Илья Косынкин
Руководитель разработки продуктов для безопасности промышленных систем

PT ISIM 5

Строй промышленный СОИБ на PT ISIM!

Промышленный СОВ + Антивирус + Asset Management + Vulnerability Management

PT ISIM 5

PT ISIM 5 — система обеспечения киберустойчивости промышленных инфраструктур

Функции PT ISIM

- **СОВ** для АСУТП
- **Vulnerability Management** для АСУТП
- **Антивирус** для АСУТП
- **Asset Management** для АСУТП
- **EDR** для АСУТП
- **Контроль техпроцесса**

→ **Киберустойчивость** промышленной инфраструктуры

→ **Комплаенс** Соблюдение требований регуляторов и отраслевых стандартов

→ **Доступность данных** о состоянии промышленных инфраструктур для внешних систем

PT ISIM 5. Кейсы использования

Кейс 1

Комплаенс
Соблюдение требований регуляторов и отраслевых стандартов

- СОВ для АСУТП

Кейс 2

Комплаенс
Соблюдение требований регуляторов и отраслевых стандартов

- СОВ для АСУТП
- Антивирус для АСУТП

Кейс 3

Комплаенс
Соблюдение требований регуляторов и отраслевых стандартов

Киберустойчивость
промышленной инфраструктуры

Доступность данных
о состоянии промышленных инфраструктур для внешних систем

- СОВ для АСУТП
- Антивирус для АСУТП
- Asset Management для АСУТП
- Vulnerability Management для АСУТП
- EDR для АСУТП
- Контроль техпроцесса

Инвентаризация активов

Asset Management — «знай что защищаешь»

Решаемые задачи

Знать какие активы развернуты в технологической сети
и каковы их роли

Отслеживать изменения в конфигурации
которые могут привести к брешам в инфраструктуре

Оценивать текущий уровень НЕзащищенности
уязвимости, слабости конфигурации

Процедуры

Сбор данных об активах
Как подключиться к сети и собрать данные, не повлияв на работу сети

Регулярная актуализация данных об активах
Данные постоянно меняются и их нужно обновлять

Подходы

Пассивный анализ трафика

Инвентаризация хостовым агентом
ISIM Endpoint

Инвентаризация сетевым сканнером
Активный опрос (SSH, WMI, промышленные протоколы)

Как выбрать подход к инвентаризации технологической сети

Пассивный анализ трафика

Решаемые задачи

- Обнаруживать подключения к сети новых устройств
- Обнаруживает нарушения сетевой сегментации

Использовать всегда

если есть техническая возможность собрать трафик

Активное подключение к устройствам

Решаемые задачи

- Контролировать изменения конфигурации устройств
- Собирать сведения для Vulnerability Management

Есть возможность установить хостовый агент?

ДА

А это значит:

- Совместимая ОС
- Организационно одобрено

Или хостовый агент УЖЕ установлен ради Антивируса или Мониторинга безопасности

Использовать:

ISIM Endpoint

Нет

Например:

- ПЛК
- Устаревшие ОС
- Сетевые устройства
- Организационный запрет

Использовать:

Сетевой сканнер

PT ISIM 5. Карта сети

Контроль воздушного зазора

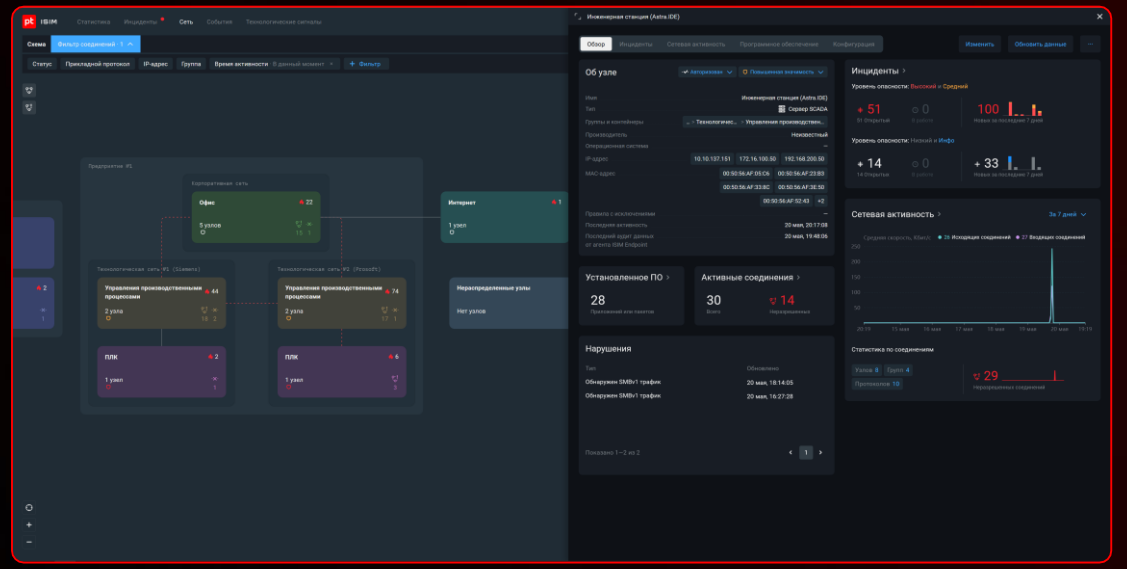
Обнаружение выходов в интернет и забытых каналов связи с корпоративной сетью

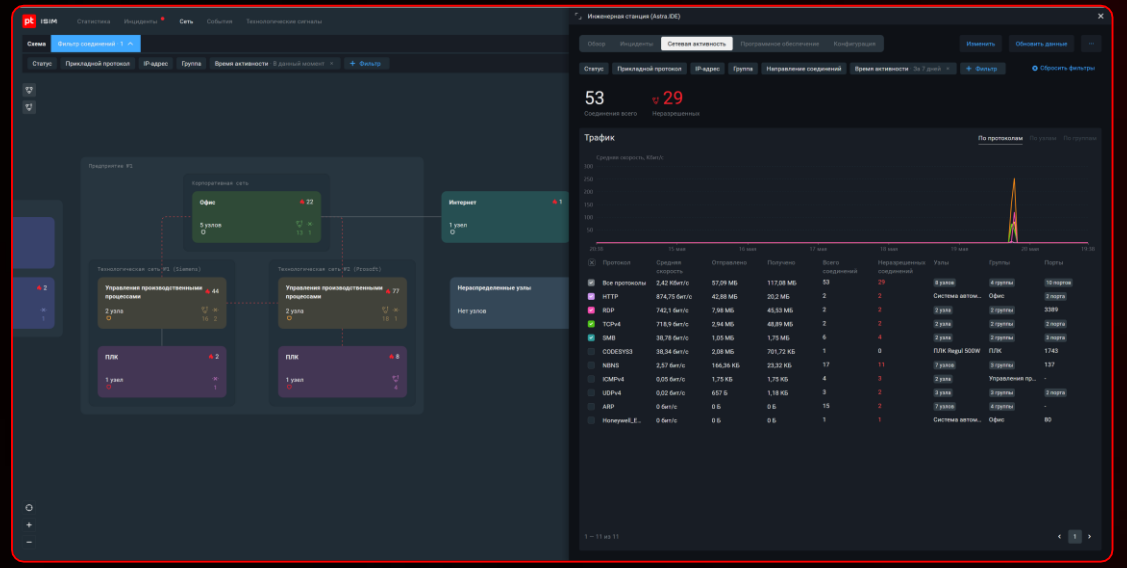
Автонаполняемые группы узлов

Для определения принадлежности хоста установке или внешней сети

Визуализация состояния безопасности

Для отдельных групп узлов, с возможностью дрилл дауна до отдельных хостов и инцидентов

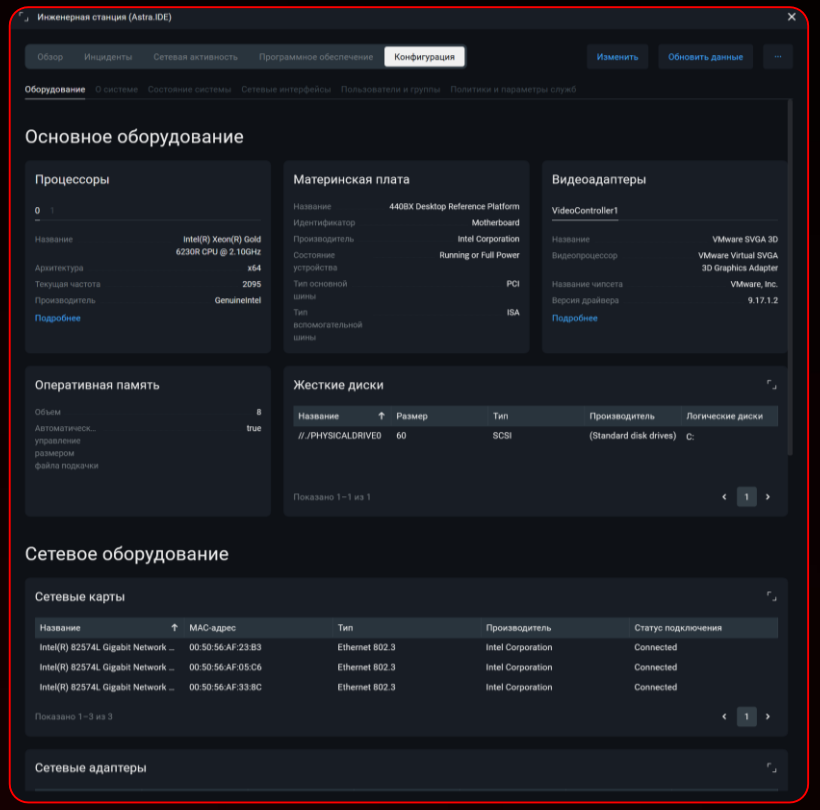




PT ISIM 5. Контроль конфигурации

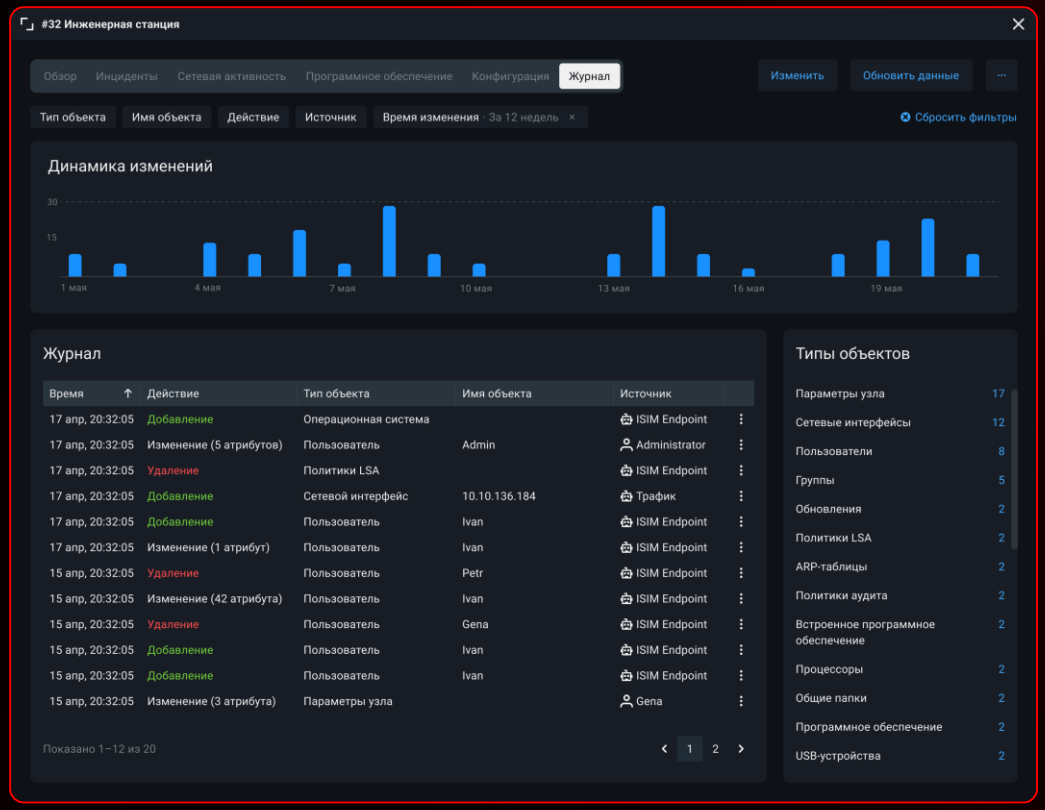
Полная информация по хосту

ПО, Hardware, установленные патчи и т.п.



Журнал изменений конфигурации

Автоматически логируем записи типа «Установлено новое ПО»



Программно-аппаратный комплекс PT ISIM

Кросс - отраслевое решение

Широкая линейка конфигураций в сочетании с функциями контроля безопасности открытых и проприетарных технологий автоматизации для применения в различных типах OT-инфраструктур

Кросс-функциональное решение

Набор инструментов экспертного уровня для решения задач ИБ, ИТ и АСУ подразделений промышленных предприятий

Отечественное решение для критических инфраструктур

Отечественное ПО,ОС

ПАК в реестре Минцифры

ПО сертифицировано ФСТЭК и протестировано на совместимость отечественными вендорами АСУ ТП

Вопросы

Задать вопрос по теме выступления

@PT ICS News

Новый канал о PT ISIM и OT Security

Ссылка на новый OT Cybersecurity Framework в канале!

Спасибо!