ПРЕИМУЩЕСТВА

+ **Безопасность технологического процесса.** Архитектура пассивного мониторинга PT ISIM исключает нежелательное воздействие на технологический процесс — в отличие от других популярных средств защиты информационной безопасности АСУ ТП.
+ **Контроль целостности сети.** PT ISIM автоматически инвентаризирует элементы сети, включая компоненты промышленной системы управления, и непрерывно контролирует целостность технологической сети.
+ **Визуализация инцидентов.** PT ISIM обладает удобными средствами графического отображения элементов сетевой топологии и технологического процесса (мнемосхемы). Это позволяет визуализировать инциденты ИБ в том числе и на уровне бизнес-логики промышленного сегмента.
+ **Корреляция событий.** PT ISIM эффективно выявляет длительные многоэтапные атаки, анализируя события информационной безопасности и связывая их в логические цепочки. Цепочка событий позволяет наглядно представить развитие инцидента во времени и в нужный момент принять соответствующие меры по предотвращению угрозы.
+ **Оперативное реагирование на инциденты ИБ.** В случае возникновения инцидента PT ISIM предоставляет ответственным сотрудникам информацию, соответствующую их полномочиям. Оперативный персонал располагает минимальным набором инструментов, необходимых для поддержки административных регламентов, а служба ИБ получает полный доступ к информации об инцидентах для их расследования.
+ **Учет специфики предприятия.** PT ISIM позволяет контролировать векторы атак, уникальные для промышленного объекта. Для настройки механизма контроля этих векторов используются данные, получаемые в результате исследования защищенности АСУ ТП предприятия.
+ **Соответствие требованиям промышленной среды.** Физические условия эксплуатации в промышленности бывают крайне агрессивными. Промышленное исполнение PT ISIM подбирается с учетом специфики отрасли и защищаемого предприятия.

PT INDUSTRIAL SECURITY INCIDENT MANAGER: НОВЫЙ УРОВЕНЬ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ

Современные промышленные объекты — это сложные автоматизированные предприятия, управляющие транспортом, производством, распределением ресурсов, добычей полезных ископаемых в режиме 24/7. Обеспечение кибербезопасности промышленных объектов — высокоприоритетная задача, поскольку атаки на них могут не только вывести из строя дорогостоящее оборудование и остановить производственный цикл, но также стать причиной техногенных катастроф.

Значительное усиление конвергенции корпоративных и производственных IT-инфраструктур сопровождается минимальным вниманием к вопросам кибербезопасности, что серьезно повышает сопутствующие риски. На начало 2018 года выявлено более 175 000 компонентов АСУ ТП, подключенных напрямую к сети Интернет. Также опыт Positive Technologies в проведении работ по анализу защищенности АСУ ТП в 2017 году показал, что в 73% промышленных компаний возможны преодоление сетевого периметра и доступ к корпоративному сегменту ЛВС. Большинство недостатков безопасности на сетевом периметре связаны с ошибками конфигурации. В то же время 82% промышленных организаций не готовы противостоять внутреннему нарушителю, который стремится проникнуть из корпоративной сети в технологическую.

Чувствительность компонентов АСУ ТП к кибератакам остается стабильно высокой на протяжении многих лет. По данным ежегодного исследования Positive Research, большая часть опубликованных в 2017 году уязвимостей была обнаружена в компонентах АСУ ТП лидирующих производителей, таких как Siemens, Advantech, Schneider Electric и Moxa, и более половины найденных уязвимостей имеют критическую и высокую степень риска. Процесс устранения уязвимостей при этом совершенно непрозрачен: больше 50% известных уязвимостей либо вовсе не исправлены, либо производитель не сообщает о времени их устранения.

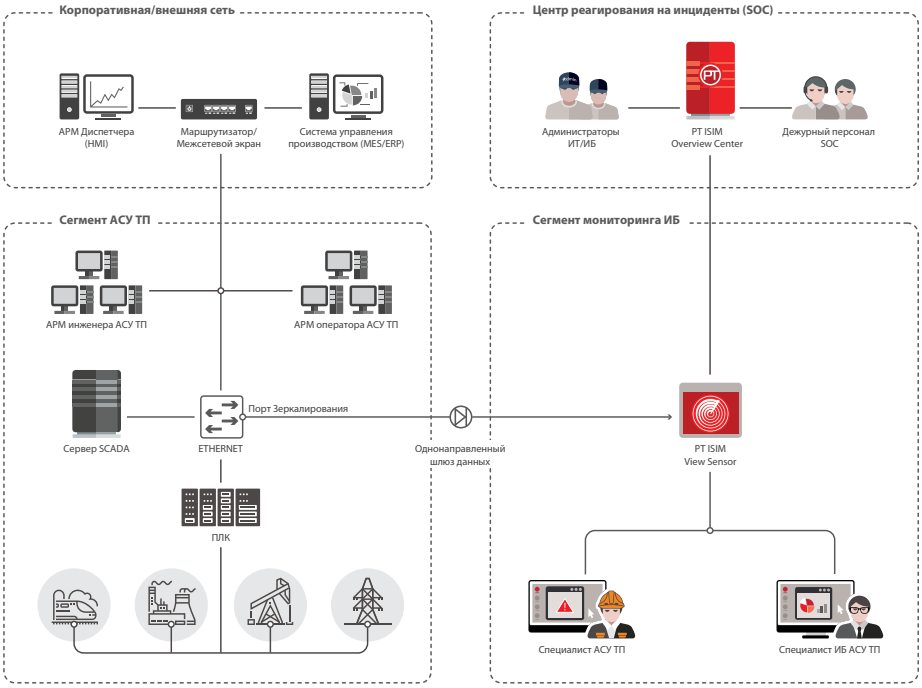
Система анализа и управления инцидентами PT Industrial Security Incident Manager, разработанная компанией Positive Technologies, призвана помочь решить актуальные проблемы и вывести промышленную кибербезопасность на новый уровень.

PT ISIM View Sensor

PT ISIM ПОМОГАЕТ:

+ **Обнаружить и предотвратить действия злоумышленников.** В отличие от других решений PT ISIM представляет инцидент в виде связной цепочки событий, а также визуализирует развитие атаки на сетевой топологии и мнемосхеме технологического процесса. Это позволяет обнаружить действия злоумышленника и вмешаться до того, как будет нарушен технологический процесс, нанесен невосполнимый ущерб оборудованию или появится опасность физического вреда людям.
+ **Расследовать инциденты безопасности без остановки техпроцесса.** PT ISIM хранит копию сетевого трафика технологического сегмента, что позволяет в любой момент провести ретроспективный анализ и расследовать инцидент, не оказывая влияния на работу АСУ ТП.
+ **Обеспечить соответствие требованиям регулирующих организаций.** PT ISIM обеспечивает реализацию широкого перечня мер защиты АСУ ТП в соответствии с 187-ФЗ, требованиями приказов ФСТЭК № 31, 239 и является ключевым звеном для системы ГосСОПКА, позволяющим выстроить эффективное взаимодействие с ведомственными и корпоративными центрами системы для обеспечения мониторинга и реагирования на инциденты ИБ.

ПРИМЕР РАЗВЕРТЫВАНИЯ



ПРИНЦИП РАБОТЫ PT ISIM

PT ISIM обеспечивает непрерывный мониторинг сетевой активности и позволяет выявлять уязвимости и хакерские атаки на промышленную сеть предприятия. PT ISIM не оказывает влияния на технологический процесс, сетевую инфраструктуру и промышленное оборудование, поскольку подключается однонаправленным способом, физически исключающим какое-либо воздействие.

PT ISIM использует для анализа копию трафика технологической сети, детектирует события кибербезопасности и выявляет связи между ними. Интеллектуальная система корреляции событий позволяет PT ISIM обнаруживать нелегитимные действия нарушителя и представлять их в виде наглядной цепочки шагов развития атаки (в том числе потенциальной). Уникальные возможности визуализации инцидентов в PT ISIM помогают оперативно определять векторы распределенных во времени атак и соотносить их с элементами как сетевой инфраструктуры, так и технологического процесса промышленного объекта. Кроме того, сохраненная копия трафика позволяет в любой момент провести ретроспективный анализ и расследование инцидента.

PT ISIM помогает бороться с различными угрозами безопасности, включая несанкционированное подключение к сети, подбор паролей к компонентам системы, неправомерное исполнение управляющих команд, подмену проектов ПЛК и прошивок промышленного оборудования. PT ISIM позволяет выявлять и внутренние угрозы, такие как потенциально опасные действия персонала и ошибки конфигурации.

В состав решения на базе PT ISIM также входит набор компонентов, необходимых для организации центра оперативного управления комплексной распределенной системой промышленной кибербезопасности (security operation center, SOC).

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays