positive technologies

MaxPatrol O2

Автопилот для результативной кибербезопасности

90%

компаний испытывают нехватку кадров ИБ

71%

недопустимых для компании событий могут быть реализованы атакующими в течение месяца

100%

инфраструктур компаний могут быть полностью взяты под контроль внутренним злоумышленником

93%

сетевых периметров может преодолеть злоумышленник и получить доступ к локальной сети

Метапродукт **MaxPatrol O2** обнаруживает злоумышленника, определяет захваченные им ресурсы, прогнозирует сценарий развития атаки с учетом недопустимых для компании событий, и останавливает атаку до того, как компании будет нанесен непоправимый ущерб.

Моделирует действия злоумышленников

Предсказывает, к каким недопустимым событиям может привести подозрительная активность и сколько шагов осталось до реализации рисков.

Выявляет цепочки хакерской активности

Анализирует данные от сенсоров Positive Technologies, включенных в состав метапродукта, и выделяет из них атакующие, атакованные и захваченные ресурсы. Сопоставляет ресурсы и строит цепочки активности с учетом знаний о техниках и тактиках злоумышленников. В каждой цепочке присутствует визуализация пути, пройденного злоумышленником, а также прогноз, куда он будет двигаться дальше.

Автоматизирует расследования

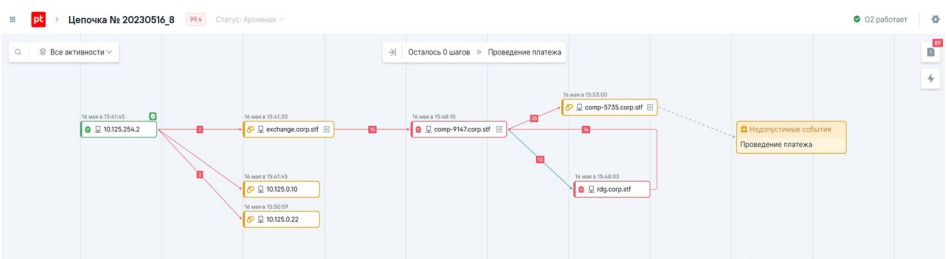
Использует данные от сенсоров Positive Technologies, чтобы построить полный контекст атаки и провести расследование.

Оценивает степень опасности угроз

MaxPatrol O2 видит захваченные злоумышленником ресурсы и предсказывает близость реализации недопустимого события. Основываясь на этих данных, система переводит цепочку атаки в статус «Требует внимания», после чего автоматически останавливает хакера или информирует оператора, чтобы он принял решение.

Останавливает злоумышленника

Учитывает риски для бизнес-процессов и предлагает оптимальный сценарий реагирования. Сценарий может быть реализован автоматически или в ручном режиме, если его нужно скорректировать.



В чем заключается **концепция метапродуктов**,
и почему их нельзя отнести к классам IRP/SOAR/XDR

ПРЕИМУЩЕСТВА:

Делает невозможной
реализацию недопустимых для бизнеса событий

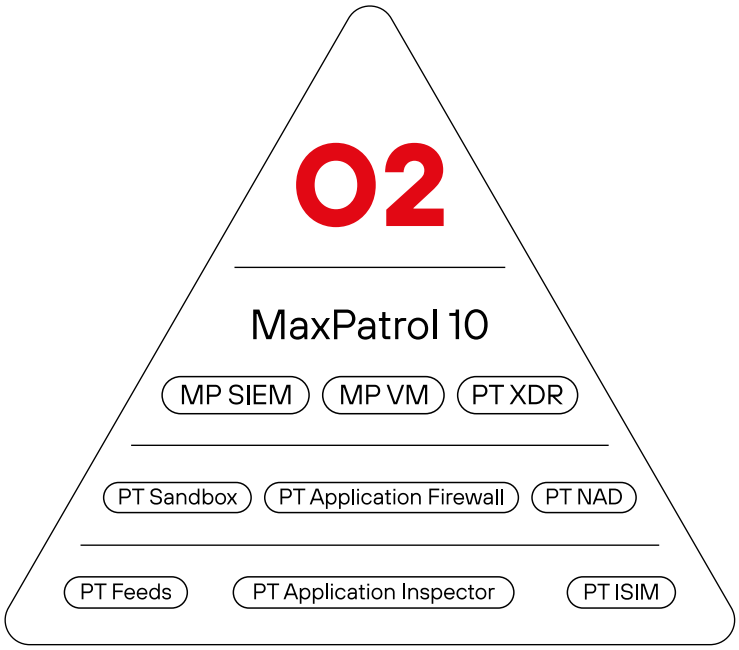
Автоматизирует работу SOC
в процессах обнаружения, расследования и реагирования на инциденты

Знает, как действует злоумышленник,
благодаря накапливаемому опыту Positive Technologies в регулярных киберучениях, BugBounty «Positive dream hunting» и Standoff

Не требует специалистов высокой квалификации
для эффективной работы метапродукта

Экосистема Positive Technologies

Объединяет продукты Positive Technologies, которые работают как сенсоры, обмениваются знаниями и обеспечивают комплексную защиту IT-систем компании с минимальным вовлечением человека в процесс



Как работает MaxPatrol O2

ptsecurity.com
pr@ptsecurity.com

MAXPATROL-O2_PB_A4.RUS.0032.23.MAY.17.2023