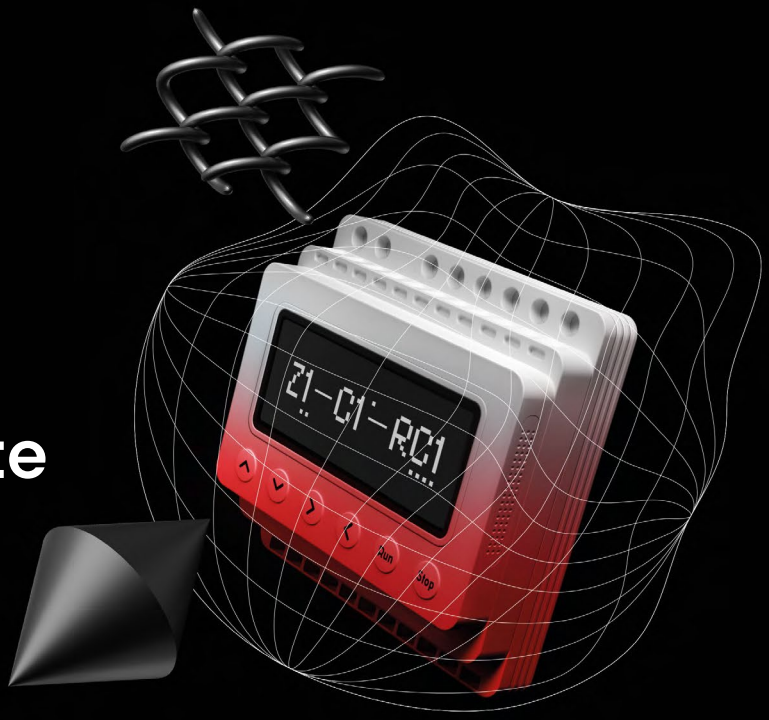
positive technologies

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 ранних этапах развития атаки в промышленных средах и своевременно на них отреагировать. Платформа обеспечивает комплексную безопасность в индустриальном 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». Является центральным узлом для платформы PT ICS.
- **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. MaxPatrol VM интегрируется с MaxPatrol SIEM. Оба продукта работают в едином интерфейсе.
- **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. Продукт интегрируется с PT ISIM: все объекты, обнаруженные в трафике технологической сети, отправляются в PT Sandbox и проходят статический и динамический анализ. Продукт позволяет настраивать среду эмуляции (состав ПО, механизмы deception) с учетом специфики промышленной 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. EDR-агенты передают подозрительные объекты на анализ в PT Sandbox.

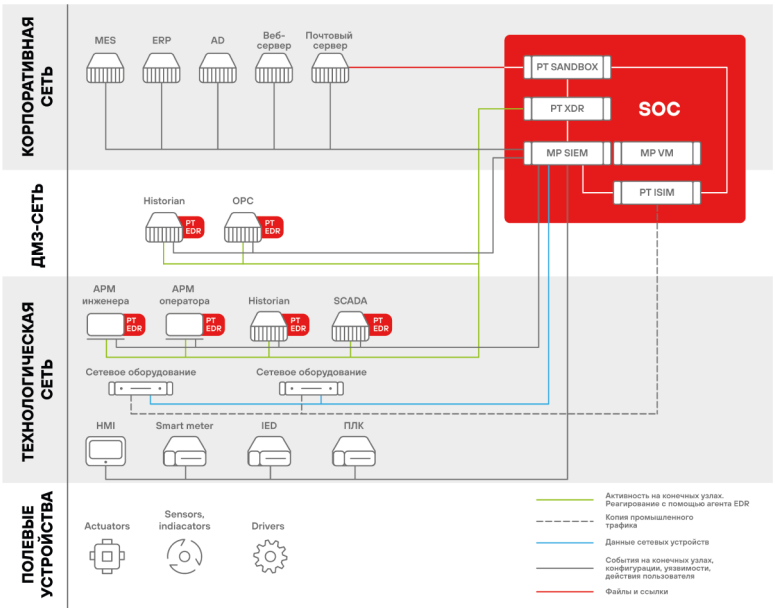
Бесплатный пилот PT Industrial Cybersecurity Suite — первой комплексной платформы для защиты промышленности от киберугроз

Каждая пятая атака на промышленность приводит к остановке бизнеса

Более **80% атак** на промышленность происходит с применением ВПО

60% промышленных компаний не могут обеспечить кибер-устойчивость 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. PT ICS объединяет все технологии каждого продукта и помогает защитить промышленное предприятие целиком.
- **Видит каждый шаг злоумышленника.** Платформа PT ICS позволяет построить систему ИБ так, чтобы обнаружить злоумышленника на всех этапах развития атаки и предотвратить реализацию неприемлемых для бизнеса рисков. Продукты в составе платформы помогают аналитику SOC оценить на какой стадии атаки находятся злоумышленники и спрогнозировать их дальнейшие шаги. PT Sandbox блокирует вредоносное ПО в почтовом трафике, а EDR-агенты PT XDR дают возможность выборочного реагирования на конечных узлах в сетях 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 продолжат 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
pr@ptsecurity.com

PT-ICS_PB_A4.RUS.0004.02.SEP.12.2022