positive technologies

PT Industrial Security Incident Manager

Предоставляет уникальное сочетание инструментов и экспертизы для контроля безопасности и мониторинга технологических сетей, IIoT-систем промышленных предприятий и объектов инженерной инфраструктуры.

PT Industrial Security Incident Manager контролирует безопасность технологической сети, выявляет нелегитимные операции, действия злоумышленников и активность ВПО.

PT ISIM – система глубокого анализа технологического трафика.

Промышленная инфраструктура любого масштаба — как на ладони

Трехкомпонентный механизм разбора трафика позволяет PT ISIM собрать максимум информации о промышленной сети: ресурсах, структуре, сетевых взаимодействиях — и мгновенно выявлять в трафике аномалии, изменение технологических параметров, активность ВПО и попытки эксплуатации уязвимостей.

Быстрое определение вектора атаки и целей злоумышленника

PT ISIM автоматически объединяет тысячи инцидентов безопасности в единичные цепочки событий, помогая специалистам по ИБ быстрее определить направление кибератаки и цели злоумышленника, проактивно реагировать на угрозы и расследовать инциденты.

Информационное пространство, объединяющее ИБ, ИТ и производство

PT ISIM вовлекает в управление безопасностью промышленных систем все технические подразделения предприятия, предоставляет инструменты и информационное пространство, чтобы объединить их усилия для предотвращения недопустимых событий.

Области применения

- Автоматизированные системы управления технологическими процессами на промышленных предприятиях
- Промышленные предприятия и производства с распределенной инфраструктурой
- Системы управления инженерной инфраструктурой городских и муниципальных служб, центров обработки данных, деловых и торговых центров
- Автоматизированные системы управления субъектов КИИ
- Промышленный интернет вещей (IIoT)
- Системы управления движением рельсового транспорта
- DICOM — совместимые системы и сети медицинских учреждений

Сценарии использования

Инвентаризация технологической сети и выявление новых узлов

PT ISIM позволяет контролировать целостность сети, обнаруживать появление новых узлов (рабочих станций, контроллеров, сетевых устройств), мгновенно выявлять нарушения изоляции технологической сети.

Выявление аномалий и угроз в технологическом трафике

PT ISIM может в реальном времени обнаруживать нелегитимный удаленный доступ к компонентам АСУ ТП, активность ВПО (вирусов, троянов, шифровальщиков), создание прокси-серверов и туннелей, использование слабых паролей и паролей по умолчанию.

Обнаружение эксплуатации уязвимостей и других техник злоумышленников

PT ISIM умеет определять атаки на Windows- и Linux-системы, на стандартное сетевое оборудование и промышленные устройства. Для обнаружения актуальных угроз безопасности PT ISIM постоянно пополняется новой экспертизой.

Выявление опасных технологических команд

PT ISIM выявляет перепрошивку ПЛК, форсирование переменных, очистку памяти — легитимные, но редко происходящие в работающей АСУ ТП операции.

Соблюдение требований регулирующих организаций

PT ISIM помогает обеспечить выполнение приказов ФСТЭК № 31, № 239, норм закона № 187-ФЗ о безопасности объектов КИИ, помогает выстраивать взаимодействие с центрами ГосСОПКА.

Обнаружение ВПО в трафике и передача подозрительных файлов на анализ

PT ISIM извлекает передаваемые по сети файлы для анализа в PT Sandbox, чтобы выявить распространение ВПО, в том числе не обнаруживаемое классическими антивирусами.

PT ISIM: ключевые цифры

8000 правил

и индикаторов промышленных угроз «из коробки» охватывают промышленное ПО и оборудование в инфраструктурах на Windows и Linux

Более 130

разбираемых протоколов, поэтому PT ISIM можно использовать во всех основных отраслях промышленности, IIoT-системах и медицинских DICOM-сетях

Заходите в телеграм-чат о PT ISIM

Загрузите подробное техническое описание

Отправьте заявку на пилотный проект