POSITIVE TECHNOLOGIES

ПТ Ведомственный центр

Система управления инцидентами и взаимодействия с ГосСОПКА

ОСОБЕННОСТИ РЕШЕНИЯ

Взаимодействие с ГосСОПКА
в двустороннем формате: обмен информацией об инцидентах и актуальных угрозах

Автоматическое создание карточки инцидента
в необходимом формате, согласно требованиям НКЦКИ

Автоматическое получение инцидентов из MaxPatrol SIEM с возможностью выбора инфраструктуры для мониторинга, например только критической

Разграничение прав доступа
для специалистов группы реагирования

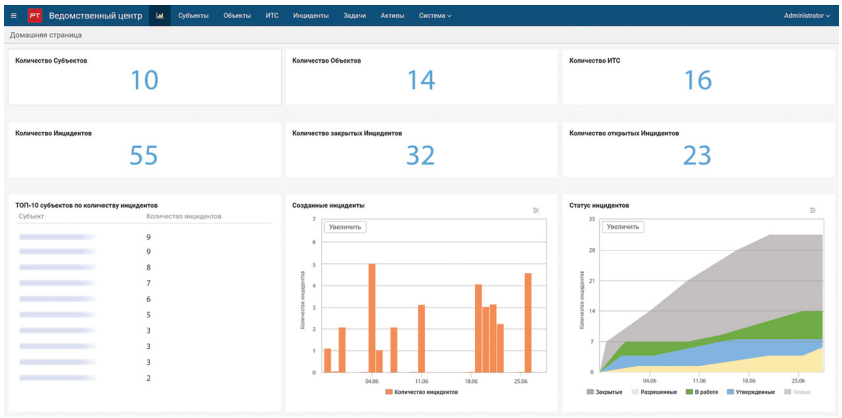
Подробнее о продукте

Согласно Федеральному закону от 26.07.2017 № 187-ФЗ о безопасности критической информационной инфраструктуры, субъекты КИИ обязаны незамедлительно информировать о кибератаках Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

«ПТ Ведомственный центр» — система управления инцидентами, которая автоматизирует процесс реагирования на инциденты и информирует о них НКЦКИ.

Ключевые задачи

- Регистрация инцидентов путем создания заявок на их обработку (карточек инцидентов)
- Назначение приоритетов и статусов
- Указание источников информации об инцидентах
- Назначение ответственных за реагирование
- Назначение сроков реагирования
- Отработка инцидентов по шаблонам реагирования
- Отчеты о новых инцидентах
- Учет взаимодействия с НКЦКИ



Дашборды помогают руководителю контролировать работу центра ГосСОПКА

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

- Учет субъектов (организаций) и их объектов, в том числе дочерних, для контроля зон ответственности
- Учет критических информационных инфраструктур и ресурсов
- Сбор информации об уязвимостях информационных систем

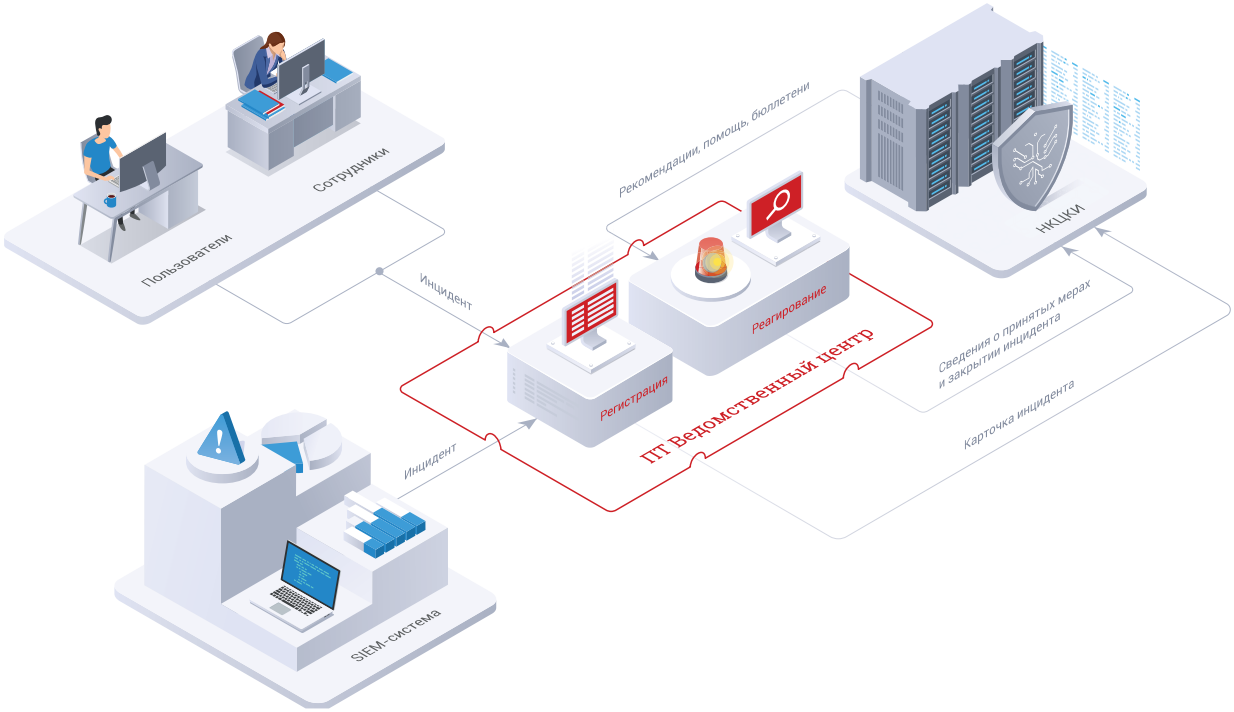
Результаты применения

- **Соответствие требованиям законодательства** о необходимости регистрации инцидентов, управления ими и информирования НКЦКИ.
- **Отправка сведений об инцидентах в срок** за счет мониторинга обработки инцидентов.
- **Экономия времени специалистов** по ИБ благодаря автоматическому созданию карточки инцидента и применению шаблонов реагирования.

Как работает

После получения информации об инциденте из SIEM-системы или от пользователей IT-инфраструктуры в «ПТ Ведомственном центре» создается карточка инцидента (в соответствии с его типом). Оператор системы дополняет карточку необходимыми сведениями и отправляет ее в НКЦКИ в окне онлайн-чата. По запросу специалист может получать от НКЦКИ рекомендации по реагированию и расследованию.

По мере реагирования оператор информирует НКЦКИ о его ходе, принятых мерах и закрытии инцидента.



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.

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays