



MaxPatrol Carbon

Предвидеть кибератаки и действовать на опережение

Атаковать — легче Защищать — все сложнее



Сложное больше
не значит редкое

1 из 2

атак нарушают основную
деятельность компании,
а 67% — приводят к утечке
чувствительных данных¹

ИИ играет
на темной стороне

×20

выросла скорость
эксплуатации уязвимостей
и реализации сложных атак
из-за доступности ИИ²

Количество уязвимостей
выходит из-под контроля

1 млн +

уникальных уязвимостей
в NVD³ прогнозирует
Gartner к 2030 году⁴

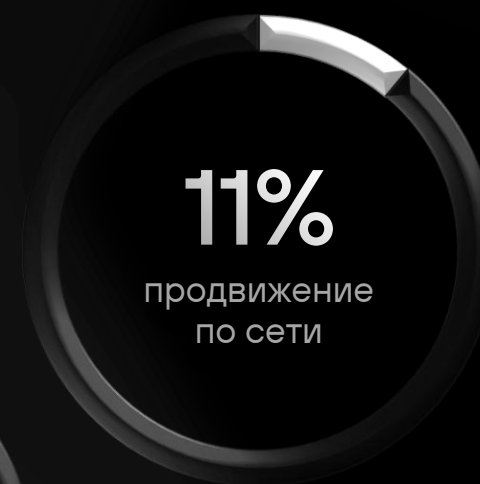
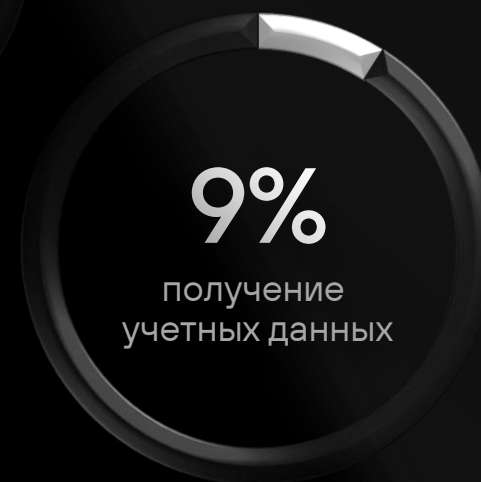
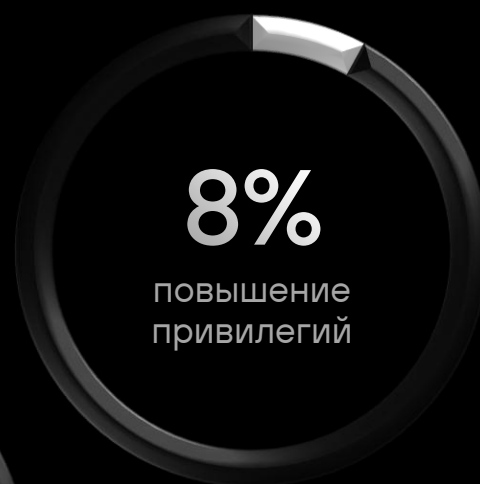
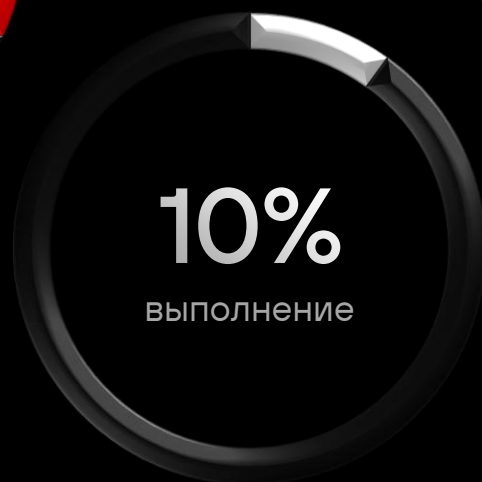
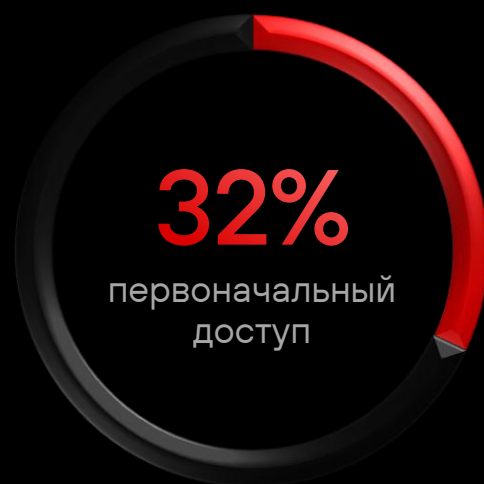
¹ Источник: Сводная статистика по успешным атакам на организации, Positive Technologies

² Источник: Данные X Threat Intelligence, интеллектуальной платформы Сбера по управлению киберугрозами

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

⁴ Исследование аналитического агентства Gartner

Уязвимость — это одна из многих возможностей на пути атакующего



Процент эксплуатации уязвимостей на разных этапах реализации атаки на основе аналитики Positive Technologies, Mandiant M-Trends, Red Canary, CTID и CISA

Путь атаки состоит из комбинации угроз



Exposures — это источники угроз в инфраструктуре компании, уязвимости в широком смысле слова, те недостатки безопасности, которые могут быть использованы злоумышленниками при атаке

Традиционные подходы перестают работать



1 Нет полной видимости площади атаки

Нет полноценной инвентаризации активов, что приводит к появлению слепых зон в инфраструктуре

1

2 Нет времени и ресурсов

Для быстрого выявления и устранения обнаруженных недостатков требуется много ИТ-специалистов и времени

2

3 Нет приоритизации угроз на основе опасности для бизнеса

Нет понимания, что делать в первую очередь, чтобы защитить критически важные активы

3

4 Нет возможности оценить результат

Нет инструментов оценки эффективности принимаемых мер — SLA не является показателем защищенности инфраструктуры

4

5 Нет текущего статуса защиты

Нет понимания текущего уровня киберустойчивости инфраструктуры

5

Атака реализована и хакеры достигли своих целей

РЕЗУЛЬТАТ

Эволюция подхода к управлению уязвимостями



Exposure management в мире



CTEM

Continuous Threat Exposure Management (CTEM) — методология непрерывного управления киберугрозами от Gartner



Gartner

К 2028 году организации, внедрившие CTEM, снизят риск взлома минимум на 70% по сравнению с теми, кто опирается только на CVSS



Вектор развития в России



Центр стратегических разработок (ЦСР) 2026

Рынок консолидирует задачи смежных классов решений по управлению уязвимостями в единый подход по управлению экспозицией рисков для нейтрализации реальных угроз.

1

Спрос смещается от классического управления уязвимостями к управлению экспозицией рисков (exposure assessment and management)

2

Exposure management объединяет данные об активах, уязвимостях, конфигурациях, идентичностях и угрозах

3

Цель — приоритизировать исправление или изоляцию именно тех дефектов системы, которые реально повышают вероятность успешной атаки

Глобальный рынок VM&EM



IDC Worldwide Device Vulnerability
& Exposure Management Market Share 2025

2,8%

CrowdStrike

4%

ServiceNow

12,5%

Rapid7

17,3%

Qualys

Vulnerability &
Exposure Management
Market Share 2024*

2,4%

Positive Technologies

34,4%

Остальной рынок

26,6%

Tenable

*According to the IDC study "Worldwide Device Vulnerability
and Exposure Management Market Shares, 2024." September 2025



8,1%

CAGR of the global
vulnerability and exposure
management solutions market

IDC

MaxPatrol Carbon

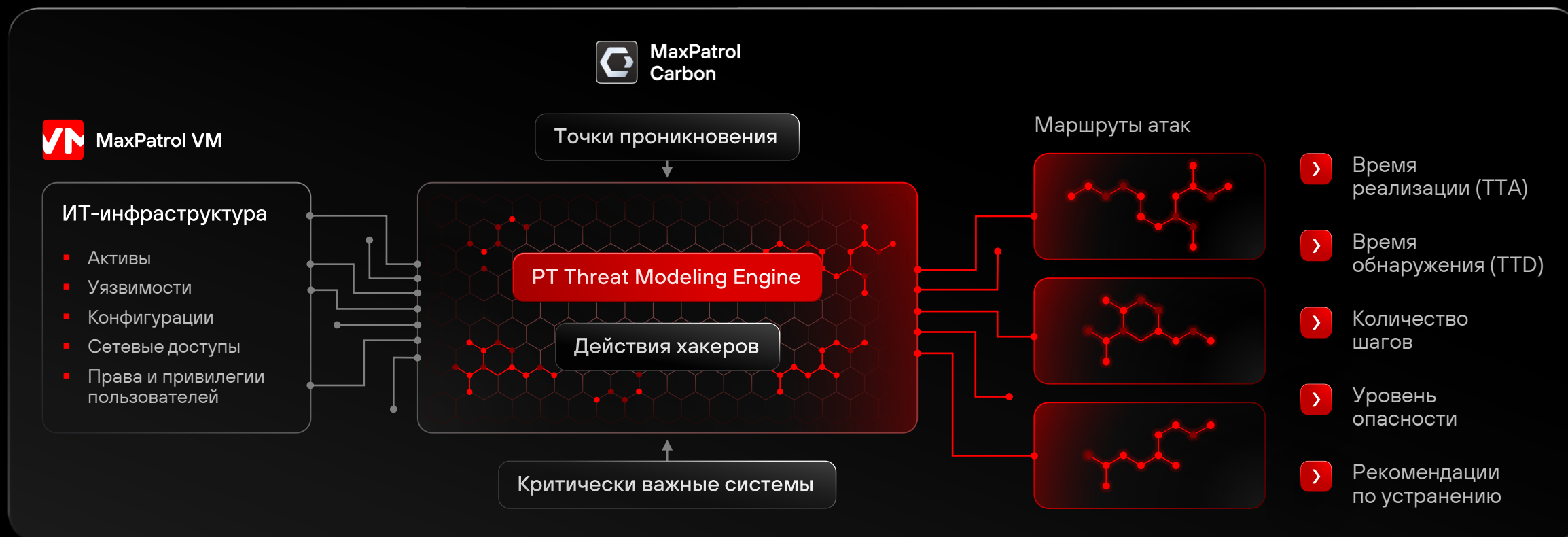
Интеллектуальная система
для проактивного управления
киберустойчивостью компании



MaxPatrol Carbon



Строит цифровую копию инфраструктуры в виде графа, моделирует все возможные пути атаки на критически важные системы, выявляет наиболее опасные угрозы и помогает вовремя устранить их, делая это безопасно, без нагрузки на системы и без вмешательства в их работу



PT Threat Modeling Engine

Уникальная технология моделирования киберугроз

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

4

Действия
атакующих

3

Привилегии
пользователей

2

Уязвимости и ошибки
конфигураций

1

Карта активов
и их связей



Что такое действие атакующего



Действие — это комбинация тактик и техник, которая позволяет атакующему перемещаться между компонентами системы. В большинстве случаев одно действие включает несколько техник или подтехник из матрицы MITRE ATT&CK

81%

Текущее покрытие матрицы MITRE ATT&CK MaxPatrol Carbon и его сенсорами

Примеры действий хакера на маршруте кибератаки



Дамп памяти процесса LSASS



Эксплуатация уязвимостей



Использование мисконфигураций



Манипуляции с учетной записью



Подбор паролей

Передвижение хакера в инфраструктуре под видом пользователя



RPC и SMB
Удаленное выполнение команд



RDP и SSH login
Подключение к удаленному APM или серверу



GitLab, 1C, ДБО login и др.
Аутентификация в рискованных системах

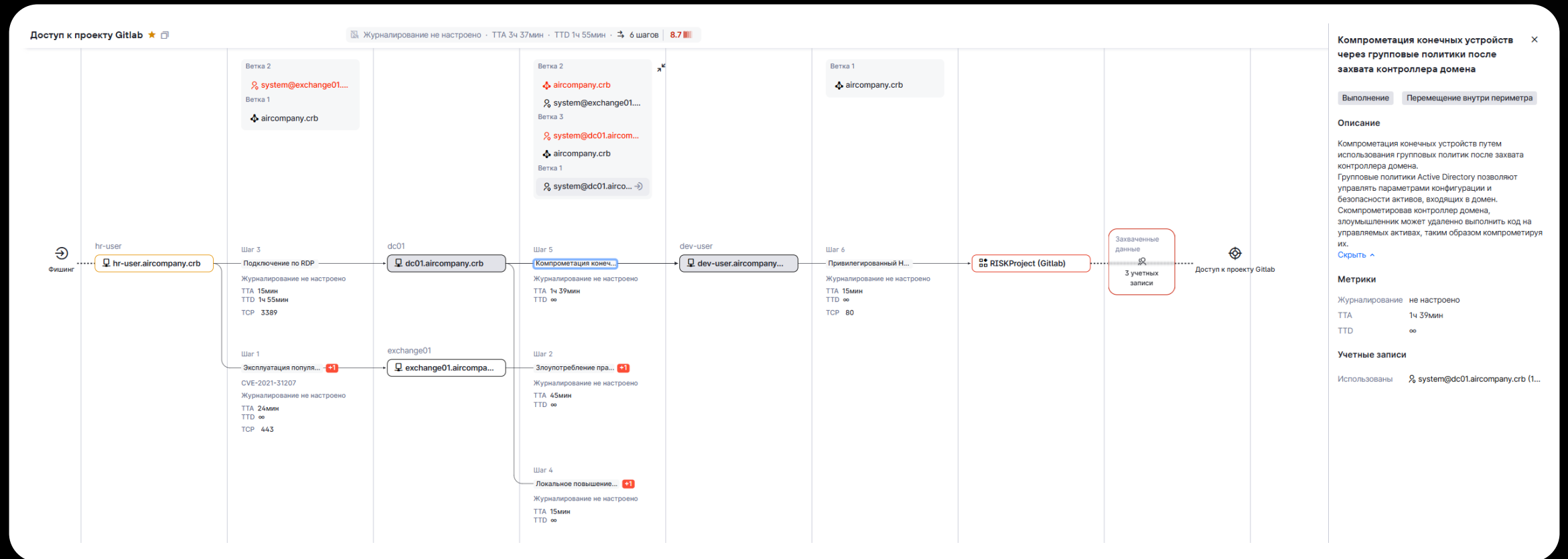


Маршрут атаки



Визуализация каждого маршрута атаки с учетом:

- последовательности шагов действий злоумышленника
- времени атаки (ТТА)
- времени обнаружения (ТТД)
- рекомендаций по нейтрализации захваченных учетных записей



Рекомендации для устранения источников угроз



MaxPatrol VM

Устранение уязвимостей

Устранение технических уязвимостей на активах



MaxPatrol HCC

Контроль конфигураций активов

Проверка конфигураций на соответствие требованиям безопасности и контроль изменений



User Compliance*

Контроль привилегий пользователей

Управление правами и привилегиями учетных записей



Network Compliance*

Контроль сетевого доступа

Создание правил и политик сетевого доступа, а также контроль соответствия им



Asset management

Инвентаризация активов

Проведение первичного аудита ИТ-актива, а также контроль актуальности данных аудита



MaxPatrol SIEM

Мониторинг источников

Настройка источников и проверка поступления событий от них

ИНФРАСТРУКТУРНЫЕ РЕКОМЕНДАЦИИ*

Общие рекомендации, которые формируются на основании информации об ИТ-инфраструктуре

Эти рекомендации не относятся непосредственно к действиям и графу атак, а описывают лучшие практики по настройке инфраструктуры в целом

* Функциональность MaxPatrol Carbon



Единый центр управления площадью атаки



Проактивное управление киберустойчивостью



Exposure management с MaxPatrol Carbon позволяет:



Анализировать всю потенциальную площадь атаки



Прогнозировать пути развития атаки, оценивать их опасность и заранее устранять



Централизованно управлять всеми угрозами, а не только уязвимостями



Приоритизировать задачи на основе бизнес-рисков



Оценивать результативность принимаемых мер



Контролировать и повышать уровень киберустойчивости

Невозможно защитить то, чего не видно...



АКТИВЫ

Аудит ИТ-инфраструктуры

Необходимо максимальное покрытие активов сканированием в режиме аудита

СЕТЬ

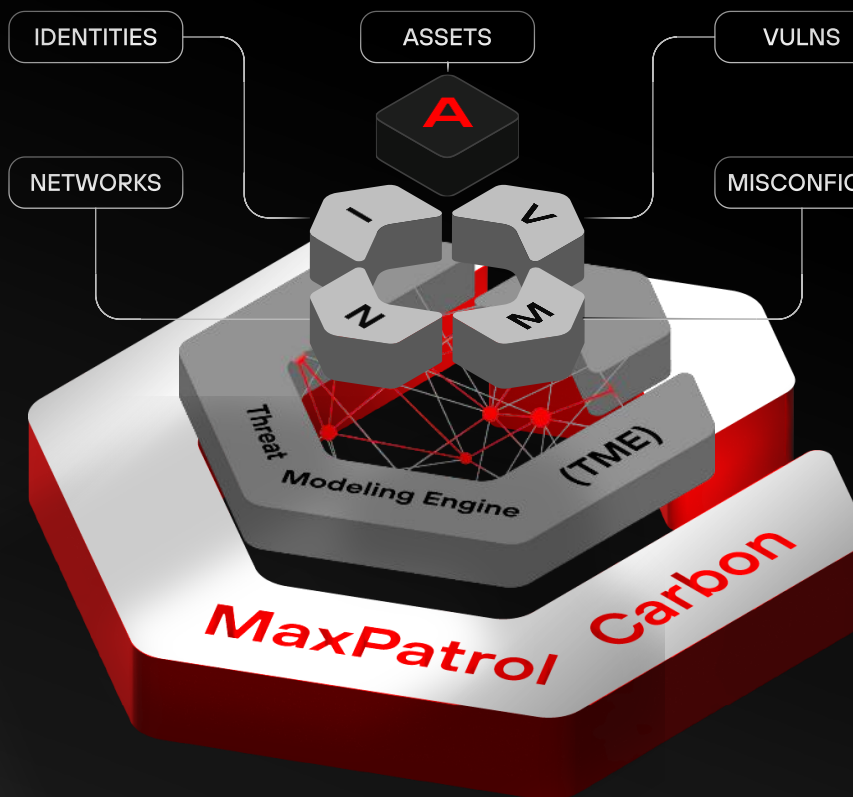
Сканирование сетевых устройств

Необходимо, чтобы рассчитать сетевую достижимость и определить поверхность атаки

УЧЕТНЫЕ ЗАПИСИ

Доменные и локальные

Необходимо знать обо всех пользователях и их привилегиях (сканирование доменов)



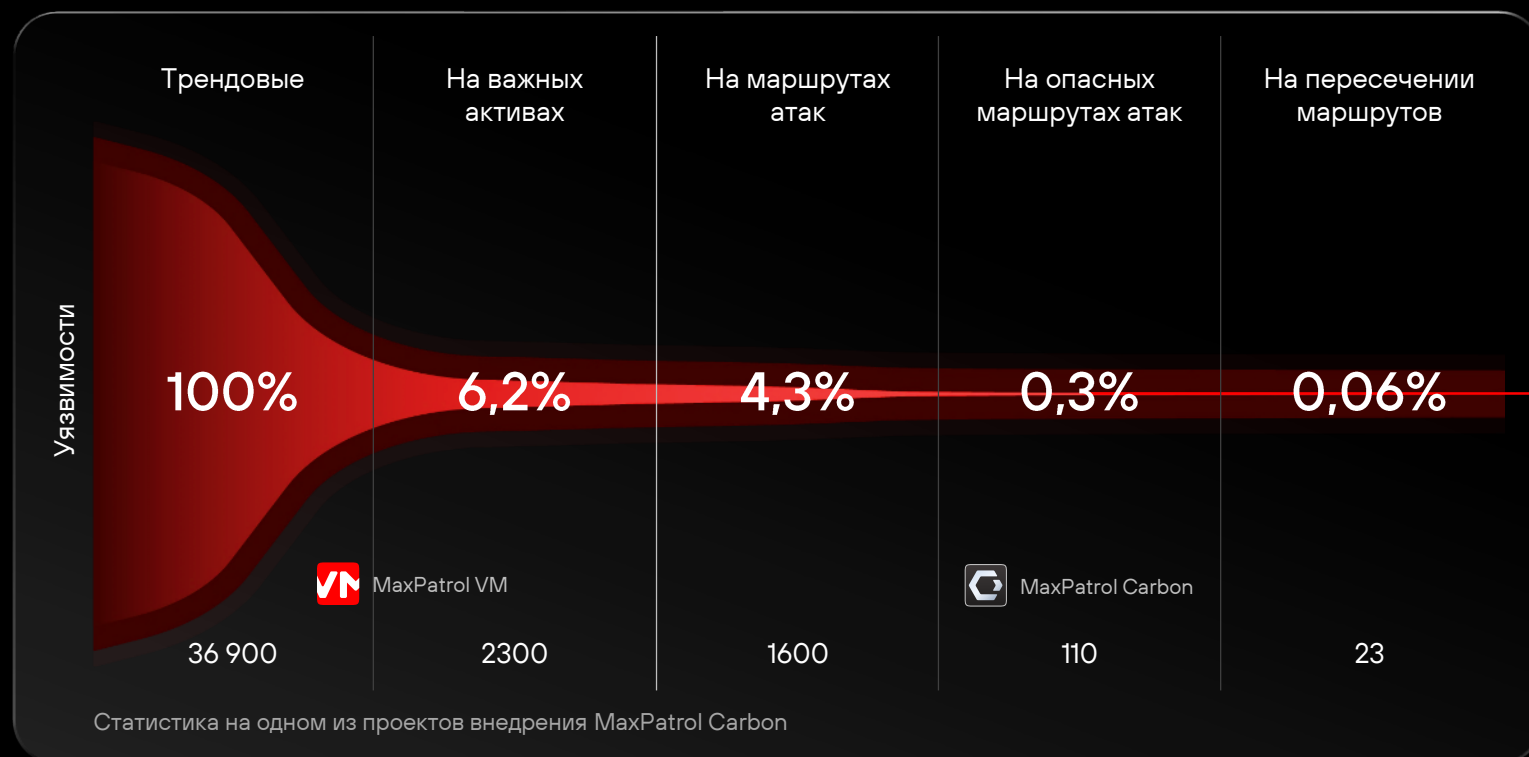
MaxPatrol VM



MaxPatrol HCC

Всю информацию об инфраструктуре получаем от MaxPatrol VM с модулем MaxPatrol HCC

Для киберустойчивости важен не объем задач, а их приоритет



Два актива

требуют наибольшего внимания, чтобы предотвратить самые быстрые и опасные пути реализации атаки

До 5% от всех уязвимостей

на критически важных активах надо устранить для нейтрализации большинства опасных маршрутов



Важный факт: MaxPatrol Carbon анализирует опасность всех недостатков инфраструктуры, а не только уязвимостей, с точки зрения возможных путей атак и централизованно приоритизирует все меры защиты

Делай меньше — защищай больше



Результат, подтвержденный на практике



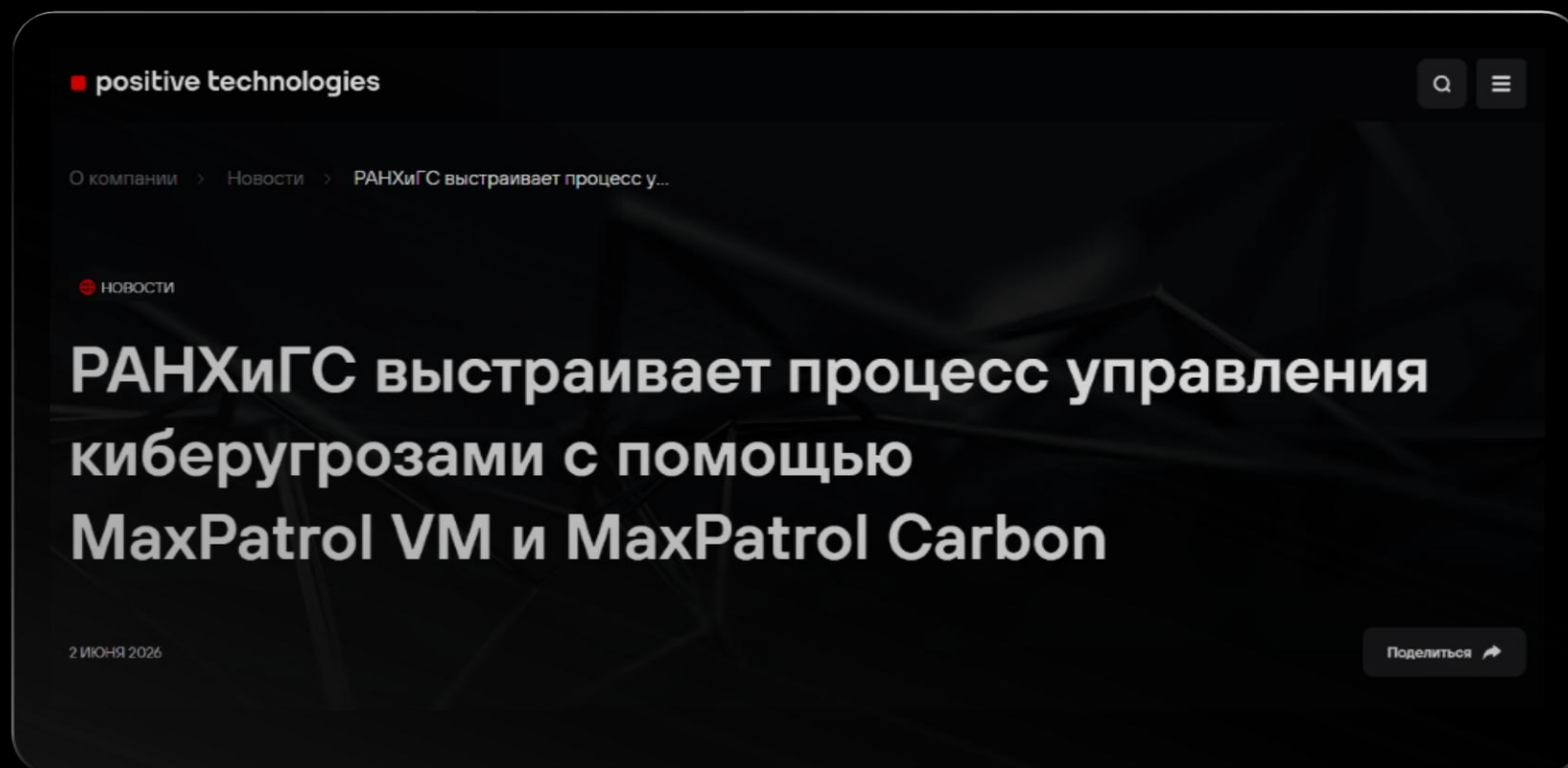
MaxPatrol Carbon
позволяет командам ИБ и ИТ

СНИЗИТЬ*
трудозатраты
более чем
на 80%

и сосредоточить усилия
на ключевых мерах для повышения
киберустойчивости компании

* Благодаря точной приоритизации задач. На основе результатов первых внедрений

История успеха



Узнать больше
ptsecurity.com

Предвидеть атаки и управлять киберустойчивостью — с MaxPatrol Carbon



1

Предвидеть пути атакующих

MaxPatrol Carbon моделирует пути компрометации критически важных систем, оценивает опасность и помогает заранее устранить их

2

Эффективно управлять приоритетами

Централизованно управляет всеми источниками угроз и выстраивает работу с ними в зависимости от степени опасности для бизнеса

3

Контролировать киберустойчивость и оценивать результат

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

Действуйте на опережение с MaxPatrol Carbon

Константин Маньяков

Лидер продуктовой практики
MaxPatrol Carbon



kmanyakov@ptsecurity.com



ptsecurity.com



Официальная страница
MaxPatrol Carbon

ptsecurity.com



Медиаматериалы
о MaxPatrol Carbon

telegra.ph

