positive technologies

MaxPatrol Carbon

Интеллектуальная система
для проактивного управления
киберустойчивостью компании

А знаете ли вы, что...

Сложное больше не значит редкое

1 из 2

атак нарушают основную деятельность компании, а 71% приводят к утечке чувствительных данных[1]

ИИ играет на темной стороне

×20

выросла скорость эксплуатации уязвимостей и реализации сложных атак из-за доступности ИИ[2]

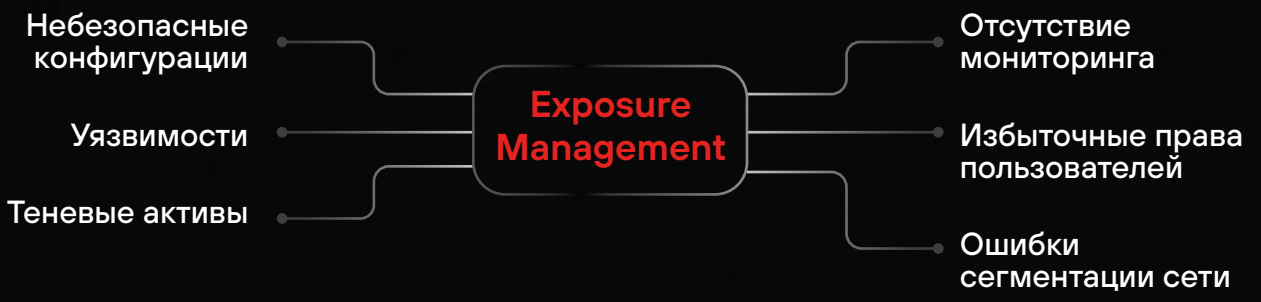
Рост числа уязвимостей выходит из-под контроля

1 000 000

уникальных уязвимостей в NVD[3] прогнозирует Gartner к 2030 году[4]

Однако управлять только уязвимостями недостаточно

Злоумышленники используют комбинации различных недостатков инфраструктуры, чтобы достичь своих целей



Традиционные подходы перестают работать

- Команды ИБ тонут в отчетах, а объем задач создает избыточную нагрузку на ИТ-специалистов
- Нет ресурсов и экспертизы, чтобы связать технические недостатки с реальными сценариями атак
- Руководству нужны понятные бизнес-метрики, а не длинные отчеты со списками угроз

[1] Источник: Сводная статистика по успешным атакам на организации, Positive Technologies

[2] Источник: Данные X Threat Intelligence, интеллектуальной платформы Сбера по управлению кибеугрозами

[3] Национальная база данных уязвимостей (National Vulnerability Database, NVD): nvd.nist.gov

[4] Исследование аналитического агентства Gartner Tech FutureSight: Preemptive Cybersecurity Is the Only Way to Secure Emerging AI Attack Surfaces

Предвидеть кибератаки и действовать на опережение с MaxPatrol Carbon

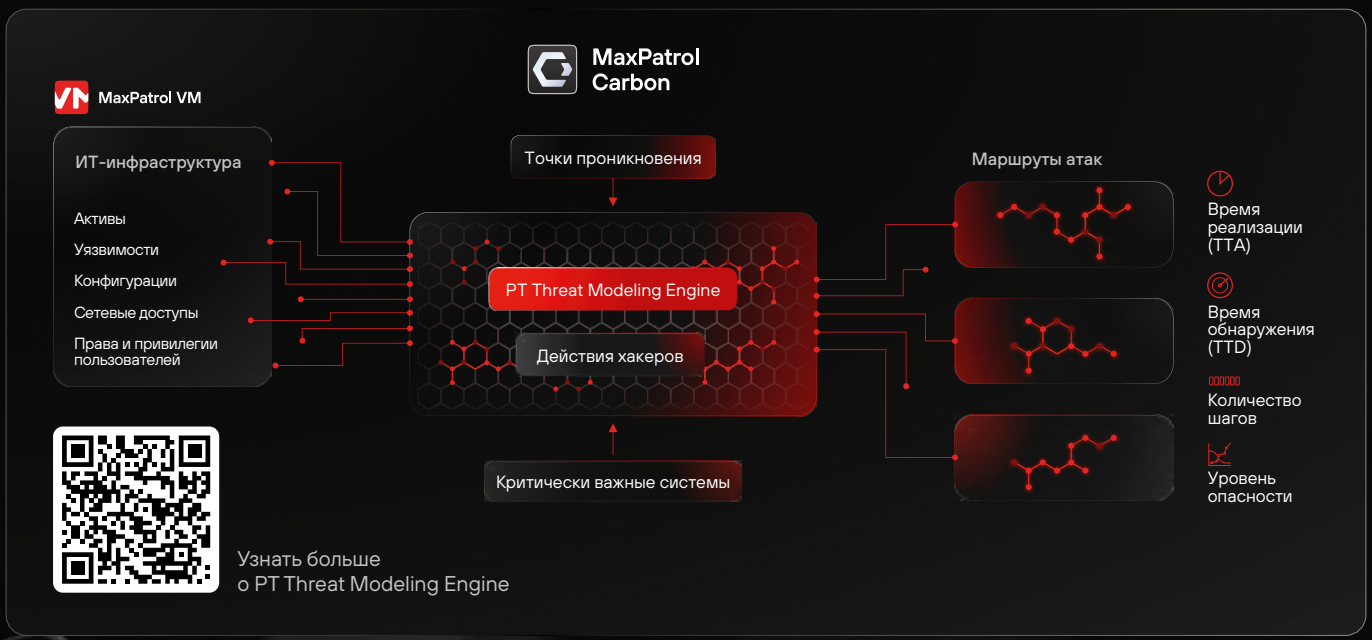
MaxPatrol Carbon анализирует все потенциальные угрозы в инфраструктуре с точки зрения злоумышленника, моделируя пути компрометации критически важных активов, и помогает своевременно устранять наиболее опасные недостатки, чтобы непрерывно повышать устойчивость компании к кибератакам

Фокус на сценариях атак и целевом устранении угроз позволяет

- Анализировать всю потенциальную площадь атаки
- Прогнозировать пути развития атаки и оценивать их опасность
- Управлять всеми угрозами, а не только уязвимостями
- Приоритизировать задачи на основе бизнес-рисков
- Оценивать результативность принимаемых мер
- Контролировать и повышать уровень киберустойчивости

Внутри — уникальная технология моделирования киберугроз PT Threat Modeling Engine

Автоматически строит граф возможностей атакующего на основе знаний о реальных действиях хакеров, учитывает текущее состояние инфраструктуры и все ее недостатки



Узнать больше о PT Threat Modeling Engine

MaxPatrol Carbon строит цифровую копию инфраструктуры в виде графа и моделирует все возможные пути атаки, делая это безопасно, без нагрузки на системы и без вмешательства в их работу

MaxPatrol Carbon на практике доказывает, что для киберустойчивости важен не объем задач, а их приоритет

Статистика на одном из проектов внедрения MaxPatrol Carbon

Ключевые преимущества

Проактивное управление киберустойчивостью

MaxPatrol Carbon автоматически моделирует пути кибератак к критически важным системам, оценивает их опасность и помогает устранить их до атаки

Принцип «делай меньше — защищай больше»

Позволяет сосредоточиться на действительно важных задачах, учитывает реальную степень опасности угроз для бизнеса и показывает, какие меры дадут наибольший эффект

Измеримые результаты и бизнес-контекст

Делает анализ киберустойчивости измеримым, переводя технические недостатки в понятные метрики и упрощая взаимодействие отделов ИБ, ИТ и топ-менеджмента

Действуйте на опережение и защитите самое ценное

Узнать больше о MaxPatrol Carbon

Актуальное покрытие техник из матрицы MITRE ATT&CK