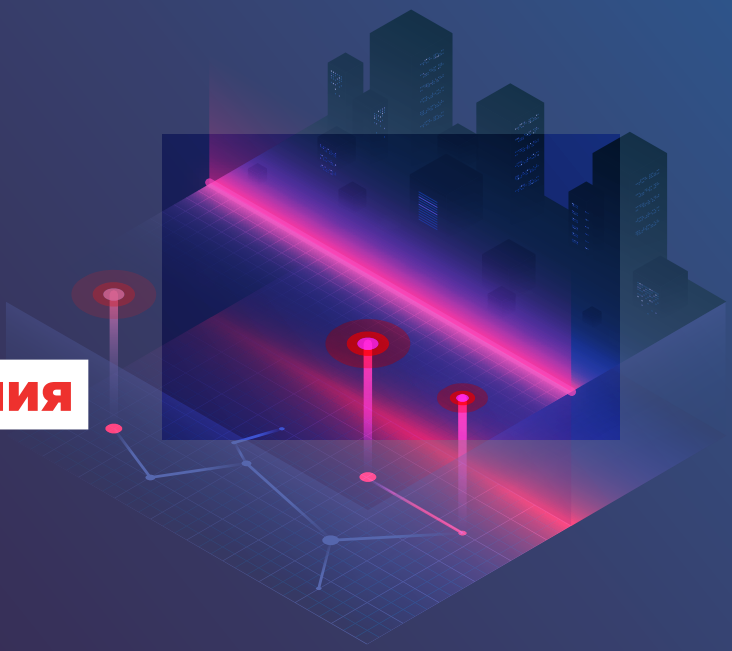
positive technologies

Комплекс для раннего выявления сложных угроз



От 1 до 5 дней
уходит на взлом 90% компаний

9 из 10 жертв
не подозревают, что их взломали

197 дней
в среднем проходит от момента взлома до его обнаружения

60% атак
распространяются в инфраструктуре горизонтально

Решение

Комплекс предназначен для выявления и предотвращения целевых атак. Он позволяет максимально быстро обнаружить присутствие злоумышленника в сети и воссоздать полную картину атаки для детального расследования.

Полный обзор

Выявляет присутствие атакующего как на периметре, так и в инфраструктуре

Ретроспектива

Автоматически выявляет не обнаруженные ранее факты взлома инфраструктуры

Экспертиза

Расширяет возможности по расследованию атак благодаря экспертизе Positive Technologies

Ключевые возможности

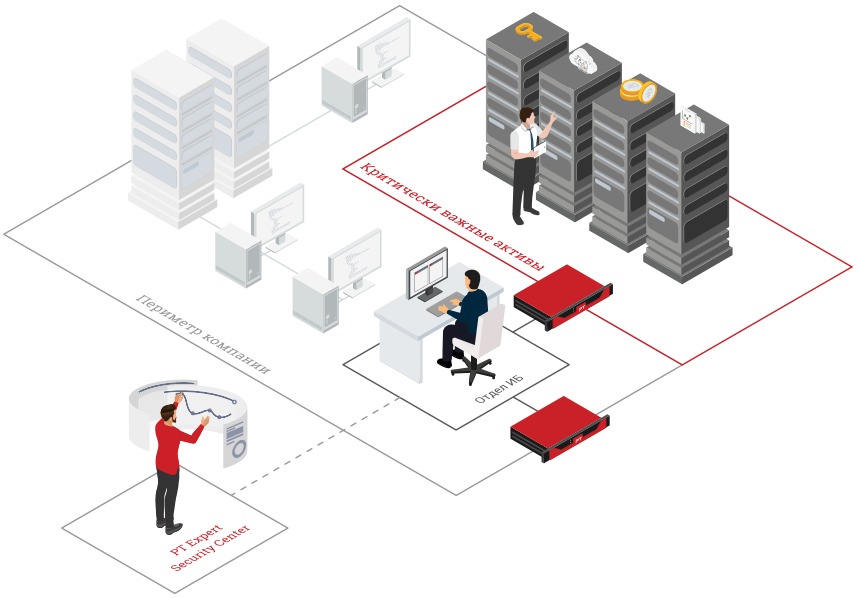
Выявляет атаки по большому количеству признаков
Социальная инженерия, применение вредоносных программ и хакерских инструментов, нарушение политик безопасности, эксплуатация уязвимостей ПО, атаки на контроллер домена, горизонтальное перемещение внутри инфраструктуры, эксфильтрация данных и другие злонамеренные активности — неважно, каким образом действуют злоумышленники, решение позволит их найти.

Сокращает время скрытого присутствия злоумышленника
Решение обнаруживает не выявленные ранее атаки с помощью ретроспективного анализа. После обновления баз знаний и репутационных списков запускается повторный анализ трафика и объектов, который позволяет максимально быстро обнаружить скрытое присутствие злоумышленника.

Защищает от неизвестных и новейших угроз
В решение входит продвинутая «песочница», которая не дает вредоносному объекту распознать виртуальную среду и видит все создаваемые им файлы и системные процессы. Это позволяет выявить опасную активность, внешне не связанную с вредоносным ПО.

Как это работает

Система может быть развернута как на периметре, так и перед критически важными активами в инфраструктуре. Это позволяет выявлять активность злоумышленников, даже если они уже проникли в сеть.



Задачи по расследованию инцидентов берут на себя эксперты PT Expert Security Center, которые уже шесть лет расследуют сложные атаки и следят за активностью хакерских группировок.

Посмотрите вебинар

Закажите бесплатный пилот

Преимущества

Защищает от наиболее актуальных для России угроз. Знания Positive Technologies об актуальных методах взлома российских компаний и глубокая экспертиза в обеспечении безопасности сложных инфраструктур позволяют решению эффективно выявлять даже самые новые угрозы.

Сокращает время реагирования и расследования инцидентов. Решение хранит записи сырого трафика, необходимые параметры сессий, детальный граф поведения вредоносного ПО. Это позволяет оперативно выявить следы компрометации, отследить перемещение злоумышленника и выработать компенсирующие меры.

Не передает данные об атаках и объектах за пределы компании. Все данные анализируются внутри компании и не покидают ее периметр. Это позволяет избежать нежелательного распространения данных об атаках и ущербе.

Позволяет выполнять требования законодательства. Решение помогает соответствовать требованиям по защите КИИ, персональных данных, информации в ГИС, в АСУ ТП и в информационных системах общего пользования.

ptsecurity.com
pr@ptsecurity.com