



PT ISIM

Система для обеспечения киберустойчивости
технологической инфраструктуры



24
года

экспертизы
в разработке
и исследованиях

сильная команда

>2,5k

сотрудников

500+

партнеров



МОСКОВСКАЯ
БИРЖА

Первая и единственная
публичная компания в области
кибербезопасности
на Московской бирже
(MOEX: POSI)

Входим в топ-50 компаний
на Московской бирже
(основной индекс IMOEX)



Positive
Technologies 

25+

высокотехнологичных
продуктов и решений
в портфеле

2000

крупных компаний из всех отраслей — наши клиенты

200k+

акционеров

Специфика киберугроз для технологической инфраструктуры

Актуальные киберугрозы для промышленных предприятий России



Промышленный сектор — лидер по числу атак на российские организации

1

19% успешных атак в 2025 году

83%

3

атак совершены с помощью легитимного ПО

Доля инцидентов, связанных с подрядчиками, в России вдвое превышает общемировую величину

2

33%

4

кибератак приводят к нарушению основной деятельности предприятия

Почему технологическую (OT) инфраструктуру нельзя защищать как ИТ-инфраструктуру



Другие активы

1

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

Другие протоколы

2

Промышленные протоколы, в том числе проприетарные: Modbus, OPC вместо TCP/IP

Иная цена ошибки

3

Сбой в ОТ — это остановка производства или авария, а не простой сервиса

!

Поэтому инструменты ИБ для ИТ-сети здесь не результативны.
ОТ-инфраструктура требует собственных решений, спроектированных под ее специфику

Угрозы для ОТ-инфраструктуры



Что делает ОТ-инфраструктуру уязвимой



Отсутствие сегментации сети



Отсутствие мониторинга штатной работы и эксплуатации ОТ-инфраструктуры



Устаревшее или уязвимое ПО и версии протоколов без возможности обновления или патчинга



Неконтролируемый прямой или удаленный доступ подрядчиков и авторизованного персонала



Непроектные устройства и АРМ, в том числе с выходом в интернет



Небезопасная эксплуатация:

- непроверенные USB-устройства
- установка нелегитимного ПО
- использование паролей по умолчанию и общих учетных записей
- несогласованное изменение конфигурационных настроек и привилегий



Какие угрозы могут быть реализованы



- Заражение ОТ-инфраструктуры вредоносным ПО
- Целевые атаки с низким уровнем сложности
- Перехват или блокирование управления оборудованием, техпроцессом или самой ОТ-инфраструктурой
- Неавторизованная эксплуатация, вывод из строя и аварии на производстве
- Неавтоматизированное чтение и запись тегов в ПЛК
- Подмена файлов проектов в SCADA и HMI
- Запуск инженерного и управляющего ПО в АСУ ТП



Киберустойчивость технологической (OT) инфраструктуры невозможно обеспечить точечными решениями

Необходим единый подход к защите сети,
узлов и технологического процесса



PT ISIM 6

Обеспечивает киберустойчивость
технологических инфраструктур,
инженерных систем и объектов КИИ



PT ISIM 6 сегодня



Результативная кибербезопасность технологической инфраструктуры

- Один продукт для всей ОТ-среды* — от инвентаризации активов до реагирования на инцидент
- Единый контекст событий сети, хостов, ПЛК и технологического процесса



Соответствие регуляторным и отраслевым стандартам

Помогает выполнять требования Приказов № 239 и № 31 ФСТЭК России по защите объектов КИИ



Интеграция данных в корпоративную аналитику

Передаёт данные о событиях, активах и технологических процессах в SIEM-систему и озера данных, делая их доступными для централизованного контроля защищённости и принятия управленческих решений

*ОТ (operational technology) — технологии управления производственными процессами

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



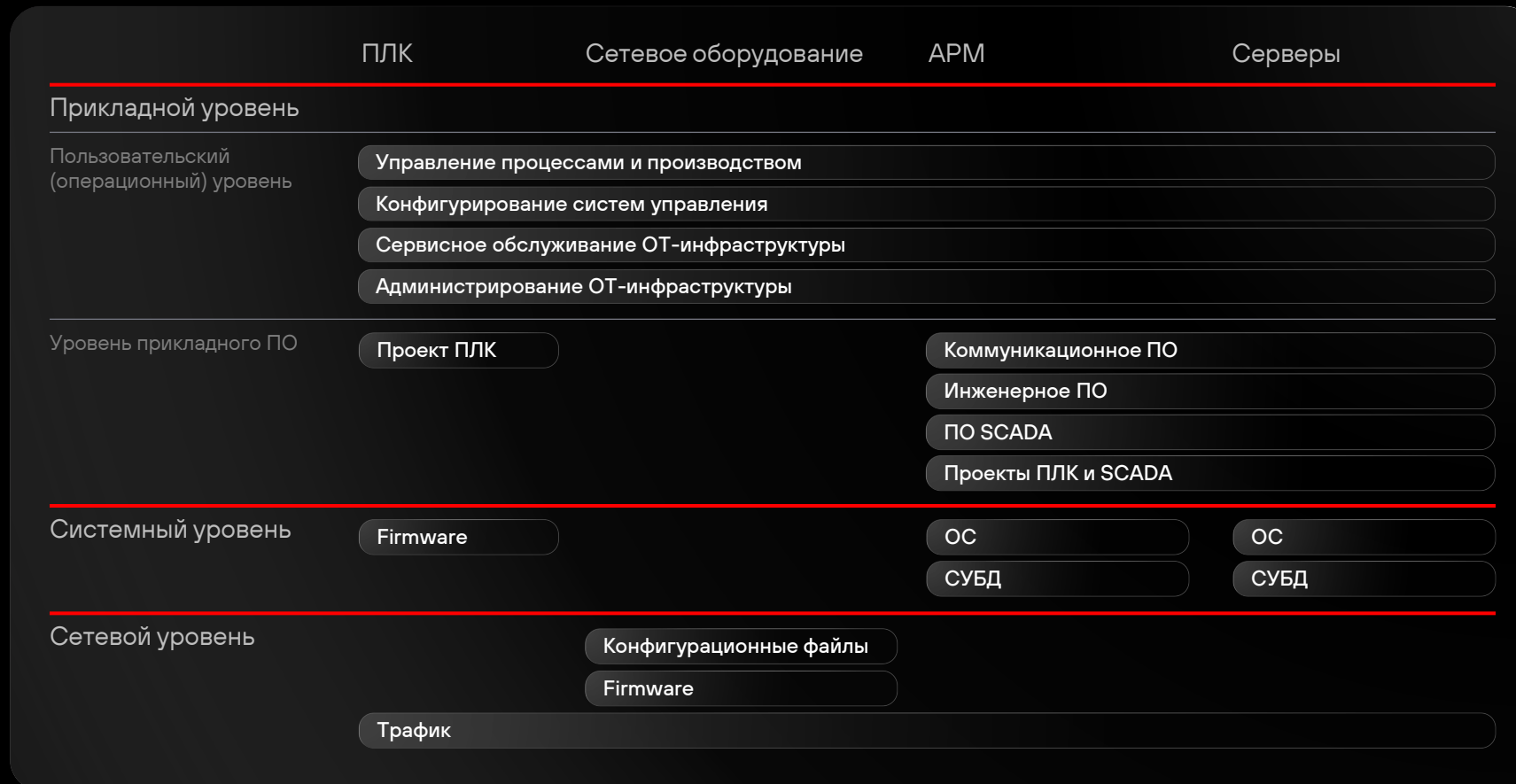
Управление событиями
безопасности (SIEM)

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

Промышленная экспертиза



PT ISIM выявляет специфичные для технологических сетей техники атак в поддерживаемых SCADA-системах: подмену проектов, подбор паролей, нелегитимный запуск инженерных утилит и другие признаки компрометации



130+

Поддерживаемых вендорских платформ АСУ ТП

16 000

Правил и индикаторов промышленных угроз

10+

Поддерживаемых вендорских платформ АСУ ТП

Результаты работы PT ISIM



Раннее выявление проникновений в среду АСУ ТП через ИТ-инфраструктуру и действий нарушителя изнутри ОТ-инфраструктуры (сотрудник, подрядчик)



Своевременное обнаружение вредоносного ПО до влияния на техпроцесс



Выявление скрытых каналов доступа к АСУ ТП



Обнаружение уязвимого ПО, слабых паролей или паролей по умолчанию, устаревших протоколов



Контроль опасных команд или атак на ПЛК и оборудование

Неавторизованное подключение к производству, опасные команды, манипуляции и вмешательство в технологический процесс под видом легитимного пользователя может нарушить устойчивость работы производственных активов и привести к остановке бизнеса, авариям, штрафам и потерям

PT ISIM дает наблюдаемость и контроль инфраструктуры, обеспечивая тем самым ее киберустойчивость и защиту

PT ISIM 6 управляет поверхностью атаки



Инвентаризация активов
(asset management)

Управление уязвимостями
(vulnerability management)



Инвентаризация активов и управление уязвимостями



PT ISIM обеспечивает полную видимость активов и помогает выявлять уязвимости до того, как ими воспользуется злоумышленник



ASSET MANAGEMENT

Инвентаризация активов

PT ISIM формирует актуальную карту активов ОТ-контура

- Инвентаризация ПО и оборудования, контроль изменений конфигураций оборудования
- Учет пользователей и сетевых подключений



VULNERABILITY MANAGEMENT

Выявление уязвимостей

PT ISIM определяет состояние безопасности

- Обнаруживает и приоритизирует уязвимости по уровню опасности для инфраструктуры
- Предоставляет рекомендации по устранению уязвимостей



Используемые технологии

- Пассивный анализ трафика
- Инвентаризация с помощью хостового агента ISIM Endpoint
- Инвентаризация с помощью сетевого сканера: активный опрос (SSH, WMI, промышленные протоколы)
- Сканер промышленных контроллеров (ПЛК)
- Сканер сетевых устройств
- База уязвимостей для ИТ- и ОТ-сегментов

Управление уязвимостями в АСУ ТП



> Windows- и Linux-системы являются типовыми на верхнем уровне технологической сети.

К ним применимы те же уязвимости, что и в корпоративных сетях

> С уязвимостями можно бороться, если знать, какие уязвимости есть в инфраструктуре и правильно их приоритизировать

Используйте Positive Technologies OT cybersecurity framework* для построения процессов управления уязвимостями технологических сетей (vulnerability management)



PT ISIM 6 защищает рабочие станции и серверы АСУ ТП



Антивирус (EPP)

Защита конечных узлов
и реагирование (EDR)



Защита конечных узлов и реагирование



EDR

Защита конечных точек и реагирование

- Выявление несанкционированного доступа
- Обнаружение атак living off the land, когда злоумышленник использует легитимные инструменты системы
- Выявление OT-специфичных техник в SCADA: подмена проектов, подбор паролей, нелегитимный запуск инженерных утилит



EPP

Антивирусная защита

- Автоматическая блокировка массовых угроз, либо только обнаружение там, где автоматическая блокировка невозможна
- Выполнение мер приказа № 239 ФСТЭК России. Сертифицированное средство антивирусной защиты обязательно для всех категорий КИИ

PT ISIM сертифицирован как:

- средство антивирусной защиты (СAB3)
- средство обнаружения и реагирования на уровне узла (COP)

Варианты поставки

- PT ISIM EPP (антивирус)
- PT ISIM EDR, включающий PT ISIM EPP

Лицензируется per host — поштучно

Лицензирование



- Входит в лицензию
- Не входит в лицензию
- ◐ Ограниченный функционал
- Доступно в Q4'2026

Артикул	PT-ISIM-EDR	PT-ISIM-AV
Мониторинг	●	○
Аудит узлов	●	●
Реагирование	●	◐
Продвинутое обнаружение	●	○
Контроль сменных носителей	●	●
Контроль приложений	●	●
Антивирусная защита	●	●

PT ISIM EPP

Лицензия на подключение агентов PT ISIM Endpoint Protection Platform (EPP) для антивирусной защиты промышленных конечных устройств.

Включает базовое реагирование: работу с файлами и процессами, remote shell, изоляцию узлов, завершение процессов

PT ISIM EDR

Лицензия на подключение агентов PT ISIM EDR (модули EDR и модули обеспечения антивирусной защиты конечных устройств)

PT ISIM Антивирус: архитектура



Рабочее место инженера
АСУ ТП, SCADA, HMI

PT ISIM Endpoint Agent

PT ISIM Endpoint Protection Platform (EPP)

Другие модули PT ISIM Endpoint EDR

Аудит ПО, ОС

Обнаружение угроз на ОС
и прикладное ПО, включая SCADA

ОПЕРАЦИОННЫЕ СИСТЕМЫ

Windows: 7-10

Windows Server: 2012-2019

Linux: Debian, Ubuntu, CentOS, Red Hat

Российские версии Linux: Astra Linux,
AlterOS, «РЕД ОС», «Альт Линукс»

Мониторинг и реагирование

Централизованная настройка политик

Обновление экспертизы

Сервер
PT ISIM View Server
или PT ISIM Collector

Консоль ISIM VIEW Server

Управление

Данные

PT ISIM 6 обеспечивает мониторинг технологической инфраструктуры



Анализ сетевого трафика
(NTA)

Контроль
технологического процесса

Управление
событиями ИБ (SIEM)



Мониторинг технологической инфраструктуры



NTA

Анализ сетевого трафика

- PT ISIM анализирует технологический трафик и выявляет угрозы в режиме реального времени
- Поддерживает широкий спектр промышленных и сетевых протоколов



ОТ-ПРОЦЕССЫ

Контроль технологического процесса

PT ISIM контролирует технологический процесс и выявляет действия, способные повлиять на безопасность и непрерывность производства

- Отслеживает отклонения технологических параметров и выход за критические уставки
- Выявляет передачу опасных технологических команд (перепрошивка ПЛК, форсирование переменных, очистка памяти)



SIEM

Управление событиями ИБ

PT ISIM объединяет события безопасности из различных источников инфраструктуры и обеспечивает централизованный мониторинг

- Собирает события с сетевых устройств, серверов, рабочих станций, ПЛК
- Нормализует и коррелирует события безопасности из различных источников
- Выявляет сложные цепочки атак и признаки компрометации
- Проводит проактивный поиск угроз в технологической инфраструктуре
- Выполняет централизованный поиск и расследование инцидентов безопасности

PT ISIM 6: анализ журналов с устройств АСУ ТП



Устройства в АСУ ТП

EDR



SCADA

EDR



APM инженера



Сетевое
оборудование



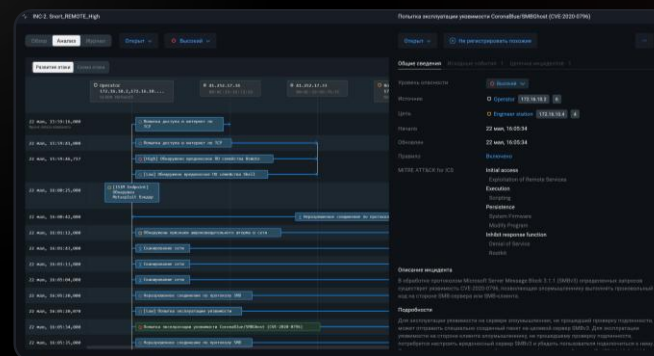
ПЛК

Нормализованные
события и алерты

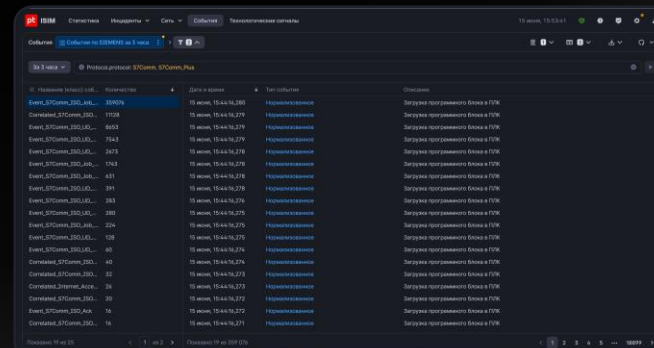


PT ISIM 6
Включает SIEM
для АСУ ТП

Безагентный сбор журналов
Нормализация и обнаружение
угроз на сервере PT ISIM



Браузер событий



С РТ ISIM 6 данные из удаленных
и изолированных сегментов
доступны в едином контуре
мониторинга



PT ISIM Collector



PT ISIM Collector



Компонент для сбора и первичной обработки инвентаризационных, событийных и технологических данных с конечных узлов и сетевого трафика, а также для управления агентами



Собирает

- Данные о конфигурациях узлов сети
- Исходные события с узлов сети
- События безопасности с узлов сети
- Копию сетевого трафика



Использует

- Сетевой сбор событий из журналов OS, SW, FW
- Сетевой опрос и сканирование узлов сети
- PT ISIM Endpoint Agent для сбора событий и конфигурационных данных серверов и рабочих станций
- Технологии SPAN, RSPAN, ERSPAN, Port Mirroring для сбора копии сетевого трафика



Выполняет

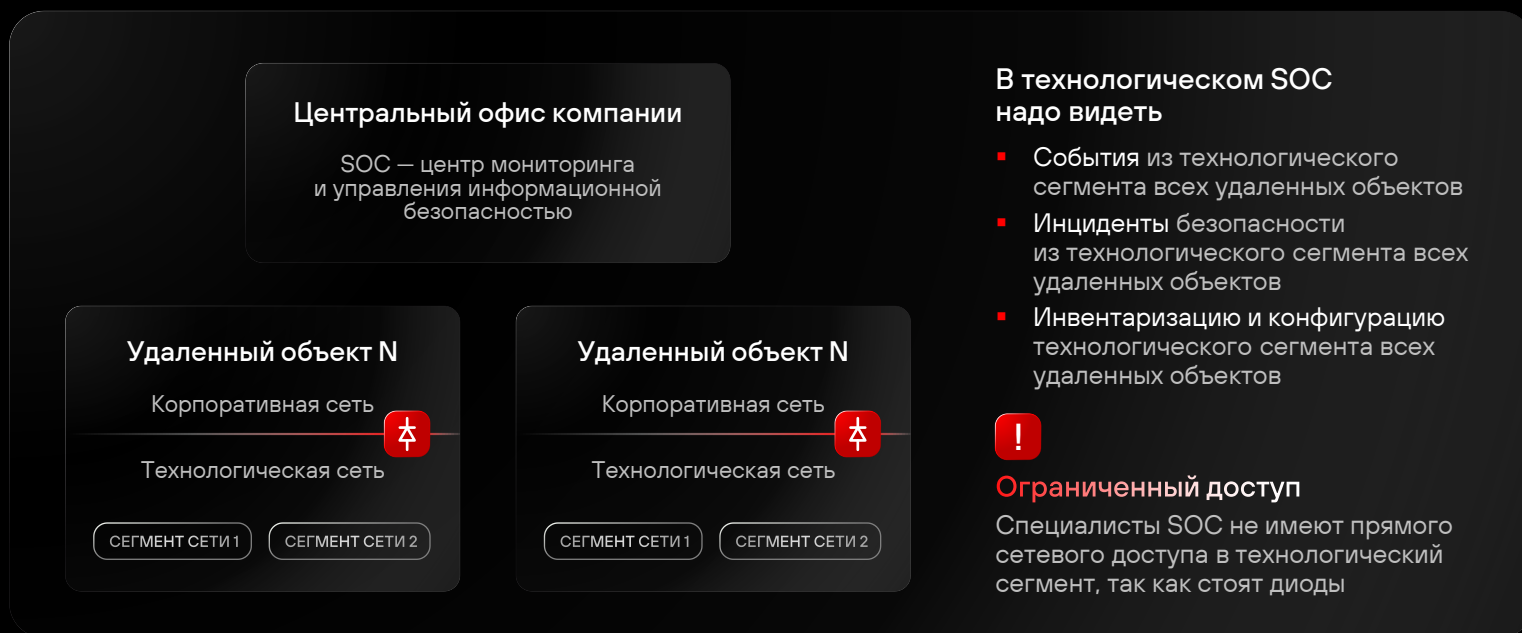
- Нормализацию событий и их отправку в PT ISIM View Server
- Структурирование инвентаризационной информации
- Глубокий анализ копии сетевого трафика, нормализацию сетевых событий, отправку их в PT ISIM View Server
- Управление PT ISIM Endpoint Agent



PT ISIM Collector



Компонент для сбора и первичной обработки инвентаризационных, событийных и технологических данных с конечных узлов и сетевого трафика, а также для управления агентами



Применяется в сегментах распределенных систем управления и на изолированных производственных площадках



Работает в сегментах с односторонней передачей данных без нарушения изоляции защищенного контура

Используйте Positive Technologies OT cybersecurity framework* для разработки архитектуры комплексных систем кибербезопасности ОТ-инфраструктур

*Positive Technologies OT cybersecurity framework доступен на сайте <https://ptsecurity.com/products/isim/>

Программно- аппаратный комплекс РТ ISIM

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



Программно-аппаратный комплекс PT ISIM



NS-1050		NS-2010
Функциональность продукта	- PT ISIM NTA (до 100 Мбит) - PT ISIM Collector	- PT ISIM NTA 100, 500 Мбит и 1 Гбит - PT ISIM Collector - PT ISIM Endpoint Server - PT ISIM Overview Center - PT ISIM VM и Log Collector
Процессор	1 x Intel Atom, 16 ядер	1 x Intel Xeon Scalable Gen5, 32 ядра
ОЗУ	32 ГБ DDR4 ECC DIMM	128 ГБ DDR5 ECC RDIMM
Дисковое пространство	480 ГБ SSD	1 + 3.8 ТБ SSD (-M1) 2x1 + 2x3.8 ТБ SSD (-M2)
Сетевой интерфейс RJ45	2 Гбит/с	4 Гбит/с (расширяется до 20 Гбит/с) — можно добавлять сетевые карты
Сетевой интерфейс SFP/RJ45	4 Гбит/с	До 20 Гбит/с
Операционная система	Astra Linux Special Edition «Воронеж»	Astra Linux Special Edition «Воронеж»
ГИСП и реестр ПАК Минцифры	ПАК PT ISIM NS-1050 ЕВРГ.466539.002 ↗ Реестровая запись № 28964 от 28.07.2025 ↗	ПАК PT ISIM NS-2010 ЕВРГ.466539.002-01 ↗ Реестровая запись № 28967 от 28.07.2025 ↗

Реализация требований регуляторов



PT ISIM позволяет выполнить важную часть требований закона № 239 ФСТЭК по защите объектов КИИ

Аудит безопасности (АУД)

Покрывает
требований

93%



Антивирусная защита (АВЗ)

Покрывает
требований

100%



Предотвращение вторжений, компьютерных атак (СОВ)

Покрывает
требований

100%



Реагирование на компьютерные инциденты (ИНЦ)

Покрывает
требований

100%



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



03



Как работает PT ISIM 6

Схема работы PT ISIM



Решение на базе PT ISIM



Схема с коллекторами

Сбор копии трафика, сбор событий, опрос устройств и управление агентами осуществляется распределенными по сегментам АСУ ТП или технологической сети коллекторами. Во View Server передаются метаданные. Передача метаданных между коллектором и View Server может выполняться через диод данных

1

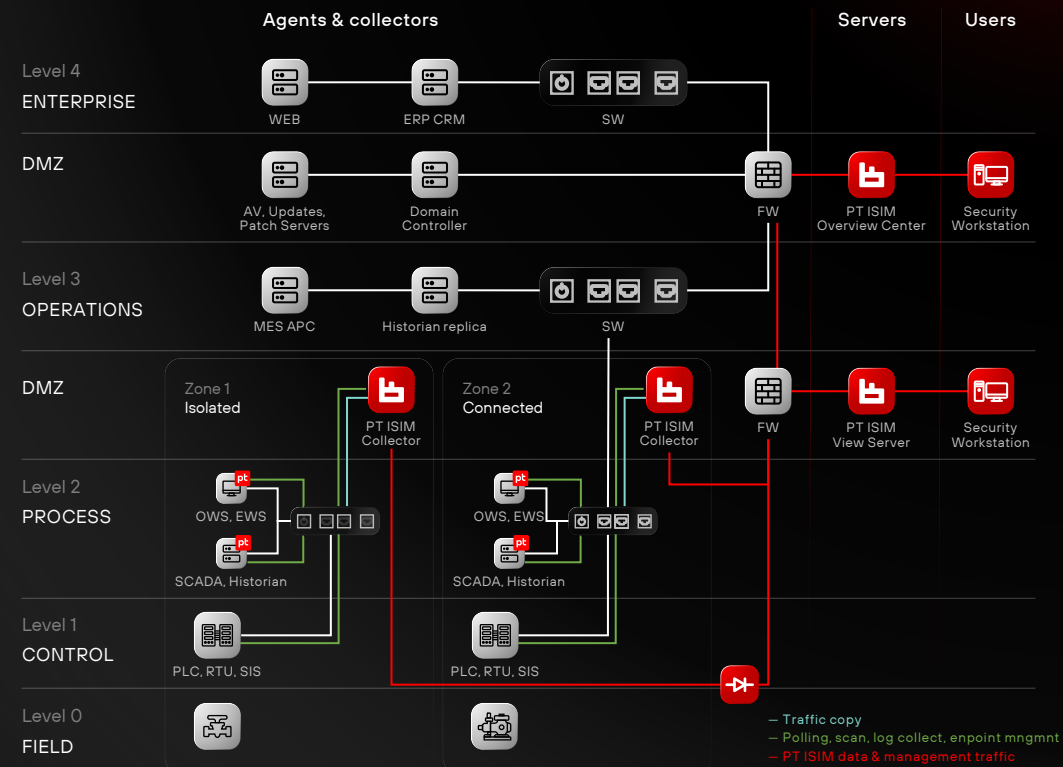
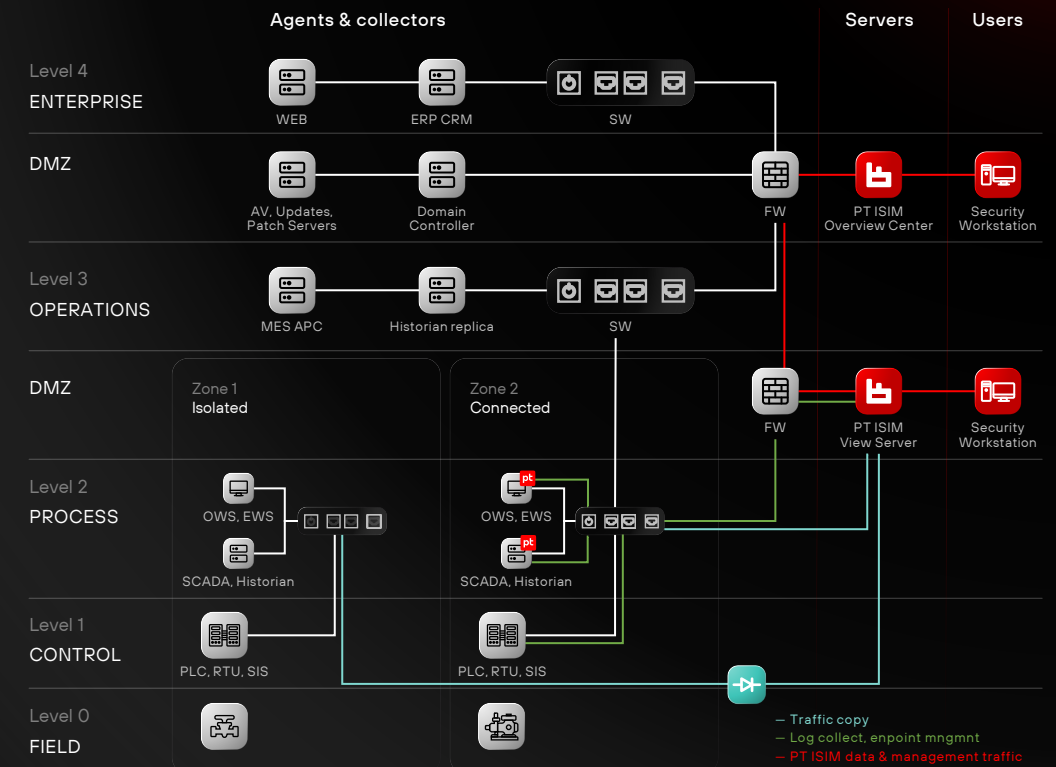


Схема без коллекторов

Анализ копии трафика, сбор событий, опрос устройств и управление агентами осуществляется централизованно PT ISIM View Server

2



Компоненты PT ISIM



ОБЯЗАТЕЛЬНЫЕ КОМПОНЕНТЫ

PT ISIM View Server

Анализирует и хранит сетевой трафик, получает события безопасности с агентов и управляет ими. Устанавливается на уровне сегмента сети АСУ ТП или всей производственной площадки

ОПЦИОНАЛЬНЫЕ КОМПОНЕНТЫ

Агенты PT ISIM Endpoint

Устанавливаются на SCADA-серверы и рабочие места. Собирают события безопасности операционных систем и прикладного ПО АСУ ТП, обеспечивают антивирусную защиту

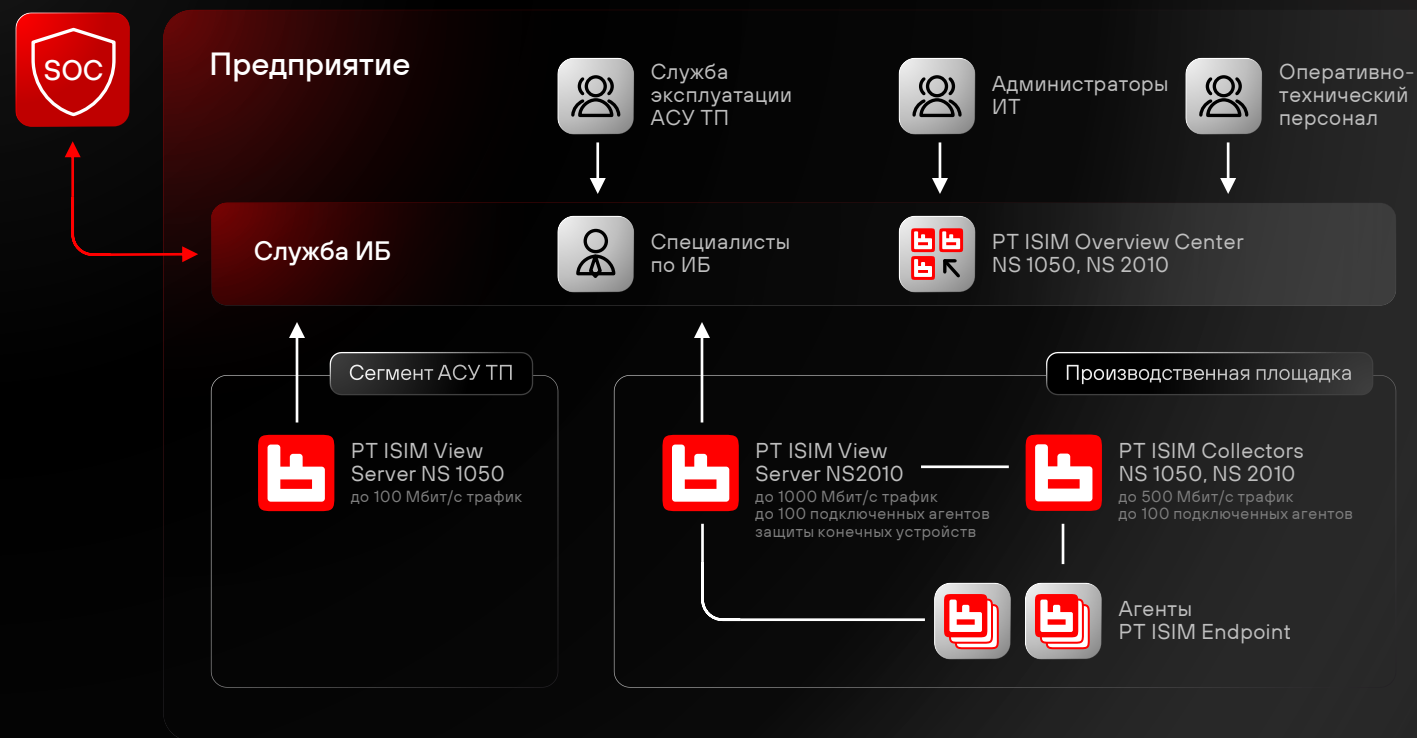
PT ISIM Overview Center

Собирает события с подчиненных сенсоров, используется для их централизованной настройки и обновления. Устанавливается на уровне ситуационного центра (SOC)

PT ISIM Collector

Коллектор для анализа трафика удаленных сегментов в единый интерфейс мониторинга технологической сети PT ISIM View Server с экономией в использовании канала связи

Компания или холдинг



Демонстрация возможностей PT ISIM 6

PT ISIM — единая точка мониторинга безопасности

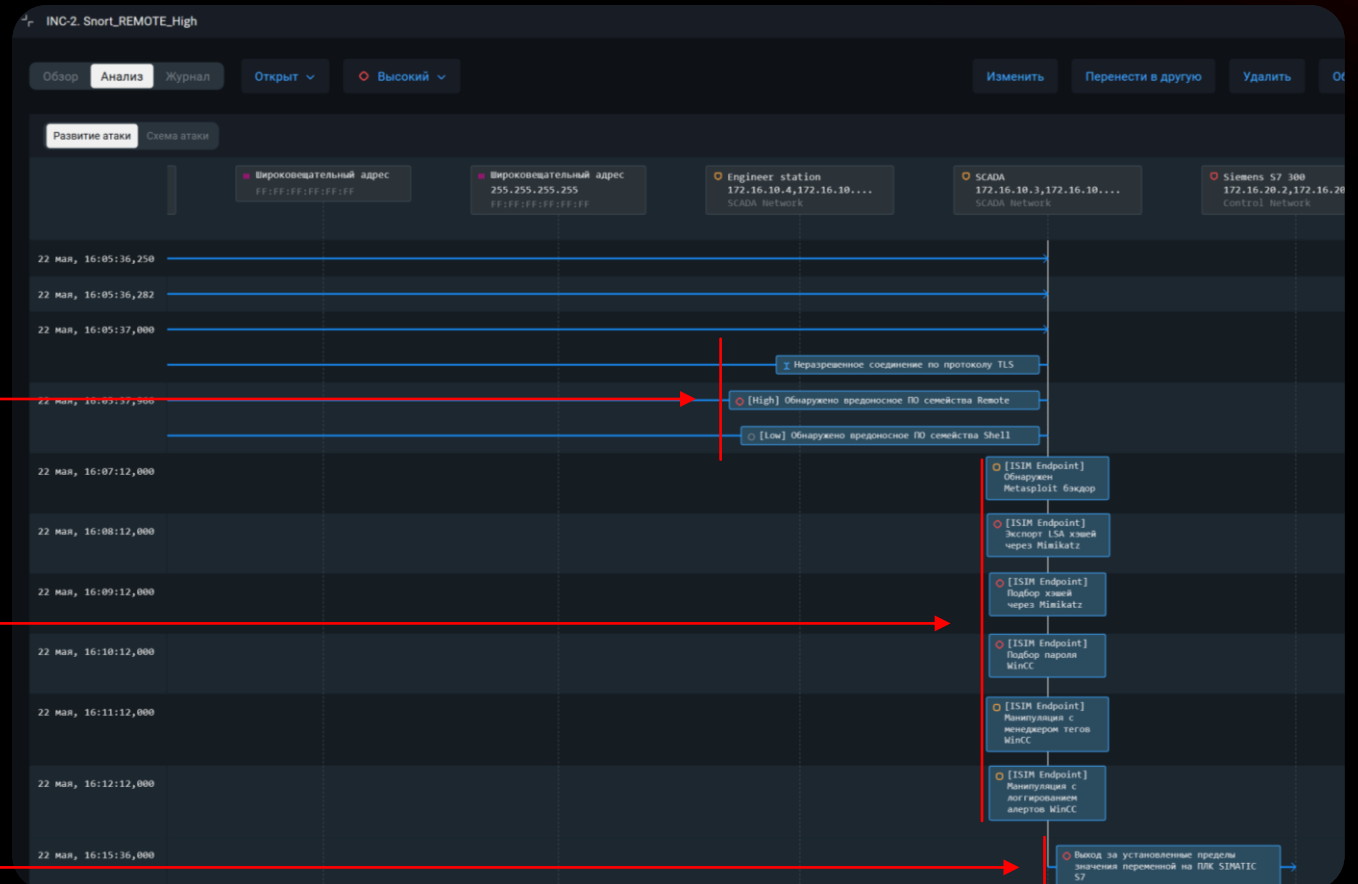


> Обнаружение атак и аномалий в трафике технологической сети

> Обнаружение атак на APM и серверы SCADA

+ события антивируса

> Обнаружение отклонений в параметрах технологического процесса

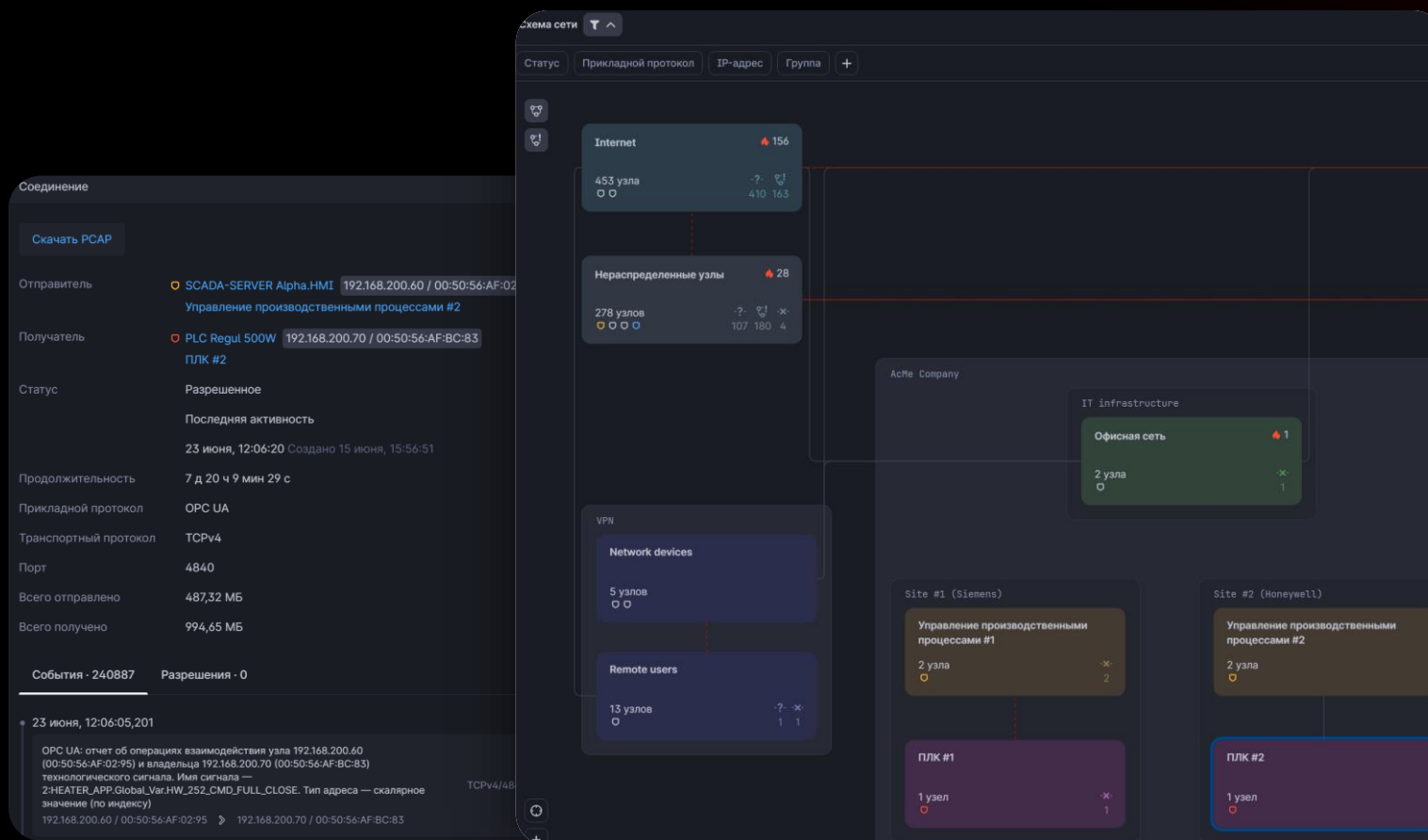


Удобный мониторинг крупных инфраструктур



> Карта сети позволяет легко ориентироваться в инфраструктурах с десятками тысяч узлов, предоставляя возможность:

- объединять узлы в группы и контейнеры, контролировать соединение между ними
- отслеживать подключения к интернету и к корпоративной сети
- получать детальную информацию по узлам, соединениям и инцидентам в один клик

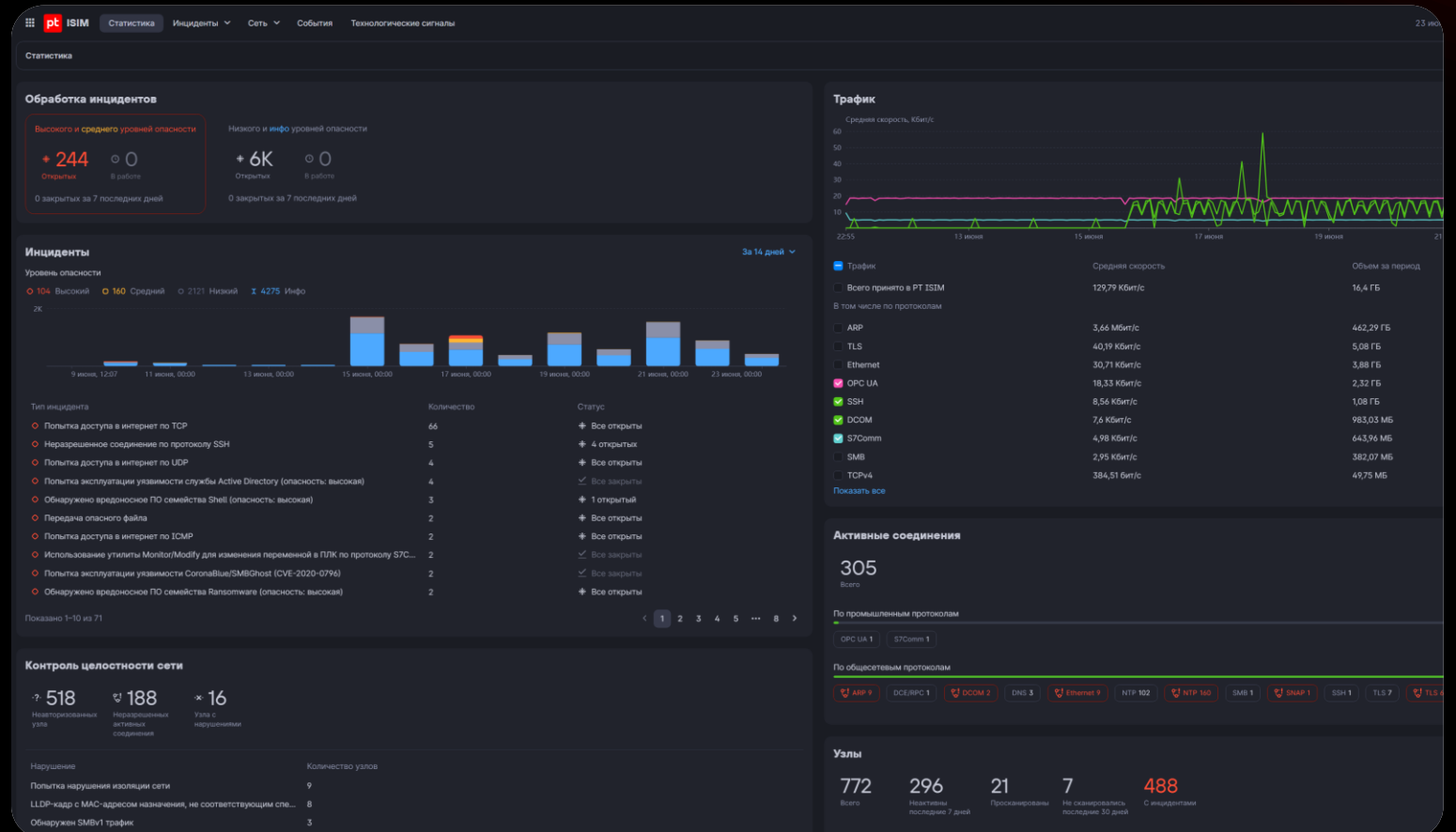


Быстрая оценка ключевых показателей безопасности



➤ На дашборде — все ключевые показатели безопасности технологической сети:

- состав и структура сети
- выявленные инциденты
- новые и неразрешенные узлы соединения



Контроль технологических сигналов



Модуль контроля технологических сигналов позволяет создавать пользовательские правила для выявления:

- отправки критически важных команд телеуправления
- отклонений в ключевых показателях технологического процесса

Это позволяет вовремя обнаружить отклонения в работе промышленного оборудования и предотвратить технологическую аварию

Технологические сигналы							
Все данные							
Статус	Имя	IP-адрес	Типы и статусы операций	Протокол	+		
✓	T 100	172.16.20.2	C2:02:4F:10:00:08	TCPv4	102	Не используется	Чтение, 3s
✓	0.0.0	172.16.20.2	C2:02:4F:10:00:08	TCPv4	102	Не используется	Чтение, 3s
✓	0.2367	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.TT_266B	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.TT_256A	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.TT_255	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.HW_242_CMD_FULL_CLOSE	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.HW_232_CMD_FULL_CLOSE	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.TT_245	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.TT_244A	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.TT_245	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение
✓	2:HEATER_APP.Global_Var.HW_242_CMD_FULL_CLOSE	192.168.200.70	00:50:56:AF:BC:83	TCPv4	4840	Не используется	Чтение

Новое правило

[Назад](#)

Глубина проверки сигнатур

Только ошибки

Регистрируемый инцидент

Удалить

Общие сведения

Условие

Регистрируемое событие

Условие

Технологический сигнал

2:HEATER_APP.Global_Var.TT_220_OP

Тип данных: Float

Критерий 1

Последнее значение

Больше чем

70

Критерий 2

Тип операции

Запись

Критерий 3

Последнее значение

Равно одному из значений

33

66

99

+ Еще значения

Добавить критерий

Карта сети

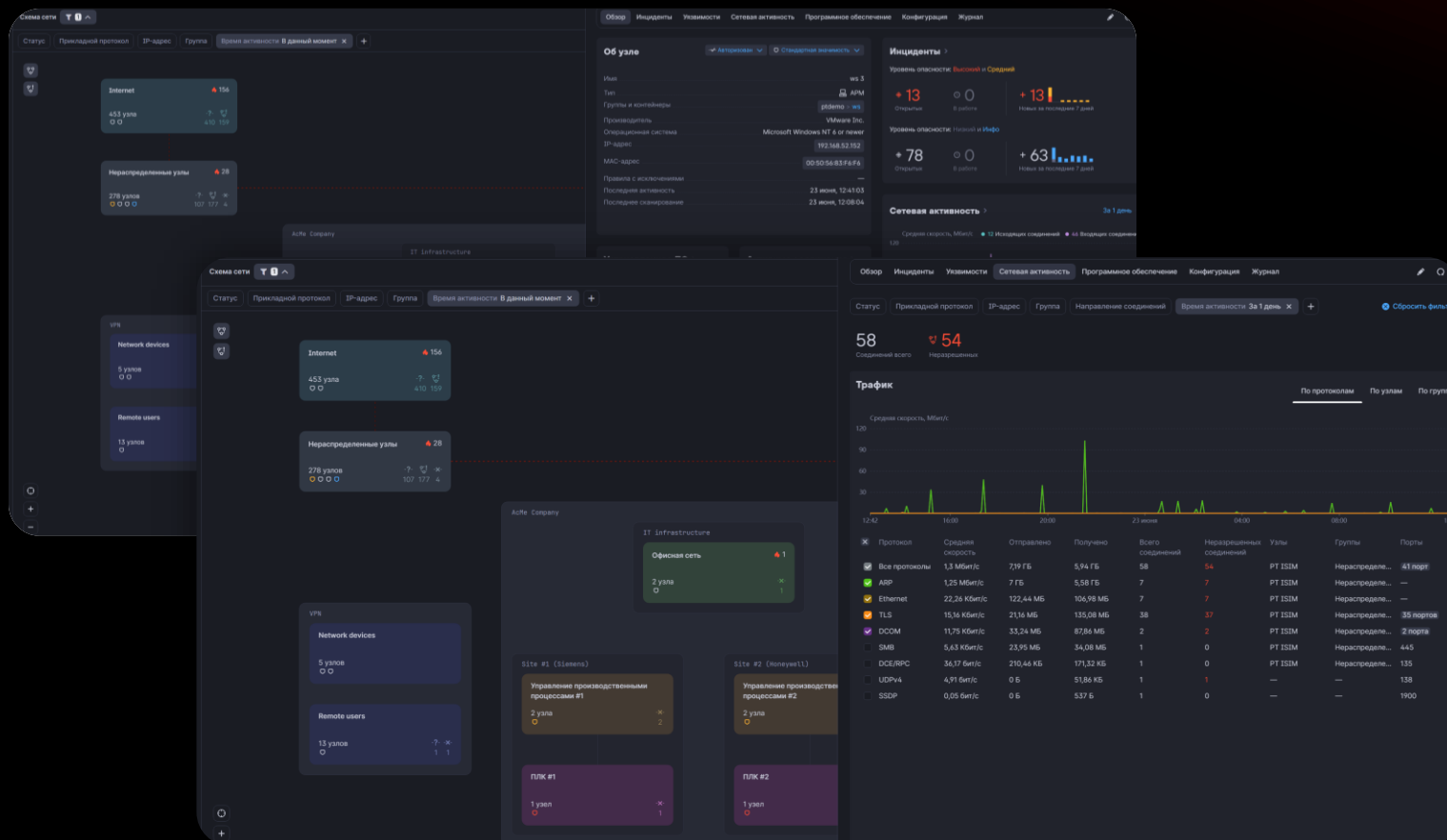


Автонаполняемая группа узлов

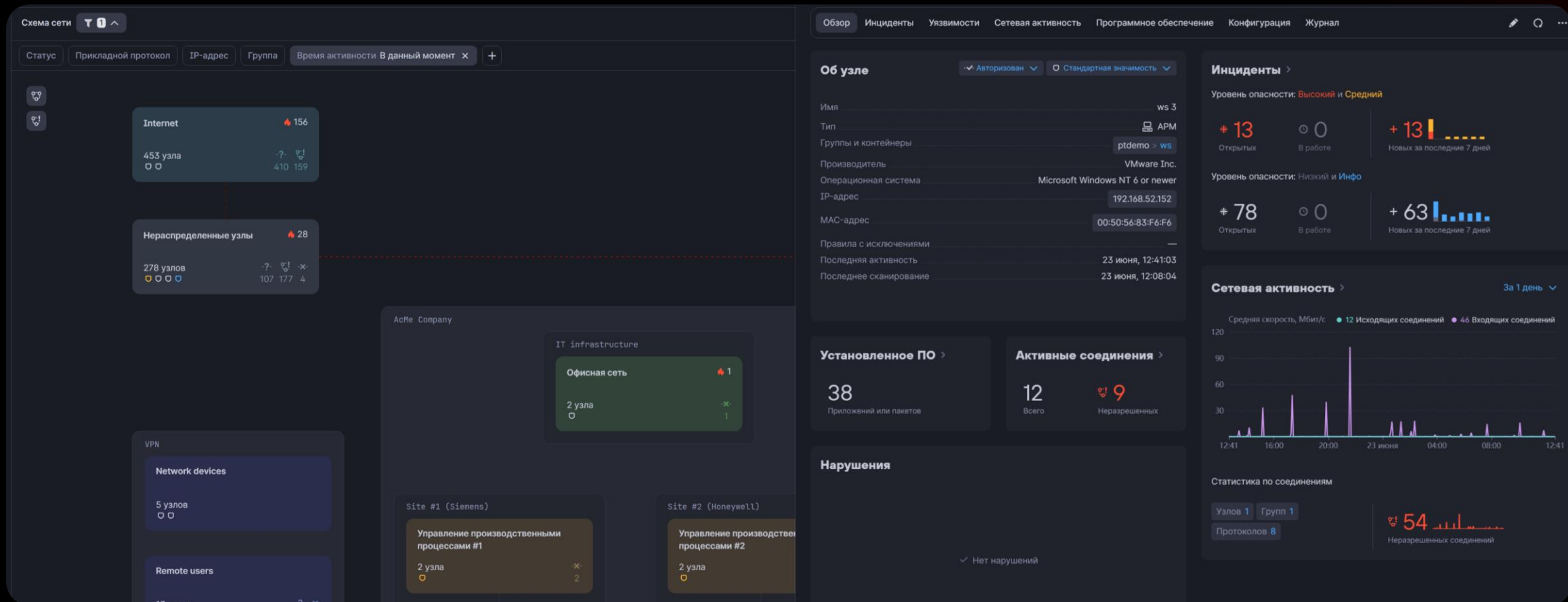
Для определения принадлежности хоста установке или внешней сети

Визуализация состояния безопасности

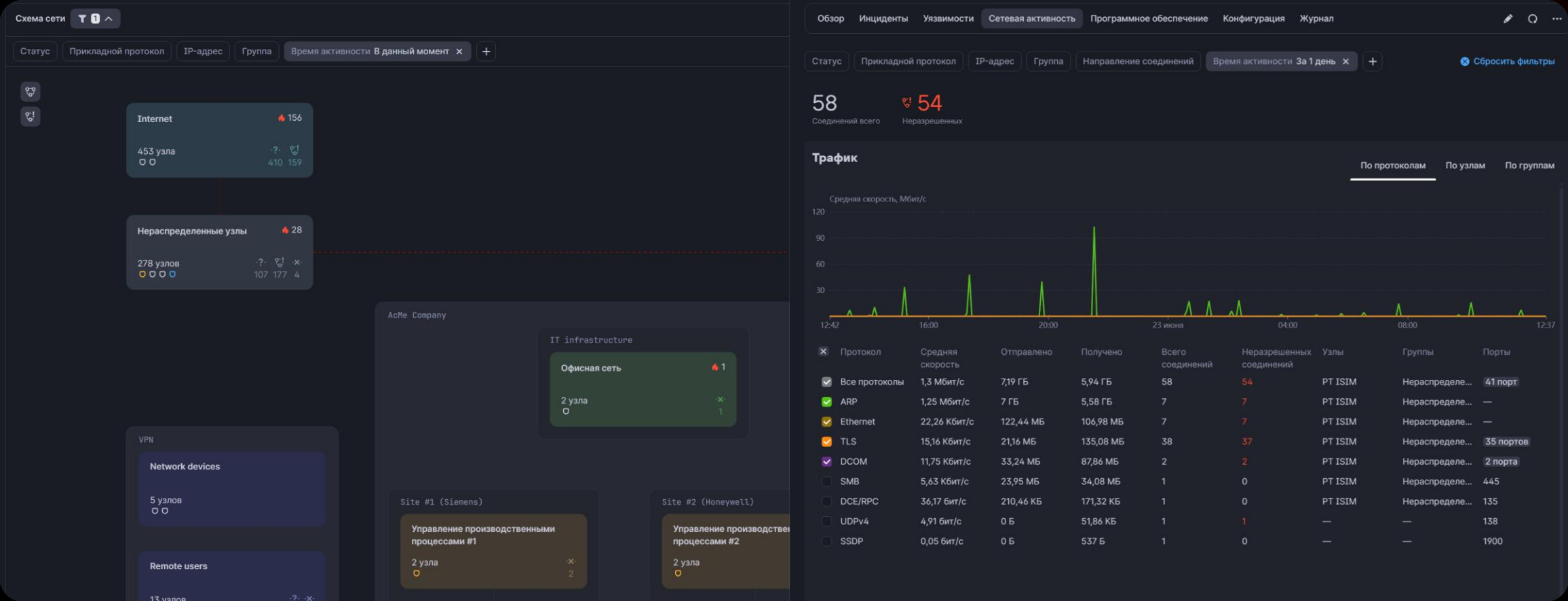
Для отдельных групп узлов, с возможностью перехода к отдельным хостам и инцидентам



Карта сети: дашборд



Карта сети: сетевая активность



Управление активами



Полная информация по хосту:

ПО, оборудование, установленные патчи, пользователи и т. п.



Сбор данных с помощью EDR или сетевого сканера

EDR безопасней, сетевой сканер поддерживает устройства, где нельзя поставить EDR



Понятное представление данных

Сгруппированные данные с фокусом на самом важном

The screenshot displays a web-based management console for a host. The top navigation bar includes tabs for Overview, Incidents, Vulnerabilities, Network Activity, Software Assurance, Configuration, and Logs. The main content area is divided into two sections: 'Basic Hardware' and 'Network Hardware'.

Основное оборудование

Процессоры

0	
Название	Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz
Архитектура	x64
Текущая частота	2597
Производитель	GenuineIntel
Подробнее	

Материнская плата

Название	440BX Desktop Reference Platform
Идентификатор	Motherboard
Производитель	Intel Corporation
Состояние устройства	Running or Full Power
Тип основной шины	PCI
Тип вспомогательной шины	ISA

Видеоадаптеры

VideoController1	
Название	VMware SVGA 3D
Видеопроцессор	VMware Virtual SVGA 3D Graphics Adapter
Название чипсета	VMware, Inc.
Версия драйвера	8.16.7.8
Подробнее	

Оперативная память

Объем	4
Автоматическое управление размером файла подкачки	true

Жесткие диски

Название	Размер	Тип	Производитель	Логические диски
\\./PHYSICALDRIV...	40	SCSI	(Standard disk driv...	C:

Показано 1-1 из 1

Сетевое оборудование

Сетевые карты

Название	MAC-адрес	Тип	Производитель	Статус подключения
Intel(R) 82574L Gigabit Networ...	00:50:56:83:F6:F6	Ethernet 802.3	Intel Corporation	Connected

Показано 1-1 из 1

Сетевые адаптеры

Описание	Название	Идентификатор	Включен	Тип	IP-адреса	MAC-адрес
Intel(R) 82574L Giga...	Ethernet0	10	true	Ethernet 802.3	2 адреса	00:50:56:83:F6:F6
Microsoft Kernel Deb...		8	false			
WAN Miniport (IKEv2)		9	false			
WAN Miniport (IP)		5	false	Ethernet 802.3		62:F6:20:52:41:53



Контроль конфигураций узлов



Журнал изменений конфигурации

Автоматически журналирует записи типа «Установлено новое ПО»



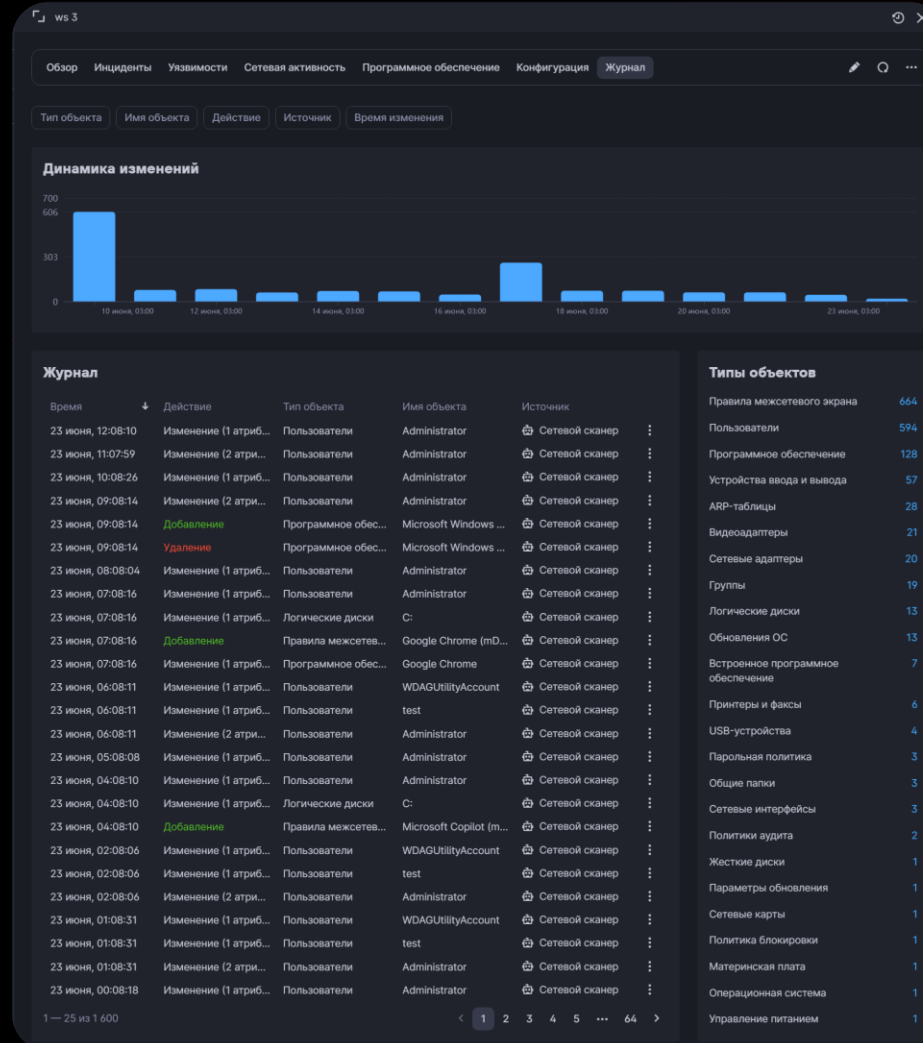
Пользовательские правила*

Пример: регистрируйте инцидент, если в группе хостов «SCADA Servers» было обнаружено новое USB-устройство



Аналитика по всем активам*

Для анализа конфигурационных данных ПО со всех узлов



Контроль конфигурации сетевых устройств



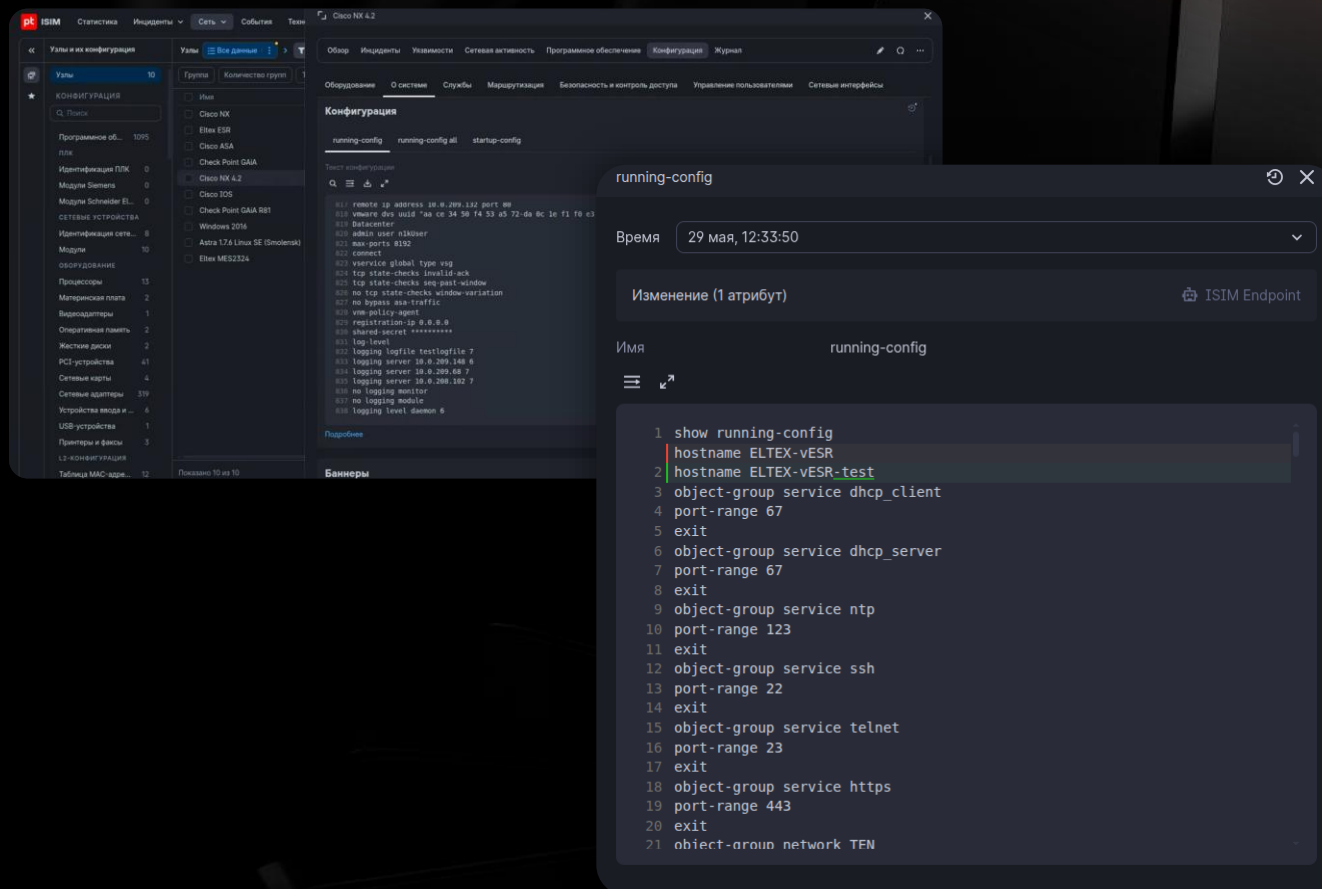
> Сканирование сетевых устройств

Сбор данных о конфигурации коммутаторов, маршрутизаторов и межсетевых экранов:

- Cisco ASA 8, 9
- Cisco IOS 12, 15
- Cisco NX-OS 4-7
- Eltex серия ESR, Eltex ROS (MES)
- Checkpoint GAIa OS 80.10 и выше

> Контроль конфигураций

Отображение конфигурации сетевого устройства, контроль изменений, подсвечивание строк с изменениями в конфигурационном файле сетевых устройств



Сетевой сканер



Сканирование Windows и Linux

Создание задач на сканирование, просмотр статистики запусков и журналов по каждой цели, безопасное хранение учетных данных

Сканирование ПЛК

Сбор данных о модели, вендоре, прошивке модулей ПЛК

Сканирование сетевых устройств*

Получение ARP-таблиц и настроек

pt

ISIM

Статистика

Инциденты

Сеть

События

Технологические сигналы

12 марта, 17:00:00

🔔

🛡️

⚙️

🔄

🌐

Задачи на сканирование узлов

Фильтр

Добавить задачу

Настроить таблицу

Обновить сейчас

Статус

Название

Цель

Сканер

Запуск по расписанию

Фильтр

+ Фильтр

Статус	Название	Цели сканирования	Количество целей	Тип сканера	Запуск по расписанию	Ближайший запуск	Последний запуск	Результаты последнего запуска	Статистика последних запусков
Запущена	Аудит PLC 1	192.168.1.2-192.168.1.30, 192.168.1.5	100	Linux	Включен	15 авг, 10:00	12 авг, 10:00	🟢 90 (+5) 🟡 10 (-5)	<

Аудит PLC 1

ИзменитьОбновить данные

Параметры задачи

Применение изменений...

Название

Аудит PLC 1

Статус задачи

Запущена

Создана

12 окт 2024, 10:00:00

Изменена

—

Тип сканера

Windows

Цели сканирования

192.168.1.2-192.168.1.30, 192.168.1.5, 192.168.5.12

Количество целей

100

Число одновременно сканируемых целей

5

Расписание

Запуск по расписанию

Включен

Дни запуска

Пн, Вт, Сб

Время запуска

01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 +20

Время в часовом поясе сервера (UTC+3)

Запуски

Средняя продолжительность запуска

32 мин 10 сек

Следующий запуск

21 мая 10:00

Журнал запусков

Начало	Завершение	Длительность	Количество целей	Результат запуска
21 мая 10:00	В процессе...	15 м	100	1 (+1) 2
20 мая 10:00	20 мая 12:00	2 ч	100	90 (+5) 10 (-5) Не все цели просканированы
19 мая 10:00	19 мая 11:00	1 ч	100	85 (+85) 15 (-85) Не все цели просканированы

Запуск

Скачать все логиОбновить данные

Цели сканирования

192.168.1.2-192.168.1.30, 192.168.1.5, 192.168.5.12

Начало

17 мая 10:00

Завершение

17 мая 15:30

Длительность

5 ч 30 м

Результаты запуска

3 успешных - 1 новая

3 неуспешных

Не все цели просканированы

Цели

Фильтр

Статус	Цель	Начало	Завершение	Длительность	Лог
✓	192.168.1.2	17 мая 10:00	17 мая 10:01	1 м	Посмотреть Скачать
✓	192.168.1.5	17 мая 10:00	17 мая 10:01	1 м	Посмотреть Скачать
✓	192.168.1.7	17 мая 10:00	17 мая 10:01	1 м	Посмотреть Скачать
✗	192.168.1.9	17 мая 10:02	17 мая 10:05	3 м	Посмотреть Скачать
✗	192.168.1.10	17 мая 10:02	17 мая 10:05	3 м	Посмотреть Скачать
✗	192.168.1.12	17 мая 10:02	17 мая 15:30	5 ч 28 м	Посмотреть Скачать

*В планах на 2026 год

Управление уязвимостями



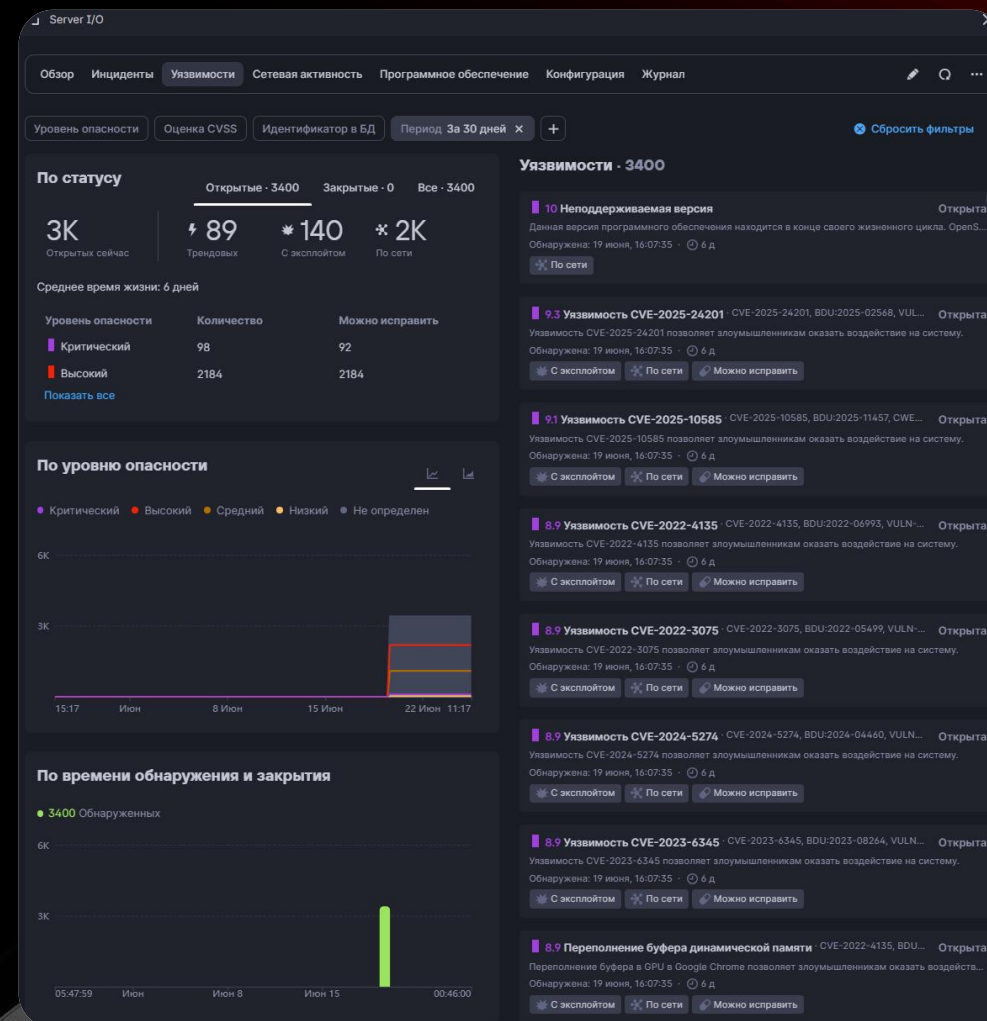
Уязвимости на узле

Просмотр всех уязвимостей, обнаруженных на узле, в отдельной вкладке, на главной странице узла и в списке ПО



По всей инфраструктуре

Представление данных для анализа всех уязвимостей в инфраструктуре



Управление уязвимостями: карточка уязвимости



pt ISIM

Статистика

Инциденты

Сеть

События

Технологические сигналы

Узлы и их конфигурация

Узлы

21

КОНФИГУРАЦИЯ

Поиск

Программное об... 1588

плк

Идентификация ПЛК 4

Модули Siemens 3

Модули Schneider EL... 2

СЕТЕВЫЕ УСТРОЙСТВА

Идентификация сете... 7

Модули 13

ОБОРУДОВАНИЕ

Процессоры 8

Материнская плата 2

Видеоадаптеры 2

Оперативная память 3

Жесткие диски 2

PCI-устройства 40

Сетевые карты 2

Сетевые адаптеры 389

Устройства ввода и... 14

USB-устройства 8

Принтеры и факсы 7

L2-КОНФИГУРАЦИЯ

Таблица MAC-адре... 12

Сети VLAN 259

Узлы

Все данные

Группа

Количество групп

Тип

Роль в инциденте

Нарушения

Последнее сканирование По 25 июня, 15:09

Имя	Значимость	Последняя активность	Группа	Статус	Тип	Про...
Server I/O	Высокая	25 июня, 15:16:21	Scada Network	Авторизован	OPC-серв...	Неиз...
PT MC	Пониже...	25 июня, 15:16:09	Нераспределен...	Авторизован	APM	VMw...
ws 3	Станда...	25 июня, 15:15:52	ws	Авторизован	APM	VMw...
ws 1	Станда...	25 июня, 15:14:55	ws	Авторизован	APM	VMw...
#128 VMware Inc.	Не зада...	25 июня, 15:14:33	Internet	Авторизован	Коммутат...	Cisco
HMI	Высокая	25 июня, 10:58:26	Scada Network	Авторизован	APM опер...	Неиз...
#417 VMware Inc.	Не зада...	15 июня, 16:20:51	Internet	Не авторизован	Неизвест...	VMw...
Siemens S1500	Высокая	10 июня, 23:25:57	Plc	Авторизован	ПЛК	Неиз...
Engineer station	Высокая	10 июня, 23:25:53	Service	Авторизован	APM	Неиз...
Router 0	Высокая	10 июня, 22:58:29	Network devi...	Авторизован	Маршрут...	Неиз...
ws 4	Станда...	6 ноя 2025, 12:40:51	ws	Авторизован	APM	VMw...
Test Drive	Станда...	6 ноя 2025, 12:28:34	Нераспределен...	Авторизован	APM	VMw...
ws 2	Станда...	5 ноя 2025, 10:35:45	ws	Авторизован	APM	VMw...
#613	Не зада...		Нераспределен...	Не авторизован	Неизвест...	Неиз...
#614	Не зада...		Нераспределен...	Не авторизован	Неизвест...	Неиз...
#615	Не зада...		Нераспределен...	Не авторизован	Неизвест...	Неиз...
#616	Не зада...		Нераспределен...	Не авторизован	Неизвест...	Неиз...
#617	Не зада...		Нераспределен...	Не авторизован	Неизвест...	Неиз...
#618	Не зада...		Нераспределен...	Не авторизован	Неизвест...	Неиз...
#619	Не зада...		Нераспределен...	Не авторизован	Неизвест...	Неиз...
#620	Не зада...		Нераспределен...	Не авторизован	Неизвест...	Неиз...

Server I/O

Обзор

Инциденты

Уязвимости

Сетевая активность

Програм...

Уровень опасности

Оценка CVSS

Идентификатор в БД

Пери...

По статусу

Открытые · 3400

Закрытые · 0

В...

3К

Открытых сейчас

89

Трендовых

140

С эксплойтом

2K

По сети

Среднее время жизни: 6 дней

Уровень опасности	Количество	Можно исправить
Критический	98	92
Высокий	2184	2184

Показать все

По уровню опасности

Критический	Высокий	Средний	Низкий	Не определен
-------------	---------	---------	--------	--------------

6К

3К

15:17

Июн

8 Июн

15 Июн

22 И

10 · Неподдерживаемая версия

Обновить данные

Общие сведения

Другие узлы с этой уязвимостью · 1

Уровень опасности

Критический

Статус

Открыта

Дата публикации в БД

11 сен 2023

Метки

По сети

Возможные последствия

Обнаружена

19 июня, 16:07:35

Время жизни

6 дней

Описание уязвимости

Данная версия программного обеспечения находится в конце своего жизненного цикла. OpenSSL Project больше не будет бесплатно предоставлять обновления безопасности, обновления программного обеспечения или какую-либо официальную поддержку вообще. Дальнейшее использование данной версии может привести к проблемам с безопасностью.

Оценка по CVSS v3

Общая

10

Базовая

10 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Временная

10 E:X/RL:U/RC:X

Как исправить

Данная версия OpenSSL используется в сторонних продуктах.Способы решения проблемы:1) установите последнюю версию продукта, в котором используется OpenSSL;2) свяжитесь с разработчиком продукта, в котором используется уязвимая версия OpenSSL;3) откажитесь от продукта, в котором используется уязвимая версия OpenSSL.

Полезные ссылки

<https://www.openssl.org/source/>

С каким ПО связана уязвимость

Название

OpenSSL

Вспомогательные сервисы и материалы



Что еще поможет в освоении продукта

- Тест-драйв
- Платформа тренажера PTEdTech для обучения работе с продуктом
- Наш обучающий курс по предотвращению атак на АСУ ТП
- Демо системы и сценарии
- Методический документ OT Security Framework



Наши услуги

- Пилотные внедрения (силами команды PT ISIM)
- Обучение продукту и тематике
- Наш MDR-сервис для мониторинга ОТ-инфраструктуры

Где применяется PT ISIM



ОТРАСЛИ



Энергетика



Нефтегазовая
промышленность



Химическая
промышленность



Горнодобывающая
промышленность



Пищевая
промышленность



Транспортная
инфраструктура



ПулкОВО

Прежде всего PT ISIM заинтересовал нас тем, что может максимально подстроиться под наши потребности, в том числе и будущие. Решение на его базе гибко масштабируется и экономично в плане аппаратного обеспечения.

[Читать историю успеха ↗](#)



РЖД

Это первый практический опыт в мире обеспечения киберзащищенности микропроцессорных систем управления движения поездов. Мы благодарны компании «РЖД» за инициацию этого проекта и помощь в его осуществлении. Полученные результаты могут быть интересны для пользования за рубежом.

[Читать историю успеха ↗](#)



Запросить
тест-драйв



ptsecurity.com/products/isim/

Новости
о продукте



t.me/pt_ics_news

Спасибо

