

PT ISIM netView Sensor

Простое решение сложных задач промышленной кибербезопасности



Обнаружение и предотвращение кибератак на АСУ ТП

Встроенная обновляемая база данных промышленных угроз PT ISIM позволяет PT ISIM netView Sensor оперативно выявлять подготовку к кибератакам на ПО и оборудование АСУ ТП, а также обнаруживать эксплуатацию известных уязвимостей промышленных систем.



Контроль информационного взаимодействия в АСУ ТП

PT ISIM netView Sensor автоматически строит карту сетевых коммуникаций АСУ ТП. Это позволяет своевременно выявлять нарушения сегментации сети, наличие нерелевантного и небезопасного трафика, а также оповещать о неавторизованном доступе в сеть и к компонентам АСУ ТП.



Обеспечение соответствия требованиям регуляторов

PT ISIM netView Sensor обеспечивает реализацию широкого перечня мер защиты АСУ ТП в соответствии с 187-ФЗ, требованиями приказов ФСТЭК № 31 и 239, а также является ключевым звеном для ГосСОПКА, позволяющим выстроить эффективное взаимодействие с ведомственными и корпоративными центрами системы для обеспечения мониторинга и реагирования на инциденты ИБ.



Выявление неавторизованного управления системами

Контроль каналов управления АСУ ТП в условиях, когда наладка и обслуживание производится различными подрядчиками, в том числе удаленно, — один из самых сложных и важных элементов ИБ в АСУ ТП. PT ISIM netView Sensor позволяет оперативно выявлять факты неавторизованного управления системами (например, загрузку проекта в ПЛК или изменение конфигурации), производимого удаленно или из пределов сети АСУ ТП.



Инвентаризация сетевых активов АСУ ТП

PT ISIM netView Sensor автоматически собирает необходимую информацию об активных элементах сети (коммутаторах, АРМ, ПЛК и RTU) и представляет ее в удобном пользователю виде. Автоматизированная актуализация данных о составе сети позволяет выявлять потенциально опасные изменения (нарушения сегментации, неправомерный доступ) и вовремя реагировать на них.



Расследование инцидентов ИБ

PT ISIM netView Sensor хранит копию сетевого трафика технологического сегмента, что позволяет в любой момент провести ретроспективный анализ и расследовать инцидент, не оказывая влияния на работу оборудования АСУ ТП и технологический процесс.



Инфраструктура промышленного предприятия — продукт эволюции и модернизаций, поэтому она зачастую плохо документирована и может включать одновременно устаревшие и новые системы. Как правило, ее кибербезопасность вызывает множество вопросов. Тенденции законотворчества ведут к тому, что на каждом промышленном предприятии должны появиться подразделения или сотрудники, отвечающие за кибербезопасность АСУ ТП. Им придется быстро и эффективно выполнять множество новых и сложных задач без ущерба для технологического процесса: осуществлять мониторинг технологической сети, контролировать состав сети и конфигурации сетевых узлов, управлять специфичными событиями и инцидентами безопасности.

PT ISIM netView Sensor помогает решить все эти задачи, не требуя от пользователей специальных знаний. Аппаратно-программный комплекс без предварительной кропотливой настройки подключается к технологическому сегменту в режиме Plug and Play. За несколько часов система в процессе самообучения выполнит инвентаризацию ресурсов сети, построит карту информационного взаимодействия, выявит недостатки сегментации и возьмет на себя работу по наблюдению за безопасностью технологических ресурсов предприятия. В режиме непрерывного мониторинга она будет выявлять изменения сети и сможет идентифицировать потенциальные угрозы для АСУ ТП. Полученная информация послужит основой для формирования дальнейших планов по усилению защищенности технологического сегмента, а также отчетов и нормативных документов, требуемых в соответствии с Федеральным законом № 187-ФЗ и приказами ФСТЭК № 31 и 239.

PT ISIM netView Sensor

Уникальный программно-аппаратный комплекс для непрерывного мониторинга защищенности АСУ ТП и управления инцидентами ИБ

Positive Technologies

Unified Chassis PT ISIM-CH15-N3



Система на базе стандартного серверного шасси.

В стоимость включены лицензия на ПО и сервисы технической поддержки на год.

996 300 Р

Positive Technologies

Unified Chassis PT ISIM-CHA-24



Система на базе промышленного серверного шасси.

В стоимость включены лицензия на ПО и сервисы технической поддержки на год.

1 644 200 Р

Поддержка

Сертификат на дополнительные сервисы расширенной технической поддержки.

Для одной лицензии PT ISIM netView Sensor, на год.

146 000 Р

PT ISIM netView Sensor — продукт класса систем мониторинга ИБ АСУ ТП.

Он обеспечивает непрерывный анализ трафика сегментов технологической сети, позволяет инвентаризировать сетевые активы, выявлять неавторизованную активность и своевременно сигнализирует о недочетах в информационной безопасности АСУ ТП и кибератаках на промышленную сеть предприятия. Решение на базе PT ISIM netView Sensor легко масштабируется в случае необходимости. Это возможно за счет тесной интеграции со всей продуктовой линейкой PT ISIM и другими продуктами Positive Technologies. Система работает как источник информации об инцидентах безопасности распределенного промышленного SOC и является ключевым компонентом, реализующим требования ГосСОПКА в технологическом сегменте.



Низкая стоимость владения. Минимум усилий при внедрении и эксплуатации — не требует сложной настройки и экспертных знаний.



Автоматическая непрерывная инвентаризация сети АСУ ТП и оповещение о критических изменениях.



Не оказывает влияния на технологический процесс, сетевую инфраструктуру и промышленное оборудование.



Позволяет выявить до 80% актуальных угроз сети АСУ ТП за счет использования встроенной базы данных промышленных угроз PT Industrial Security Threat Indicators.



Уникальный источник необходимой информации об инцидентах ИБ АСУ ТП.



Подходит для промышленных предприятий любого размера и профиля деятельности.



Соответствует требованиям по защите объектов КИИ Ф3-187, приказов ФСТЭК № 31 и 239 и ГосСОПКА.

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

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.