CASUBELL

УЗНАЙТЕ, ЧТО ВИДИТ ИНТЕРНЕТ

Внешняя оценка цифровой поверхности компании

CasuBell помогает обнаружить публичные домены, адреса и сервисы, проверить выбранные риски и понять, какие исправления важнее всего.

НЕ ЕЩЁ ОДИН СПИСОК ПОРТОВ

Это рабочее место для согласованного внешнего обследования: от инвентаризации доступных активов до списка наблюдений и рекомендаций для администратора.

ПОЛЬЗА ДЛЯ ЗАКАЗЧИКА

Понять
какие активы отвечают из интернета

Оценить
какие наблюдения требуют внимания

Действовать
получить приоритеты и меры исправления

Проверка проводится в согласованных границах и с выбранным уровнем активности. Результат — понятная картина внешней поверхности, а не обещание абсолютной безопасности.

01 / ЗАДАЧА

Публичный периметр меняется незаметно

Новый сервис, забытый поддомен или устаревшая панель могут остаться доступными после запуска.

Активы теряются из виду

Команды часто знают основные сайты, но не всегда видят все поддомены, IP и сервисы, которые отвечают снаружи.

Сервисы открыты шире нужного

Порты и административные интерфейсы могут быть доступны из интернета, хотя предназначались для ограниченного круга пользователей.

Версия — ещё не доказательство

Сигнал о возможной CVE полезен, но номер версии может не учитывать исправление производителя или дистрибутива.

Результаты трудно превратить в план

Длинный перечень сканирования без контекста не отвечает на вопрос: что исправлять первым и как снизить риск.

ЧТО ТАКОЕ CASUBELL

CasuBell — панель для инвентаризации и технической проверки внешних активов. Она объединяет обнаружение связанных ресурсов, проверку доступных сервисов и модулей оценки, сохраняет наблюдения и формирует отчёт с приоритетами.

КАКУЮ ЗАДАЧУ РЕШАЕТ

Помогает ответить на три практических вопроса:

1. Что именно доступно извне?
2. Какие наблюдения требуют проверки или исправления?
3. С чего разумно начать и кто должен действовать?

Фокус — на том, что наблюдаемо снаружи. Внутренний аудит и анализ исходного кода являются отдельными видами работ.

02 / ВОЗМОЖНОСТИ

От обнаружения — к контексту

Объём выбирается под область проверки: от одной веб-цели до согласованного списка публичных диапазонов.

Активы и DNS

Поиск связанных поддоменов и доменов, разрешение DNS, текущие и исторические привязки имён к IP.

Порты и сервисы

Проверка доступности выбранных TCP-портов, сетевые отпечатки, баннеры, TLS-сертификаты и настройки.

Веб-поверхность

Проверки заголовков, известных путей и файлов, раскрытых секретов, форм и параметров.

Активные проверки

Выбранные проверки SQLi, XSS, SSTI, SSRF, обхода путей и других классов — только в согласованном объёме.

Инфраструктура

Модули для SSH, SMB, RDP, DNS, UDP-сервисов, оборудования и некоторых административных интерфейсов.

CVE и география

Локальное сопоставление продуктов с базой CVE, контекст KEV/EPSS; опциональная SVG-карта с локальной GeoIP-базой.

ВАЖНО: УРОВЕНЬ АКТИВНОСТИ НАСТРАИВАЕТСЯ

Пассивное определение по DNS, сертификатам и ответам сервисов отличается от активных проверок, которые отправляют специальные запросы приложению. Проверки учётных данных, UDP, загрузок и другие чувствительные модули требуют отдельного согласования и могут влиять на систему.

Для публичного IPv4-сканирования диапазон ограничен 4 096 адресами; широкие диапазоны требуют разбивки и отдельного планирования.

Проверка PHP2Shell в текущей версии неинвазивна: оценивает доступные признаки версии и не исполняет команды на сервере. Это сигнал для сверки, а не доказательство эксплуатации.

03 / РАБОТА

Как устроено обследование

Каждый запуск начинается с определения того, что разрешено проверять и насколько активно.

01 Согласуем область

Домены, IP-диапазоны, URL, исключения, окно работ и контакт для остановки.

02 Подбираем профиль

Выбираем цели и модули. Чувствительные проверки и допустимую нагрузку согласуем отдельно.

03 Запускаем и наблюдаем

Задачи показывают прогресс; запуск можно остановить. Результаты сохраняются в панели.

04 Разбираем и передаём

Отделяем прямые наблюдения от предположений, расставляем приоритеты и формируем отчёт.

ЧТО ПЕРЕДАТЬ ПЕРЕД СТАРТОМ

Цели	Список доменов, URL и публичных диапазонов.
Полномочия	Письменное подтверждение права на проверку всех целей.
Ограничения	Исключения, окно работ, допустимая интенсивность.
Ответственный	Технический контакт и канал экстренной остановки.

Сканирование выполняется только в согласованных границах. Владение доменом не означает разрешения проверять системы третьих лиц, на которые он указывает.

04 / РЕЗУЛЬТАТ

Отчёт с приоритетами и объяснением

Не просто «найдено»: что наблюдалось, насколько это надёжно и что можно сделать дальше.

Краткое резюме

Сводка результатов по целям и сервисам, приоритетные наблюдения и общий контекст риска.

Карточки находок

Цель, сервис, описание, серьёзность, CVSS и связанные сведения об эксплуатации — когда они доступны.

План исправления

Для поддерживаемых типов находок отчёт предлагает практические меры: обновление, ограничение доступа или изменение конфигурации.

Контекст приоритета

Могут учитываться публичный эксплойт, CISA KEV и EPSS. Эти сигналы помогают планировать разбор, но не заменяют оценку владельца системы.

ЧИТАЙТЕ НАХОДКИ С УЧЁТОМ УВЕРЕННОСТИ

Подтверждено

Проверка показала результат на этой цели: например, отражённое значение или доступный файл.

Потенциально

Совпали версия, отпечаток или косвенный признак. Нужна сверка: исправление могло быть включено производителем или дистрибутивом.

Информация

Наблюдение о сервисе или конфигурации для инвентаризации и укрепления защиты.

КАК ЗАКАЗЧИК ПОЛУЧАЕТ ОТЧЁТ

В панели CasuBell открывается отдельная HTML-страница отчёта. Её можно распечатать или сохранить в PDF через диалог браузера — для всех сохранённых результатов либо по конкретной цели.

01 Приоритеты

02 Описание риска

03 Сведения по цели

04 Рекомендации

Отчёт отражает сохранённые наблюдения. Это не анализ исходного кода, не полный сетевой журнал и не гарантия отсутствия уязвимостей.

05 / ГРАНИЦЫ

Честная оценка начинается с ясных ожиданий

Внешнее обследование — полезный слой контроля, но не замена всем видам аудита безопасности.

Что входит

Наблюдаемая из интернета поверхность согласованных целей, сетевые и выбранные прикладные проверки, сохранённые находки и меры по снижению риска.

Чего оно не обещает

Полного обнаружения всех уязвимостей, проверки внутренней сети или исходного кода, безошибочного определения версии и гарантии отсутствия риска.

ЧТО ВЛИЯЕТ НА РЕЗУЛЬТАТ

- Сервисы могут скрывать версии, ограничивать запросы или показывать разное содержимое по географии и учётным данным.
- Совпадение версии с CVE может быть ложноположительным: производитель мог перенести исправление без изменения номера версии.
- Активные проверки создают сетевые запросы; некоторые модули способны повлиять на нагрузку, учётные записи или содержимое приложения. Их включают по согласованию.
- Сторонние хостинги, CDN и облачные ресурсы входят в область только при наличии разрешения на проверку.

РЕЗУЛЬТАТ ДЛЯ ЗАКАЗЧИКА

Карта внешней поверхности.
Список приоритетов.
Понятные следующие действия.

Начать можно с ограниченного пилота: согласовать цели и профиль, получить результаты и решить, какие проверки или меры нужны дальше.

CasuBell предназначен для авторизованного обследования. Проверка проводится только в рамках согласованного разрешения и области.