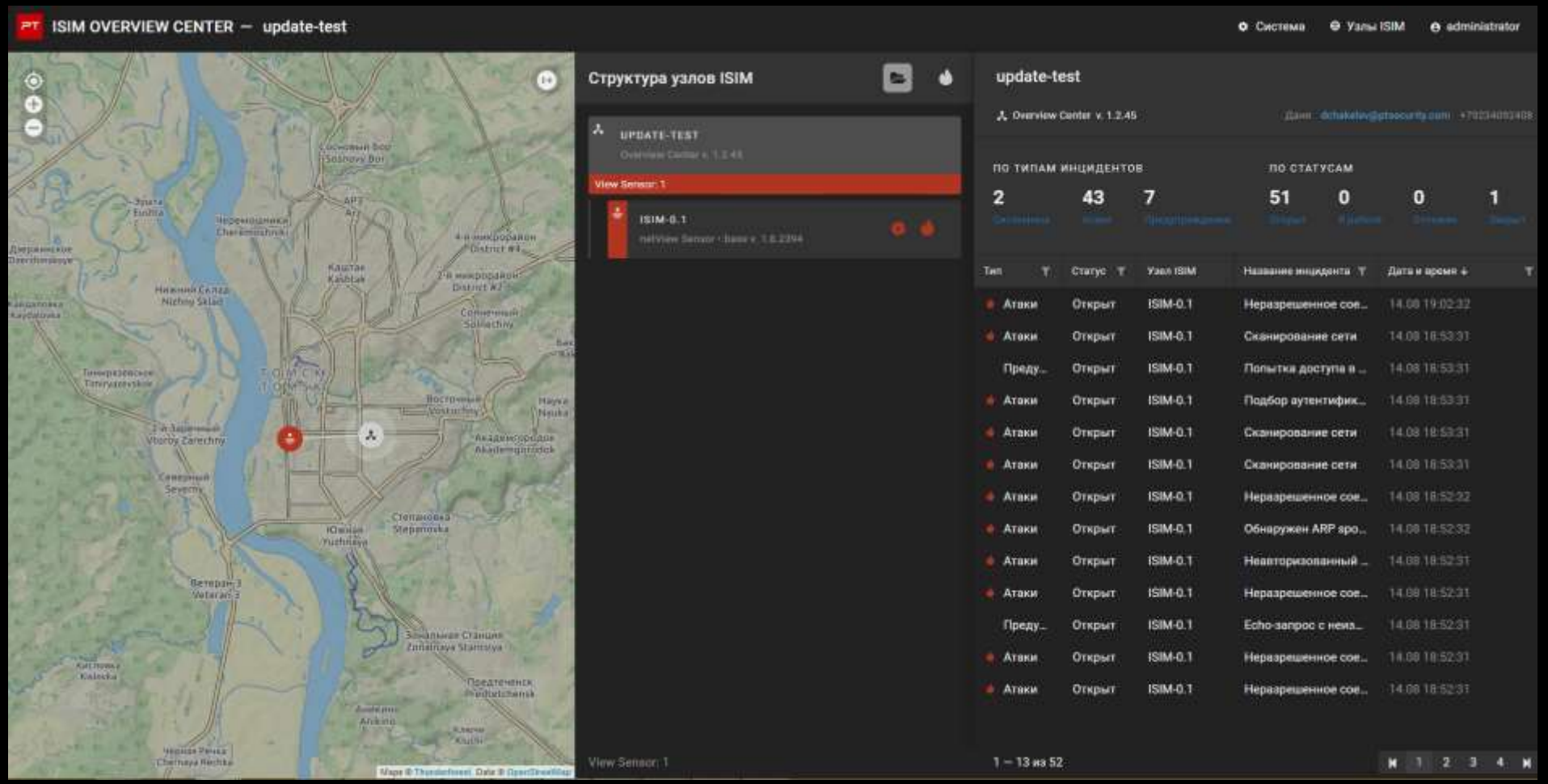
Отсутствие реакций систем АСУ ТП на закритические режимы

Эксплуатация уязвимостей, нацеленных на вывод оборудования АСУ ТП из строя

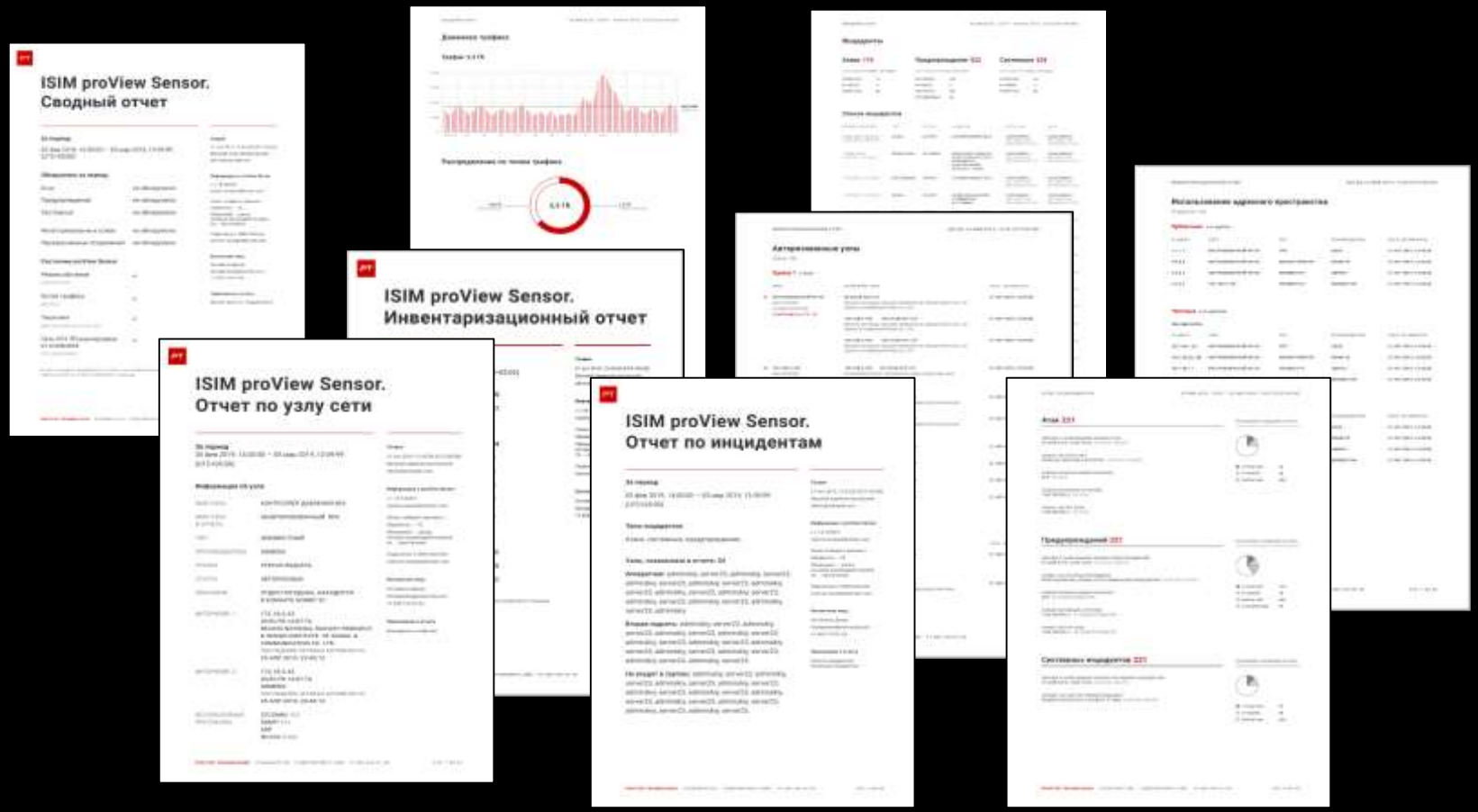
Интерфейс сенсора PT ISIM



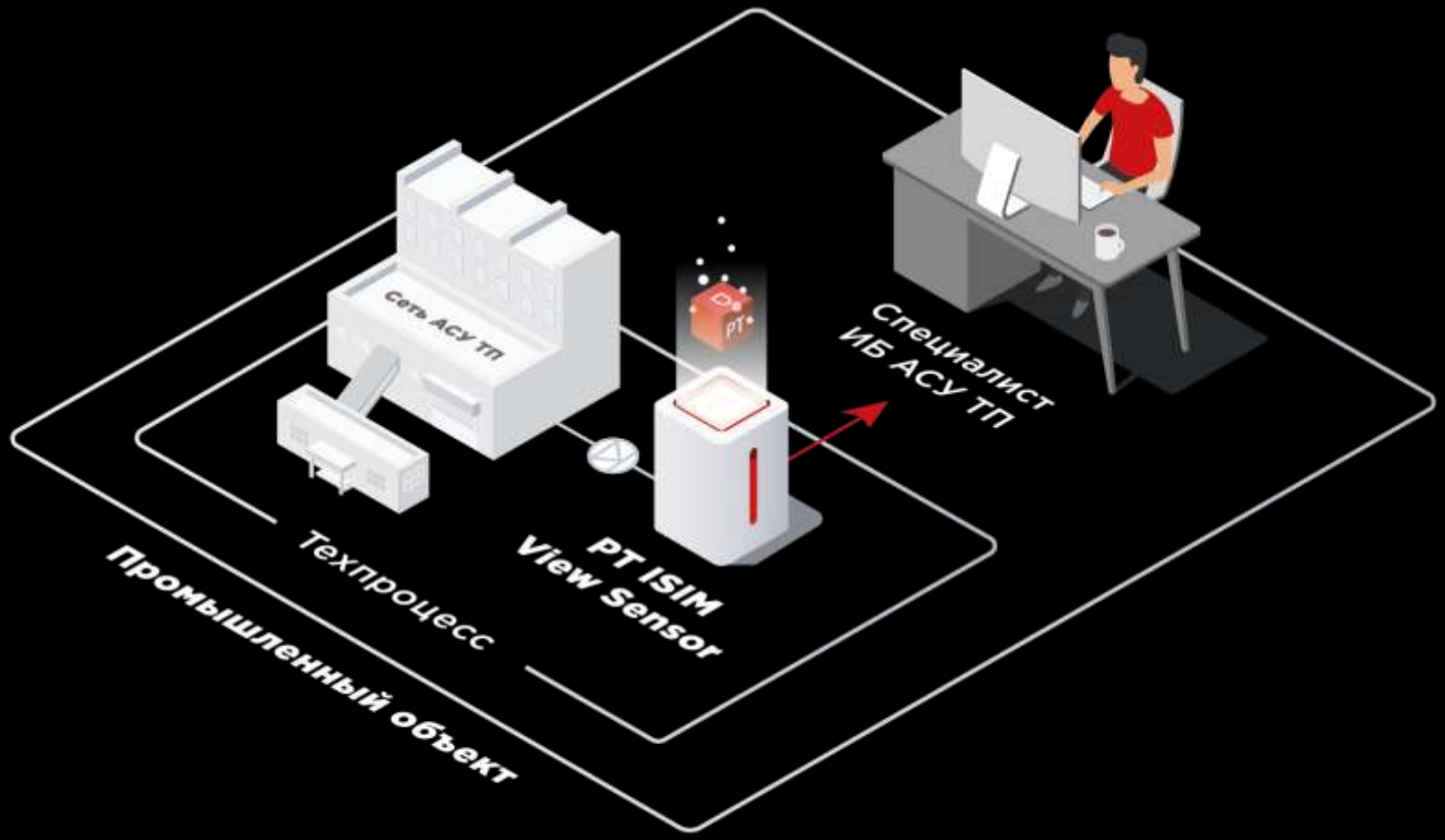
Интерфейс Overview Center



Отчеты

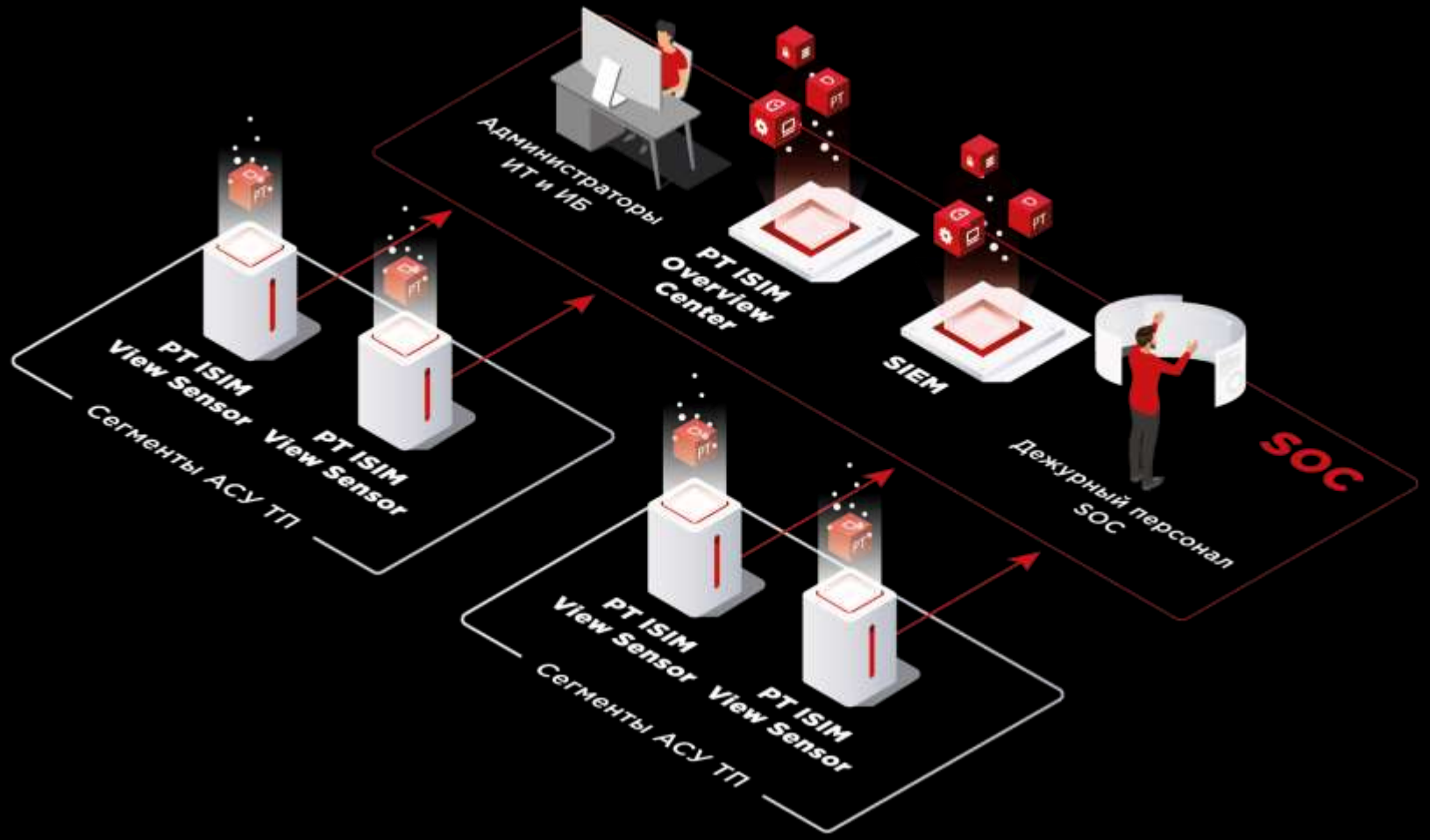

ISIM proView Sensor.
Сводный отчет
ISIM proView Sensor.
Инвентаризационный отчет
ISIM proView Sensor.
Отчет по узлу сети
ISIM proView Sensor.
Отчет по инцидентам

Сценарий 1.
Автономная инсталляция



- На защищаемую площадку (сегмент АСУ ТП) устанавливается **PT ISIM View Sensor**
- Не требуется глубокое предварительного обследование сети АСУ ТП
- Пуско-наладочные работы не требуют остановки тех-процесса и **занимают меньше 1 часа**
- Идеально подходит для пилотных проектов, защиты небольших инфраструктур, а также для поэтапного масштабирования решения на больших предприятиях.

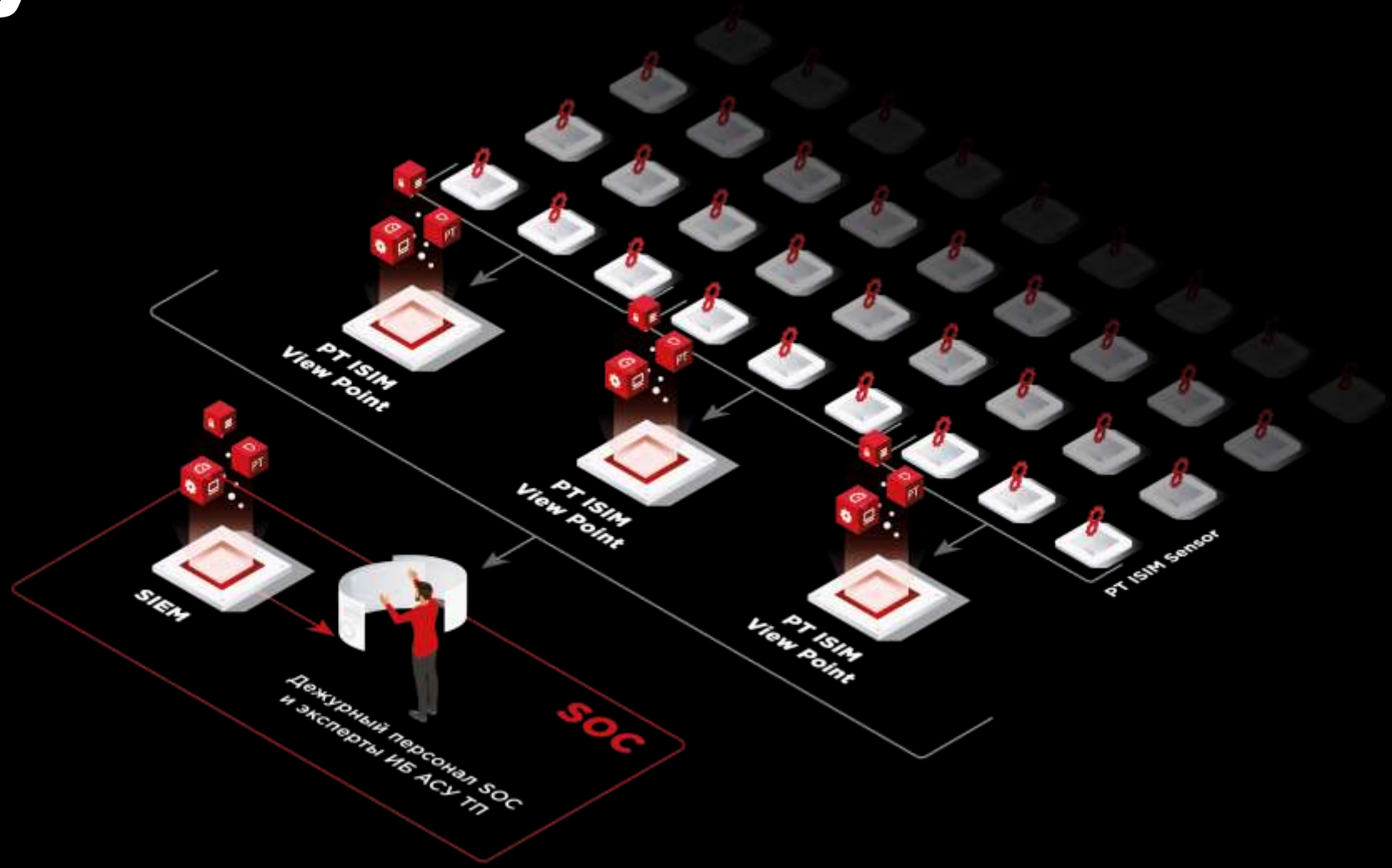
Сценарий 2.
Промышленный SOC



- На каждую из защищаемых площадок устанавливается **PT ISIM View Sensor**
- **Все сенсоры централизовано управляются и обновляются** с помощью PT ISIM Overview Center, установленном в SOC предприятия
- Информация об инцидентах и отдельных технологических событиях передается от сенсоров в SIEM и анализируется специалистами в SOC предприятия
- За счет выявления признаков нарушений ИБ как на технологическом, так и корпоративном уровне **становится возможным построить наиболее полную картину инцидента ИБ и предотвратить его дальнейшее развитие**

Сценарий 3. Контроль ИБ слабонагруженных АСУ ТП

- При большом количестве слабонагруженных сегментов АСУ ТП **целесообразно использовать недорогие и компактные PT ISIM Sensor** без пользовательского интерфейса
- При этом сенсоры **централизованно управляются с помощью консолей PT ISIM View Point, визуализирующих всю необходимую информацию**: события, инциденты, карту сетевых коммуникаций
- Информация об инцидентах и отдельных технологических событиях передается от агрегирующих консолей в SOC предприятия для дальнейшего обогащения и анализа



Преимущества PT ISIM

Простота внедрения и эксплуатации

- Автоматическое обучение и пассивное подключение к сети АСУ ТП
- Удобные дашборды для оперативного анализа ситуации
- Информативные отчеты для сотрудников различного уровня

Легкая встраиваемость в процессы мониторинга ИБ

- Гибкая интеграция с действующими системами центра оперативного реагирования (SIEM)
- Дополнение существующих политик ИБ за счет контроля технологических аспектов функционирования АСУ ТП

База индикаторов промышленных угроз

- Постоянно пополняемая база сигнатур и правил обнаружения нарушений ИБ для промышленных сетей PT ISTI*
- На конец 2019 года содержит более 4000 правил.

** - Positive Technologies Industrial Security Indicators*

Более 60 проектов

- **PT ISIM** на объектах металлургии + **MP SIEM**
- **PT ISIM** на объектах Ж/Д + **MP SIEM** в SOC
- **PT ISIM** на ГЭС + **MP SIEM** в SOC
- **PT ISIM** на ПС 220 кВ + **MP 8** + **MP SIEM** в SOC
- 4 летний НИОКР, разработан тиражируемый **ПТК**

Полезные ссылки

Заказать пилот: https://www.ptsecurity.com/ru-ru/products/isim/

Бесплатная версия PT ISIM freeView: https://www.ptsecurity.com/ru-ru/products/isim-free-view/

Telegram-канал: https://t.me/isimpt


Спасибо
за внимание!
ptsecurity.com