

PT ISIM как инструмент CISO для контроля киберустойчивости ОТ

Дмитрий Даренский

Руководитель практики промышленной
кибербезопасности

ТОП-3 причины защищать ОТ инфраструктуру



Безопасность людей и предотвращение катастроф

Недопущение аварий и техногенных катастроф, и, как следствие, угрозы безопасности персонала и населению

Непрерывность производства

Недопущение остановки технологических процессов (простоев) и, как следствие, колоссальных финансовых и имиджевых рисков

Защита коммерческой тайны

Предотвращение кражи интеллектуальной собственности

Кибербезопасность ОТ — не статья расходов, а условие устойчивости производства и бизнеса

Почему технологическую (OT) инфраструктуру нельзя защищать как ИТ



1

Другие активы

PLC, HMI, SCADA, инженерное ПО, как правило вне зоны действия инструментов ИБ для ИТ

2

Другие технологии

Промышленные протоколы, «жесткий» реалтайм, много legacy, не обновляемый / не патченный софт, многолетний uptime

3

Другие последствия атак

Остановка производства и разрушение производственных активов, масштабные аварии, опасность для здоровья и жизни людей

Поэтому ИБ-инструменты и метрики эффективности для ИТ-сети здесь не результативны. OT требует собственных ИБ-решений и критериев оценки, учитывающих эту специфику





PT ISIM 6

Обеспечивает киберустойчивость
технологических инфраструктур,
инженерных систем и объектов КИИ



Возможности PT ISIM 6



PT ISIM покрывает все этапы кибератаки — от инвентаризации активов и управления уязвимостями до обнаружения вторжений и антивирусной защиты, обеспечивая глубокую промышленную экспертизу



Инвентаризация активов
(asset management)



Антивирусная защита (AV)



Анализ сетевого трафика
(COB*, NTA)



Управление уязвимостями
(vulnerability management)



Защита конечных устройств
и реагирование (EDR)



Контроль
технологического процесса

PT ISIM доступен в виде ПО, виртуального образа или доверенного ПАК.
Гибкая система лицензирования с оплатой только нужных функций



Управление событиями
безопасности (SIEM)

*COB — система обнаружения вторжений (согласно профилю ФСТЭК), или IDS, NTA, сетевой сенсор, анализатор трафика

Сертификат ФСТЭК

PT ISIM 5.9 сертифицирован ФСТЭК России



Сертификат ФСТЭК России № 4182, действительный до 2030 г., по следующим профилям:

- COB уровня сети четвертого класса защиты (ИТ.COB.C4.ПЗ)
- САВЗ типа «А» четвертого класса защиты (ИТ.САВЗ.А4.ПЗ)
- САВЗ типа «Б» четвертого класса защиты (ИТ.САВЗ.Б4.ПЗ)
- САВЗ типа «В» четвертого класса защиты (ИТ.САВЗ.В4.ПЗ)



Согласно формуляру, продукт может применяться в качестве:

- Сертифицированного средства обнаружения и реагирования (СОР)
- Сертифицированного средства контроля состава технических средств, обнаружения и контроля устранения уязвимостей программного обеспечения и операционных систем (VM)
- Сертифицированного средства сбора и анализа информации о событиях, регистрируемы в журналах аудита элементов информационных систем (SIEM)



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 4182

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
9 декабря 2019 г.

Выдан: 9 декабря 2019 г.

Переоформлен: 14 мая 2026 г.

Действителен до: 8 августа 2025 г.

Срок действия продлен до: 8 августа 2030 г.

Постоящий сертификат удостоверяет, что программное изделие «Система мониторинга защищенности и управления инцидентами информационной безопасности промышленных систем Positive Technologies Industrial Security Incident Manager», разработанное и производимое АО «Позитив Текнолоджиз», является программным средством анализа и корреляции событий безопасности информации и реагирования на них, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.COB.C4.ПЗ» (ФСТЭК России, 2012), «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ» (ФСТЭК России, 2012), «Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла» (ФСТЭК России, 2025) - по 4 классу защиты и заданию по безопасности 83128364.ISIM 3Б 01, при выполнении указаний по эксплуатации, приведенных в формуляре 83128364.ISIM 30 01.

Сертификат выдан на основании технического заключения от 05.11.2019, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ» (аттестат аккредитации от 15.09.2016 № СЗИ RU.0001.01БИ00.Б010), экспертного заключения от 11.11.2019, оформленного органом по сертификации АО «ППО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.А007), технического заключения от 18.06.2020, оформленного испытательной лабораторией АО «ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ», технических заключений от 03.04.2023, 02.10.2024 и 07.04.2026, оформленных АО «Позитив Текнолоджиз», и экспертного заключения от 01.08.2025, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Заявитель: АО «Позитив Текнолоджиз»

Адрес: 107061, г. Москва, инт.р.: муниципальный округ Преображенское, Преображенская пл., д. 8, помещ. 60

Телефон: (495) 744-0144

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах инфраструктуры) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации



Программно-аппаратный комплекс PT ISIM



Отечественное комплексное решение,
готовое к работе, с полной поддержкой из одного окна



Состав ПАК

- Аппаратная платформа
- ОС Astra Linux
- ПО PT ISIM
- Расширенная техническая поддержка с авансовой заменой оборудования на следующий рабочий день



Решение для КИИ (ПП № 1912)

- Отечественное ПО, ОС и ПАК в реестре Минцифры
- Аппаратные платформы в реестре РЭП Минпромторга
- ПО сертифицировано ФСТЭК и протестировано на совместимость отечественными вендорами АСУ ТП

NS-1050



NS-2010



КРІ киберустойчивости ОТ инфраструктуры

язык, на котором ИБ говорит с бизнесом



Портфель КРІ киберустойчивости

Эффект для бизнеса (C-level)

Видимость активов и
обнаружение угроз



Прямое влияние на непрерывность производства и доступность оборудования при среднем и высоком уровне автоматизации /цифровизации

Контроль доступа и
сегментация сети



Защита от каскадных отказов и рисков для безопасности персонала

Устойчивость и
влияние на бизнес



Соответствие требованиям регуляторов, управляемость страхового риска, обоснование инвестиций в кибербезопасность ОТ

Метрики оценки кибербезопасности ОТ инфраструктуры это не про технический отчёт ИБ-департамента — это индикаторы устойчивости и непрерывности всего производства и бизнеса

Видимость и обнаружение

видеть угрозу раньше, чем она станет аварией



Точность инвентаризации ОТ-активов

ЧТО ИЗМЕРЯЕТСЯ

Доля ОТ-активов,
автоматически обнаруженных и
классифицированных: вендор,
модель, версия прошивки.

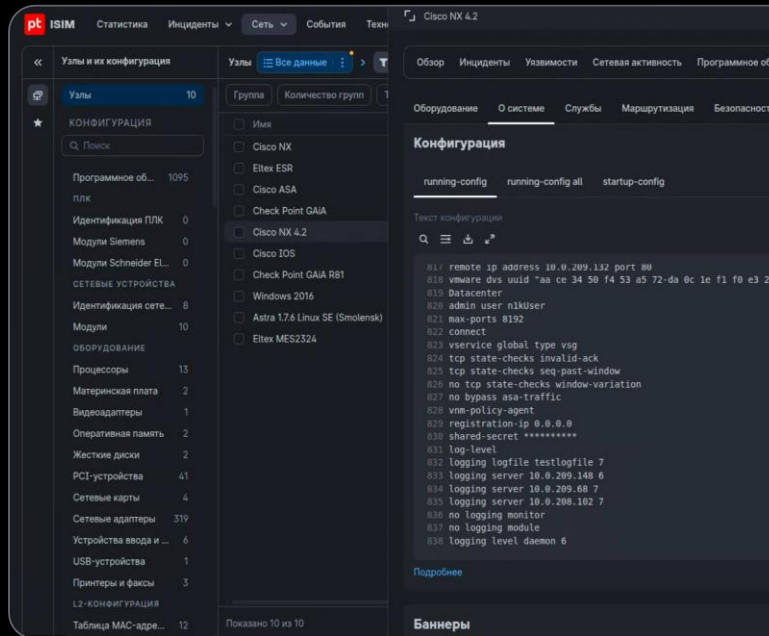
ЗНАЧИМОСТЬ ДЛЯ РУКОВОДИТЕЛЯ

Достоверная база для
планирования ТОиР и бюджета на
ЗИП; сокращает «неизвестную»
поверхность атаки.

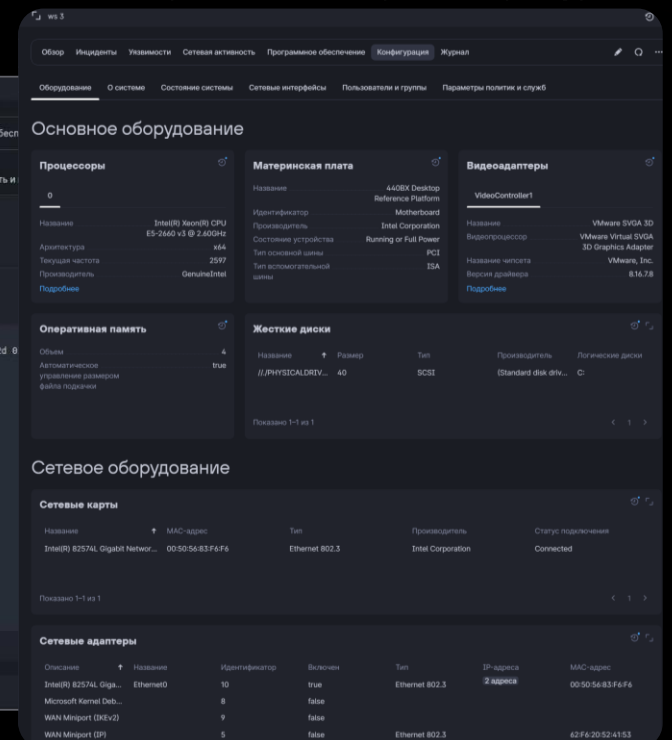
PT ISIM:

поддержка данных об ОТ-активах в актуальном состоянии

Инвентаризация ПО и конфигураций



Инвентаризация аппаратных ресурсов



Видимость и обнаружение

видеть угрозу раньше, чем она станет аварией



MTTD в ОТ-сегментах

ЧТО ИЗМЕРЯЕТСЯ

Среднее время от появления угрозы (аномальный трафик, подозрительные файлы и действия пользователей) до её регистрации в SOC.

ЗНАЧИМОСТЬ ДЛЯ РУКОВОДИТЕЛЯ

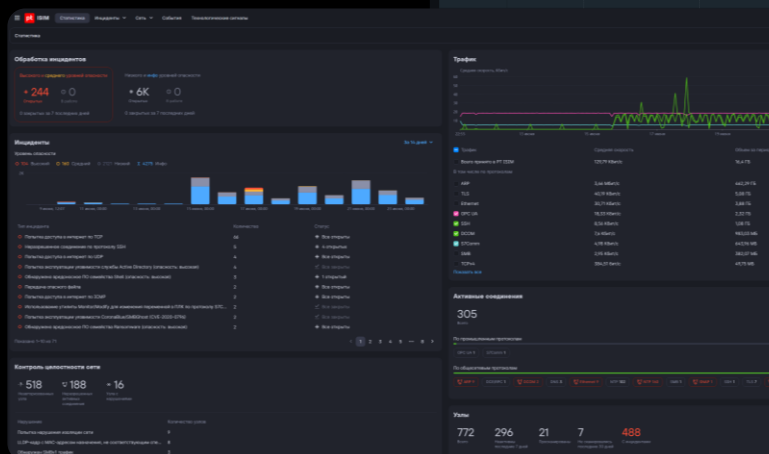
Сокращение времени присутствия злоумышленника в контуре, влияющего на оборудование и техпроцесс.

* MTTD - Mean Time to Detect

PT ISIM:

Обнаружение атак во всей ОТ-инфраструктуре,
Снижение времени обнаружения за счёт встроенной экспертизы и автоматизации

Контроль ключевых показателей безопасности инфраструктуры



Обнаружение атак и аномалий в трафике технологической сети

Обнаружение атак на APM и серверы SCADA + события антивируса

Обнаружение отклонений в параметрах технологического процесса

Контроль доступа и сегментация

не дать инциденту распространиться



Доля защищённых high-risk legacy-активов

ЧТО ИЗМЕРЯЕТСЯ

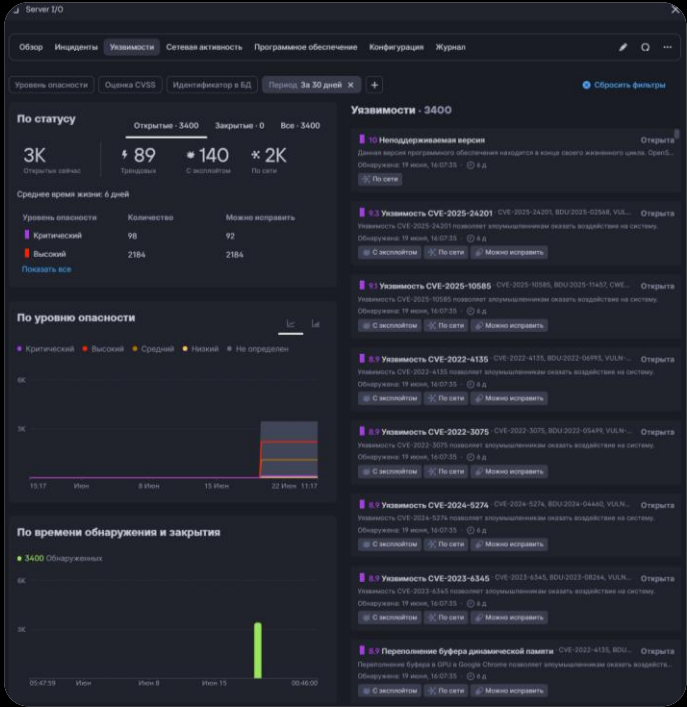
Доля критичных активов с уязвимым ПО без патчей, для которых внедрены компенсирующие меры защиты.

ЗНАЧИМОСТЬ для РУКОВОДИТЕЛЯ

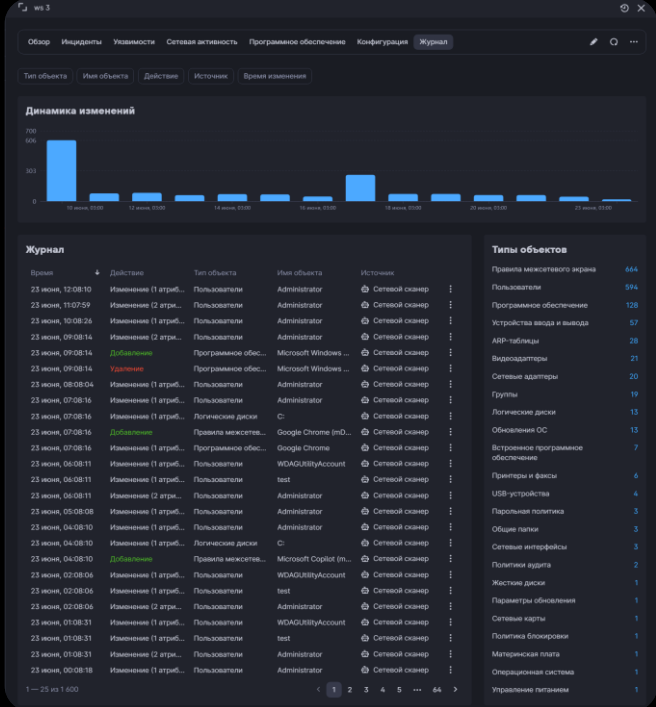
Контроль остаточного риска для устаревшего, но по-прежнему рабочего оборудования.

PT ISIM:
Инвентаризация, ручная и авто-классификация по уровню критичности. Контроль конфигураций legacy-активов

Контроль уязвимостей



Контроль изменений конфигураций



Контроль доступа и сегментация

не дать инциденту распространиться



Алерты бокового перемещения между сегментами

ЧТО ИЗМЕРЯЕТСЯ

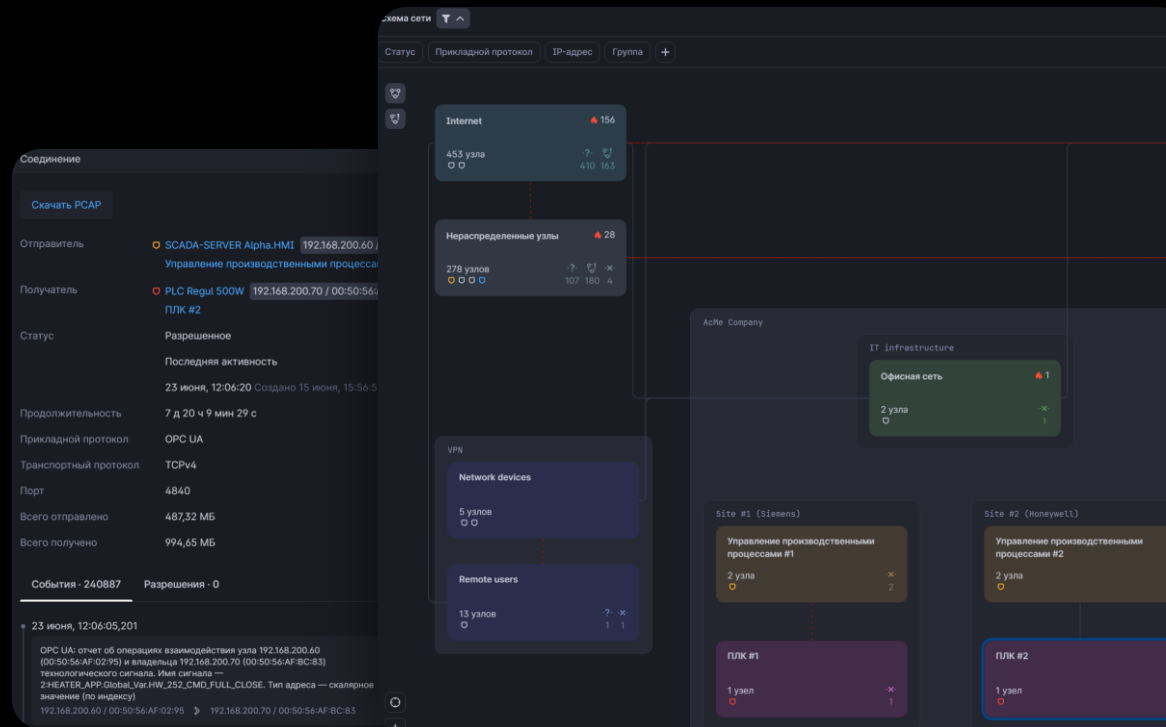
Частота обнаружения сетевых соединений через границы зон (например, HMI → ERP, PLC → SIS).

ЗНАЧИМОСТЬ ДЛЯ РУКОВОДИТЕЛЯ

Эффективность сегментации; изоляция критичных сегментов АСУ ТП друг от друга.

PT ISIM:

Обнаружение инцидентов связанных с боковым перемещением между сегментами и повышением привилегий



- группировка узлов в группы и контейнеры (зоны/сегменты), контроль соединений между ними;
- отслеживание подключения к интернету и к корпоративной сети;
- детальная информация по узлам, соединениям и инцидентам – в один клик.

Устойчивость и влияние на бизнес от инцидента ИБ к непрерывности производства



KPI 7



**MTBF* в связке с
киберинцидентами**

ЧТО ИЗМЕРЯЕТСЯ

Корреляция наработки
оборудования на отказ и
режимов эксплуатации с ИБ-
инцидентами.

**ЗНАЧИМОСТЬ ДЛЯ
РУКОВОДИТЕЛЯ**

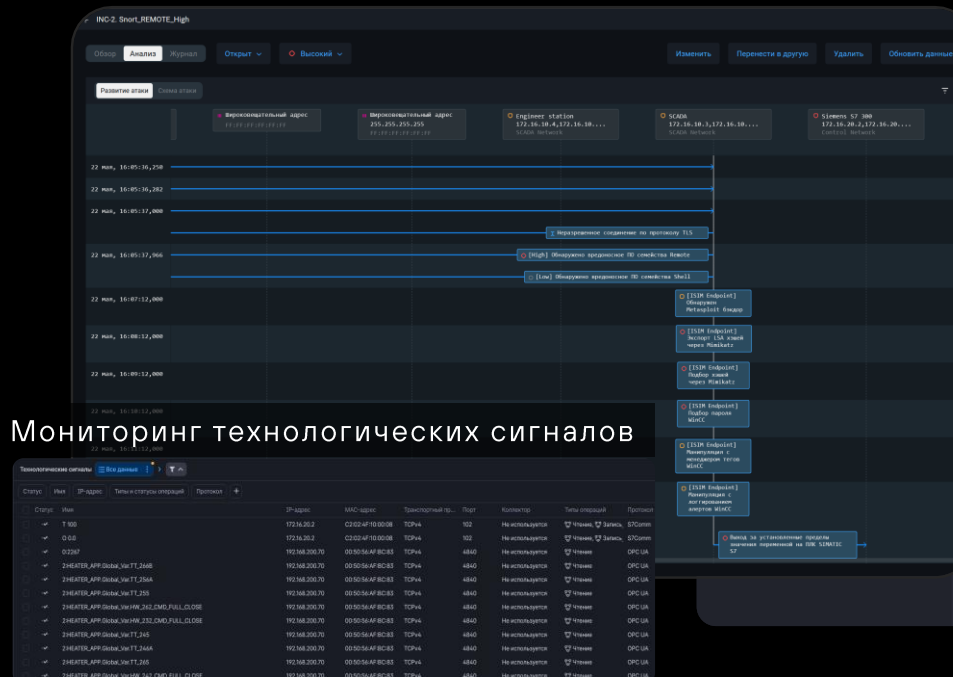
Отделяет реальные отказы
оборудования от последствий
атак или мисконфигурации —
точность диагностики.

*MTBF - Mean Time Between Failures

PT ISIM:

Контроль отклонений технологических сигналов и команд, корреляция и объединение
в один контекст с инцидентами кибербезопасности

Общий контекст событий ИБ и технологических отклонений



Настройка обнаружения
отклонений
технологических сигналов

The screenshot shows the configuration interface for detecting technological signal deviations. It includes a 'Регистрируемый инцидент' (Registrable incident) section with a 'Удалить' (Delete) button. Below this is a 'Условие' (Condition) section with a dropdown menu for 'Технологический сигнал' (Technological signal) set to '2HEATER_APP.Global_Var.TT_220_OP' and a 'Тип данных: Float' (Data type: Float). The 'Критерий 1' (Criterion 1) section shows 'Последнее значение' (Last value) set to 'Больше чем' (More than) 70. The 'Критерий 2' (Criterion 2) section shows 'Тип операции' (Operation type) set to 'Запись' (Write). The 'Критерий 3' (Criterion 3) section shows 'Последнее значение' (Last value) set to 'Равно одному из значений' (Equal to one of the values) with a list of values: 33, 66, 99, and a '+ Еще значения' (More values) button. A 'Добавить критерий' (Add criterion) button is at the bottom.

Устойчивость и влияние на бизнес от инцидента ИБ к непрерывности производства



MTTR* по критичным уязвимостям (CVSS)

ЧТО ИЗМЕРЯЕТСЯ

Среднее число дней на закрытие новой критической уязвимости в ОТ-оборудовании и ПО.

ЗНАЧИМОСТЬ для РУКОВОДИТЕЛЯ

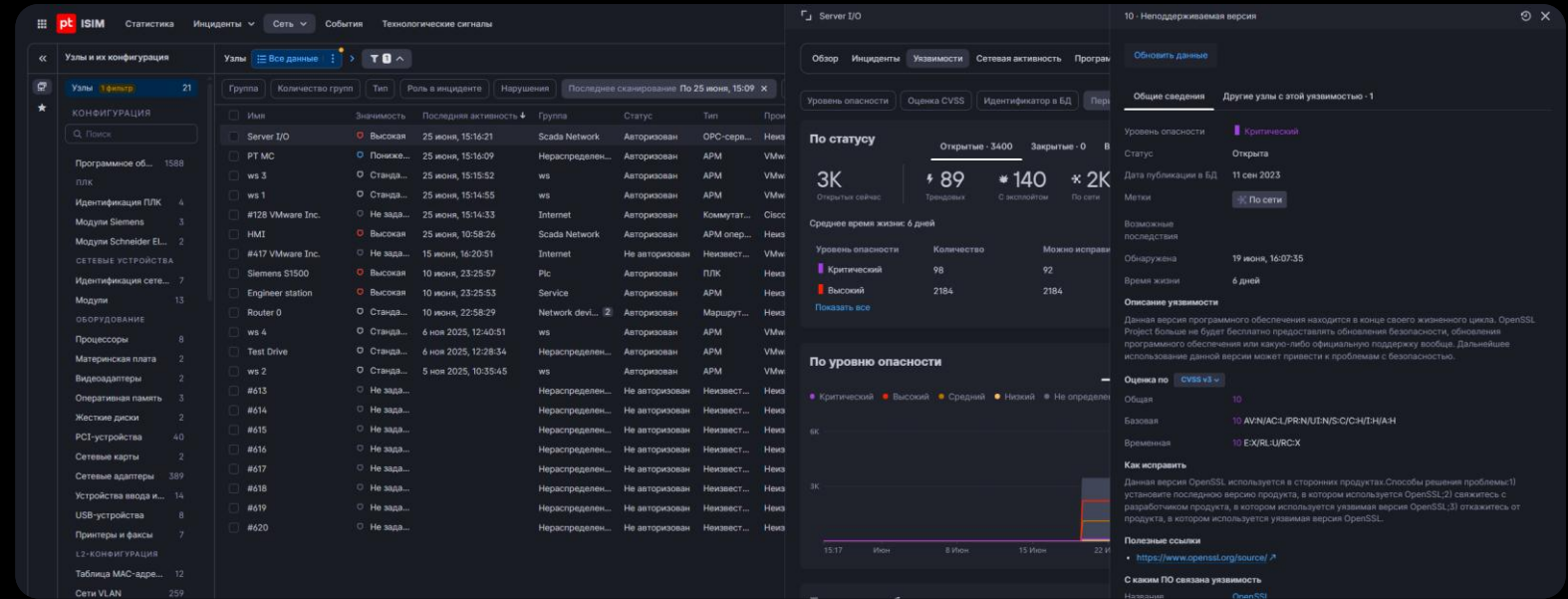
Минимизирует вероятность реализации известной угрозы в контролируемой ОТ - инфраструктуре.

*MTTR — Mean Time to Remediate

PT ISIM:

Обнаружение и приоритизация уязвимости ОТ-активов.

Отслеживание изменений, появления и закрытия уязвимостей.



PT ISIM – мощный инструмент

- для формализации контроля и метрик оценки киберустойчивости ОТ
- для сбора и агрегации необходимых данных о состоянии и изменениях ОТ
- для поддержания актуальности и достоверности информации о состоянии ОТ





Как приручить всю эту мощь?

- Не утонуть в объёме данных и информации
- Не заблудиться в анализе и выводах
- Не запутаться во всех функциях продукта

И главное – не потерять время,
необходимое для предотвращения
угрозы и защиты предприятия

Как LLM приземляется в продукты кибербеза



LLM Помощники

Рутинные задачи в существующих продуктах

- Создать правило
- Написать фильтр
- Собрать отчет
- Развернуть продукт

С них все начали, но это не то, ради чего стоило бы говорить о новой эре

Поддержка принятия решений

Равноправное с человеком участие LLM в принятии решений в новых продуктах

- Общение с продуктом на естественном языке, как возможность начать произвольную задачу
- Автоматический анализ данных в продукте, а не просто «40» запросов-ответов

Их все делают. Нужно начинать пилотировать. Вы поймете какими они могут быть, вендор получит обратную связь. Существующие продукты используйте как сенсоры.

Автоматическая защита

LLM автономно выполняет всю работу, человек подтверждает важные решения.

- LLM принимает решение false или нет
- LLM реагирует и останавливает хакера
- LLM говорит как улучшить внедрение, зная ВАШУ инфраструктуру

Куда мы как индустрия идём. Но ключевой вопрос в доверии. Доверие подтверждается только доказанными тестами.

LLM в PT ISIM

*до конца 2026



Решаемые задачи



Запросы на естественном языке в одном окне по любым данным

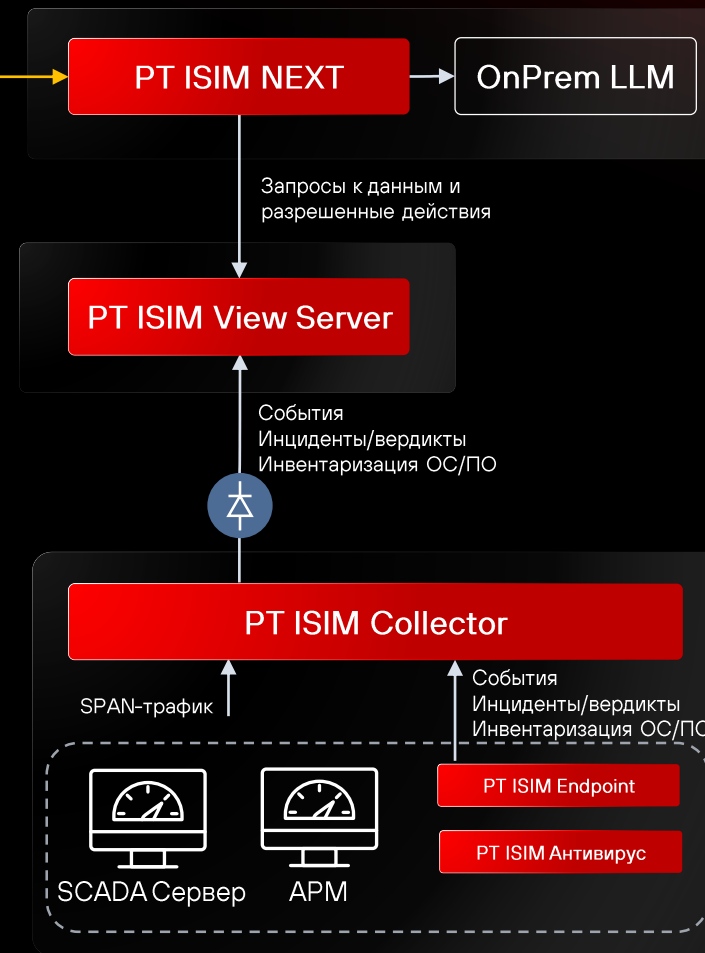
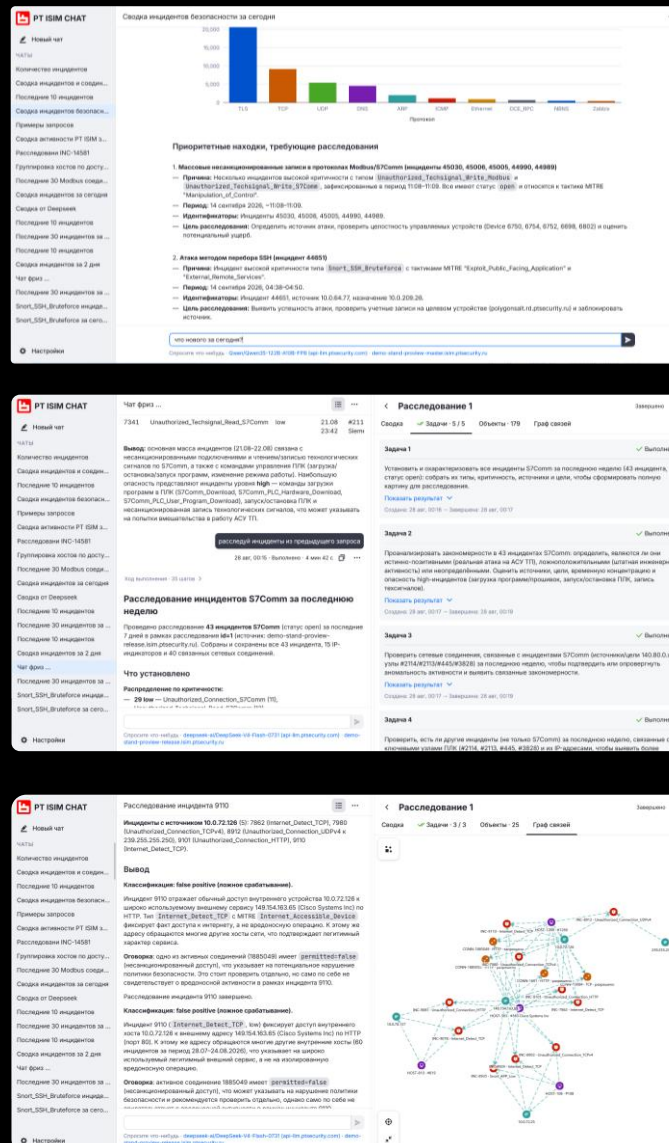


Автоматическое расследование инцидентов и рекомендации по реагированию

планирование расследования и оценка алертов, соединений, событий, трафика, для составления наиболее полной картины происшествия



Автоматизация мониторинга безопасности по всей инфраструктуре





habrahabr.ru/company/pt



pt@ptsecurity.com



ptsecurity.com



Новости о
продукте

https://t.me/pt_ics_news



Запросить
тест-драйв

<https://ptsecurity.com/products/isim/>



Спасибо!