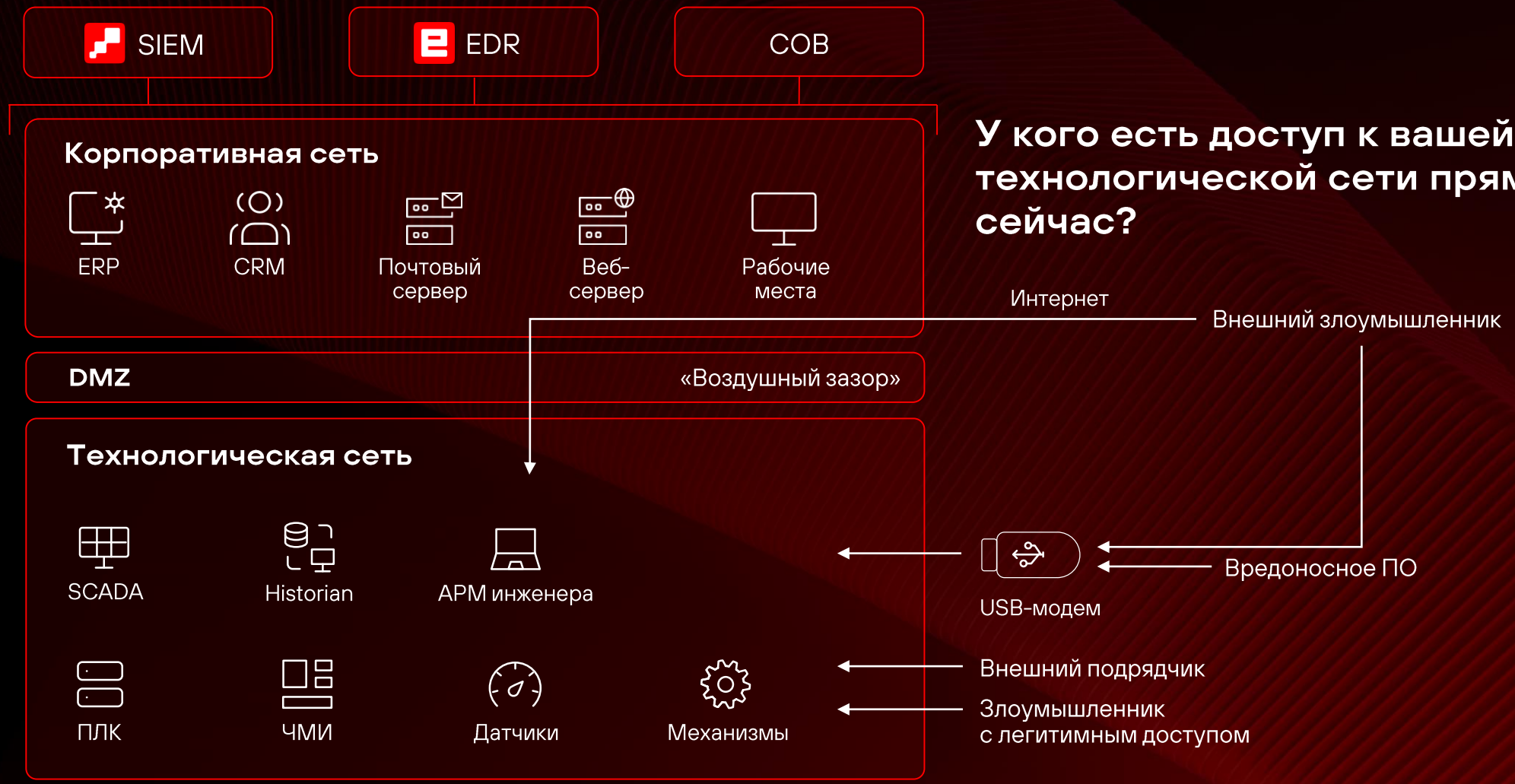
PT ISIM

PT Industrial Security Incident Manager

Источники угроз



У кого есть доступ к вашей технологической сети прямо сейчас?

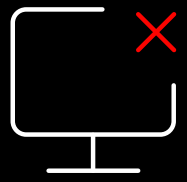
Уязвимости в промышленных инфраструктурах

По данным Positive Technologies, в среднем на промышленном предприятии выявляется от одного до пяти грубых нарушений, таких как:

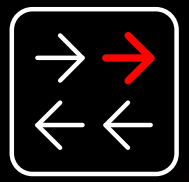
- Наличие непроектных АРМ с выходом в интернет
- Отсутствие защиты точек доступа
- Удаленное подключение к технологической сети
- Наличие неавторизованных каналов связи
- Отсутствие сегментации сети и паразитный трафик
- Использование словарных паролей и паролей по умолчанию

Каждое нарушение несет в себе риски кибербезопасности

Защиты конечных узлов и периметра недостаточно



Из-за ограниченных аппаратных ресурсов, устаревших операционных систем и проприетарных технологий не на все устройства можно установить СЗИ



Инвентаризация и отслеживание изменений в крупной промышленной ИТ-инфраструктуре — нетривиальная задача, предприятия не всегда знают о своих активах

Большой объем коммуникаций остается в пределах технологической сети, этот трафик не проходит через межсетевой экран — угрозы нужно выявлять и в трафике внутри сети

Что делать?

Решение – система анализа сетевого трафика

Системы класса NTA (network traffic analysis) сфокусированы на выявлении злоумышленников внутри сети

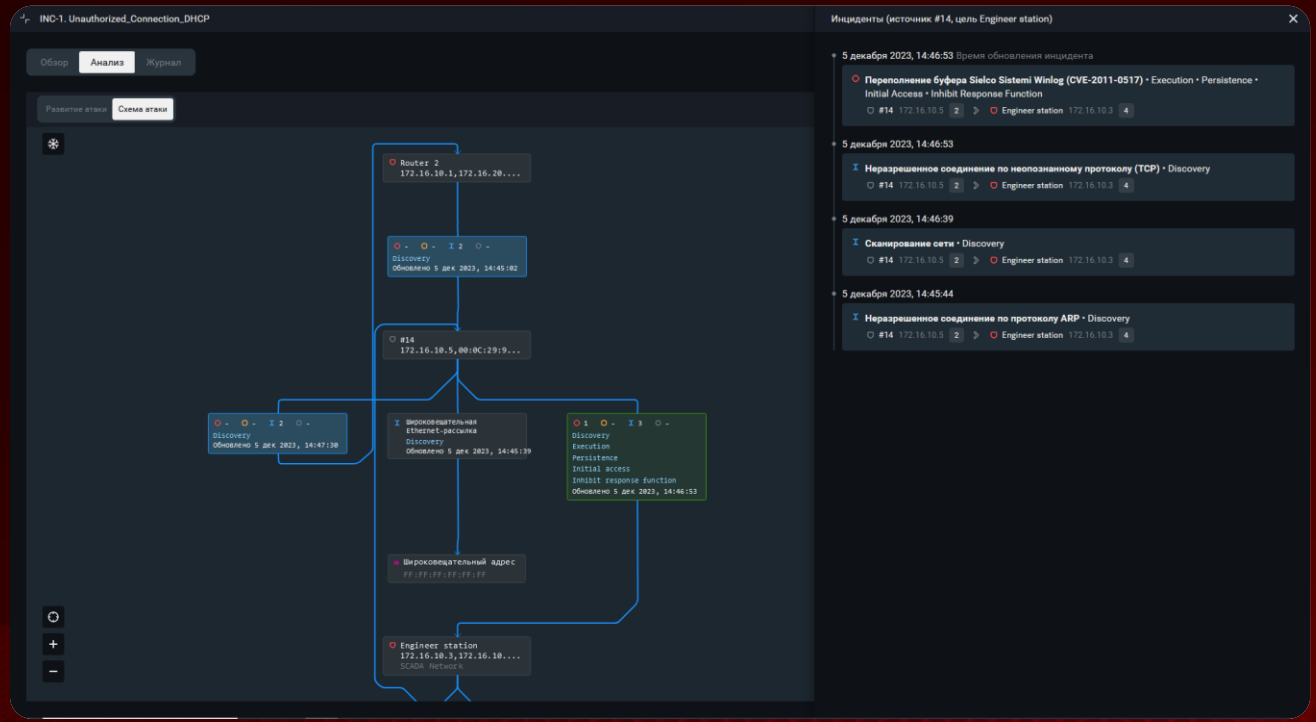
Они детально разбирают трафик и сохраняют его исходную копию — это позволяет проводить расследования и восстанавливать цепочки атак

Без NTA-решения специалисты по ИБ и ИТ-администраторы не увидят событий безопасности в промышленной сети

PT ISIM — промышленная NTA-система

PT ISIM предоставляет уникальное сочетание инструментов и экспертизы для контроля безопасности и мониторинга технологических сетей, IIoT-систем промышленных предприятий и объектов инженерной инфраструктуры.

PT ISIM анализирует трафик в промышленных сетях, выявляет нелегитимные операции, действия злоумышленников и активность ВПО.



Какие задачи решает PT ISIM

Наблюдаемость и контроль изменений
технологической сети дают возможность повысить киберустойчивость инфраструктуры

Мониторинг безопасности
позволяет предотвращать опасные технологические нарушения

Обнаружение и анализ угроз
помогают защищать сеть и поддерживать непрерывность технологических и бизнес-процессов

- Обеспечивает инвентаризацию технологической инфраструктуры и контроль изменений
- Выявляет аномалии и события безопасностив технологическом трафике
- Детектирует опасные технологические команды
- Обнаруживает эксплуатацию уязвимостей и другие техники злоумышленников
- Обнаруживает ВПО и отправляет подозрительные файлы на анализ
- Помогает соблюдать требования регулирующих организаций

Области применения PT ISIM

- Автоматизированные системы управления технологическими процессами промышленных предприятий
- Автоматизированные системы управления субъектов КИИ
- Системы управления инженерной инфраструктурой социально значимых городских и муниципальных объектов
- Системы управления движением рельсового транспорта
- Системы управления в распределенных производственных инфраструктурах
- Системы промышленного интернета вещей (IIoT)
- DICOM-совместимые системы и сети медицинских учреждений

Кому полезен PT ISIM

Ответственным за информационную безопасность

Помогает защитить критически важную инфраструктуру предприятия от актуальных киберугроз

Ответственным за работоспособность ИТ-инфраструктуры

Помогает обеспечить устойчивую работу всей информационной инфраструктуры предприятия

Ответственным за непрерывность производства

Помогает предотвратить аварии и остановку производственных процессов

Сценарии использования PT ISIM

01

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.

Сценарии использования PT ISIM

02

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.

Сценарии использования PT ISIM

03

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.

Сценарии использования PT ISIM

04

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.

Сценарии использования PT ISIM

05

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.

Сценарии использования PT ISIM

06

Обнаружение ВПО в трафике и отправка подозрительных файлов на анализ

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

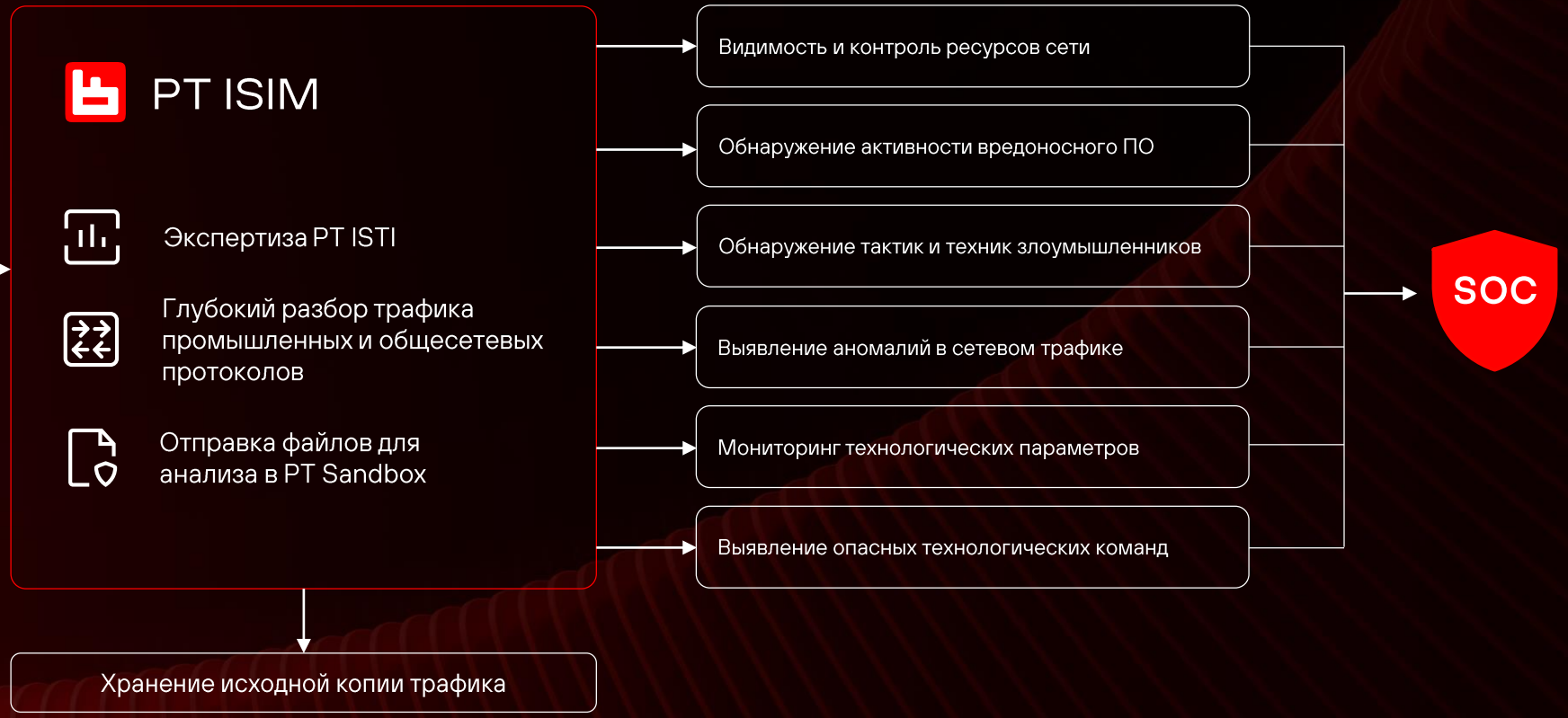
PT ISIM извлекает передаваемые по сети файлы для анализа в PT Sandbox, чтобы выявить нелегитимную передачу прошивок ПЛК, проектов SCADA или распространение ВПО, в том числе не обнаруживаемого классическими антивирусами.

Как работает PT ISIM

PT ISIM захватывает и разбирает сетевой трафик (130+ протоколов)

Трафик со SPAN-порта коммутатора

Экспертиза PT ISTI позволяет на ранней стадии определять атаки на Windows и Linux, стандартное сетевое оборудование и промышленные устройства. Содержит 8000 правил и индикаторов угроз



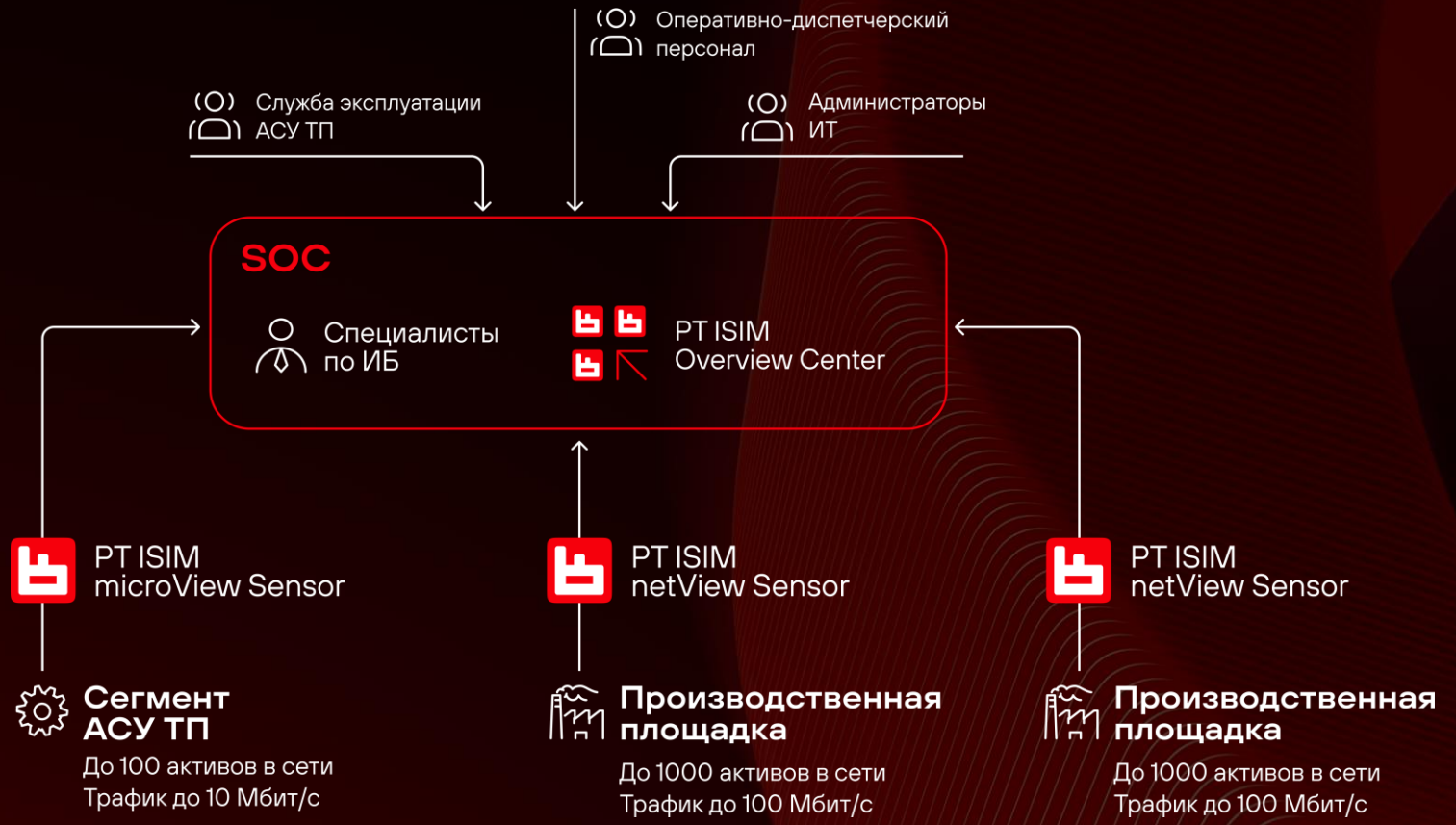
Компоненты PT ISIM

PT ISIM View Sensor

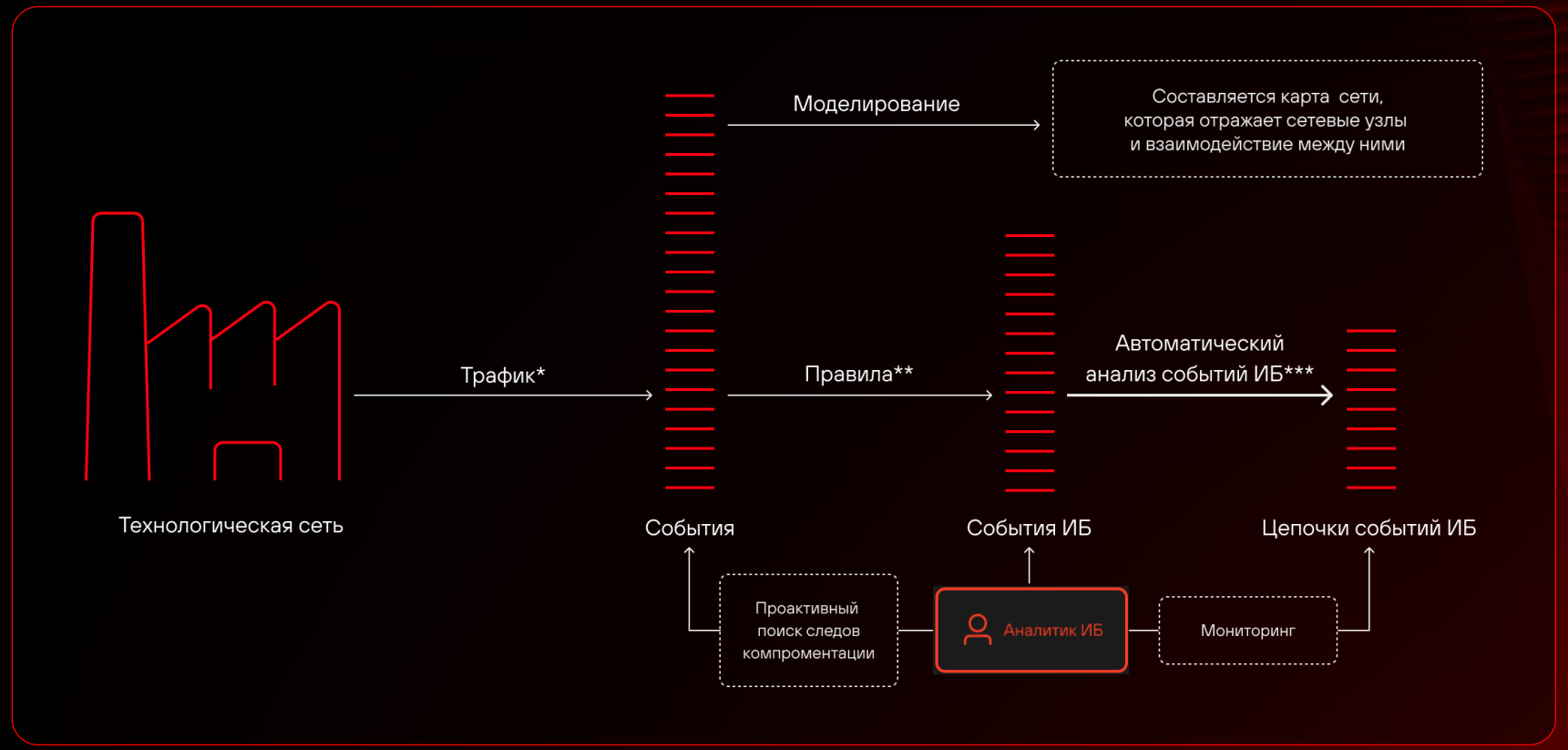
Сенсоры PT ISIM View Sensor применяются для анализа и хранения сетевого трафика, устанавливаются на уровне сегмента сети АСУ ТП, в котором расположены АРМ операторов, серверы SCADA и ПЛК

PT ISIM Overview Center

Сервер управления Overview Center устанавливается на уровне SOC или ЦОД и собирает события с подчиненных сенсоров, а также используется для их централизованной настройки и обновления



Алгоритм обработки трафика



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

**
Нормализованные и отфильтрованные сообщения проверяются на соответствие корреляционным правилам.

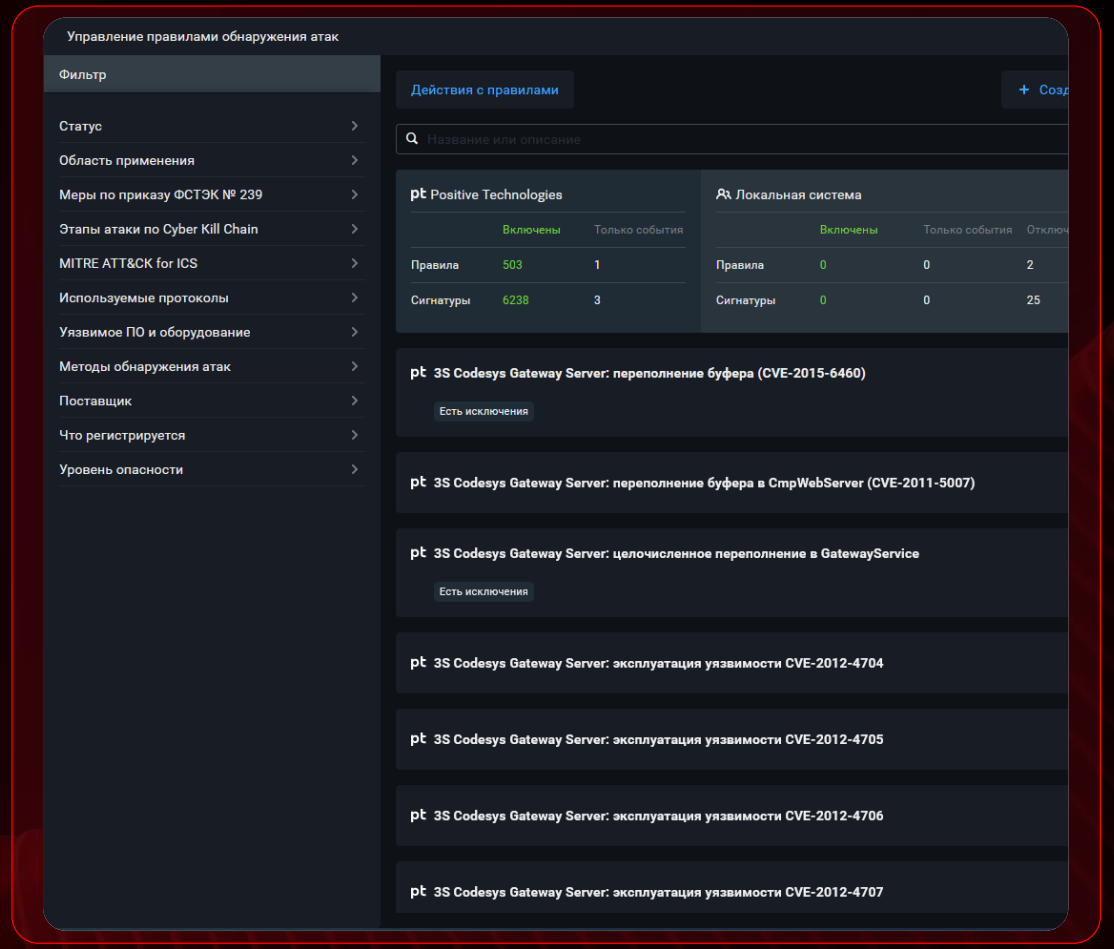
***
Если правило срабатывает --- регистрируется событие ИБ. Связанные события объединяются в цепочки, подготовленные для расследования

Технологическая экспертиза

8000+

правил и индикаторов промышленных угроз «из коробки»

Охватывают промышленное ПО и оборудование в инфраструктурах на Windows и Linux



«АдАстра»
«АМТ-ГРУП»
«Атомик Софт»
«Монитор Электрик»
«МПС софт»
НПФ «КРУГ»
«Прософт-Системы»
СПИК СЗМА
ЦИФРА ЦИП
ЧЭАЗ
«ЭКРА»
«Элара»
ABB
AVEVA
B&R
Emerson
GE
Hirschmann
Honeywell
MOXA
Mitsubishi
PLC Technology
Rockwell Automation
Siemens
Schneider Electric
Yokogawa
и другие

PT ISIM
Страница на сайте
ptsecurity.com

PT ICS
Подписывайтесь
на телеграм-канал
продукта

Спасибо!