
attack
killer
НЕПРЕРЫВНАЯ ПРОАКТИВНАЯ
ЗАЩИТА ВЕБ-РЕСУРСОВ

Сегодня практически все организации используют Интернет как один из каналов обслуживания. Рост потребности в веб-разработках и оттягивание ресурсов крупными холдингами породили дефицит разработчиков. В сочетании с желанием компаний экономить это привело к падению уровня безопасности приложений. Количество успешных атак на прикладном уровне растёт. Отмечается рост комплексных кибератак с применением разного типа воздействия: DDoS, использование уязвимостей веб-инфраструктуры или ошибок в коде приложения, заражение компании-жертвы специализированным вредоносным ПО.

Эксперты, способные противостоять атакам, в ещё большем дефиците, чем веб-программисты.

Постоянные обновления программного обеспечения добавляют ошибок — новых преимуществ вашим противникам в кибервойне.

Реагировать на уже свершившиеся события неэффективно, неудобно и дорого. Необходимо комплексное решение, которое охватывает все этапы жизненного цикла веб-ресурса.

ЕСЛИ…

- Вам важно, чтобы Ваш веб-ресурс был всегда доступен
- Веб-приложение – это инструмент генерации прибыли для Вас
- Ваше веб-приложение работает с персональными данными и\или платежными реквизитами
- Веб-ресурс – это часть ключевых бизнес-процессов Вашей компании
- Вам важен контент веб-приложения
- Вы используете заказные разработки

▶ ВАМ НЕОБХОДИМО РЕШЕНИЕ ATTACK KILLER

ПОЧЕМУ ATTACK KILLER?

Простое и удобное решение: сквозная интеграция различных инструментов обеспечения безопасности в единый интерфейс делает работу с системой удобной, а обучение пользователей – легким и эффективным. Пользователь получает понятные настраиваемые отчеты с рекомендациями.

Эффективная защита: искусственный интеллект ядра и использование машинного обучения в работе функциональных компонентов Attack Killer позволяет снизить вероятность успешных атак практически до нуля, обеспечивая при этом менее 1% ложных срабатываний.

Безопасность на всем жизненном цикле приложения: специализированный сканер исходного кода обеспечивает безопасность всего цикла разработки и использования бизнес- приложений

НЕПРЕРЫВНАЯ БЕЗОПАСНОСТЬ ДЛЯ НЕПРЕРЫВНОСТИ БИЗНЕСА

Обеспечение доступности ресурсов: автоматическое обнаружение и гарантированное предотвращение масштабных и комплексных DDoS-атак

Обеспечение целостности и конфиденциальности данных: предотвращение хакерских атак на веб-приложение и обнаружение уязвимостей веб-инфраструктуры

Обеспечение безопасного обновления приложений: автоматизированный контроль качества исходного кода программ на соответствие требованиям по безопасности разработки

Непрерывная безопасность – это необходимость для

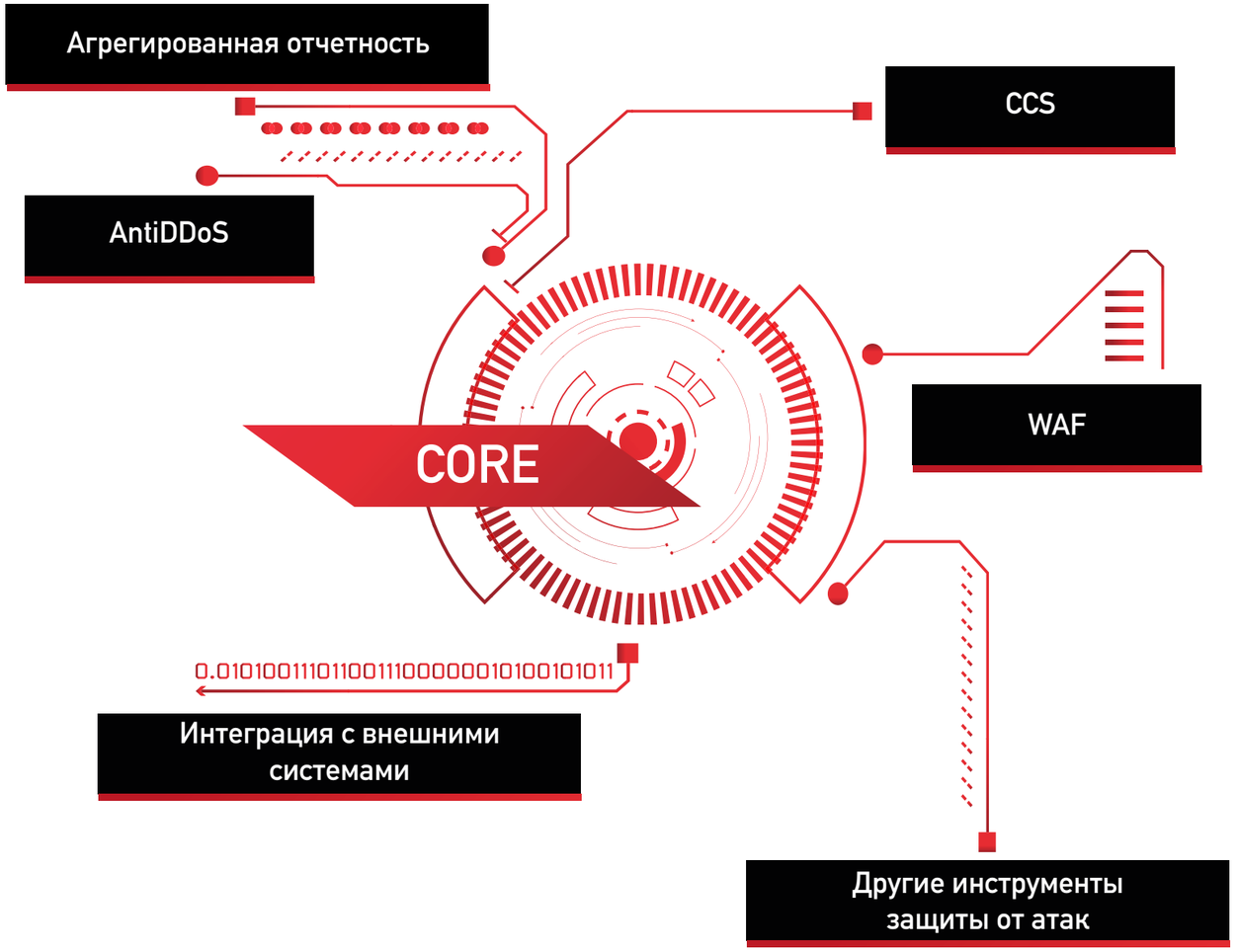
- бизнес-заказчика – вовремя запущенный бизнес, лояльные клиенты и прибыль;
- разработчика – время на исправление ошибок без давления со стороны;
- сотрудника ИБ – безопасно эксплуатируемая система.

ЧТО ТАКОЕ МАТРИЦА БЕЗОПАСНОСТИ

Матрица безопасности – это принцип построения полностью автоматической проактивной защиты веб-приложений от всех видов атак. В основе Матрицы безопасности лежит использование искусственного интеллекта, что позволяет решить проблему защиты веб-приложений в компаниях, которые не могут себе позволить организовать полноценный центр отражения атак.

ПРИНЦИПЫ ПОСТРОЕНИЯ МАТРИЦЫ БЕЗОПАСНОСТИ

1. Интеграция разработки, средств анализа защищённости и настроек средств защиты.
2. Объединение управления и мониторинга всех средств защиты в одном месте.
3. Комбинирование самообучения с прямым автоматическим управлением настройками на основе анализа приложения.
4. Проектирование и построение систем защиты с учетом предполагаемого роста бизнеса.



ЗАДАЧИ МАТРИЦЫ БЕЗОПАСНОСТИ

1. Обеспечение доступности веб-ресурса.
2. Надежная защита чувствительной информации: коммерческих секретов или персональных данных пользователей.
3. Безопасность проведения финансовых транзакций, осуществляемых через ресурс организации.
4. Защита от подмены информации или размещения противоправного контента.
5. Сохранение позиций ресурса в поисковой выдаче даже при попытках злоумышленников совершить манипуляции с кодом.
6. Защита от атак, направленных на посетителей сайта через размещения вредоносного кода на страницах ресурса.

КАК ЭТО РАБОТАЕТ УЖЕ СЕЙЧАС

В настоящее время принципы Матрицы безопасности используются в решении Attack Killer.

ATTACK KILLER AntiDDoS

- Защита даже самых нагруженных веб-проектов от DDoS-атак любой мощности
- Паразитный трафик отсекается на уровне фильтрующих узлов, к ресурсу доставляется уже очищенный трафик
- Пользователи узнают о попытках атак только из отчетов

ATTACK KILLER CUSTOM CODE SCANNER (CCS)

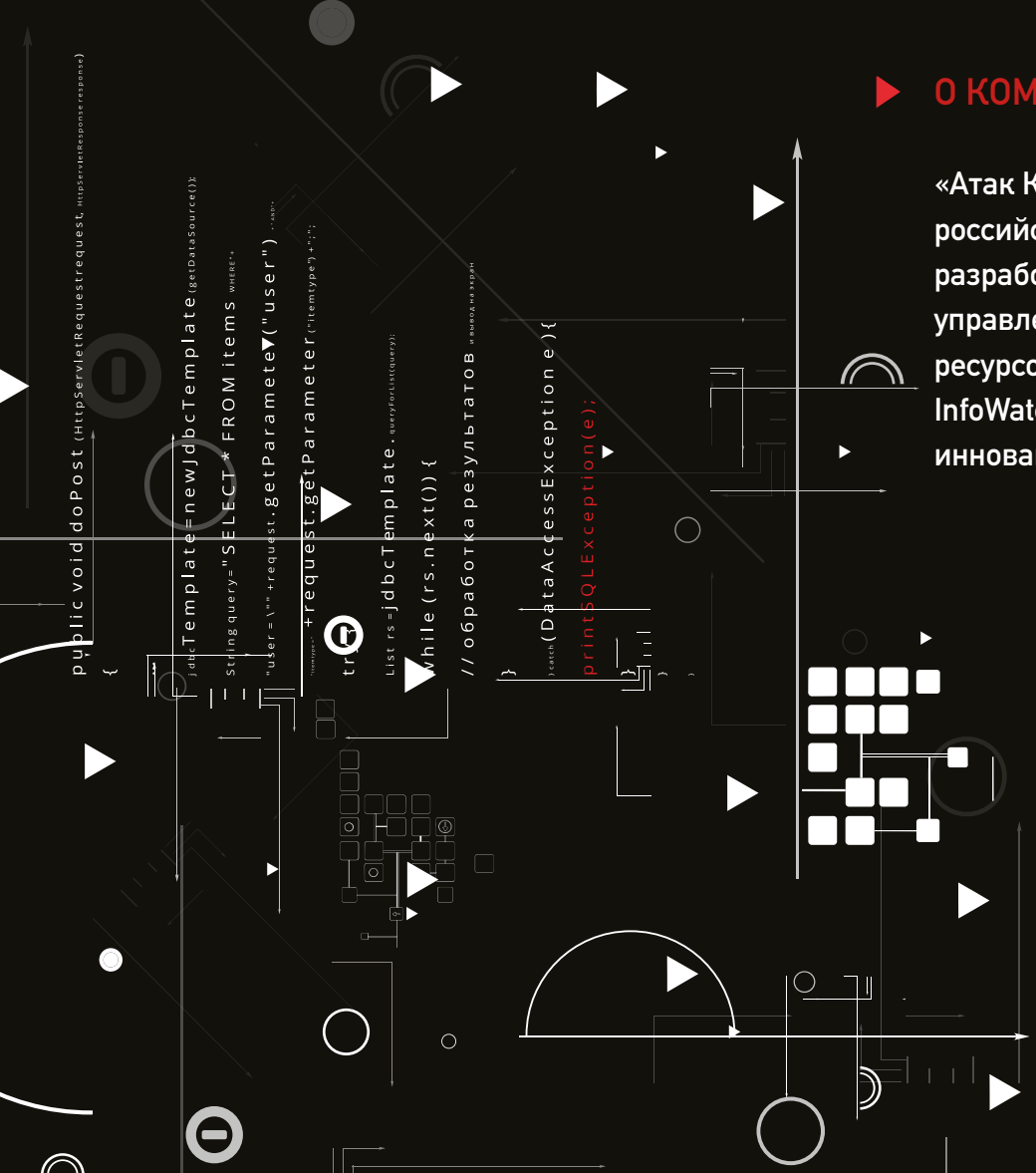
- Поиск ошибок в исходном коде с учетом требований безопасного программирования
- Поддержка всех известных языков программирования (Java, PHP, JavaScript, C# и др.)
- Для интерпретации отчетов не требуется специальной квалификации

ATTACK KILLER WEB APPLICATION FIREWALL (WAF)

- Непрерывный поиск уязвимостей приложений и активная защита от хакерских атак в автоматическом режиме
- Автоматическая адаптация к изменениям ресурса благодаря алгоритмам самообучения
- Простые и наглядные отчеты

О КОМПАНИИ

«Атак Киллер» (Attack Killer) – первая российская компания, занимающаяся разработкой и внедрением систем управления комплексной защитой веб-ресурсов. Входит в Группу компаний InfoWatch, является резидентом инновационного центра «Сколково».



www.attack-killer.com

+7 (495) 22-900-22
+7 (499) 37-251-74
sales@attack-killer.com