Кибергигиена как ключевой элемент цифровой трансформации в современном бизнесе

SOLAR

В эпоху стремительной цифровизации бизнеса вопросы кибербезопасности выходят на первый план.

Кибергигиена - это комплексный подход, направленный на поддержание информационной безопасности организации и обеспечение устойчивости к киберугрозам. Этот стратегический элемент играет ключевую роль в успешной цифровой трансформации современных компаний.

Артем Избаенков

Заместитель директора по продуктовому развитию ГК “Солар”

Член правления АРСИБ

Член РОЦИТ

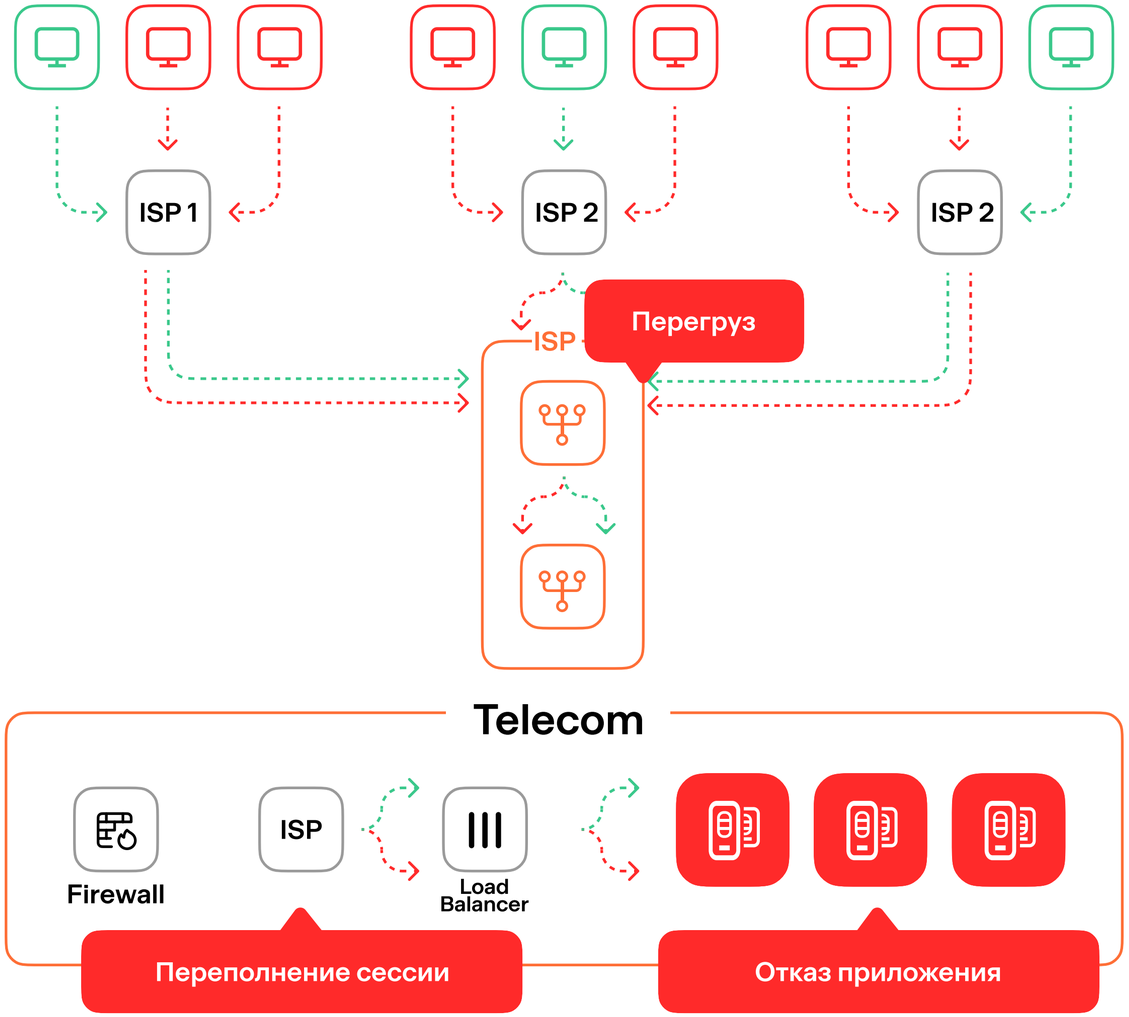
DDoS-атака

Во время DDoS-атаки заражённые хосты (боты) из разных сетей перегружают ресурсы сервера, канала или приложения нелегитимным трафиком. Тем самым они не позволяют легитимным пользователям получить доступ к информации.

Сложность современных DDoS-аттак

Сегодня DDoS можно разделить на 3 типа:

1. Перегрузку канала
2. Переполнений таблиц сессий
3. Отказ сервиса (приложения)



Как влияют DDoS-атаки на бизнес

Как объёмные атаки, так и атаки уровня приложения могут привести к отказу в обслуживании сервисов в бизнесе, тем самым закрыв доступ к множеству ресурсов.

- ✕ Недоступность ресурсов клиентов
- ✕ Недоступность call-центра
- ✕ Огромные убытки по нарушению SLA
- ✕ Недоступность всех сервисов

Недоступность сервисов влечет не только финансовые потери

IT-отдел

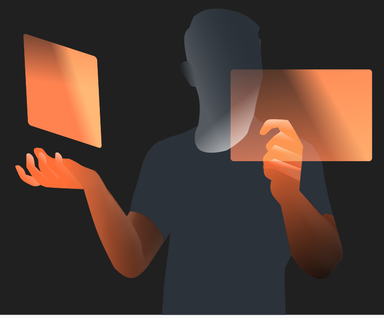
Сколько людей требуется для отражения DDoS-атаки?

Help Desk

Сколько звонков будет во время атаки?

Потеря данных

Сколько ручной работы нужно сделать, если сервис прерван?



Напрасная работа

Каков объем работы, проделанной зря, если сервис недоступен?

Штрафы

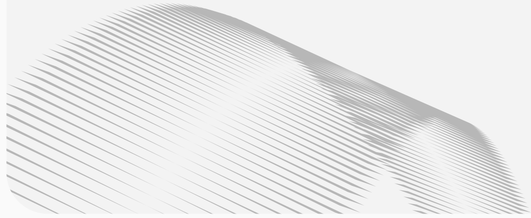
Сколько необходимо выплатить при нарушении SLA?

Потеря бизнеса

Сколько стоит потеря новых клиентов?

Ущерб репутации

Сколько стоит ущерб имиджу компании?



Кибервойна и Хактивисты

- Госструктуры
- Телеком операторы
- Металлургия
- Крупный E-commerce
- Электроэнергетика
- Машиностроение
- Нефтегазовая отрасль
- Авиакомпании
- Доменные регистраторы
- Банки
- Хостинговые компании
- Грузоперевозчики
- Платежные системы
- Информационные порталы
- Электронные торговые площадки

Тренды DDoS-атак 2023

Атаки уровня L7 (приложения) на web инфраструктуру

1

Целенаправленные атаки на DNS сервера компаний

2

Обьем атак ботнетов на РФ легко перешёл границу в 1,2 Тбит/с и более 500 Mppss

3

Рост Мощности + Длительности атак >1 Тбит/с >10 дней

4

Существенную долю ботов составляют боты из РФ

5

Использование облачных ЦОДов для организации и монитизации DDoS атак

6

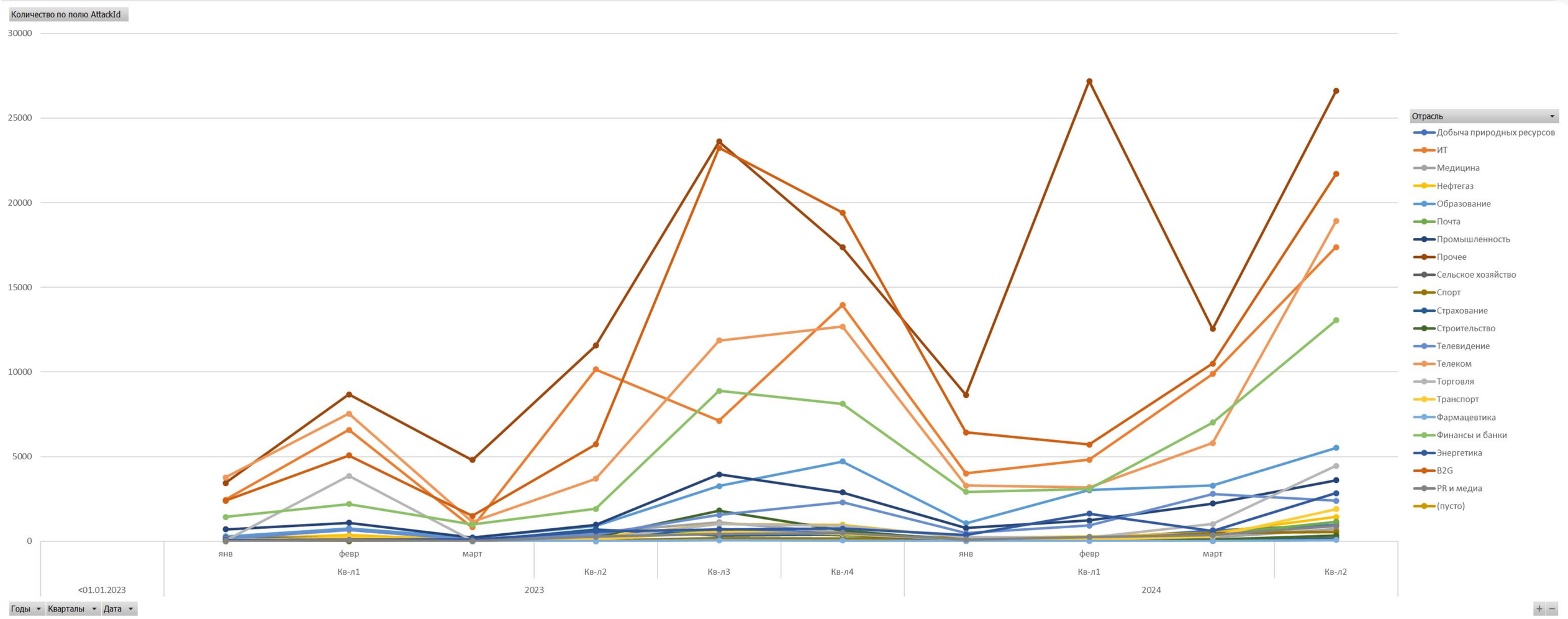
"Ковровые" атаки на инфраструктуру

7

Bad Gateway

502

Статистика DDoS атак 2023/2024



Самые распространенные бот-атаки

DoS- и DDoS-атаки

Боты генерируют огромное количество запросов, чтобы сделать ресурсы недоступными.

Брутфорс

Боты взламывают аккаунты с помощью автоматического перебор паролей.

Скрейпинг

Боты собирают данные с сайтов и могут, например, передать их конкурентам или использовать для спам-рассылок и т.п.

Поиск уязвимостей

С помощью ботов злоумышленники ищут уязвимости приложений и эксплуатируют zero-day уязвимости.

Исчерпание товаров (Denial of Inventory)

Товары: например, заполнить корзины или забронировать весь товар.

Реальные пользователи не смогут его купить, но товар так и не будет продан.

Рекламный фрод

Боты могут кликать на платную рекламу.

В итоге компания платит за трафик, который не конвертируется в покупки, ухудшаются позиции сайта в поисковой выдаче.

Скальперские покупки

Злоумышленники автоматически скупают ограниченный товар, чтобы перепродать его дороже.

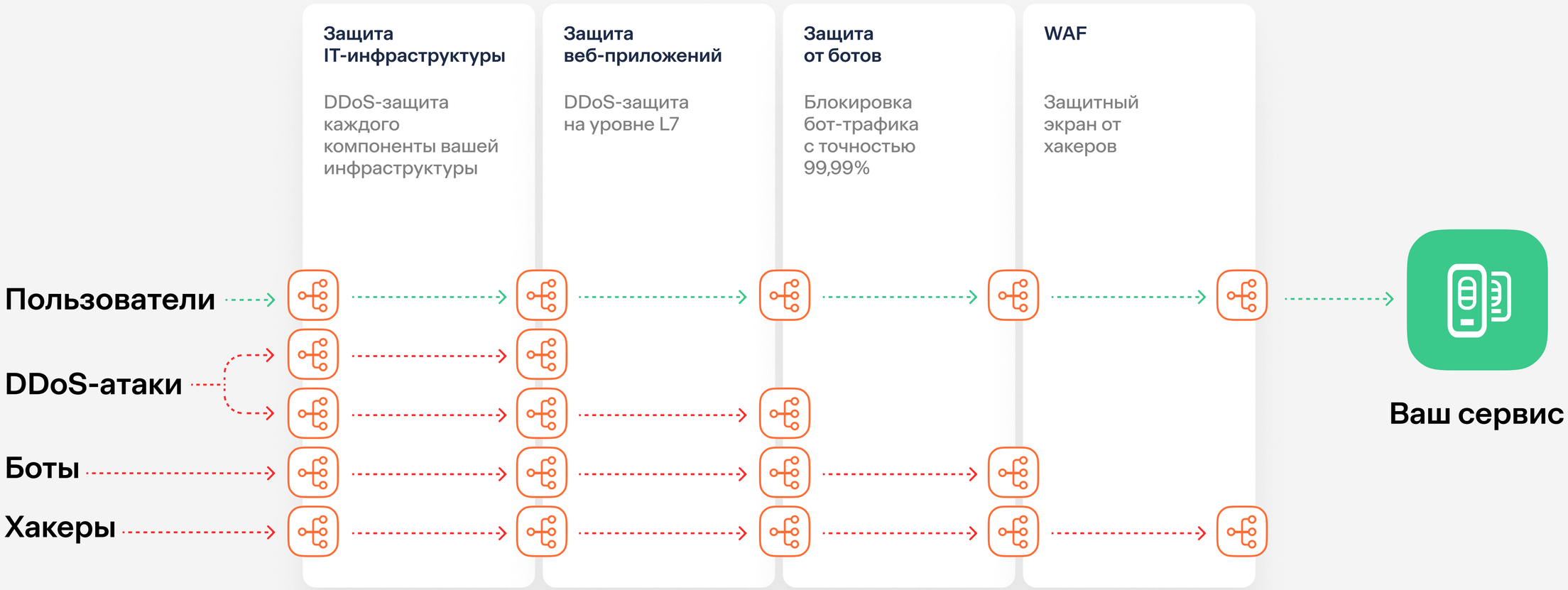
Искаженная аналитика

Бот-трафик искажает реальную картину поведения пользователей. Компании не получают достоверных данных и не могут оптимизировать конверсии.

Кардинг

Боты могут использовать украденные данные карт, чтобы покупать товары без участия владельцев карт.

Сложность современных DDoS-аттак



Защита от DDoS-атак

1

Мониторинг трафика

Постоянный мониторинг сетевого трафика позволяет своевременно обнаруживать признаки DDoS-атак и реагировать на них.

2

Фильтрация трафика

Использование специализированных систем фильтрации трафика помогает отсеивать вредоносные запросы и защищать ключевые ресурсы от перегрузки.

3

Масштабирование инфраструктуры

Возможность быстрого масштабирования вычислительных мощностей позволяет противостоять даже самым мощным DDoS-атакам.

Защита веб-приложений

SOLAR

Защита от DDoS

Использование решений для защиты от DDoS-атак, таких как специализированные фильтры и балансировщики нагрузки, помогает обеспечить доступность веб-приложений даже при массированных атаках.

Защита от ботов

Внедрение систем обнаружения и блокировки ботов предотвращает использование автоматизированных скриптов для взлома, сбора данных и других вредоносных действий.

Защита от хакерских атак

Применение веб-приложенческих межсетевых экранов (WAF) позволяет выявлять и блокировать попытки взлома, инъекции кода и другие типичные хакерские атаки.

Интересные кейсы

Правительственный ЦОД | Клиент

Проблема

После событий 24 февраля команда по ИБ ЦОД поменяла провайдеров и подключила защищенные решения, но во время. построения защищенных каналов, остались уязвимые места, которые позволяли злоумышленникам провести небольшую DDoS атаку и положить всю инфраструктуру региона.

Решение

Проведено стресс-тестирование, предоставлен отчет об язывимостях. разработано совместное решение на базе двух независимых операторов с защитой от DDoS атак.

Планируется размещение очистителей непосредственно в регионе.

Онлайн бронирование авиакомпаний | Клиент

Проблема

Целью ИТ Армии Украины было вывести из строя работу авиакомпаний. Случайным образом одной из целей стала система регистрации онлайн бронирования. Успешная атака поралезовала работу аэропортов и привела к огромным убыткам.

Решение

Трафик перемаршутизирован через защищенный BGP стык на серых адресах, атака зафильтрована. построены дополнительные резервные стыки.

Агрегатор e-mail рассылки | Клиент

Проблема

Целью ИТ Армии Украины Был один крупный е-сот, на части доменов был сервис агрегатора рассылки. В связи с чем он оказался под массированной атакой в следсвтии которой остановилась треть рассылки по РФ для гос и бизнес структур

Решение

Трафик перемаршутизирован через защищенный BGP стык на серых адресах, атака зафильтрована. построены дополнительные резервные стыки.

Организована защита веб-приложений в течении 1-2 часов после начала атаки

ТОП-5 СМИ РФ | Клиент

Проблема

SEO оптимизация сайта стала ухудшаться. По определенным поисковым запросам касательно СВО, сайт находился даже не в топ 10 ссылок.

Была выявлена ботовая активность направленная на ухудшения поисковых позиций сайта.

Решение

Командой был выявлен ботнет в Новосибирске, который вел хитрую деятельность с более чем 4 000 виртуальных машин и уникальных IP адресов из РФ. Его работа заключалась в малоактивном посещении определенных статей сайта, что снижала его SEO и понижала рейтинг для поисковых систем, выводя зарубежные ресурсы в ТОП. Ботнет был заблокирован средствами Антибот системы.

ТОП-10 Банк РФ | Клиент

Проблема

Злоумышленники использовали уязвимость в бизнес-логике: в личный кабинет можно было войти с помощью СМС.

Боты отправляли огромное количество запросов на отправку СМС. В результате на отправку сообщений клиент потратил миллионы рублей за пару часов

Решение

В первую очередь мы исправили уязвимость: ввели ограничение на количество запросов СМС.

Далее подлкючили защиту от ботов и срезали все нелегитимные запросы.

В зашите от ботов использовали дополнительные метрики, чтобы детально выявлять и блокировать вредоносный трафик.

SOLAR

Кибергигиена - ключ к цифровой безопасности

Кибергигиена является неотъемлемой частью успешной цифровой трансформации современного бизнеса. Комплексный подход к обеспечению информационной безопасности, включающий защиту от DDoS-атак, веб-приложений, электронной почты, а также обучение сотрудников и мониторинг угроз, позволяет организациям укрепить доверие клиентов, повысить устойчивость к киберрискам и сохранить конкурентоспособность в цифровую эпоху.

Дальнейшее развитие и внедрение передовых практик кибергигиены должно стать стратегическим приоритетом для современных компаний, стремящихся к успешной и безопасной цифровой трансформации.

SOLAR

Артем Избаенков

Заместитель директора по продуктовому развитию ГК “Солар”

Член правления АРСИБ

Член РОЦИТ