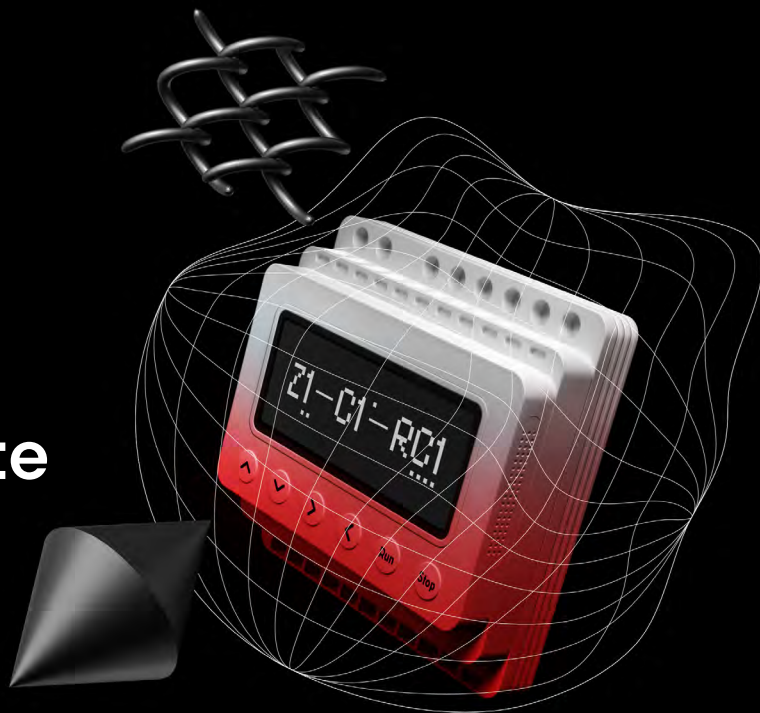


# PT Industrial Cybersecurity Suite

Первая комплексная платформа  
для защиты промышленности  
от киберугроз



Промышленные предприятия постоянно наращивают объем цифровизации. Одни и те же IT-компоненты находят применение в автоматизации операционных и технологических процессов. Это значит, что для злоумышленника нет особой разницы, что атаковать: корпоративную или технологическую сеть. Способы и сценарии нападения одинаковы. При этом уровень кибербезопасности производственных систем часто ниже, чем в корпоративных. Нивелировать отставание поможет платформа **PT Industrial Cybersecurity Suite** (PT ICS).

## В состав PT ICS входят:

- **Продукты.** MaxPatrol SIEM, MaxPatrol VM, PT ISIM, PT Sandbox, PT XDR – комбинация ключевых продуктов Positive Technologies обеспечит комплексную кибербезопасность всего предприятия, включая сегмент АСУ ТП (SCADA).
- **Сервисы.** Полный спектр услуг по анализу защищенности промышленных систем и услуги PT ESC по обнаружению, реагированию и расследованию сложных инцидентов в АСУ ТП (SCADA).

## Решение

PT ICS помогает обнаружить злоумышленника на всех этапах развития атаки в промышленных средах и своевременно на них отреагировать. Платформа обеспечивает комплексную безопасность в промышленном сегменте компании, начиная от сетевых узлов и заканчивая технологическими устройствами.

## Продукты PT ICS

- **MaxPatrol SIEM** для промышленности. Контролирует активность программного обеспечения и поведение пользователей на конечных узлах. Обнаруживает во всей IT-инфраструктуре предприятия инциденты информационной безопасности и позволяет наладить процесс управления ими. Поддерживает иностранные и отечественные компоненты АСУ ТП (SCADA) «из коробки».
- **MaxPatrol VM** для промышленности. Помогает построить эффективный процесс управления уязвимостями для всего предприятия. Собирает полные данные о компонентах технологической сети, выявляет уязвимости и контролирует их устранение.
- **PT ISIM.** Осуществляет глубокий анализ трафика технологических систем. Предоставляет инструменты для проактивного поиска угроз (threat hunting), автоматически строит вектор атаки и делает ретроспективный анализ трафика. Поддерживает более 100 сетевых протоколов.
- **PT Sandbox** для промышленности. Обнаруживает в файлах и ссылках неизвестное ВПО, нацеленное на компоненты АСУ ТП (SCADA) иностранных и отечественных производителей. Осуществляет статический и динамический анализ объектов как с узлов, так и из других источников. Дает возможность настроить среду эмуляции, «приманки» и состав ПО с учетом специфики компании.
- **PT XDR** для промышленности. EDR-агенты PT XDR собирают и анализируют данные с конечных узлов, помогают осуществлять проактивный поиск угроз (threat hunting) и блокировать киберугрозы. Поддерживает популярные ОС «из коробки». Агенты адаптированы для работы на предприятиях.



Бесплатный пилот PT Industrial Cybersecurity Suite — первой комплексной платформы для защиты промышленности от киберугроз



Каждая пятая атака на промышленность приводит к остановке бизнес-процессов

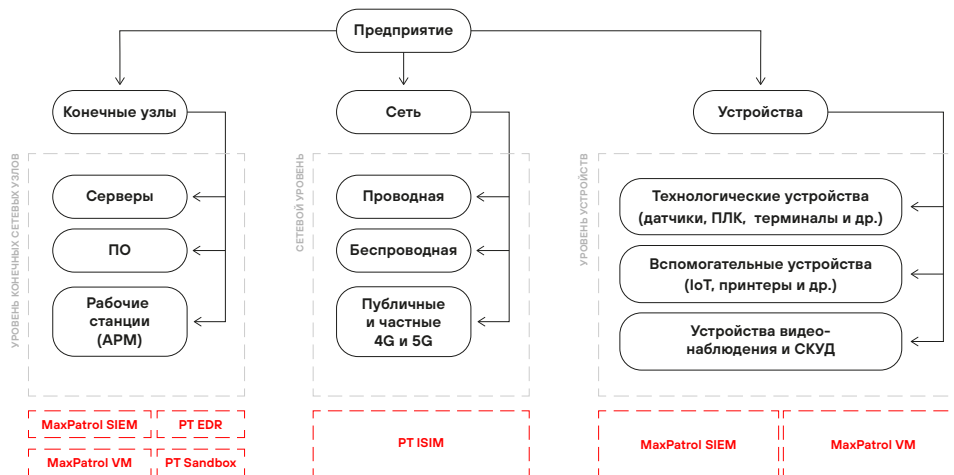


Более 80% атак на промышленность происходит с применением ВПО



60% промышленных компаний не могут обеспечить киберустойчивость бизнеса

## Как это работает



Все продукты платформы PT ICS разворачиваются в производственном сегменте компании. MaxPatrol SIEM собирает и анализирует журналы компонентов АСУ ТП. MaxPatrol VM получает всю информацию об активах и видит уязвимости в промышленном сегменте компании. PT ISIM анализирует сетевой трафик промышленного оборудования. PT Sandbox анализирует файлы и ссылки из почты, трафика, общих сетевых папок и конечных узлов АСУ ТП. PT XDR дает инструменты автоматического и выборочного реагирования на угрозы. Все это позволяет увидеть и предотвратить реализацию неприемлемых для бизнеса событий на каждом этапе развития атаки.

## Преимущества

- **Первая комплексная платформа для защиты промышленности от киберугроз.** В состав платформы входят пять хорошо зарекомендовавших себя на рынке ИБ продуктов Positive Technologies, расширенные экспертизой АСУ ТП.
- **По-настоящему защищает.** Платформа PT ICS позволяет построить систему ИБ так, чтобы обнаружить злоумышленника на всех этапах развития атаки и предотвратить реализацию неприемлемых для бизнеса рисков. EDR-агенты PT XDR дают возможность выборочного реагирования на конечных узлах в АСУ ТП.
- **Эффективное применение знакомых продуктов.** Если в компании уже установлена часть продуктов Positive Technologies, достаточно расширить существующие лицензии для поддержки промышленного сегмента. При этом специалисты продолжают работу с привычными для них инструментами ИБ.
- **Настоящий on-premise.** Все собранные данные анализируются внутри компании и не покидают периметр.
- **Импортозамещение.** Все продукты в составе PT ICS полностью российского производства и входят в реестр отечественного ПО.
- **Выполняет требования законодательства.** Платформа PT ICS помогает выполнить максимум требований приказа ФСТЭК №239, связанных с наложенными средствами защиты.

[ptsecurity.com](http://ptsecurity.com)  
[pr@ptsecurity.com](mailto:pr@ptsecurity.com)  
[vk.com/ptsecurity](https://vk.com/ptsecurity)  
[t.me/Positive\\_Technologies](https://t.me/Positive_Technologies)  
[twitter.com/ptsecurity](https://twitter.com/ptsecurity)  
[vk.com/phdays](https://vk.com/phdays)

Positive Technologies уже 20 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности. Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Telegram](#), [ВКонтакте](#), [Twitter](#), [Habr](#)), а также в разделе «[Новости](#)» на сайте [ptsecurity.com](http://ptsecurity.com).