



Что стоит за результатами и MaxPatrol VM

Как экспертиза и качество конкурируют с мировыми лидерами



Павел Попов

Руководитель продуктовой
практики инфраструктурной
безопасности

- Специализируюсь на построении процессов управления уязвимостями
- Веду отдел по развитию продуктов инфраструктурной безопасности
- Автор курса по управлению уязвимостями
- Ведущий подкаста «#Кибердуршлаг»
- Лауреат премии «Киберпросвет»
- Лауреат премии «Амбассадоры кибербеза» PHDays 2024

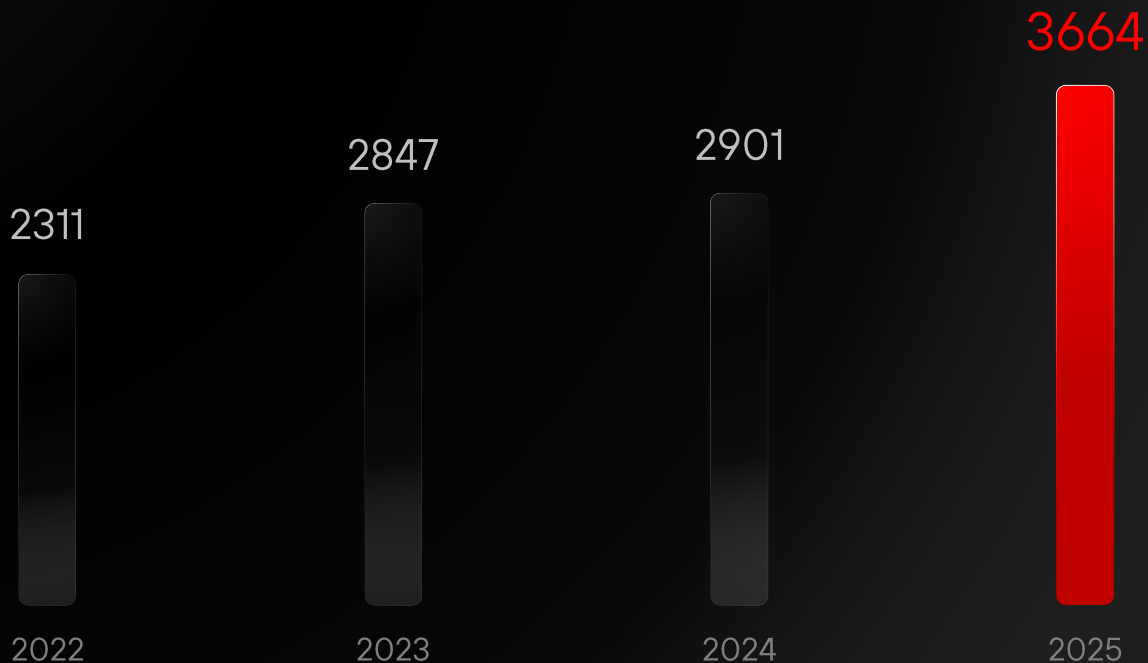


ppopov@ptsecurity.com

Атак меньше не становится



Количество
успешных атак



Последствия

Нарушение
деятельности компании

47%
атак

Утечка чувствительных
данных

64%
атак

ИИ играет на темной стороне



1 Сложное больше не значит редкое

ИИ снижает порог входа
в сложные атаки —
инструменты просты
и доступны даже новичку

2 Защитнику оставляют не недели, а считанные дни

Среднее окно до эксплуатации
уже около 5 дней, часть
атакующих цепочек теперь
собирается за минуты,
а не за недели

3 Не единичное, а серийное производство

Почти каждая третья
уязвимость начинает
эксплуатироваться в первые
сутки после раскрытия

За каждым взломом
все еще стоят
известные
уязвимости
и мисконфигурации...

32% атак

реализуются через
эксплуатацию уязвимостей
на периметре



Количество уязвимостей выходит из-под контроля



База данных уязвимостей NVD*

Сейчас:

362 тыс.
записей

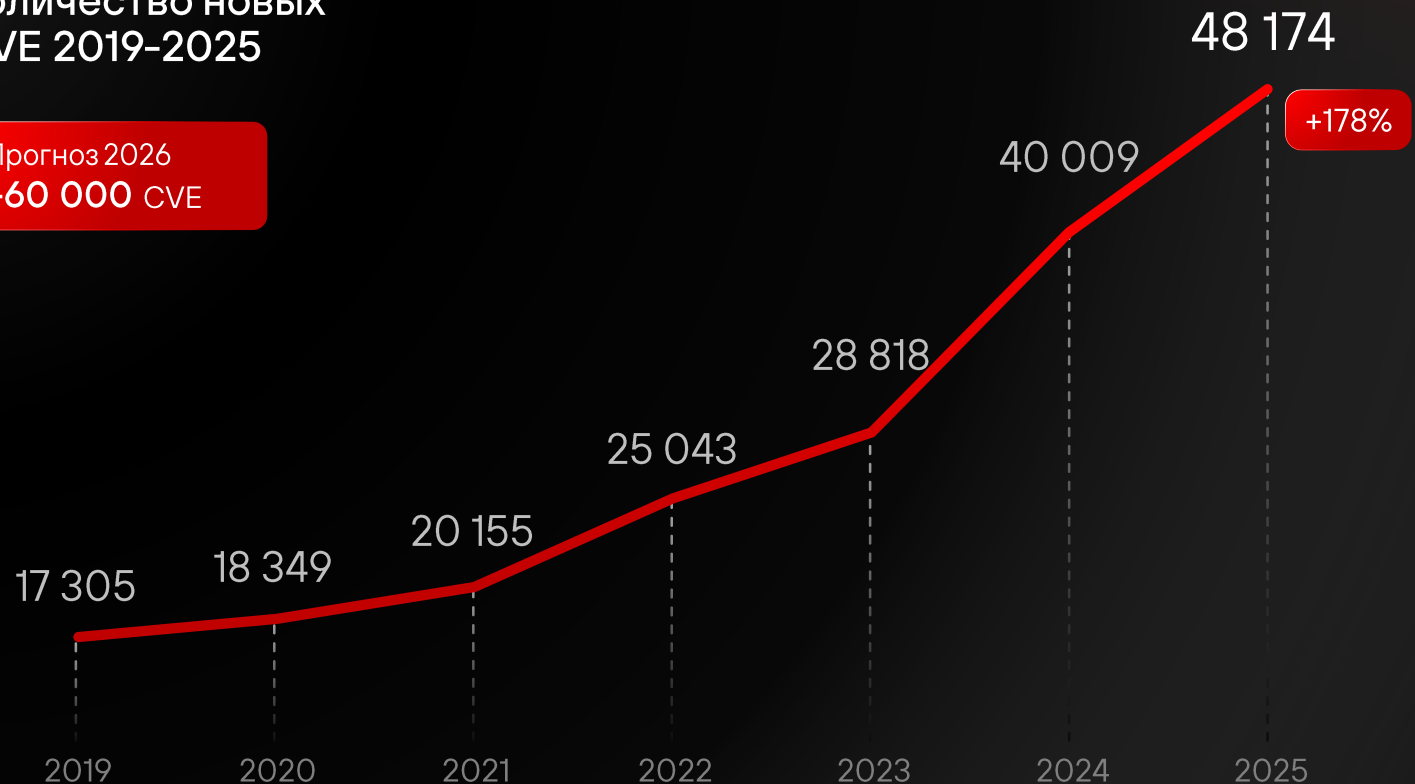
Прогноз
Gartner**
до 2030:

1 млн
записей

*Национальная база данных уязвимостей
(National Vulnerability Database, NVD): nvd.nist.gov
**Исследование аналитического агентства Gartner
[Tech FutureSight: Preemptive Cybersecurity Is the Only Way to Secure Emerging AI Attack Surfaces](#)

Количество новых
CVE 2019-2025

Прогноз 2026
+60 000 CVE



В чем проблема сложность?



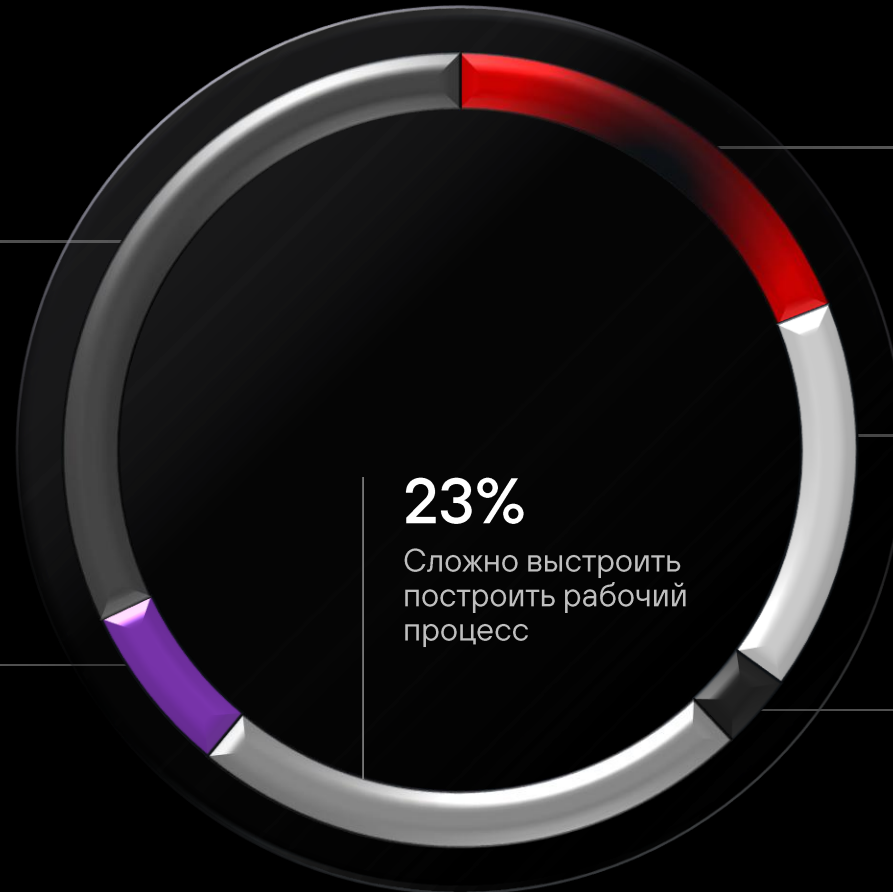
По данным опроса
AIM Live, апрель 2026

32%

ИТ не успевает или не хочет
закрывать уязвимости

7%

Сложно приоритизировать
уязвимости



23%

Сложно выстроить
построить рабочий
процесс

19%

Нет нормальной
инвентаризации активов

16%

Нет денег на покупку
VM-платформы

3%

Нет квалификации
и опыта

В чем проблема сложность?



8 АПРЕЛЯ 2026

КИБЕРБЕЗОПАСНОСТЬ

Эволюция управления уязвимостями
(Vulnerability Management)

9 АПРЕЛЯ 2025

КИБЕРБЕЗОПАСНОСТЬ

Как выстроить процесс
управления уязвимостями

17 АПРЕЛЯ 2024

КИБЕРБЕЗОПАСНОСТЬ

Управление
уязвимостями

17 МАЯ 2023

КИБЕРБЕЗОПАСНОСТЬ

Практика эффективного
управления уязвимостями 2023



Эволюция продуктов Positive Technologies



Эволюция сканера уязвимостей



сканер



Vulnerability Assessment

Эпизодическое сканирование
в режиме черного ящика
для выявления уязвимостей
и открытых портов

1998 год

Сертификация ФСТЭК закончилась в конце 2025 года
Техподдержка — до конца 2030 года

Эволюция сканера уязвимостей



XSpider

сканер



Vulnerability Assessment

Эпизодическое сканирование в режиме черного ящика для выявления уязвимостей и открытых портов

1998 год



XSpider PRO

Сканер PRO



Advanced vulnerability assessment

Периодическое сканирование в режиме черного и белого ящика, сравнение результатов, организация процесса патч-менеджмента

2025 год

Новинка — XSpider PRO

- В 2025 году запустили новый сканер уязвимостей, взявший все лучшее от своих предшественников
- Для инфраструктур до 500 хостов
- Сертификат ФСТЭК ожидается до конца лета 2026 года
- Актуальная экспертиза от MaxPatrol VM

Эволюция подхода к управлению уязвимостями



MaxPatrol 8

Legacy VM



Legacy vulnerability management

Регулярное сканирование в режиме черного и белого ящика, сравнение результатов, организация процесса патч-менеджмента

2009 год

Основные возможности

- Периодическое сканирование в режиме черного ящика для выявления уязвимостей и открытых портов
- Выпуск отчетов по задачам
- Сканирование веб-приложений
- Экспертиза от вендора
- Оценка опасности уязвимостей по шкале CVSS

Эволюция подхода к управлению уязвимостями



Legacy VM



Legacy vulnerability management

Регулярное сканирование в режиме черного и белого ящика, сравнение результатов, организация процесса патч-менеджмента

2009 год



MaxPatrol VM



MaxPatrol HCC

RBVM



Risk-based vulnerability management

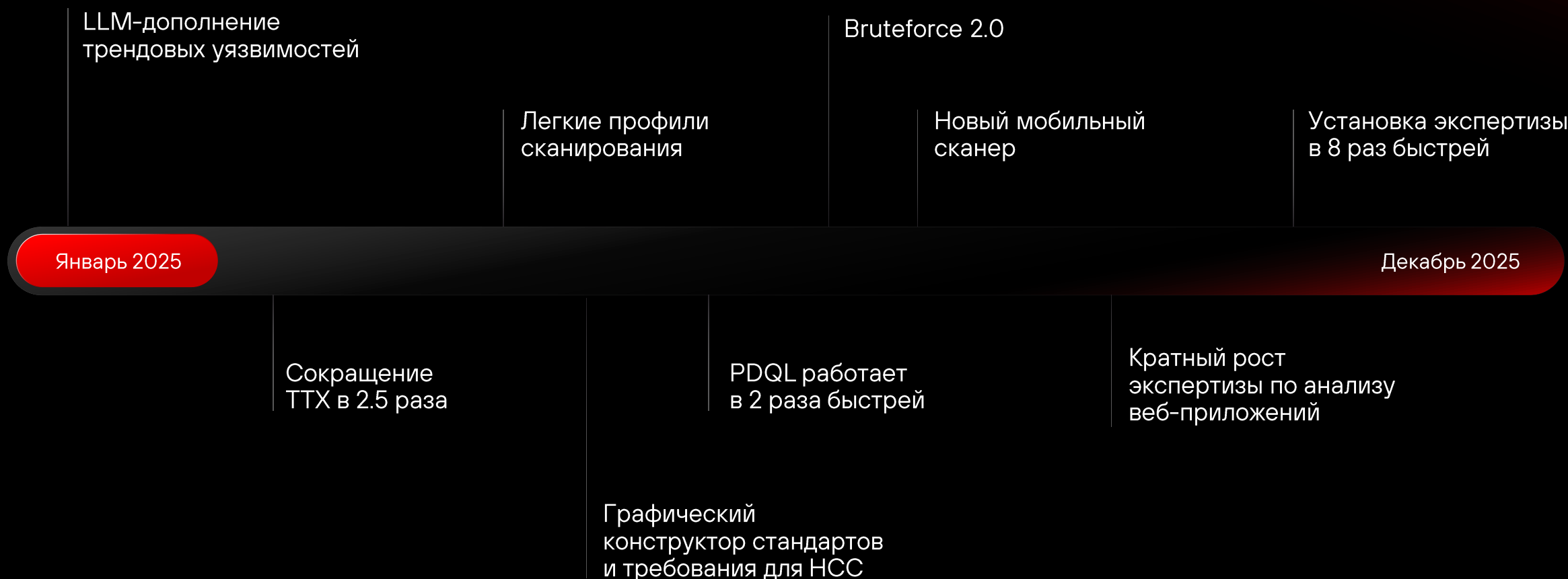
Управление активами, приоритизация уязвимостей исходя из риска: учитываются важность активов, контекст бизнеса, наличие эксплойтов и вероятность атаки

2021 год

Преимущества управления уязвимостями нового поколения

- Полная инвентаризация
- Учет важности узлов
- Расчет достижимости активов
- Хранение информации в системе
- Обработка результатов и расчет уязвимостей в режиме реального времени без повторного сканирования
- Несколько вариантов приоритизации уязвимостей
- Контроль SLA на устранение уязвимостей
- Кастомный комплаенс-контроль

Что уже появилось в 2025 году





Расчет
уязвимостей
в 2 раза быстрее

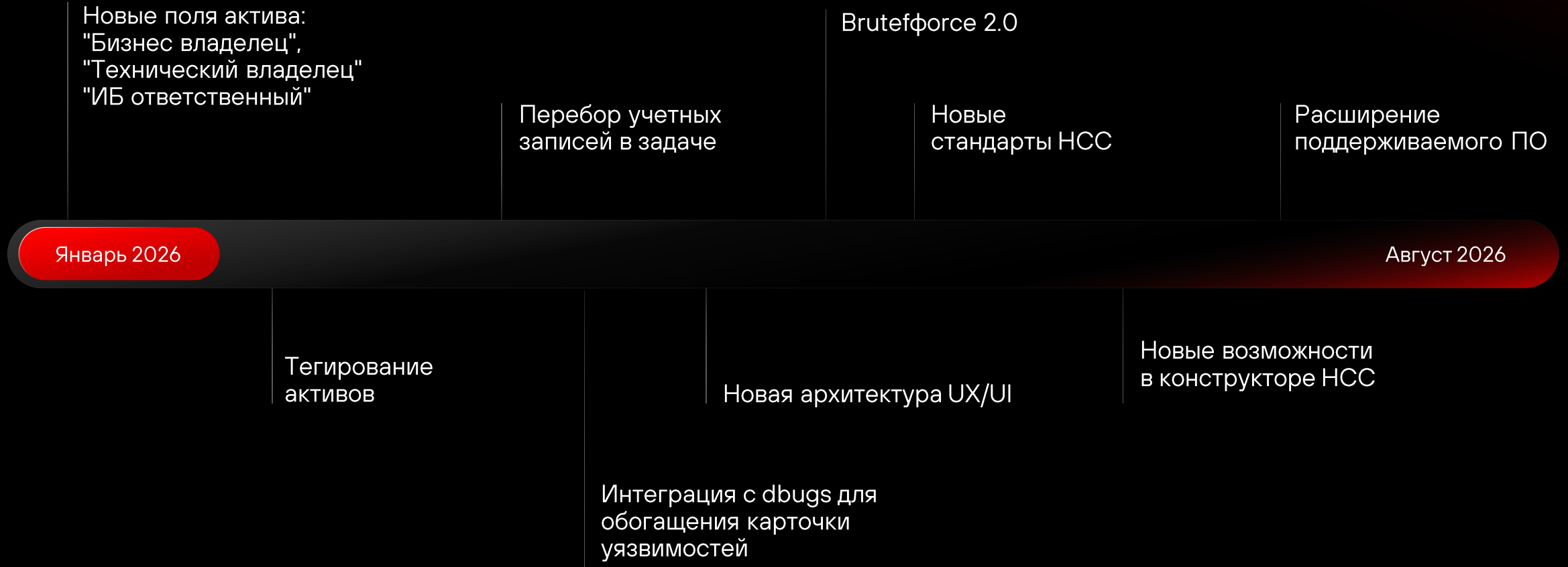


Скорость работы
интерфейса
быстрее **в 7 раз**

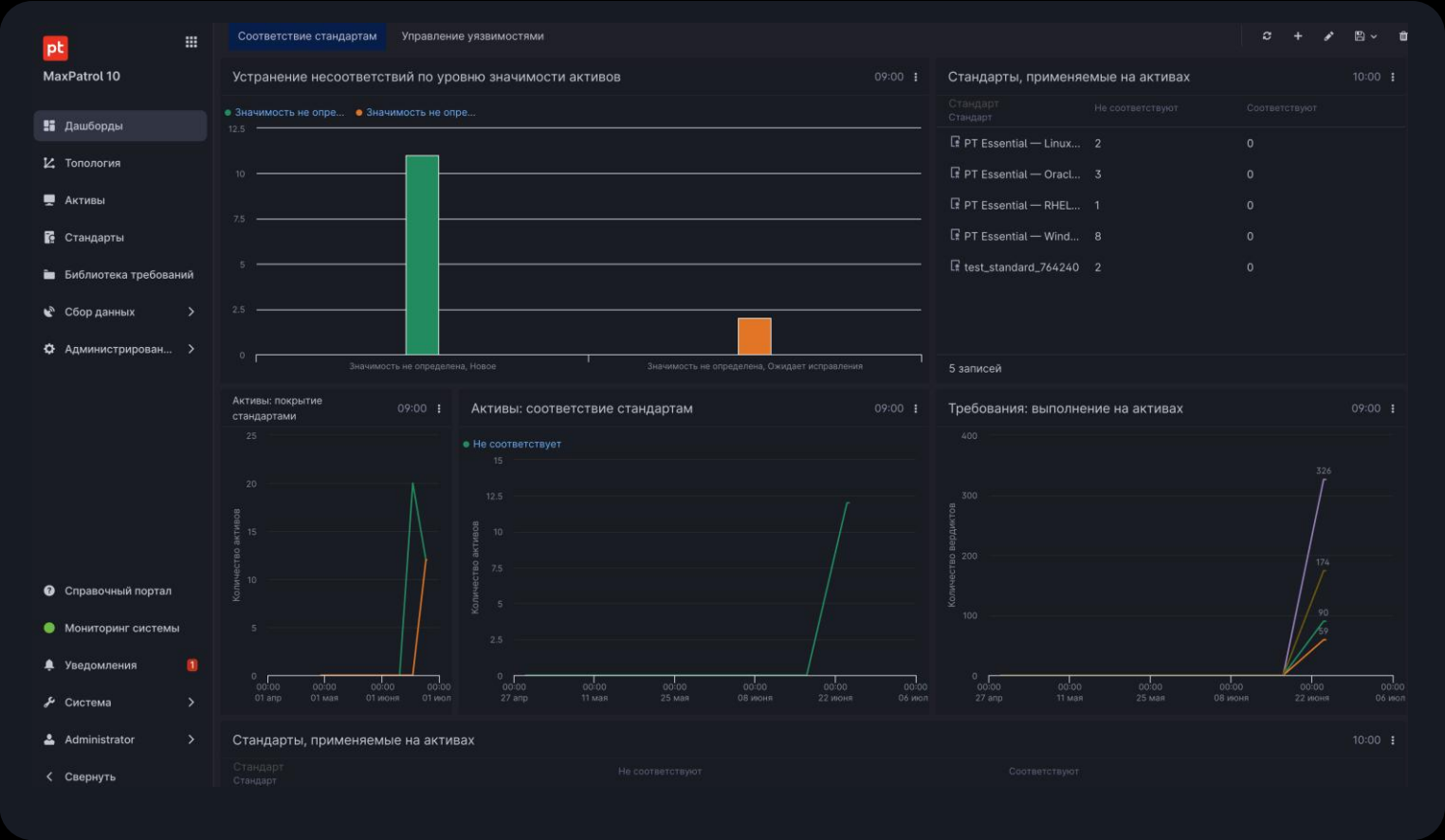


**В 3 раза
меньше ложных
срабатываний**

Что будет в 28 релизе



Новый интерфейс



Метки активов



Метки активов ×

Добавляйте метки к активам и используйте их для поиска и фильтрации

[Добавить](#)

| Изменить метки

< Новая метка

Название

Метка 1

Добавить описание

Цвет

Метк...

Метк...

Метк...

Метк...

Метк...

Метк...

Метк...

Метк...

Метк...

Метк...

Создать

Отмена

» **10.0.49.24** ↺ ⋮

Метки активов ×

Добавляйте метки к активам и используйте их для поиска и фильтрации

[Добавить](#)

| Изменить метки

Метка 1 ×

Обнаружен 07 июня, 03:13 → Последнее обновление 16 июня, 20:33
→ Устаревает 14 сентября, 20:33

Значимость не определена

Владелец актива



Бизнес-параметры

Значимость 🛡️ Не определена

Администратор безопасности

Бизнес-владелец

Технический владелец

Сводка

Уязвимости

Конфигурация

Информация о системе

OS IOS

Бизнес-параметры

Админи...	Не определен
Бизнес-...	Не определен
Техниче...	Не определен

Учетные записи



Параметры сбора данных

Импорт Экспорт

Профиль Windows Audit

Сканирование систем: 1

Windows: Через WMI, RPC и RE

Расширение сбора данных

Windows

Через WMI, RPC ...

Учетная запись win1

Дополнительные учетные записи для подбора win2 win3

Система автоматически подберет подходящую учетную запись

Показывать дополнительные параметры

Учетные записи

+ Добавить учетную запись

Группы

win1

win2

win3

Все учетные записи

1

2

Учетные записи вне групп

MaxPatrol HCC

Конструктор стандартов и требований



Создание требования

Общие параметры

Название

Описание

Важность

None

Проверяемый компонент ?

(OperatingSystem.CheckPoint.CheckPointHost)

Идентификатор требования

Правило именования проверяемого компонента

ccrule

```
1 /* Запрос данных
2 Опишите логику проверки требования
3 Подсказка */
4   checkData
5   {
6   }
7
8 /* Команды и конфигурации
9 Укажите результаты выполнения требования
10 Необязательный раздел
11 Подсказка */
12   howToFix (FAIL_NON_COMPLIANT)
13   {
14   }
15
```

Проверить на активе

Создать

Отмена

MaxPatrol HCC

Конструктор стандартов и требований



Копирование требования

Общие параметры

Название

Установить срок действия пароля (копия)

Описание

Если срок действия пароля не установлен или слишком велик, у злоумышленника будет больше времени на то, чтобы подобрать пароль и воспользоваться им для скрытого доступа к системе.

Важность

🔥 Medium

Проверяемый компонент ?

(Core.Host).Softs[Software.oVirtProject.oVirtEngi...

Идентификатор требования

oVirtBased.VirtualizationManager.AccountAndAcce

Правило именования проверяемого компонента

@Entity.Name+*+@Entity.Version

ccrule

```
1 params (  
2   @max_days int  
3 )  
4  
5 assert (  
6   @PasswordExpiration <= @max_days  
7 )  
8  
9 computability {  
10  return notNull(@Entity.GlobalUserSettings.PasswordPolicy.MaxDays)  
11 }  
12  
13 checkData {  
14  var @PasswordPolicyMaxDays = dynamic {  
15    PasswordExpiration = @Entity.GlobalUserSettings.PasswordPolicy.MaxDays  
16  };  
17  
18  filterByParameters(@PasswordPolicyMaxDays);  
19  
20  if (@ComplianceCheckContext.NonCompliantRows.Any())  
21    return FAIL_NON_COMPLIANT;  
22  
23  return SUCCESS;  
24 }  
25  
26 howToFix (FAIL_NON_COMPLIANT)  
27 {  
28  addHowToFix(  
29    format(  
30      "ovirt-aaa-jdbc-tool settings set --name=PASSWORD_EXPIRATION=  
31      @max_days  
32    )  
33  );  
34 }
```

Проверить на активе

Создать

Отмена

Приказ ФСТЭК № 117



Новый приказ ФСТЭК России № 117

Введены новые
обязательные требования

- Контроль конфигураций ИС (п. 34б, 37)
- Управление уязвимостями (п. 34в, 38)

MaxPatrol VM

- Автоматизация управления уязвимостями
- Инвентаризация и работа с ИТ-активами
- Соответствие установленным срокам устранения
- Интеграции с внешними источниками

MaxPatrol HCC

- Контроль параметров, конфигураций, стандартов
- Проверка ИС на отклонения от регламентов и стандартов безопасности
- Поддержка отечественного ПО



Защита периметра

Ваш периметр — это иллюзия



Интернет знает о вашей инфраструктуре больше, чем вы сами

90%

Компаний опираются на устаревшую CMDB



Хакер видит реальную топологию сети



Периметр прозрачен для атакующих

185.122.39.8

Неуправляемые внешние активы



70% киберинцидентов происходят через неуправляемые внешние активы, полностью обесценивая инвестиции в защиту классического периметра:

70%

Организаций

подвергались атакам, которые начинались с использования shadow-it*



74%

Организаций

столкнулись с инцидентами безопасности из-за неизвестных или неуправляемых активов (shadow IT)**

* Источник: Security Hygiene and Posture Management Report (Enterprise Strategy Group, ESG)

** Источник: Attack Surface Risk Management (Trend Micro Global Study)

Сегодня вы защищаете свою инвентаризацию, а не реальную поверхность атаки

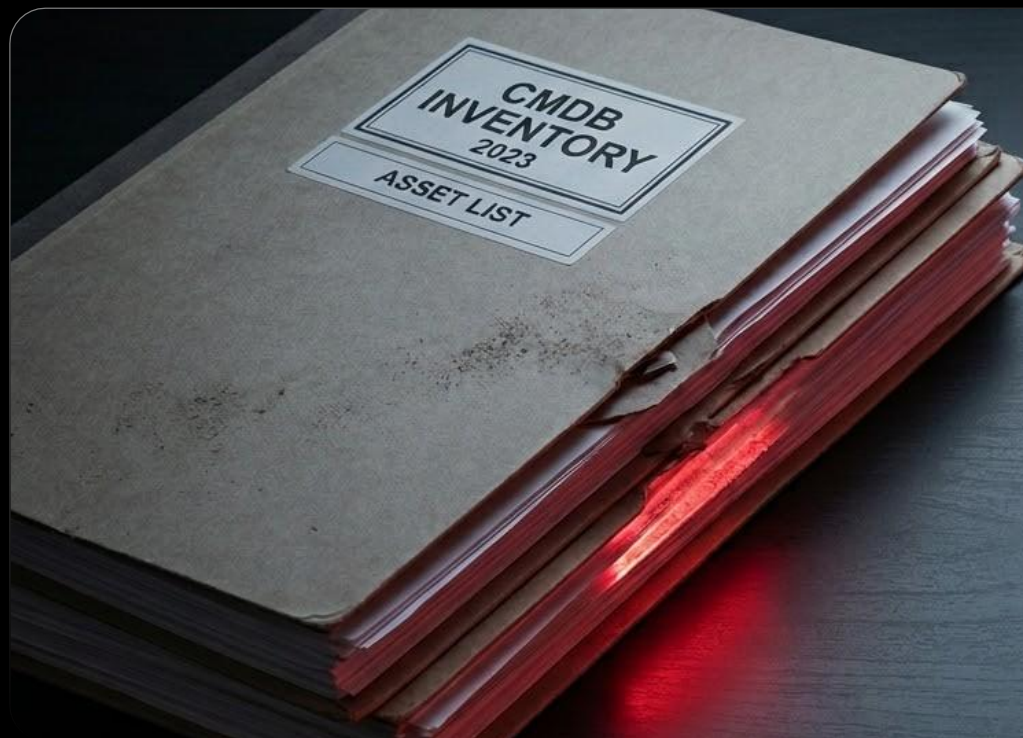


Вчера

Сканирование
известного
списка активов

Сегодня

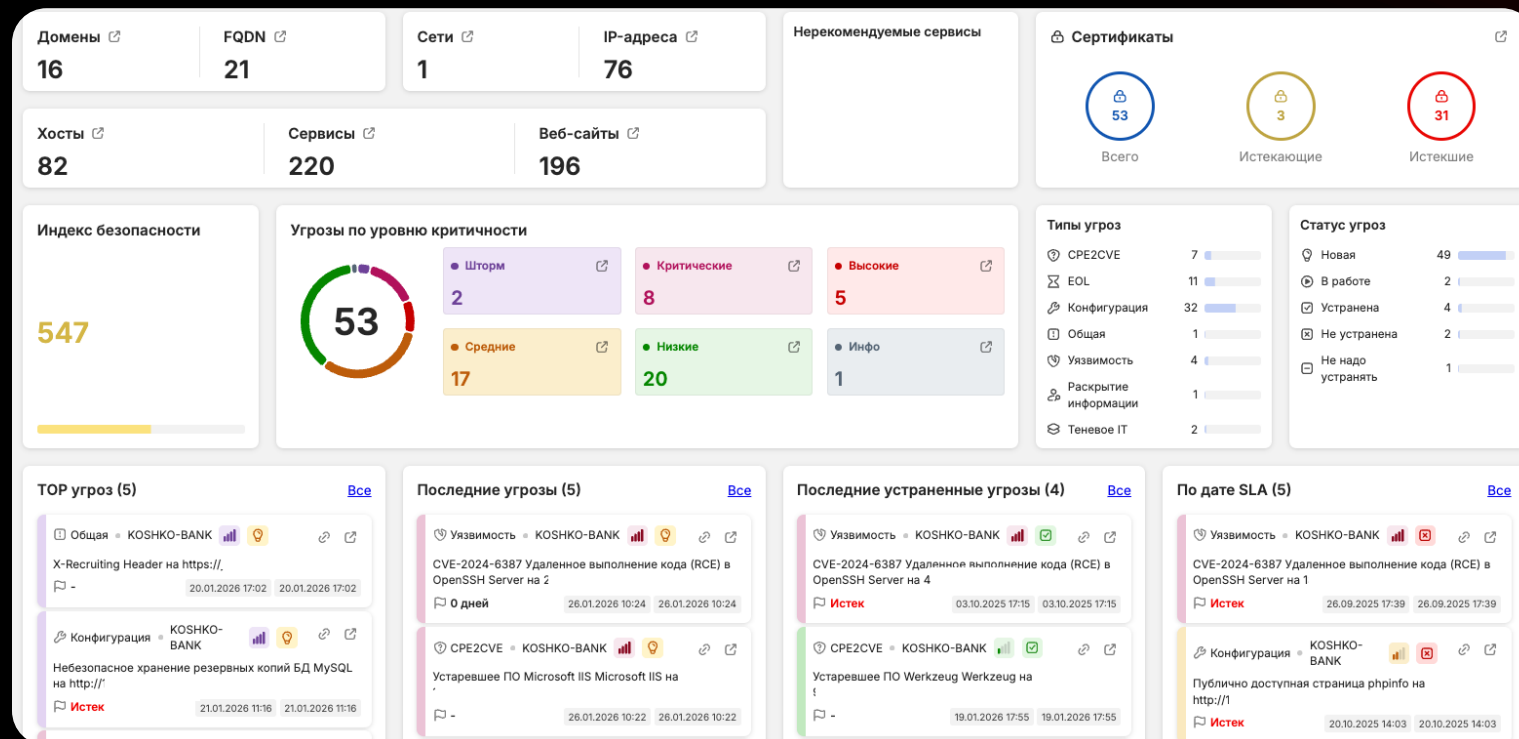
Непрерывный
анализ реальной
поверхности



Решение, позволяющее держат периметр в безопасности

Обеспечивает постоянный
мониторинг ИТ-ресурсов

Позволяет получать информацию
о потенциально уязвимых
ресурсах в течение 24 часов
с момента публикации
технических подробностей
об уязвимости



Пять ключевых преимуществ

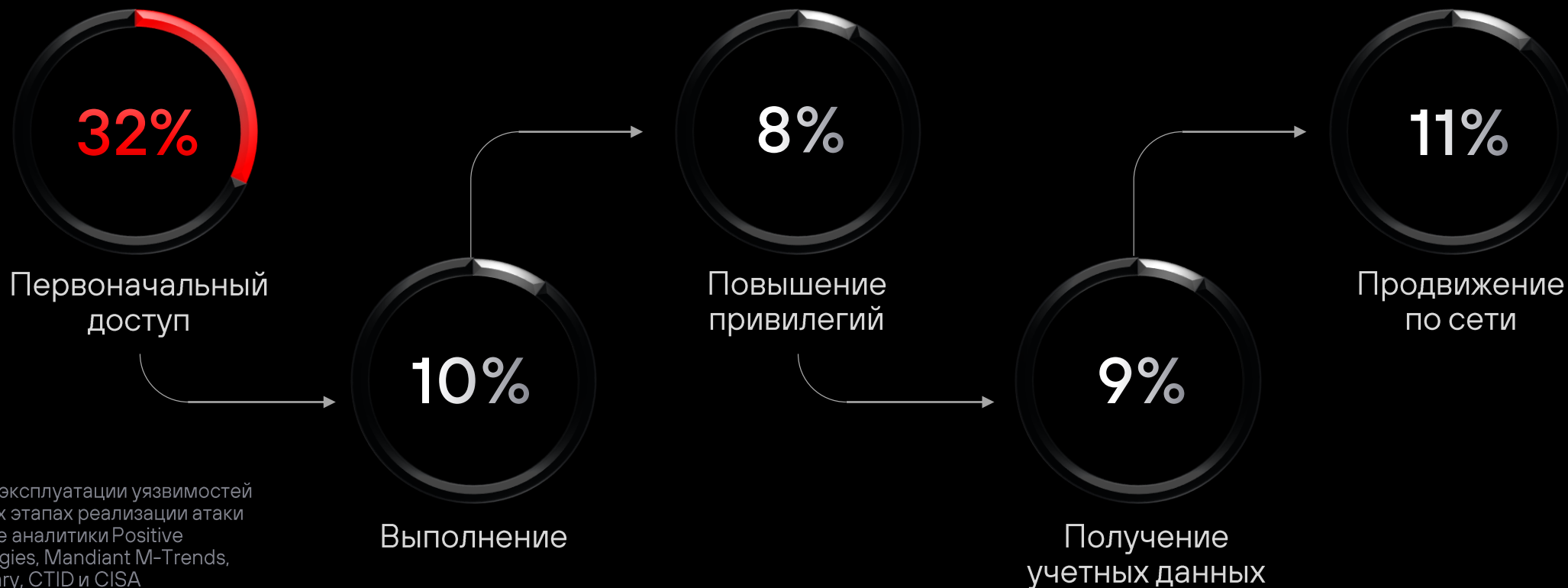


HO



Не уязвимостями
единными путь
хакера выложен...

Уязвимость — это одна из многих возможностей на пути атакующего



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.

Exposure Management – путь к киберустойчивости

УРОВЕНЬ ЗРЕЛОСТИ ИБ →

СТРАТЕГИЧЕСКИЙ

Threat
Exposure
Management

БИЗНЕС

Risk-Based
Vulnerability
Management &
EASM

ТЕХНИЧЕСКИЙ

Vulnerability
Assessment



ВИДИМОСТЬ УГРОЗ →

Активы – Уязвимости – Мiskonфигурации –
Учетные записи – Сетевой доступ



Задачи Exposure Management

- Превентивный анализ всей площади атаки
- Прогнозирование путей развития атак и оценка их опасности
- Управление всеми угрозами, а не только уязвимостями
- Приоритизация задач на основе бизнес-рисков
- Контроль и повышение уровня киберустойчивости

Методология STEM



Continuous Threat Exposure Management (STEM) — методология непрерывного управления воздействием кибератак от Gartner (2022)

Gartner

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

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



MaxPatrol Carbon:

видеть все, устранять главное



1 Предвидеть пути атакующих

MaxPatrol Carbon моделирует пути компрометации критически важных систем, оценивает их 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

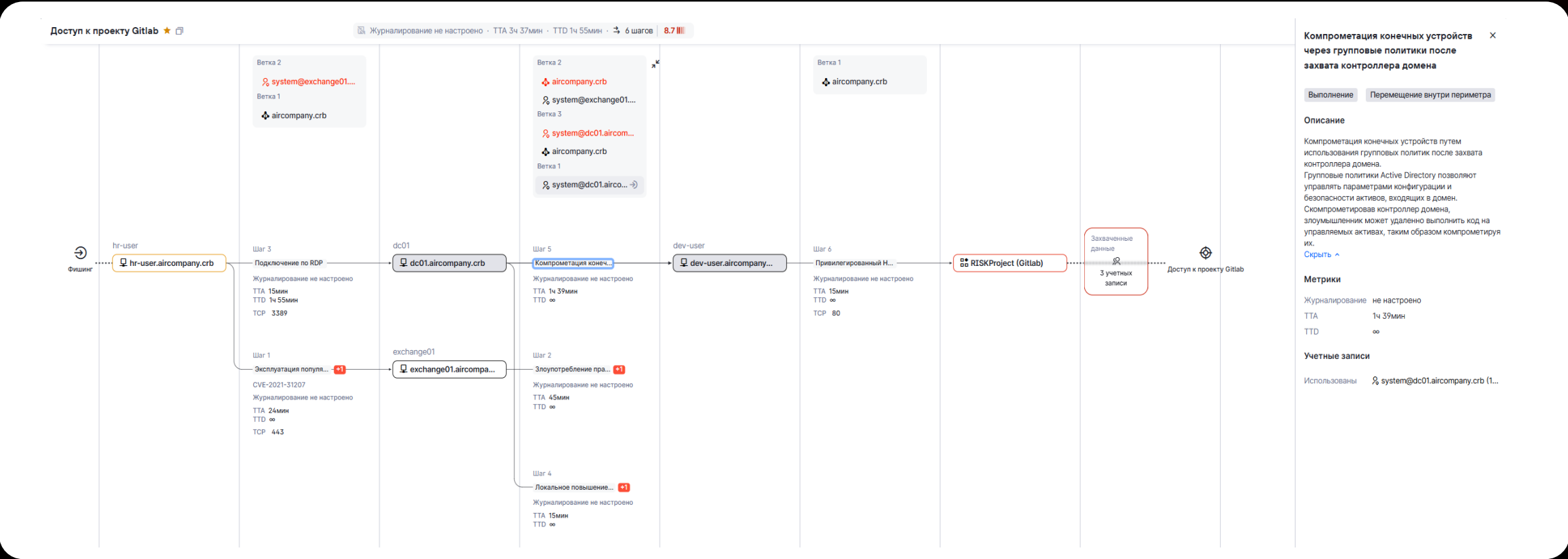


Пример маршрута атаки



Визуализация каждого маршрута атаки с учетом

- Последовательности шагов
- Времени атаки (ТТА) и времени обнаружения (ТТД)
- Действий злоумышленника
- Захваченных учетных записей
- Рекомендаций по нейтрализации



Компрометация конечных устройств через групповые политики после захвата контроллера домена

Выполнение

Перемещение внутри периметра

Описание

Компрометация конечных устройств путем использования групповых политик после захвата контроллера домена. Групповые политики Active Directory позволяют управлять параметрами конфигурации и безопасности активов, входящих в домен. Скомпрометировав контроллер домена, злоумышленник может удаленно выполнить код на управляемых активах, таким образом компрометируя их.

Скрыть

Метрики

Журналирование не настроено

ТТА 1ч 39мин

ТТД ∞

Учетные записи

Использованы system@dc01.aircompany.crb (1...

Делай меньше — защищай больше



Результат, подтвержденный на практике первых внедрений MaxPatrol Carbon — для киберустойчивости важен не объем задач, а их приоритет

Уязвимости

Количество активов 5 000

Всего (RCE, LPE)

720 400

Трендовые

36 900

На критически важных активах
(высокой значимости)

2300

На маршрутах атак

1600

На опасных маршрутах атак

110

С эксплойтом на опасных маршрутах атак

23



MaxPatrol VM



MaxPatrol Carbon

2 узловых актива,
через которые проходят
большинство опасных
маршрутов

Статистика на одном из проектов внедрения MaxPatrol Carbon

2 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

У нас есть решение для каждой задачи

pt

PT EASM



External Attack Surface Management

- Полная видимость внешнего периметра
- Снижение нагрузки на ИБ
- Фокус на внешних угрозах
- Непрерывный пентест
- Раннее выявление IoC и утечек
- Дашборды и KPI

XSpider PRO

- Полноценный взгляд изнутри на небольшую инфраструктуру
- Быстрый старт
- Pentest + Audit
- Актуальная экспертиза



Vulnerability Scanner



MaxPatrol VM

- Экспертный взгляд изнутри при масштабировании инфраструктуры
- Весь процесс в одном решении
 - Управление активами
 - Вариативность сканирования
 - Бизнес-контекст
 - Комплаенс-контроль



Risk-based VM



MaxPatrol Carbon

- Полная видимость площади атаки
- Моделирование маршрутов атак
- Приоритизация всех угроз на основе бизнес-рисков
- Оценка эффективности принятых мер
- Управление уровнем киберустойчивости



Exposure management



От управления уязвимостями

к

управлению киберугрозами

Задай
вопрос
спикеру





Спасибо за внимание!

Павел Попов

Руководитель группы инфраструктурной безопасности