positive technologies

MaxPatrol O2

Автопилот для обнаружения и остановки кибератак с минимальным участием человека

Обеспечение непрерывной киберзащиты компании требует создания центра мониторинга и реагирования на атаки (SOC — security operation center) с командой высококвалифицированных экспертов.

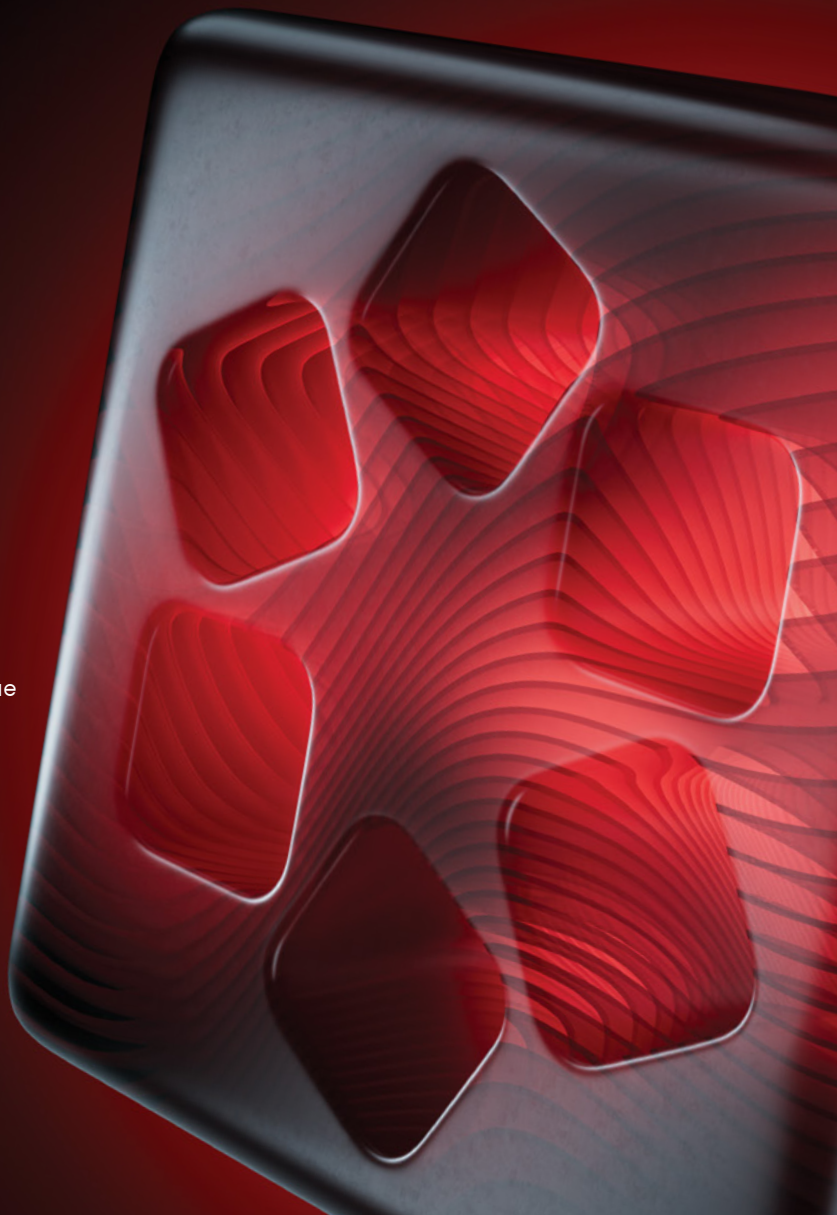
MaxPatrol O2 меняет этот подход. Метапродукт автоматизирует все сложные и рутинные процессы — от обнаружения и расследования кибератак до оперативного реагирования на них, — привлекая специалиста только для подтверждения угрозы и запуска сценария реагирования. Это позволяет достичь экспертного уровня защиты, сохраняя компактную команду специалистов по ИБ.

Метастандарт результативной кибербезопасности

Экспертный уровень защиты
Повышает уровень экспертизы SOC, обеспечивая автоматическое выявление, расследование и отражение кибератак любого уровня сложности

Быстродействие при ограниченных ресурсах
Помогает нарастить эффективность SOC: сокращает время реагирования на кибератаки, снижает нагрузку и позволяет выполнять больший объем работы без расширения штата

Полный контроль безопасности
Автоматически обрабатывает на порядок больше событий ИБ по сравнению с традиционными методами, исключая появление слепых зон и обеспечивая полную видимость аномальной активности в реальном времени



Ключевые возможности метапродукта

Выявляет цепочки кибератак в режиме реального времени

Анализирует множество отдельных событий из разных средств защиты и объединяет их в цепочки подозрительных активностей, характерных для атаки

Привлекает эксперта только к опасным активностям

Оценивает потенциальную опасность цепочек активностей и привлекает эксперта для реагирования только в случае превышения пороговых значений

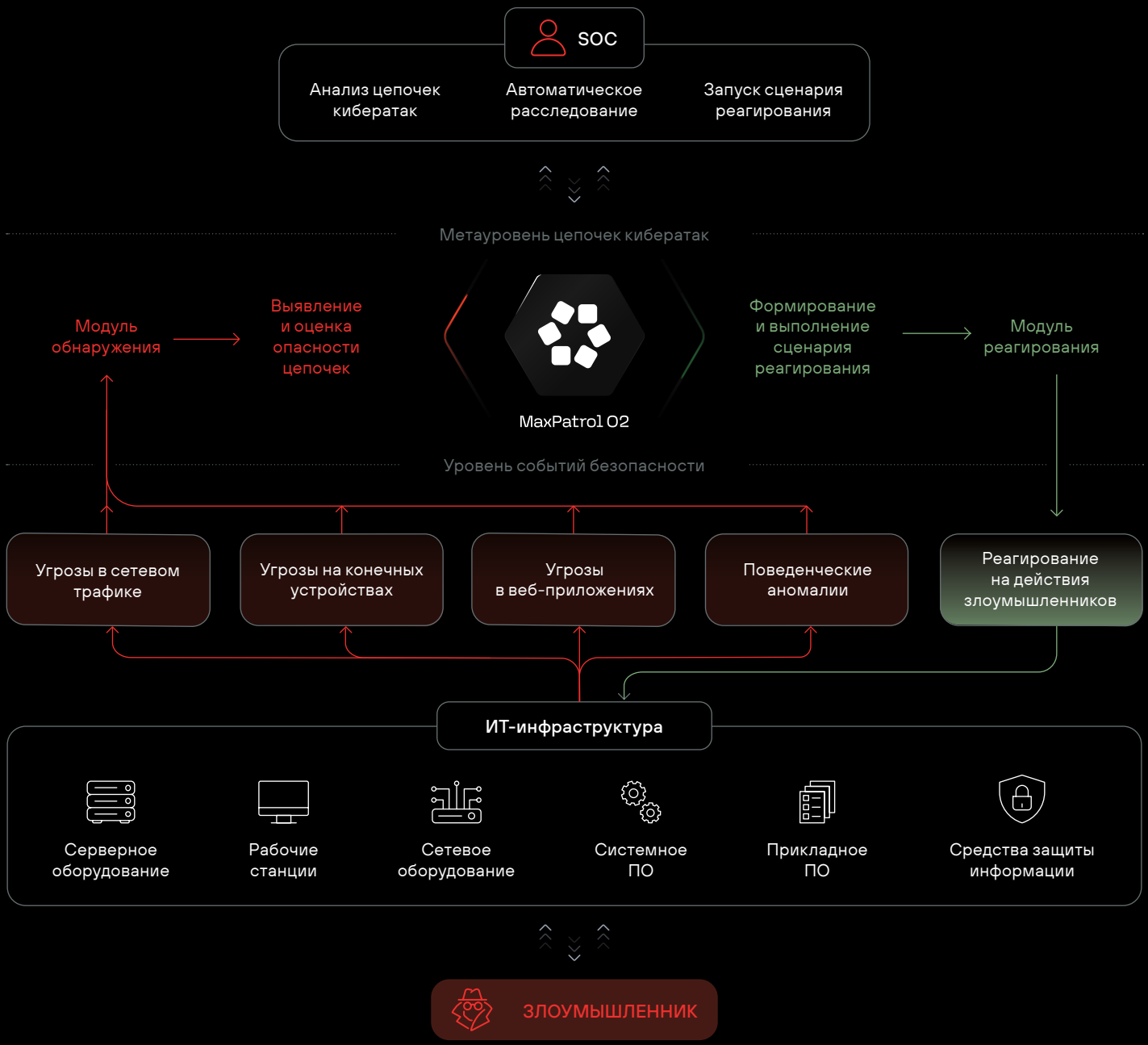
Помогает в расследовании инцидентов

В автоматическом режиме восстанавливает хронологию действий злоумышленника, визуализируя весь контекст атаки, и акцентирует внимание на самых значимых событиях и фактах

Останавливает атаку за несколько минут

Генерирует сценарий реагирования для каждой цепочки и выполняет его по нажатию одной кнопки, что позволяет быстро остановить кибератаку и вернуть контроль над захваченными ресурсами без привлечения ИТ-специалистов

Как работает MaxPatrol O2



Переведите кибербезопасность на автопилот с MaxPatrol O2

Узнайте больше