Мы защищаем,
пока вы работаете

RED
SECURITY

RED Security — открытая экосистема ИБ-решений и экспертизы для комплексной защиты бизнеса

RED SECURITY

- Непрерывный цикл снижения киберрисков
- Комплексный подход к ИБ
- Интеграция ИБ-решений в любой ИТ-ландшафт
- Решение задач клиента через быстрое подключение MSS-сервисов на базе ведущих ИБ-решений
- Команда профессионалов с опытом работы в российских и зарубежных вендорах, интеграторах и клиентах
- Предоставляем MSS-решения из защищенного облака с аттестатами:
  - 152-ФЗ до УЗ1
  - TIER 3, стандарт отказоустойчивости ЦОД

300+
Команда экспертов

10+
Лет опыта защиты лидирующего оператора связи

200+
Клиентов за 2 года существования компании

60%
Сотрудников компании — технические специалисты

Ситуация в 2024

RED SECURITY

5 мин.

Требуется злоумышленнику, чтобы зашифровать всю ИТ-инфраструктуру компании

>100 тыс.

Хакерских атак отразили специалисты RED Security SOC

Тенденции

На рынке

- Нехватка профильных специалистов и отток профессионалов в области ИБ
- Тернистый путь закупки зарубежных решений
- Увеличение количества таргетированных атак на цепочки поставок
- Усиление требований регуляторов к ИБ

В компаниях

- Нет кадров для внедрения и поддержки средств защиты информации
- Нет вычислительных ресурсов/ возможности продлить/закупить лицензии и оборудование
- Необходимо обеспечить ИБ и в головной организации, и в филиалах
- Необходимо оперативно выполнять требования законодательства

*Данные на основе открытых источников и внутренних исследований RED Security

Статистика RED Security SOC за 2024 г.

>100 тыс.

подозрений на инциденты выявил RED Security SOC за 2024 год

почти 20 часов

длилась самая продолжительная DDoS-атака

257 Гбит/с

Самая интенсивная DDoS-атака

Ключевой целью профессиональных хакеров стали объекты КИИ

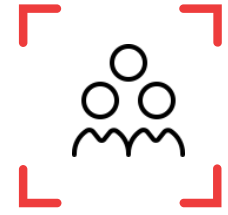
Что мы видим по итогам общения с клиентами

RED SECURITY

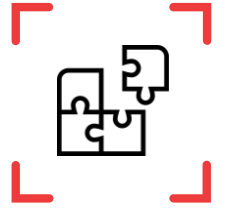
Нет единых стандартов и подходов к ИБ

Отсутствие компетенций по ИБ в штате

Отсутствие зрелых ИБ-процессов



Недостаток человеческих ресурсов → невозможность реализовать СОИБ и требования регуляторов



Зоопарк решений западных и российских вендоров

Мы предлагаем вам реализовать синергию комплексной безопасности

RED SECURITY

Сервисы кибер-безопасности (MSS)

Передовые управляемые ИБ-сервисы под ключ, которые закрывают основные задачи кибербезопасности компании

+

NGSOC

SOC нового поколения, активно использующий облачные технологии и AI/ML для оптимизации обработки инцидентов, сокращения времени реагирования и минимизации ущерба от киберугроз

+

Интеграция решений

ИБ-консалтинг и аудит для формирования дорожной карты развития ИБ, ее реализации и поддержки решений из «одного окна»

=

Комплексная безопасность

Экспертиза

MSS

Сервисы кибербезопасности
RED Security

RED
SECURITY

Центр круглосуточного мониторинга и реагирования на киберугрозы (SOC)

RED SECURITY

>8,6 млрд

анализируемых событий в сутки

>55

опытных аналитиков

- **Знаем отраслевую специфику**
  заказчики - крупные компании из различных секторов экономики
- **Реализуем эффективные процессы**
  повышение скорости реагирования и блокировки целевых атак и вредоносного ПО (вкл. шифровальщики)
- **Оптимизируем затраты на штат специалистов по ИБ**
  Мониторинг событий ИБ 24/7: 3 линии аналитиков, отдельная команда для проактивного анализа новых типов угроз
- **Берем на себя задачи**
  по взаимодействию с ГосСОПКА
- **Обеспечиваем прозрачность процессов**
  удобный личный кабинет с наглядными дашбордами и расширенной статистикой по событиям для принятия эффективных решений
- **Предоставляем гибкую тарификацию и SLA**
  по анализируемым событиям – для наилучшего соотношения цены и качества. Переводим CAPEX в OPEX

Центр мониторинга кибербезопасности RED Security SOC

RED SECURITY

>100 тыс.

хакерских атак отразили специалисты RED Security в 2024 году

>55

аналитиков линий L1, L2, L3, работающих в режиме 24/7/365

15 мин.

Среднее время реагирования на инциденты с высоким уровнем критичности

Response

Реагирование на инциденты в инфраструктуре заказчика

Облачный SOC

Мониторинг и реагирование в гибридной и облачной инфраструктурах клиента

AI

Оптимизация и ускорение процессов мониторинга и реагирования с помощью технологий искусственного интеллекта

EDR

Обнаружение вредоносной активности на конечных точках и реагирование на них

Deception

Ускорение процесса реагирования с помощью ловушек и приманок в инфраструктуре

Форензика

Расследование инцидентов и поиск следов компрометации в инфраструктуре

Анализ внешнего периметра

Регулярное сканирование внешнего периметра ИТ-инфраструктуры с целью выявить уязвимые или неиспользуемые сервисы

VMaaS

Оценка и управление уязвимостями (сканирование/анализ/рекомендации)

AMaaS

Инвентаризация активов (Asset management). Периодическое сканирование ИТ-инфраструктуры с целью выявить новые активы и определить зону покрытия SOC

TI/Threat Hunting

Собственная киберразведка

ГосСОПКА

Взаимодействие с НКЦКИ от лица субъекта КИИ

MFA

Защита доступа пользователей с помощью технологий многофакторной аутентификации

RED Security Anti-DDoS

RED SECURITY

В 1,5 раза
больше DDoS-атак мы зафиксировали в I квартале 2024 относительно H2 2023 г.

800 руб.
достаточно заплатить злоумышленникам для запуска DDoS-атаки

257 гб/сек
составила самая мощная DDoS-атака, отраженная сервисом в 2024 г.

Защита от DDoS-атак на нескольких уровнях

- Защита от атак на уровнях L3-L4
- Защита от атак на уровне L7 без раскрытия ключей шифрования HTTPS-трафика

Актуально для банков и финансовых организаций, интернет-магазинов, государственных организаций

Личный кабинет пользователя

- Статистика по всем подключенным на защиту ресурсам в онлайн-режиме
- Построение отчетов по пропущенному трафику, атакам и применяемым мерам защиты за выбранный период

Соответствует требованиям регуляторов

- Центр очистки внесен в реестр российского ПО и сертифицирован ФСТЭК России

Кастомизация под требования заказчика

- Интеграция с внутренними системами заказчика по API
- Защита на основании информации, получаемой от логов веб-серверов заказчика

RED Security WAF

RED SECURITY

ТОП-3
атакуемых отрасли – государственный сектор, финансовые организации, ретейл

В 58%
случаев инциденты приводили к прерыванию бизнес-процессов

98%
веб-приложений не защищены от атак на пользователей

Защита от различных типов атак, включая DDoS-атаки

- Защита от OWASP TOP-10 атак
- Защита от атак на API
- Защита от атак на механизмы аутентификации
- Защита от неизвестных и новых типов атак

Личный кабинет пользователя

- Статистика по подключенным к сервису веб-приложениям в онлайн-режиме
- Статистика по заблокированным запросам
- Сводка векторов атак, которые использовались чаще всего

Импортозамещение в соответствии с требованиями регуляторов

- Выполнение 250 и 166 Указов Президента РФ
- ПО фильтрующих узлов внесено в реестр российского ПО и сертифицировано ФСТЭК России, соответствует ПП №1236

Работа на базе сигнатурного анализа и позитивной модели

- Использование доступных сигнатур (правил и паттернов в трафике), а также написание новых под конкретное веб-приложение
- Возможность кастомизации правил бизнес-логики под любое веб-приложение

RED Security Antibot

RED SECURITY

73%
запросов в интернет-трафике генерируют вредоносные боты

В 20 раз
выросло количество атак, направленных на мошенничество с использованием SMS-платежей за прошлый год

24/7/365
блокируем вредоносных ботов, выполняющих кражу учётных данных, копирование контента, спам, сканирование и эксплуатацию уязвимостей

Комплексная защита веб-ресурсов от вредоносных ботов

- Защита от любых автоматизированных угроз без потери пользователей
- Многофакторные методы анализа, современные математические модели и Machine learning, мгновенная блокировка запросов ботов
- Подключаем вместе с решением Anti-DDoS для усиления защиты

Технология на базе сигнатурного, поведенческого, технологического и статистического анализа

- Полноценная работа без изменений в коде и CAPTCHA
- Блокировка ботов без влияния на SEO, актуальные белые списки
- Фильтрация нагрузки на ресурсы оптимизирует стоимость владения и повышает эффективность использования имеющихся ИТ-ресурсов

Импортозамещение в соответствии с требованиями регуляторов, соблюдение Compliance-стандартов

- API для управления и интеграции, гибкость настроек и режимов работы, поддержка PCI DSS Compliance
- Выполнение 250 и 166 Указов Президента РФ

RED Security ГОСТ VPN

RED SECURITY

500+ клиентов
под защитой RED Security, включая пользователей аттестованного сегмента облака по ФЗ-152

80+ субъектов
выездные бригады и складские помещения во всех регионах России

Свой ОКЗ
для изготовления криптоключей и ведения журнала учета СКЗИ

Надежная защита передаваемого трафика

- Шифрование трафика по протоколу IPsec с использованием современных отечественных криптографических алгоритмов (ГОСТ)
- Аутентификация устройств в сети по протоколу IKE
- Скрытие внутренней топологии сети заказчика
- Поддержка жизненного цикла ключей шифрования

Доступная интеграция в существующую инфраструктуру заказчика

- Работа с протоколами динамической маршрутизации RIP, OSPF, BGP
- Поддержка протокола 802.1Q (VLAN)
- Возможность работы через все виды NAT
- Возможность инкапсуляции IPsec-трафика в HTTP с целью обхода возможной блокировки провайдером VPN-трафика
- Организация защиты каналов связи на уровне L3 и L2

Широкие возможности резервирования

- Объединение устройств в кластер горячего резервирования (active-passive)
- Резервирование каналов доступа (multiWAN)
- Использование платформ с резервированием жестких дисков и блоков питания
- Объединение сетевых интерфейсов для обеспечения отказоустойчивости
- Поддержка протокола QoS (маркирование, приоритизация, ограничение полосы пропускания)

RED Security MFA

RED SECURITY

>81%
хакерских атак опираются на слабые или украденные пароли

52%
пользователей используют один и тот же пароль для разных учетных записей

99,9%
автоматизированных кибератак на пароль блокирует многофакторная аутентификация

Совместимость, масштабируемость, отказоустойчивость

- Мультиплатформенный открытый стек технологий
- Модульная архитектура с дублированием всех компонентов
- Поставка в виде набора контейнеров

Удобное управление в крупных организациях и сервис-провайдерах

- Многоуровневая мультиарендность с делегированием доступа
- Веб-консоль с детальной системой административных ролей

Поддержка жизненного цикла токенов OTP

- Детальные политики программных и аппаратных токенов
- Управление на уровне отдельных токенов пользователя
- Автоматические выдача и отзыв токенов
- Автоматизация основных процессов управления

RED Security Awareness

RED SECURITY

~80%
киберинцидентов вызваны человеческим фактором

▲45%
ежегодный рост числа фишинговых писем с использованием шифровальщиков

>60%
успешных фишинговых атак реализованы через персонализированные письма, сгенерированные ИИ

На старте

- Подберем оптимальный вариант поставки
- Встроим сервис в бизнес-процессы на основании данных о компании
- Подключим и настроим платформу
- Определим текущий уровень киберграмотности сотрудников

Регулярно

- Формируем и рассылаем тренировочные фишинговые рассылки
- Собираем статистику и выгружаем отчеты для отдела ИБ заказчика
- Поддерживаем работоспособность сервиса в рамках SLA
- Строим учебный трек каждого сотрудника с теоретическим и практическим обучением
- Настраиваем интеграции с информационными системами

Результат

- Снижаем количество повторных инцидентов до 80%
- Повышаем уровень осведомленности сотрудников в 3 раза
- Автоматизируем процесс обучения: больше не нужно проводить лекции, тестировать сотрудников и анализировать результаты
- Точечно обучаем сотрудников по необходимым темам: экономия времени и концентрация внимание на ключевом

Интеграция решений

RED
SECURITY

Построение комплексной защиты и интеграция решений

RED SECURITY

Интеграция ИБ-решений в любой ИТ-ландшафт независимо от уровня цифровой зрелости компании

60%
Сотрудников компании – технические специалисты

130+
Экспертов с опытом внедрения российских и зарубежных решений

60+
Российских и зарубежных вендоров в портфеле компетенций экспертов

2010 г.
Запуск центра мониторинга и реагирования на инциденты в ГК АФК

Лицензии и сертификаты регулирующих органов ИБ, в том числе на работу с СКЗИ

Отраслевая экспертиза и понимание бизнес-рисков

Большой опыт эксплуатации СЗИ для ГК АФК

Мы предлагаем:

- Анализ уровня защищенности вашей компании
- Маппинг бизнес-рисков на ИТ- и ИБ-ландшафты
- Актуализацию роадмапа и стратегии развития ИБ
- Построение комплексной защиты, усиленной RED Security SOC
- Внедрение и эксплуатацию СЗИ
- Техническую поддержку 24/7/365

- Защита ИТ-инфраструктуры
- Защита веб-приложений
- Мониторинг и реагирование на киберинциденты
- Сетевая безопасность
- Услуги/консалтинг в области ИБ

Портфель компетенций RED Security

RED SECURITY

Защита ИТ-инфраструктуры

- Защита конечных точек (EPP/EDR/XDR)
- Многофакторная аутентификация (MFA)
- Безопасность веб-доступа (SWG/proxy)
- Ловушки и приманки (Deception)
- Sandbox/DDP

Защита веб-приложений

- Безопасность веб-приложений (WAF)
- Защита от ботов (Antibot)

Мониторинг и реагирование на киберинциденты

- Мониторинг событий ИБ (SIEM)
- Реагирование на киберинциденты IRP/SOAR
- Реагирование в инфраструктуре клиента (EDR)
- Управление уязвимостями (VM)
- Киберразведка/киберобман (TI/TH)
- Анализ защищенности
- Контроль внешнего периметра
- Инвентаризация и контроль изменений

Услуги/консалтинг в области ИБ

- Экспресс-консалтинг
- Пентест
- Форензика
- Аттестация на соответствие ФЗ-152, ФЗ-187

Сетевая безопасность

- Защита от DDoS-атак (Anti-DDoS)
- Шифрование каналов связи (ГОСТ VPN)
- Межсетевое экранирование (UTM/NGFW)
- Системы анализа сетевого трафика (NTA/NAD)

RED Security — открытая экосистема ИБ-решений и экспертизы для комплексной защиты бизнеса

Кастомный подход
к каждому клиенту

Хотите повысить киберустойчивость вашей компании?

Свяжитесь с нами:

request@redsecurity.ru