Илья Косынкин
Руководитель разработки
продукта PT ISIM

Юрий Захаров
Менеджер
по продвижению PT ICS

PT ICS.
Итоги за полгода

Проекты в промышленности на базе PT Industrial Cybersecurity Suite

Нефтегаз		**3 SOC** в **3** крупнейших нефтегазовых компаниях
Горнодобывающая отрасль		**3** горнодобывающих и **2** металлургических предприятия **1 SOC** в одной из крупнейших металлургических компаний
Классическая элекрогенерация		**60+** электростанций **2 SOC** в **2** энергокомпаниях
Гидроэнергетика		**30+** гидроэлектростанций **2 SOC** в **2** генерирующих компаниях
Электросети		**20+** подстанций 220/110 кВ **3 SOC** в **3** электросетевых компаниях,
ЦОД		**1 дата центр** в национальном телеком провайдере **1** крупнейшая спортивная арена
Ж. д.		**200+** железнодорожных станций по всей стране

PT ICS. Итоги за полгода

План вебинара

1 → Особенности защиты технологических сетей PT Industrial Cybersecurity Suite

2 → Обзор продуктов для защиты АСУ ТП
Что нового вышло за Q3 и Q4 2022 года

3 → Дорожная карта PT Industrial Cybersecurity Suite на 2023 год

Особенности защиты технологических сетей. PT ICS

Бизнес-риски

- **Цифровизация** ставит технологические процессы в зависимость от корректной работы информационных систем

- **Умышленное нарушение** технологического процесса с помощью компьютерных средств — реальная угроза для бизнеса

Остановка производства

Техногенная катастрофа

Мошенничество и саботаж

Брак

Кража технологий и секретов

Источники угроз

Криминал

- Проникновение в технологическую сеть и организация несанкционированного доступа с целью его перепродажи
- Развертывание вредоносного ПО, шантаж, получение выкупа

Конкуренты

- Нечестная конкурентная борьба
- Нарушение работы бизнеса, ущерб деловой репутации, кража технологических секретов

Структуры иностранных государств

- 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

Источники угроз

24 февраля 2022 года
в ФСБ назвали
критическим уровень
угрозы кибератак на РФ

https://tass.ru/obschestvo/13846783?ysclid=lbc04lzyjq892354386

Защиты периметра недостаточно

в 96%

атак внешний злоумышленник получает доступ к ресурсам локальной сети компании

От одного часа до пяти дней

тратят злоумышленники на проникновение во внутреннюю сеть

в 100%

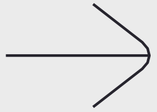
случаев внутренний злоумышленник может контролировать инфраструктуру

По результатам пентестов в 2021 и 2022 годах

Защиты периметра недостаточно

В **любую** корпоративную **сеть**, даже хорошо защищенную на периметре, **можно проникнуть**.

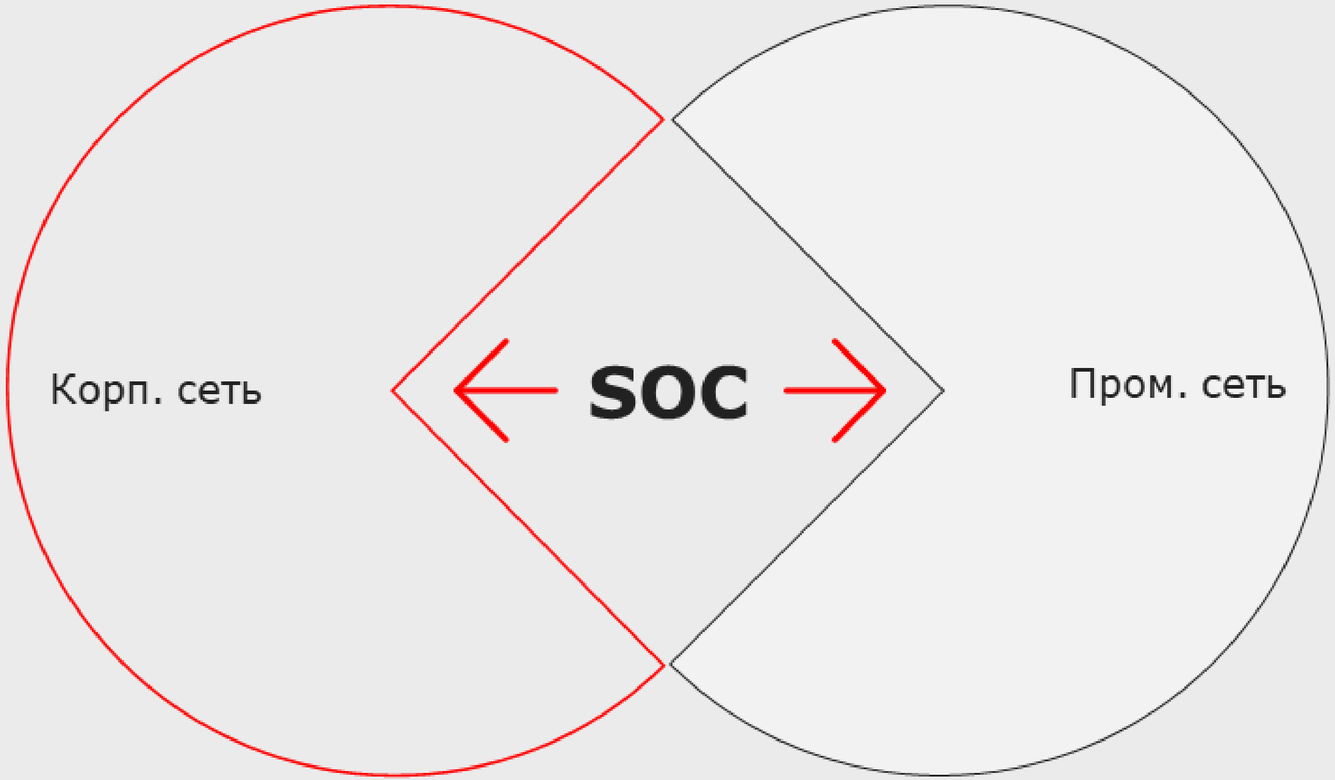
Когда **злоумышленник попадает во внутреннюю сеть, его действия остаются незамеченными** для периметровых средств защиты.



Нужно контролировать **и внешний, и внутренний трафик**

Технологическая сеть — объект защиты для SOC

- **АСУ ТП** – серая зона для security operations center
- **Нужен инструмент,** делающий происходящее в технологической сети прозрачным
- **Необходимы данные** о технологических аспектах работы для контроля бизнес-рисков



PT Industrial Cybersecurity Suite

Комплексная платформа промышленной кибербезопасности

Крупнейший в мире стек технологий и сервисов кибербезопасности для IT- и OT-инфраструктур промышленных предприятий

Для всех отраслей: энергетика, транспорт, металлургия, машиностроение, судоходные компании, медицина, ЖКХ

Легко масштабируется от одной производственной площадки до размеров промышленного холдинга и отрасли

Единая экосистема продуктов для работы с корпоративной и технологической инфраструктурой предприятия

PT Industrial Cybersecurity Suite

PT ICS

Продукты

- IM-модуль MaxPatrol SIEM
- MaxPatrol SIEM
- MaxPatrol VM
- PT ISIM
- PT XDR
- PT Sandbox

Сервисы PT ESC

- Анализ защищённости промышленных систем
- Ретроспективный анализ событий
- Расследование инцидентов
- Разработка пользовательского контента

Консалтинг

- Консалтинг по недопустимым событиям
- Создание ЦПК
- Киберучения

Единый портфель сервисов и продуктов для корпоративных и технологических ИТ-инфраструктур

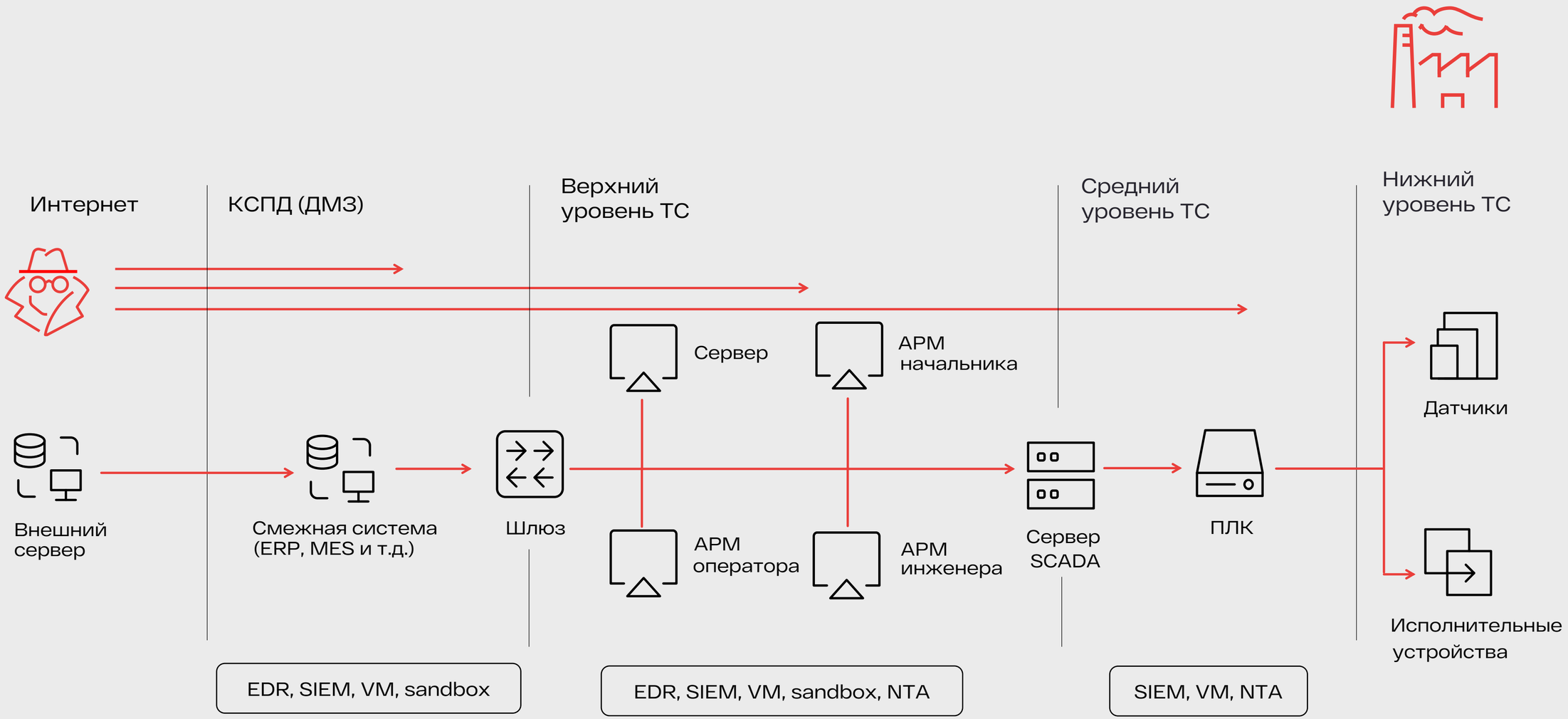
Продукты, которые уже используются в корпоративных сегментах, теперь можно полноценно применять и в сегментах OT, IIoT, ICS

PT ICS. Продукты

Все продукты, входящие в PT ICS, «дружат» с АСУ ТП и позволяют обнаружить и остановить злоумышленника до того, как он успеет нанести ущерб.

IM	**Модуль incident management в MaxPatrol SIEM**	Взаимодействие специалистов отдельных служб при информировании, реагировании и расследовании. Взаимодействие с НКЦКИ
SIEM	**MaxPatrol SIEM** Для промышленных систем	Обнаружение и управление инцидентами безопасности в промышленной инфраструктуре
VM	**MaxPatrol VM** Для промышленных систем	Управление уязвимостями индустриальных систем, патч-менеджмент
NTA	**PT ISIM** Для промышленных систем	Глубокий анализ трафика технологических сетей, выявление атак и аномалий, threat hunting
SBX	**PT Sandbox** Для промышленных систем	Обнаружение и анализ SCADA-специфичного вредоносного контента, инструментов APT
XDR	**PT XDR** Для промышленных систем	Обнаружение целевых и сложных угроз на конечных точках, реагирование

Сценарий атаки на АСУ ТП



Технологическая экспертиза в продуктах

Выводы из векторов атак

Хорошо, если злоумышленника поймали до того, как он попал в АСУ ТП

PT ICS мониторит смежные системы привычными и надежными продуктами

Мониторить только смежные системы не достаточно: есть другие вектоps атаки

Установив в АСУ ТП промышленные агенты и промышленную NTA-систему можно видеть действия злоумышленника независимо от вектора проникновения и остановить его до реализации недопустимых событий

На ранних стадиях атаки действия злоумышленника в АСУ ТП такие же, как в корпоративной сети

- Поэтому для мониторинга можно использовать стандартную экспертизу для Windows и Linux, заложенную в продукты
- Для мониторинга целевых воздействий на ключевые компоненты АСУ ТП — использовать технологическую экспертизу

Обзор продуктов PT ICS. Что вышло в 2022 году

Особенности продуктов для защиты АСУ ТП

	Экспертиза для корпоративной сети	Экспертиза для индустриальной сети	Функциональные особенности
MaxPatrol VM	✓	✓	• Сканеры SCADA, firmware • База уязвимостей технологических систем
MaxPatrol SIEM	✓	✓	• Сбор событий со SCADA, firmware • Кейс-ориентированные корреляции
PT ISIM	✓	✓	• Поддержка промышленных сетевых протоколов • Цепочки инцидентов в технологическом трафике
PT Sandbox	✓	✓	• Эмуляция технологических сред • Обнаружение SCADA и firmware-специфичного ВПО
PT XDR	✓	✓	

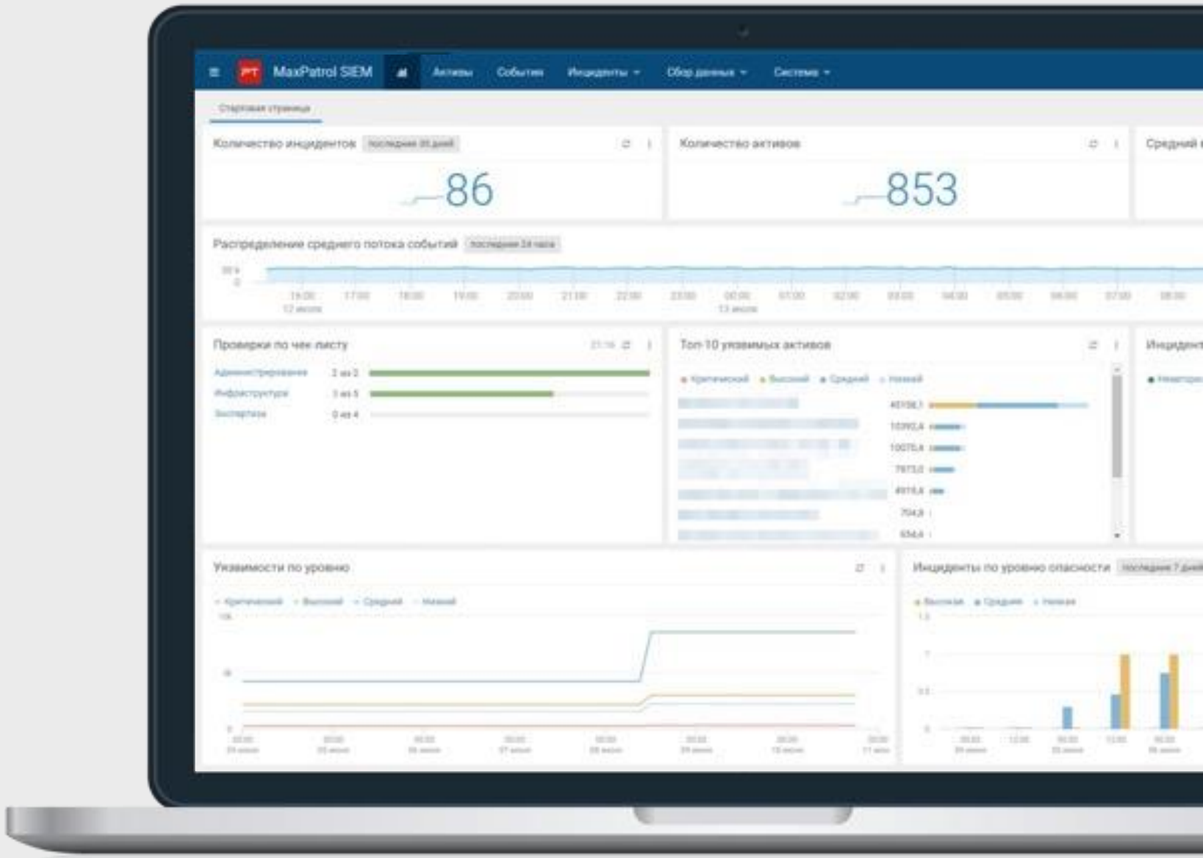
Интегрированные решения, технологическая совместимость, поддержка проприетарных технологий

АМТ-Груп	Техническая совместимость и функциональная применимость InfoDiode с MaxPatrol SIEM и PT ISIM	✓
B&R	Совместимость ПТК АСУ ТП с PT ISIM	✓
ЧЭАЗ	Совместимость ПТК «КВАНТ-ЧЭАЗ» с MaxPatrol SIEM	✓
АдАстра	Пакеты экспертиз для программного обеспечения TRACE MODE в продуктах платформы PT ICS, Совместимость с MaxPatrol SIEM	✓
AVEVA	Пакеты экспертиз для программного обеспечения Wonderware в продуктах платформы PT ICS, Совместимость с MaxPatrol SIEM	✓
Siemens	Пакеты экспертиз для программного обеспечения WinCC, PCS 7 в продуктах платформы PT ICS, Совместимость с MaxPatrol SIEM и PT ISIM Simatic NET networks	✓
Schneider Electric	Интегрированные решение на базе PT ISIM software & Magelis hardware	✓
Атомик Софт	Совместное комплексное решение на базе компонентов Alpha.Platform и PT ICS	🕓
ФГУП ЭЗАН	Совместимость со SCADA-системой «Соната» MaxPatrol 8, MaxPatrol SIEM	✓
ИнСАТ	Совместимость Master SCADA с MaxPatrol 8, MaxPatrol SIEM, PT EDR	🕓
PRO SOFT System	Совместимость ПТК на базе платформы Redkit SCADA с PT ISIM	✓
	Совместимость ПТК на базе ПЛК REGUL с MaxPatrol SIEM, MaxPatrol VM, PT EDR, PT ISIM	🕓
100+ Protocols	Siemens, Schneider Electric, Rockwell Automation, Yokogawa, Emerson, B&R, Bombardier, MOXA, Honeywell, Mitsubishi	✓ 🕓
Технологии Движения	Совместимость ПТК ДЦ ММ с PT ICS	🕓
СПИК СЗМА	Совместимость ПТК АСУ ТП на базе АРБИТР.SCADA с PT ICS	🕓

MaxPatrol SIEM для промышленности

SIEM, который работает в АСУ ТП

Система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз



Кейсы технологической экспертизы

Удалённое управление SCADA

Злоумышленник перепрограммирует ПЛК

Злоумышленник подменил проект SCADA

Злоумышленник залогинился в SCADA и может посылать из нее команды

Злоумышленник ограничил доступность ПЛК для операторов

Злоумышленник подменяет данные, которые видит SCADA

Злоумышленник ограничил доступность SCADA для операторов

Злоумышленник ворует данные из SCADA

MaxPatrol SIEM в PT ICS в 2022

Siemens

Пакет экспертизы для обнаружения атак на WinCC и PCS7

AdAstra

Пакет экспертизы для обнаружения атак на TraceMode

Aveva

Пакет экспертизы для обнаружения атак на Wonderware System Platform

Тестирование совместимости с АСУТП

Проведено тестирование на совместимость с шестью вендорами. В процессе тестирование с пятью вендорами

SIEM 7

Работа на отечественных ОС. Горизонтальное масштабирование

+ 4 новых пакета экспертизы IT

доступно через облако или оффлайн. Атаки на «1С:Предприятие» 8.3. Использование PT NAD для выявления подозрительной сетевой активности. Вредоносное ПО и нежелательные рассылки. Подозрительная активность в Yandex.Cloud

PT ISIM

NTA

для технологических сетей

Обнаружение

Автоматизированно составляет **цепочки инцидентов** на основе анализа трафика в технологической сети

Инвентаризация

Автоматически выявляет новые узлы инфраструктуры, строит схемы соединений и подсетей

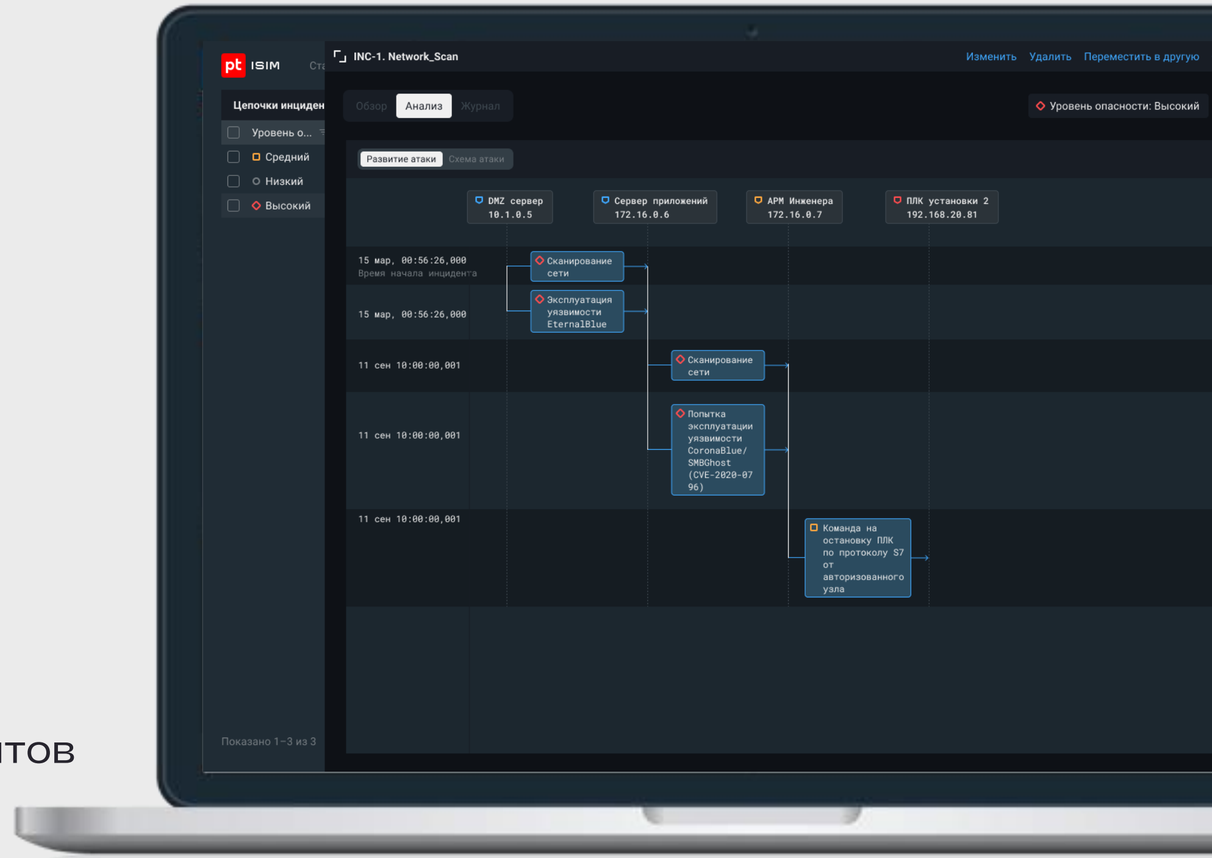
Кейсы технологической экспертизы

Использование типичных хакерских техник и инструментов

Активность вредоносного ПО в сети

Подозрительная активность в сети

Подозрительные действия, направленные на нарушения техпроцесса



PT ISIM в 2022 году

PT ISIM 4

Автоматизированное построение цепочек инцидентов

Настройка экспертизы под инфраструктуру

PT ISIM 4.3 в начале 2023 года

Создание собственных правил выявления инцидентов

Работа на отечественных ОС

+15 промышленных протоколов

Вышли в релизах PT ISIM 4.1–4.3

+1000 индикаторов промышленных угроз

Протоколы для новых отраслей

Поддержка протокола DICOM, позволяет использовать PT ISIM 4 в медучреждениях

2 пакета PT ISTI

Через облако расширена поддержка протоколов Mitsubishi SLMP, Siemens S7, добавлена поддержка Mitsubishi MELSOFT, Hirschmann HiDiscovery

PT Sandbox для промышленности

Передовая песочница

С возможностью гибкой кастомизации виртуальных сред

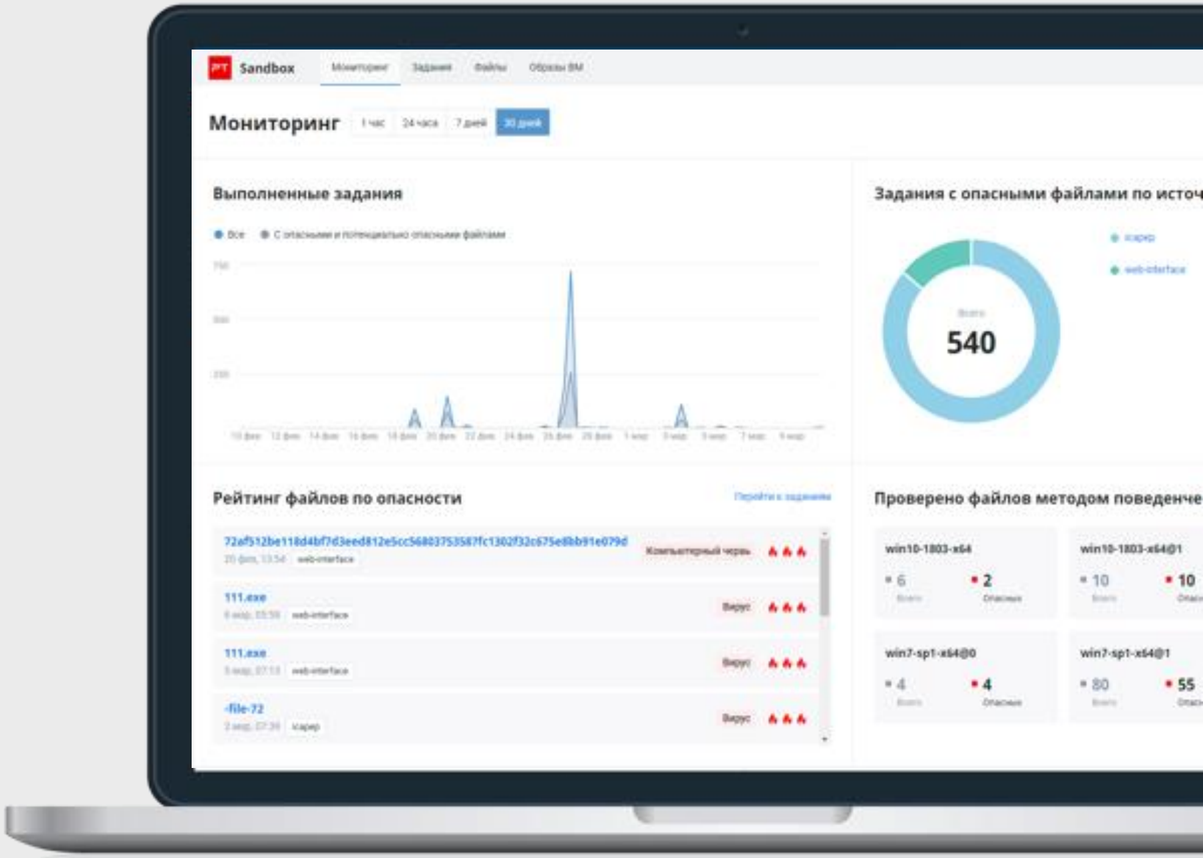
Вам на почту пришло ВПО, не обычное, а .... промышленное

Возможно, это начало целевой атаки?

Особенности для ОТ

Эмуляция технологических сред

Обнаружение SCADA- и firmware-специфичного ВПО



PT Sandbox в PT ICS в 2022 году

Siemens

Эмуляция WinCC и PCS 7, выявление ВПО, взаимодействующего с Simatic S7

Honeywell

Выявление ВПО, взаимодействующего с распределенной системой управления Honeywell серии Experion PKS

AVEVA

Эмуляция Wonderware System Platform, выявление ВПО, взаимодействующего со Schneider Modicon

AdAstra

Эмуляция TRACE MODE

и другие SCADA

Эмуляция SCADA-систем «Арбитр» и KingIOServer

PT Sandbox 4.5

Расширенная эмуляция. и выявление ВПО на Астра Linux. Выявление буткитов. Machine Learning в ПА

Дорожная карта PT ICS на 2023 год

Дорожная карта PT ISIM на 2023 год

PT ISIM 4.3
(Q1 2023)

- Создание собственных правил выявления инцидентов
- Установка на отечественные операционные системы
- Автоматическая приоритизация инцидентов на основе сведений об инфраструктуре

PT ISIM 4.4
(Q3 2023)

- Новый интерфейс схемы сети для удобного анализа больших инфраструктур
- Пакеты экспертизы

PT ISIM 5
(Q4 2023)

- Новый интерфейс для контроля технологического процесса
- Выявление аномалий в авторизованных соединениях
- Коробочная интеграция с PT MC и PT Sandbox

PT ICS. Кросс-продуктовые пакеты экспертизы, планируемые на 2023 год

PT ICS. Технологическая экспертиза

Все продукты, входящие в PT ICS, постоянно «накачиваются» кросс-продуктовой экспертизой с фокусом на платформы автоматизации и продукты конкретных производителей компонентов АСУ ТП

		Siemens WinCC, PCS 7, Simatic	**AdAstra** TRACE MODE	**AVEVA** Wonder-ware InTouch	**МПС Софт** Masterscada	**Rockwell** Allen-Bradley, Factory Talk	**Yokogawa** Centum	**Schneider Electric** Modicon	**Атомик Софт** Alpha.Platform
MaxPatrol VM	▪ Сканнеры SCADA, firmware ▪ База уязвимостей технологических систем	2023		2023	2023	2023	2023	2023	2023
MaxPatrol SIEM	▪ Сбор событий со SCADA, firmware ▪ Кейс-ориентированные корреляции	✓	✓	✓	2023	2023	2023	2023	2023
PT ISIM	▪ Поддержка промышленных сетевых протоколов ▪ Детекты на новые угрозы и атаки ▪ Цепочки инцидентов в технологическом трафике	✓	2023	2023	2023	✓	✓	✓	✓
PT Sandbox	▪ Эмуляция технологических сред ▪ Обнаружение SCADA-специфичного ВПО	✓	✓	✓	2023	2023	2023	2023	2023

Чат PT ICS в Telegram:

t.me/isimpt

Бесплатный пилот продукта:

https://www.ptsecurity.com/ru-ru/solutions/ics/#free-demo

Спасибо