POSITIVE TECHNOLOGIES

Безопасность объектов КИИ

Система безопасности значимых объектов КИИ в соответствии с требованиями закона № 187-ФЗ

ПРЕИМУЩЕСТВА СИСТЕМЫ

Единая экосистема продуктов

Все продукты интегрируются между собой, что обеспечивает максимальную автоматизацию процессов и упрощает управление информационной безопасностью.

Единая техподдержка

Техподдержка по всем продуктам оказывается через единое окно. Возможна расширенная поддержка в вариантах 8/5 и 24/7.

Отечественная разработка

Продукты в составе решения включены в реестр российских программ и имеют сертификаты ФСТЭК России (PT ISIM и PT MultiScanner находятся на сертификации).

В решение для безопасности объектов критической информационной инфраструктуры (КИИ) мы объединили продукты Positive Technologies, которые позволяют выполнить основные законодательные требования по защите значимых объектов КИИ, предотвращать и выявлять атаки и автоматизировать взаимодействие с ГосСОПКА.

Соответствуйте требованиям законодательства
Решение помогает реализовать меры защиты значимых объектов КИИ, обеспечить функционирование системы безопасности и взаимодействовать с ГосСОПКА в соответствии с требованиями закона № 187-ФЗ, приказов ФСТЭК и ФСБ России.

Выявляйте атаки на ранней стадии и в ретроспективе
Продукты Positive Technologies обнаруживают атаки на начальных этапах kill chain в режиме реального времени и позволяют выявлять ранее не обнаруженные признаки взлома с помощью ретроспективного анализа.

Непрерывно взаимодействуйте с ГосСОПКА
Решение автоматизирует процесс реагирования на инциденты и позволяет взаимодействовать с ГосСОПКА в двустороннем формате в режиме онлайн-чата.

Состав решения и покрываемые требования

	Приказ ФСТЭК № 235	Приказ ФСТЭК № 239	Приказы ФСБ № 367 и № 368
MaxPatrol 8 — система контроля защищенности и соответствия стандартам ИБ	+	+	—
MaxPatrol SIEM — система мониторинга событий ИБ и выявления инцидентов	+	+	—
PT Network Attack Discovery — система анализа сетевого трафика для выявления и расследования атак	+	+	—
PT MultiScanner — система защиты от вредоносного ПО с «песочницей»	+	+	—
PT Application Firewall — система защиты от веб-атак	+	+	—
PT ISIM — система обнаружения кибератак на АСУ ТП	—	+	—
PT Application Inspector — анализатор защищенности приложений	+	+	—
«ПТ Ведомственный центр» — система управления инцидентами и взаимодействия с ГосСОПКА	—	+	+

Ваши возможности

Выявляйте целевые атаки

Решение позволяет выстроить эффективную систему обнаружения и предотвращения целевых атак за счет оперативного выявления их признаков (как на периметре, так и в инфраструктуре), ретроспективного анализа и постоянного расширения знаний о способах детектирования угроз, добавляемых экспертами в продукты.

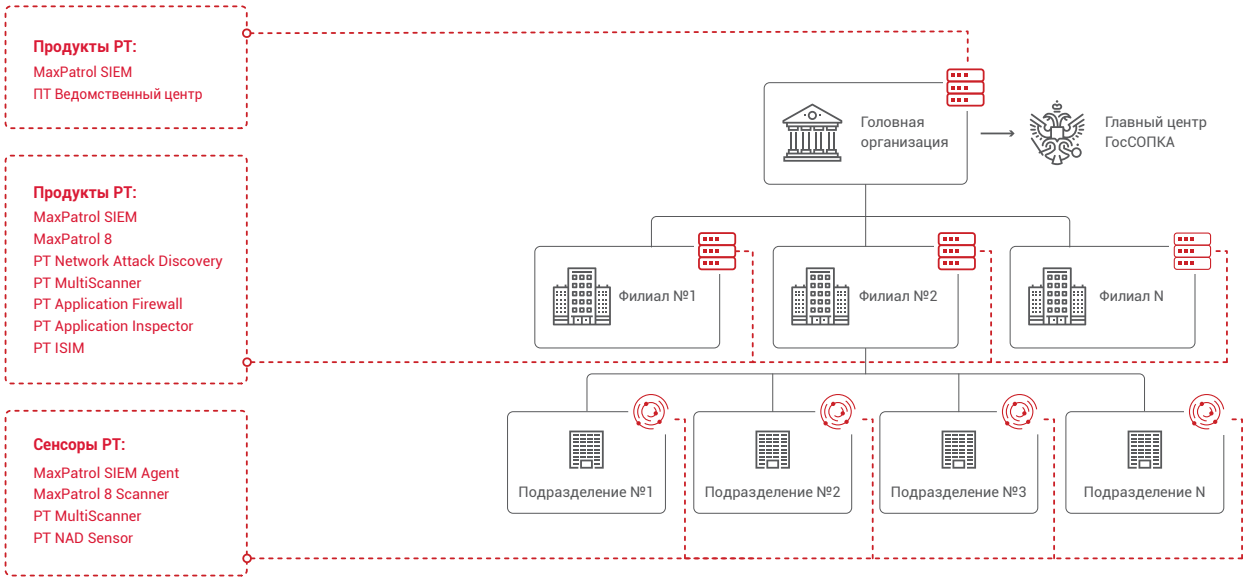
Упрощайте расследования

Хранение сырого трафика, сбор детальной информации об IT-активах, ретроспективный анализ и возможность детализации данных об атаках позволяют эффективно провести расследование.

Получите поддержку экспертов PT ESC

Специалисты центра безопасности PT Expert Security Center дополняют команду ИБ при недостатке экспертизы или полностью берут на себя задачи по выявлению атак на значимые объекты КИИ, реагированию на них и взаимодействию с НКЦКИ

Пример архитектуры решения



При многоуровневой инфраструктуре продукты Positive Technologies выстраиваются в иерархию. На нижних уровнях, где нет компетентных специалистов по ИБ или недостаточен объем бюджета на ИБ, устанавливаются сенсоры для сбора и передачи информации в крупные филиалы. Специалисты по ИБ в филиалах выявляют и расследуют атаки и отправляют данные об инцидентах в головную организацию, где консолидируется информация об инцидентах во всей компании и осуществляется взаимодействие с главным центром 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.