



Умный радар внешнего периметра

Видит все, что доступно из интернета глазами атакующего,
и помогает устранить риски до атаки

Ваш периметр — это иллюзия



Интернет знает о вашей инфраструктуре
больше, чем вы сами

90%

Компаний опираются
на устаревшую CMDB



Хакер видит реальную
топологию сети



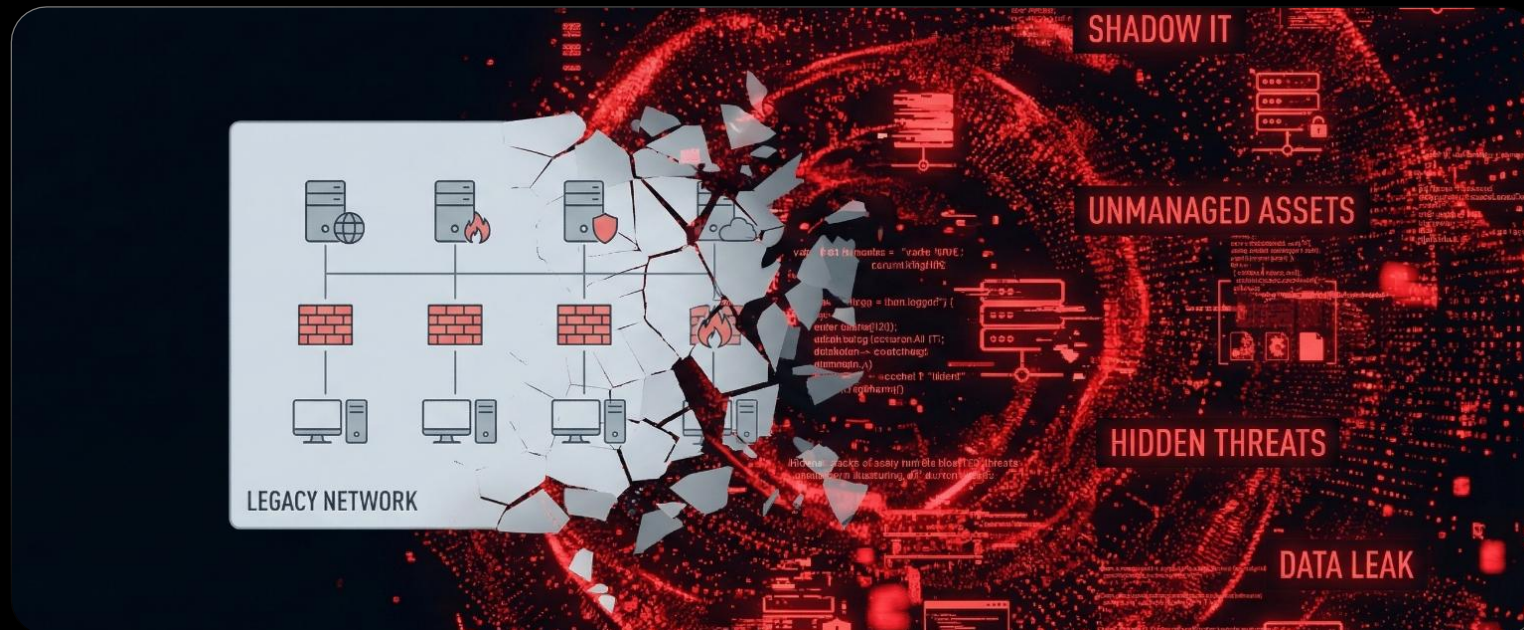
Периметр прозрачен
для атакующих

185.122.39.8

Компания тратит миллионы на эшелонированную защиту, SIEM и SOC, выстраивая неприступную крепость



- > Многомиллионные инвестиции на софт для ИБ
- > Проведение комплаенс-аудитов для галочки
- > Закрыв все порты — защищен!

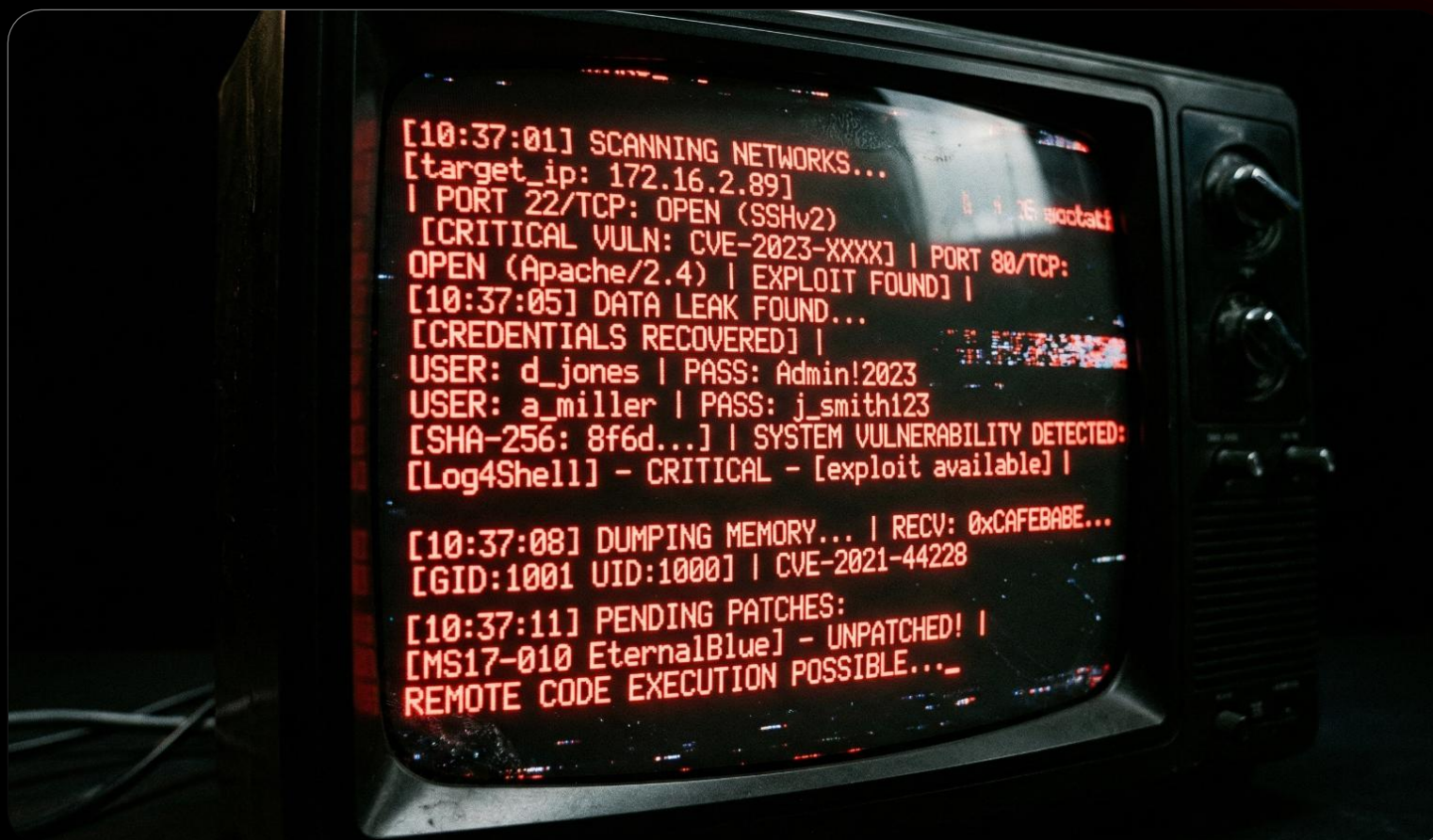


Для взлома атакующим не всегда нужна 0-day



Им нужен забытый
сервер на периметре
или незакрытая уязвимость:

- > Одна из главных целей — забытые активы
- > Известные критически опасные уязвимости, например, BDU:2025-10114



За каждым взломом стоят известные уязвимости и мисконфигурации

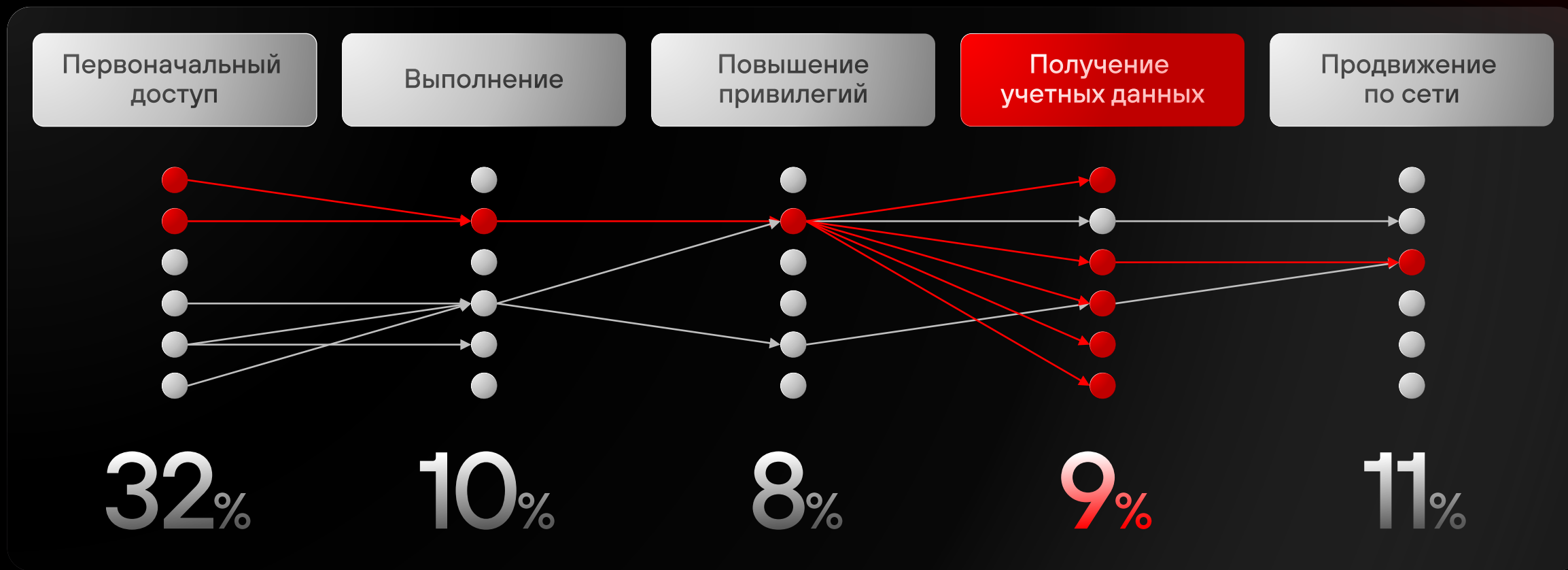


32% атак

реализуются через
эксплуатацию уязвимостей
на периметре



Эксплуатация уязвимостей



Процент эксплуатации уязвимостей на разных этапах реализации атаки
(на основе аналитики Positive Technologies, M-Trends, CTID, CISA)

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)

Облака, микросервисы и удаленка уничтожили физический периметр



Изменения происходят быстрее, чем обновляется инвентаризация:

- > DevOps: развертывание быстрее контроля
- > Бесконтрольный рост числа микросервисов
- > Ошибки конфигурации



**Разрыв между тем, что ИТ-отдел
думает, что защищает,
и тем, что реально «торчит»
в интернете, — это критически
опасный бизнес-риск**

Сегодня вы защищаете свою инвентаризацию, а не реальную поверхность атаки



Вчера

Сканирование
известного
списка активов

Сегодня

Непрерывный
анализ реальной
поверхности



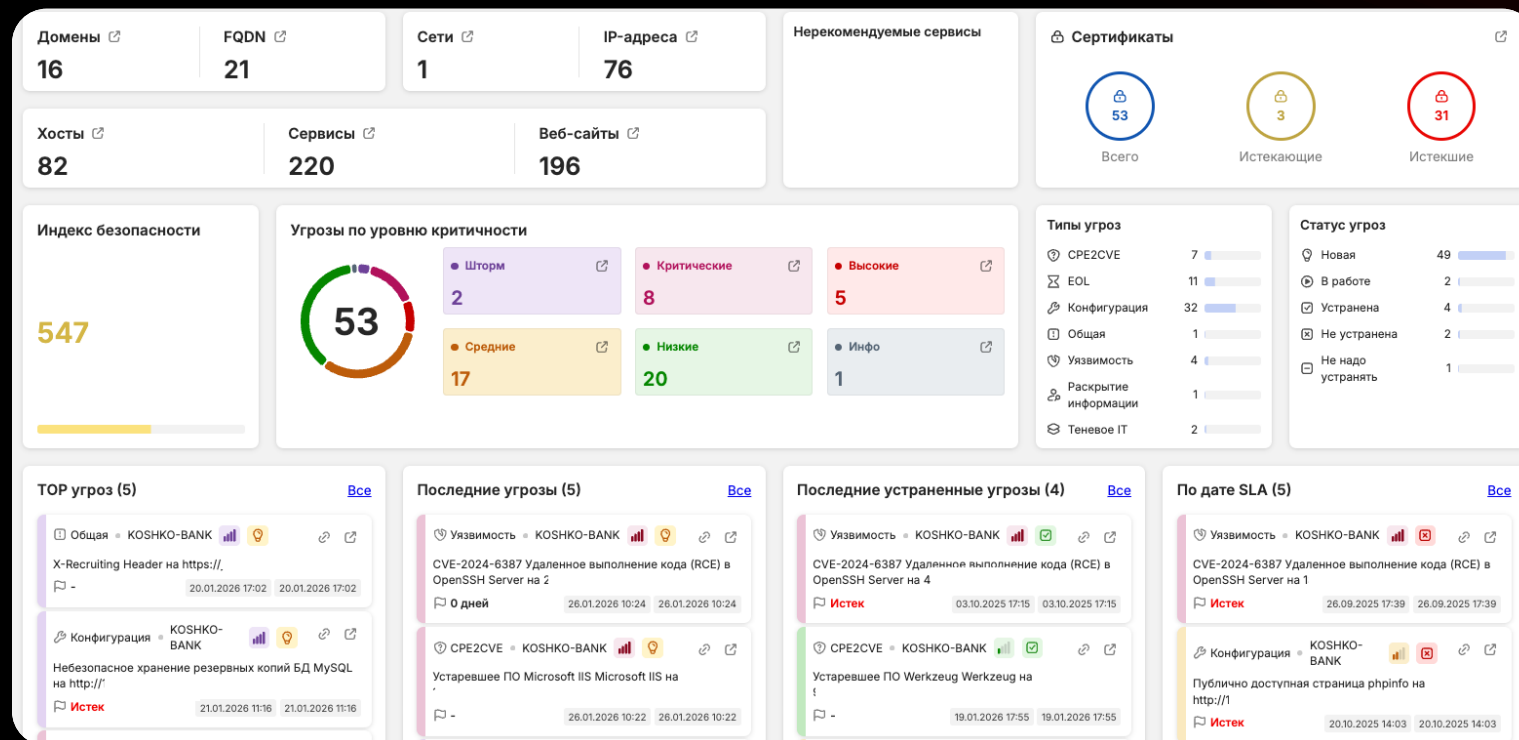


PT EASM

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



PT EASM — подтвержденная экспертиза



Непрерывный поиск, атрибуция и приоритизация угроз

3 года

непрерывного сканирования
всего Рунета

>110 млн

уникальных сервисов и узлов
идентифицировано

Эксклюзивное
знание специфики
Рунета



Учитываем информацию из единого
реестра российского ПО и базы
данных уязвимостей (БДУ ФСТЭК)

Взаимодействуем
с отечественными вендорами
и регуляторами

47 млн

IP-адресов сканируется
ежедневно

150 млн

FQDN сканируется
ежедневно

Пять ключевых преимуществ



А что внутри?



NetSlicer

Интеллектуальный OSINT-агент для картографирования внешнего периметра: доменов, IP-адресов, сертификатов, связей



TuShcan (Cokmap)

Комплекс ускоренных ML-сканеров портов и приложений.

97% точности при 1-2% трафика от брутфорса



OnoTolle AI

Автоматический триаж и группировка уязвимостей, снижение шума, генерация задач



Offensive SOC

Непрерывный пентест с участием экспертов. Углубляемся в инфраструктуру и добираемся до сложных цепочек



Dirbruter, Authbruter, Domain Auditor

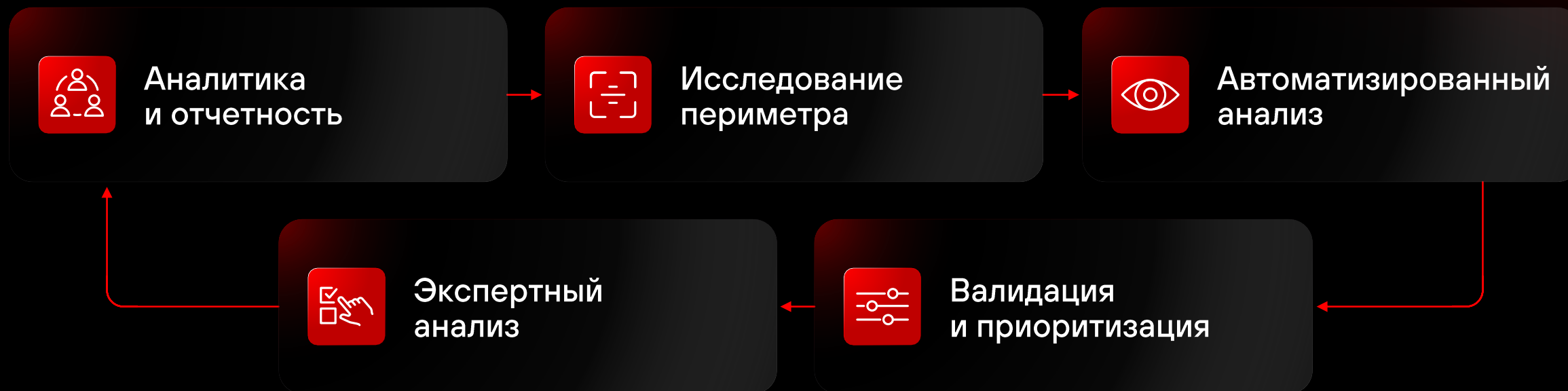
Модули перебора директорий, учетных данных и инструмент отслеживания сроков владения доменами



Brand & Leak Monitoring

Фишинг, утечки, бренд-клоны — автоматическое обнаружение и уведомления

Непрерывный процесс



Ваш периметр



Что делаем:

1

Активный и пассивный
сбор доменов,
поддоменов, URL

2

Обратный
поиск по ASN,
net_prefix

3

Полнотекстовый
поиск по ключевым
словам в баннере

4

Поиск
по схожести
контента

Что получаем:

1

Весь свой
сетевой
периметр

2

Теневые тестовые,
Dev-ресурсы (в том
числе у подрядчиков)

3

Забывшие
и неактуальные DNS-
записи с IP-адресов
на внешних хостингах

4

Фишинговые ресурсы,
ресурсы подрядчиков

Автоматизированный анализ



Что делаем:

1

Проверки на более чем 10 000 уязвимостей и ошибок конфигураций

2

Проверки на наличие известных индикаторов компрометации (IoC)

3

Профилирование инструментов под наиболее значимые ресурсы, выполнение углубленного анализа:

- Поиск конечных точек веб-приложений и API
- Поиск чувствительных данных
- Проверки с применением фаззинга и мутаций
- Проверки надежности используемых паролей, токенов доступа и т. п.

Автоматизированный анализ



Что получаем:

1

Несоответствие Security Compliance:

- ПО, не рекомендуемое к публикации
- Неподдерживаемое ПО (EOL)
- Уязвимости, определенные по версии ПО

2

- Выявленные ошибки конфигурации
- Уязвимости, определенные с помощью безопасных проверок

Обработка результатов (триаж): AI и аналитики



L1

OnoTolle AI обрабатывает все выявленные и не верифицированные ранее угрозы ИБ для фильтрации ложноположительных срабатываний

L2

- Верифицирует по наиболее критически опасным угрозам ИБ
- Корректирует уровень опасности
- Формирует достоверные PoC
- Проверяет корректность рекомендаций

L3

- Оценивает возможности расширения атаки через выявленные угрозы, потенциальный ущерб от реализации всей цепочки атаки
- Исходя из результирующего уровня опасности принимает решение о внеплановом уведомлении заказчика

Обработка результатов (триаж)



Список угроз из интерфейса

- Классификация угроз
- Работа со статусами
- Дедлайн устранения (SLA)
- Приоритизация и оценка опасности

Тип	Статус	Критичность	Адрес	IP-адрес	Порт	Название	Срок устранения
Общий	Новая	Шторм	https://js	2	443	X-Recruiting Header на https://js	-
Конфигурация	Новая	Шторм	http://1	1:	80	Небезопасное хранение резервных копий БД MySQL на http://1	2026-01-23
CPE2CVE	Новая	Критическая	1	-	22	Устаревшее ПО OpenSSH OpenSSH на 1	-
Уязвимость	В работе	Критическая	4	4	22	CVE-2024-6387 Удаленное выполнение кода (RCE) в OpenSSH Server на 4	2025-10-05
Уязвимость	Новая	Критическая	http://1	1:	8081	CVE-2024-4577 Удаленное выполнение кода (RCE) в PHP CGI на http://1:8081	2025-12-28
Уязвимость	Не устранена	Критическая	1:	1:	222	CVE-2024-6387 Удаленное выполнение кода (RCE) в OpenSSH Server на 1:222	2025-09-28
CPE2CVE	Новая	Критическая	1:	1:	443	Устаревшее ПО nginx nginx на 1:443	-
Конфигурация	Не надо устранять	Критическая	https://l	2	443	Публично доступный robots.txt файл на https://l:443	-
CPE2CVE	Новая	Критическая	-	143	443	Устаревшее ПО PHP PHP на 143:443	-
CPE2CVE	Новая	Критическая	19	1:	443	Устаревшее ПО Microsoft IIS Microsoft IIS на 19:443	-
Конфигурация	Новая	Критическая	http://	1:	80	Небезопасное хранение резервных копий БД MySQL на http://:80	2025-11-22
Уязвимость	Новая	Критическая	22	2	2	CVE-2024-6387 Удаленное выполнение кода (RCE) в OpenSSH Server на 22:2	2026-01-28

Обработка результатов (триаж)



Карточка угрозы

- > Детальный отчет по угрозе
- > Описание
- > Доказательства возможной эксплуатации
- > Рекомендации по устранению

Назад

Скачать отчет

Небезопасное хранение резервных копий БД MySQL на http://1

Опубликована: 21.01.2026 (5 дней назад)

Тип: Конфигурация • Критичность: Шторм • Статус: Новая

Теги: Угроза +

Небезопасное хранение резервных копий базы данных MySQL может привести к раскрытию конфиденциальной информации. Атакующий может использовать полученную информацию для дальнейшего развития целенаправленной атаки.

Подробности

Эксплуатация

В ходе исследования системы был найден файл копии базы данных MySQL, доступный по следующему URL-адресу:

http://1

cURL-команда для верификации:

curl -X 'GET' +https://www.c

На скриншоте ниже приведена демонстрация наличия в веб-приложении данного недостатка безопасности:

```
curl -X 'GET' +https://www.c
{
  "url": "http://1",
  "http_status": 200,
  "headers": {
    "Date": "Tue, 23 Dec 2025 07:35:00 GMT",
    "Server": "Apache/2.4.25 (Debian)",
    "Last-Modified": "Tue, 23 Aug 2022 14:40:40 GMT",
    "ETag": "\"13d-5e6e98c598ab\"",
    "Accept-Ranges": "bytes",
    "Content-Length": "317",
    "Content-Type": "application/x-sql"
  },
  "body": "CREATE TABLE users (\n  userId int,\n  username varchar(255),\n  password varchar(25)\n);\nINSERT INTO users (userId, username, password) VALUES (1, 'admin', 'admin');\nINSERT INTO users (userId, username, password) VALUES (2, 'test', 'test');\nINSERT INTO users (userId, username, password) VALUES (3, 'Bob', 'hunter2');"
```

Раскрытие конфиденциальной информации БД

Рекомендации по устранению

- Удалить файлы резервных копий из публично доступных директорий веб-сервера.
- Ограничить доступ к конфиденциальной информации.

Ссылки на источники 1

<https://cwe.mitre.org/data/definitions/922.html>

CVSSv3 7.5

EPSS -

1f

http://1

Идентификатор	-
Вендор	Apache Software Foundation
Продукт	Apache HTTP Server
IP-адрес	1
Порт	80
Протокол	tcp
Адрес	http://1

Первое наблюдение 21.01.2026

Последнее наблюдение 21.01.2026

SLA 1 день

Дедлайн 22.01.2026 23:59

Статус Истек

Хронология 5 дней

Новая : 21.01.2026 11:16 (5 дней)

Непрерывный пентест



Команда пентеста



- OSCP, OSWE, OSCP, OSEP, OSCP, OSWE, OSCP, OSEP, WAPT, BSCP, CBVH, WAPT, BSCP, CBVH
- Регулярно в топе программ BugBounty
- Более 70 уязвимостей, зарегистрированных в CVE, БДУ
- Богатый опыт проведения проектов по анализу защищенности

Построение цепочек атак

Соединяем разрозненные данные об угрозах с низким уровнем риска в сценарий полной компрометации, который виден только эксперту

Автоматизация проверок

Добавляем новые детектирующие правила и шаблоны, делая следующий цикл проверки точнее

Адаптивный анализ

Адаптируемся к нестандартным ситуациям, бизнес-процессам клиентов и выявляем угрозы, незаметные для автоматических сканеров

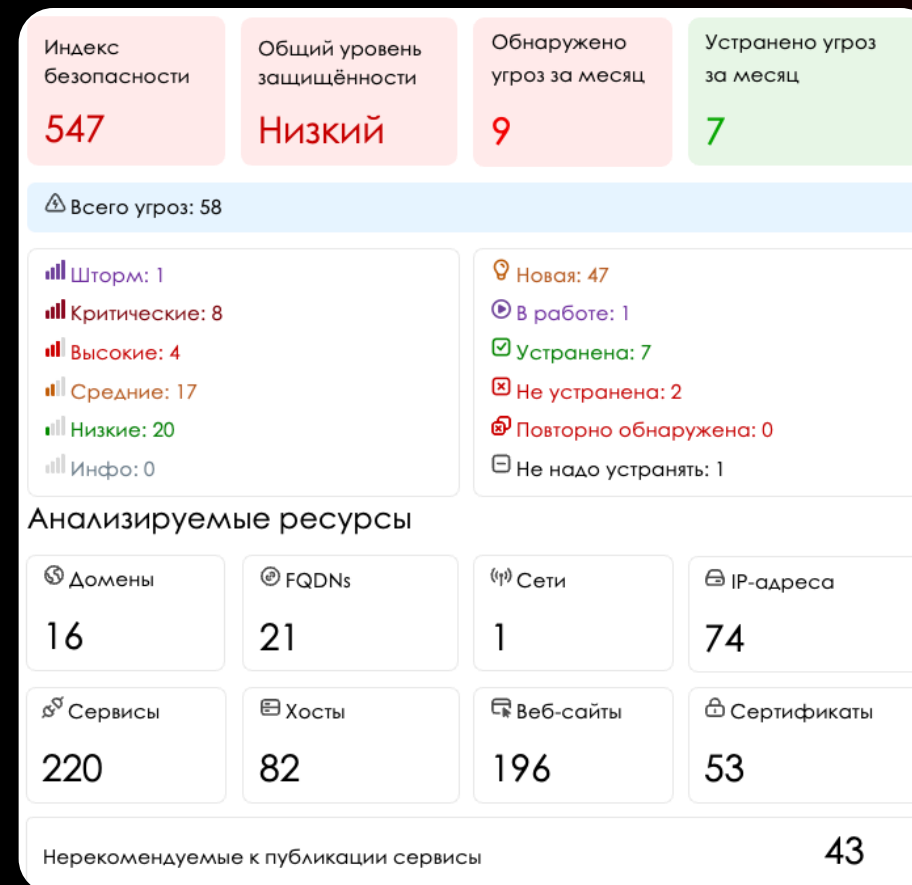


Аналитика и отчетность



Автоматизированные отчеты

- > Сводный по компании
- > Детализированный по узлу
- > Детализированный по веб-приложению
- > Детализированный по угрозе, общий по всем угрозам



Аналитика и отчетность



Автоматизированные отчеты о верифицированных угрозах

- Общее описание и статистика
- Сводная таблица по всем группам активов
- Подробная информация с возможностью гибкой кастомизации
- Поддержка API для автоматизированной отправки данных

KOSHKO-1: CVE-2024-6387 Удаленное выполнение кода (RCE) в OpenSSH Server на 1:222

Опубликована 26.09.2025
Тип Уязвимость
Критичность Критическая
Статус Новая

Описание
Уязвимость гонки состояний в обработке сигналов сервера с glibc позволяет неавторизованному удаленному злоумышленнику выполнить произвольный код с привилегиями root. Последовательность сигналов, что может привести к выполнению кода. OpenSSH является широко используемым сервером SSH для удаленного доступа. Уязвимость затрагивает версии OpenSSH от 8.5p1 до 9.8p1 на платформах, использующих glibc. OpenBSD не уязвим, так как реализацию syslog_r() в обработке сигналов.

CVSSv3 9.7

Вендор	openbsd
Продукт	openssh
IP-адрес	1
Порт	222
Протокол	tcp
URL	1
Обнаружена	1

Первое наблюдение 26.09.2025

Последнее наблюдение 26.09.2025

Эксплуатация

Для верификации отправить TCP-запрос на порт SSH сервера 1:222 и проверить banner, содержащий строку с OpenSSH и версией, например 'SSH-2.0-OpenSSH_9.8p1'. На скриншоте ниже приведена демонстрация определения уязвимой версии ПО.

Рекомендации по устранению

Обновить OpenSSH Server до версии 9.8p1 или выше. Временно можно установить параметр LoginGraceTime=0 в конфигурации sshd для уменьшения окна атаки, но это увеличивает риск DoS-атак и должно использоваться только как временная мера. Ограничить доступ к SSH с помощью файрвола и мониторинга подозрительной активности.

Ссылки на источники

<https://www.qualys.com/resshion-cve-2024-6387/>
<https://www.qualys.com/2024/07/01/cve-2024-6387/resshion.txt>
<https://nvd.nist.gov/vuln/detail/CVE-2024-6387> <https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/resshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server> <https://www.qualys.com/resshion-cve-2024-6387/>
<https://www.upguard.com/blog/openssh-vulnerability-cve-2024-6387>
<https://www.rapid7.com/db/vulnerabilities/openbsd-openssh-cve-2024-6387/>
<https://www.runzero.com/blog/openssh-servers/>
<https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/resshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server>

PT EASM vs решение класса VS, VM



PT EASM

- Находит IP-адреса, о которых вы не подозревали
- Обеспечивает анализ защищенности периметра с точечной экспертизой
- Минимум фич — максимум эффективности
- Не заменяет VS или VM-решение, так как предназначен только для периметра

VS, VM-система

- Сканер инфраструктуры ищет уязвимости только на тех узлах, IP-адреса которых вы ему дали
- Тriage уязвимостей, приоритизация — на стороне вендора
- В основном используются для поиска уязвимостей внутри инфраструктуры
- Нужны для построения процесса VM

PT EASM vs автопентест



PT EASM

- Работает в ширину. Непрерывно, 24/7/365, оценивает ваш цифровой след только на общедоступных ресурсах, не проходя внутрь инфраструктуры
- Поиск, триаж, приоритизация уязвимостей и контроль их устранения на периметре

Автопентест

- Бьет вглубь по известной цели в моменте
- Автоматизированный инструмент для имитации достижения целевых систем внутри инфраструктуры



PT EASM vs комбайны сканеров



1

- Комбайны обычно увеличивают объем сигналов и ручной разбор
- Наш контур ориентирован на результат: единая картина активов и рисков, снижение шума, подтверждение критически значимых находок, управление статусами и метриками процесса устранения

2

«Под капотом» — Nessus. Tenable прямо пишет, что в большинстве случаев ее продукты нельзя экспортировать и реэкспортировать в Россию и Республику Беларусь без лицензии BIS.

Даже без юридических тонкостей, устойчивость зависит от:

- доступа к плагинам, обновлениям, подписке (без этого качество падает очень быстро)
- наличия официальной поддержки (инциденты, уязвимости самого движка, обновления ОС, совместимость)
- санкционных ограничений (риски внезапного рубильника)

3

Практически это может превратиться в «сканер есть, детект вчерашний»

**PT EASM не отменяет
потребность в ваших
системах, а становится
глазами для VM,
предоставляя актуальную
информацию**

Еще один сенсор для применения концепции STEM

Радар раннего обнаружения для SOC

Ключевые преимущества PT EASM



1 Полная видимость периметра

Ежедневный OSINT всех активов, включая shadow IT и ресурсы подрядчиков

2 Снижение нагрузки на ИБ клиента

AI-триаж, экспертная верификация и поддержка

3 Фокус на реальных угрозах

Собственная система оценки и приоритизации угроз (CybVSS, RWD)

4 Непрерывный пентест

Вместо разового пентеста — контроль внешнего периметра 365 дней в году

5 Раннее выявление IoC и утечек

Мониторинг индикаторов компрометации и скомпрометированных учетных записей

6 Дашборды и KPI

Готовые дашборды, прозрачные метрики и автоматизированные отчеты

Лицензирование



Базовая лицензия с
SLA 10 дней



Лицензия на
расширения SLA до 5
или 1 дня



Контроль и анализ
результатов
мониторинга с SLA 10,
5 или 1 день



Дополнительные
модули

Главный параметр лицензирования — активы
(IP+FQDN+DNS имена)

Лицензирование



> Базовая лицензия

Состав программного продукта непрерывного мониторинга поверхности атак внешнего периметра организации (базовая лицензия):

- контроль 5000 распространенных портов TCP и UDP 1 (один) раз в неделю
- контроль 65 535 портов TCP 1 (один) раз в 2 (две) недели
- контроль 1000 портов UDP 1 (один) раз в 2 (две) недели
- идентификация программного обеспечения и его проверка на соответствие требованиям безопасности
- выявление уязвимостей серверного программного обеспечения
- контроль изменений во внешнем периметре организации
- уведомление о критически опасных уязвимостях 10 (десять) рабочих дней с момента возникновения уязвимости
- срок использования в течение 12 (двенадцати) месяцев

> Программный модуль выявления и уведомления о выявленных критически опасных уязвимостях за 1 или 5 дней

- дополняет «Базовую лицензию» и доступен только при ее наличии
- уменьшает SLA до 1 или 5 дней

> Программный модуль контроля выявленных уязвимостей и анализа результатов мониторинга, уведомления о выявленных критических уязвимостях за 1, 5 или 10 дней

Состав программного модуля контроля выявленных уязвимостей и анализа результатов мониторинга:

- выявление дополнительных ресурсов, потенциально связанных с организацией
- верификация наличия ложноположительных и ложноотрицательных результатов мониторинга поверхности атак внешнего периметра организации
- оценка степени опасности уязвимостей
- оценка наличия нарушений требованиям безопасности
- уведомление о результатах мониторинга 10 (десять) дней с момента возникновения уязвимости
- срок использования в течение 12 (двенадцати) месяцев
- дополняет «Базовую лицензию» и доступен только при ее наличии

> Программный модуль интеграции IRP/SOAR

> Программный модуль базы данных и отчетности

> Программный модуль SecOps

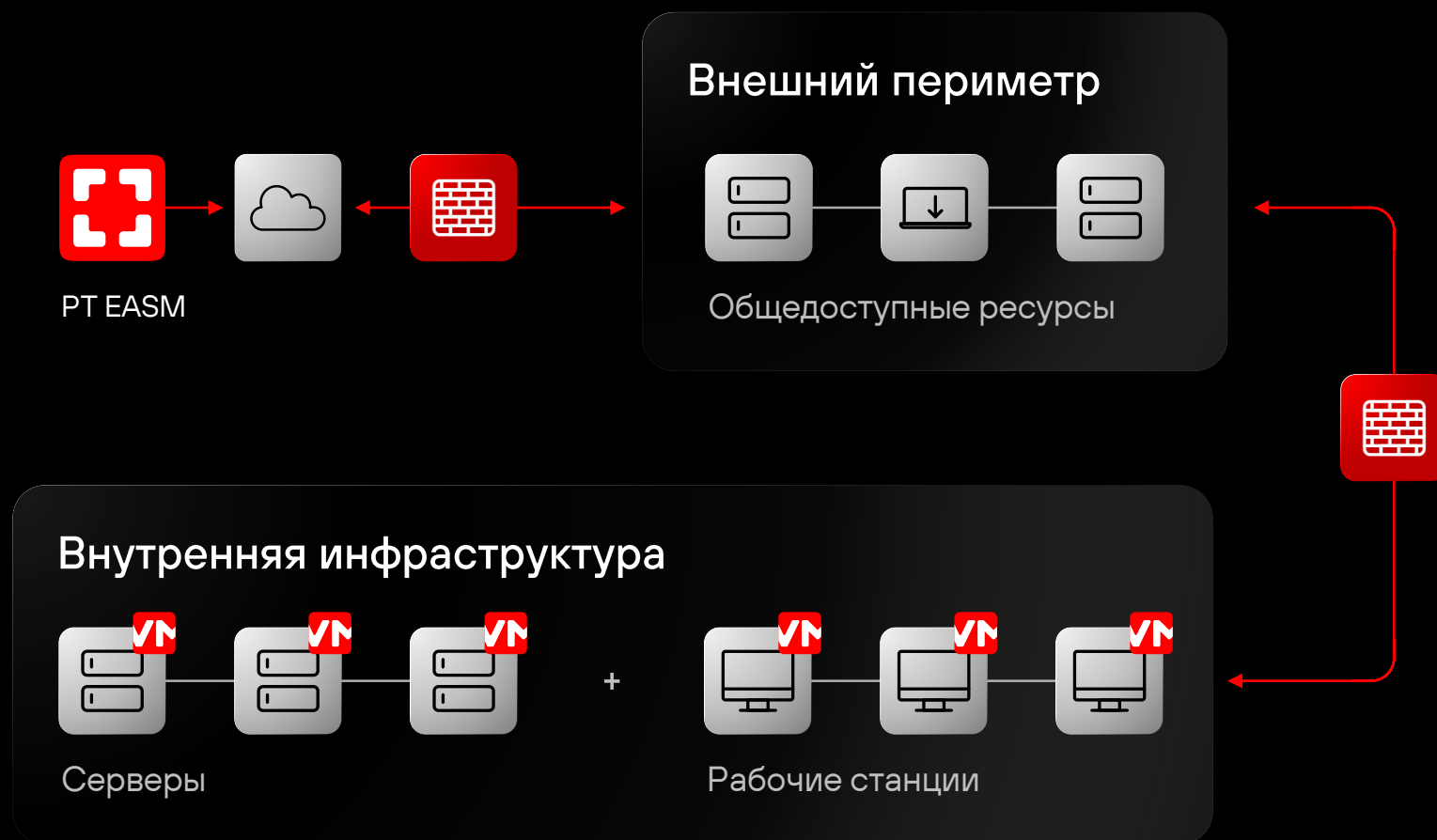
> Программный модуль PentOps

Непрерывное тестирование на проникновение:

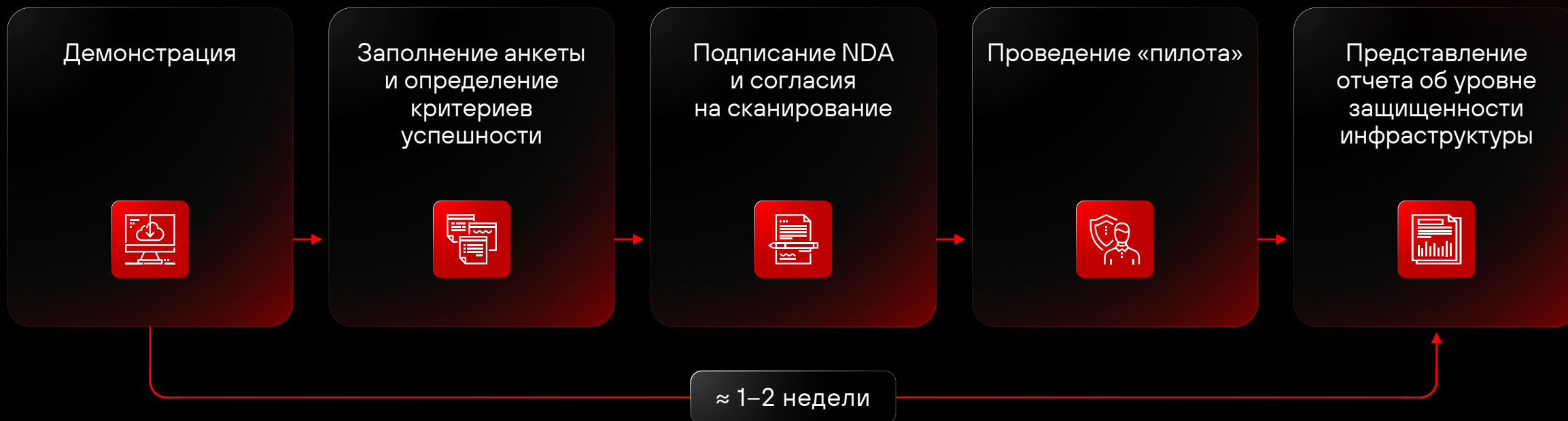
- анализ внешнего периметра организации методом тестирования на проникновение на основе методик PTES Technical Guideline, OWASP Testing Guide v4, ISO/IEC 27001:2013 и OSSTMM
- выявление уязвимостей, которые не могут быть обнаружены базовыми программными продуктами
- проверка возможности эксплуатации уязвимости
- демонстрация возможности развития атак
- срок использования в течение 12 (двенадцати) месяцев
- дополняют «Программный модуль контроля выявленных уязвимостей и анализа результатов мониторинга» и доступны только при его наличии

Главный параметр лицензирования — активы (узлы)

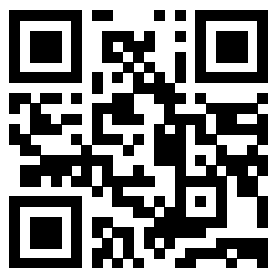
Архитектура



Пилотный проект

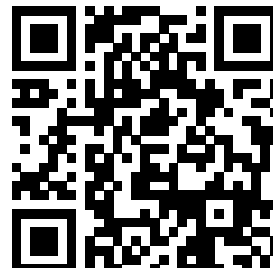


Спасибо!



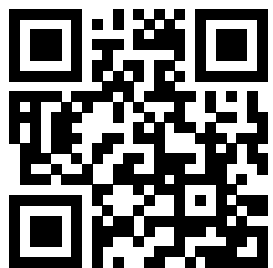
Блог РТ
на Habrahabr

[habrahabr.ru/
company/pt](https://habrahabr.ru/company/pt)



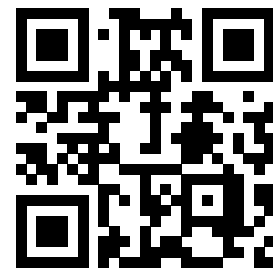
Блог РТ
в Telegram

[t.me/
positive_technologies](https://t.me/positive_technologies)



Блог РТ
во ВКонтакте

[vk.com/
ptsecurity](https://vk.com/ptsecurity)



Блог РТ Investing
в Telegram

[t.me/
positive_investing](https://t.me/positive_investing)



Узнайте больше о PT EASM



pt@ptsecurity.com



ptsecurity.com



Спасибо!