INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

INFOWATCH ATTACK KILLER

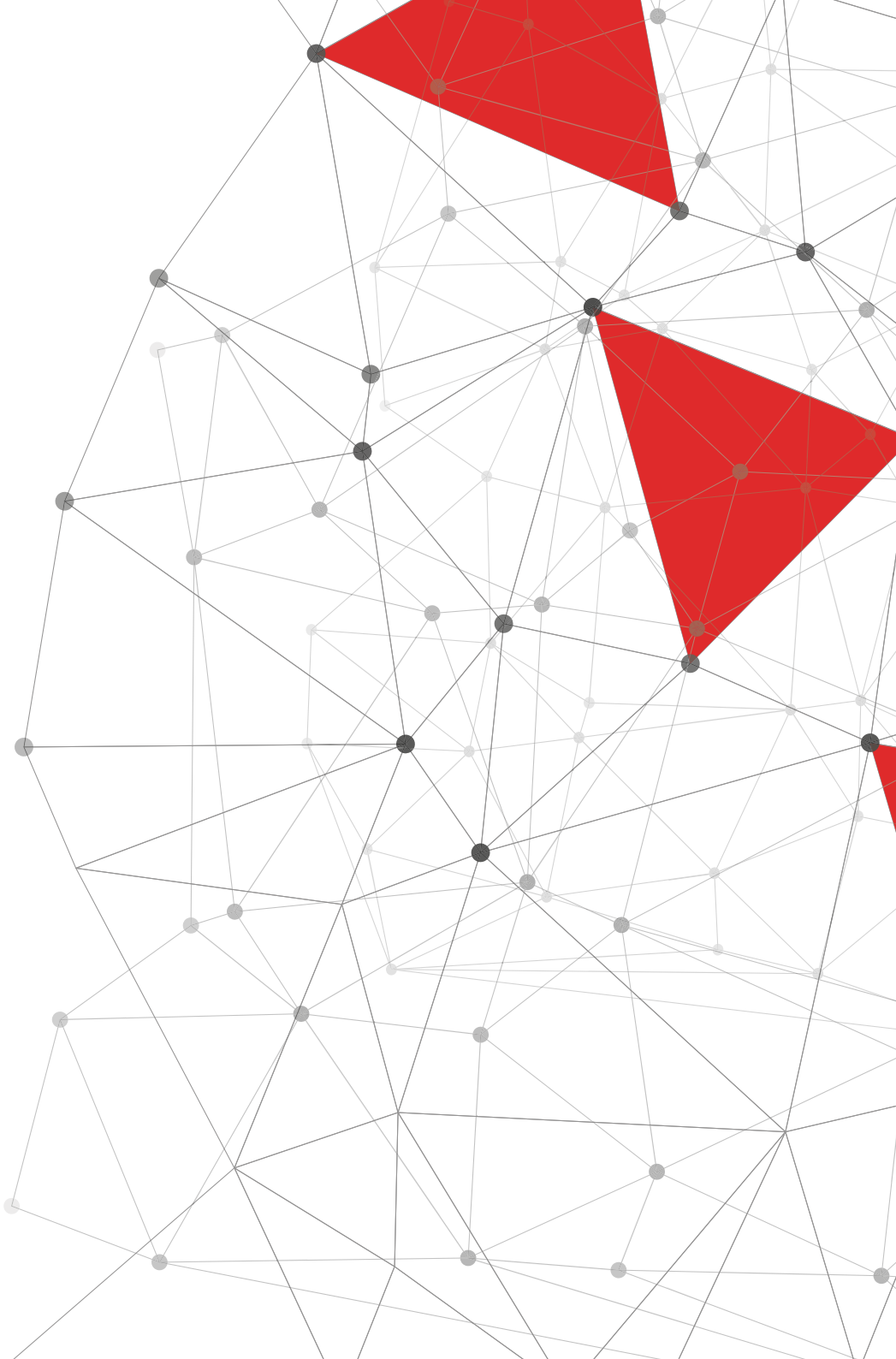
БЕЗОПАСНОСТЬ НА ВЫСОКИХ СКОРОСТЯХ

БЕЗОПАСНОСТЬ НА ВЫСОКИХ СКОРОСТЯХ

Веб-пространство – это скорость. Скорость донесения информации до аудитории, сверхбыстрое реагирование на потребности рынка, конкурентная борьба на опережение, а значит, регулярное и оперативное внедрение нового функционала веб-приложений. Работа на высоких скоростях приводит к ошибкам. Но на традиционную проверку безопасности времени не остается. Новые пользовательские возможности гораздо важней для бизнеса, чем отчеты о потенциальных угрозах, мифических хакерах и немыслимых ущербах. Тем не менее, ответственность за инциденты безопасности со специалистов не снимают.

Более 80% специалистов по информационной безопасности соглашаются с тем, что внешние угрозы сегодня наиболее опасны и популярны.
При этом, 51% считает, что веб-приложение является самой уязвимой точкой корпоративной инфраструктуры.

Нетривиальная задача безопасности сегодня, как бизнес-единицы организации, не только предотвратить ошибки программирования на самой ранней стадии, но и ускорить процесс выпуска обновлений, гарантируя их безопасность.



ЗАЩИТА НАЧИНАЕТСЯ НА СТАДИИ РАЗРАБОТКИ...

Каждое веб-приложение содержит не менее 5 критичных уязвимостей, которые могут эксплуатировать хакеры. Используя ошибки в коде, хакеры получают контроль над ресурсом, доступ к базам данных, финансовым транзакциям, платежной, клиентской и другой конфиденциальной информации.

Каждое изменение ресурса несет потенциальную угрозу: новые строчки кода – со случайной ошибкой или специально оставленной закладкой, созданная учётная запись – со слабым паролем и чрезмерными пользовательскими привилегиями, новый бизнес-процесс – с новой схемой мошенничества. **Любые изменения объекта защиты влекут обязательную перенастройку систем безопасности.**

Три года назад это не было проблемой: обновления информационных систем проходили раз в месяц или квартал. Было время на тестирование системы в лаборатории, на заказ стороннего аудита безопасности. Сегодня изменения происходят раз в 2-3 дня – для банковских систем, для промышленности – значительно реже, а для электронной коммерции – гораздо чаще.

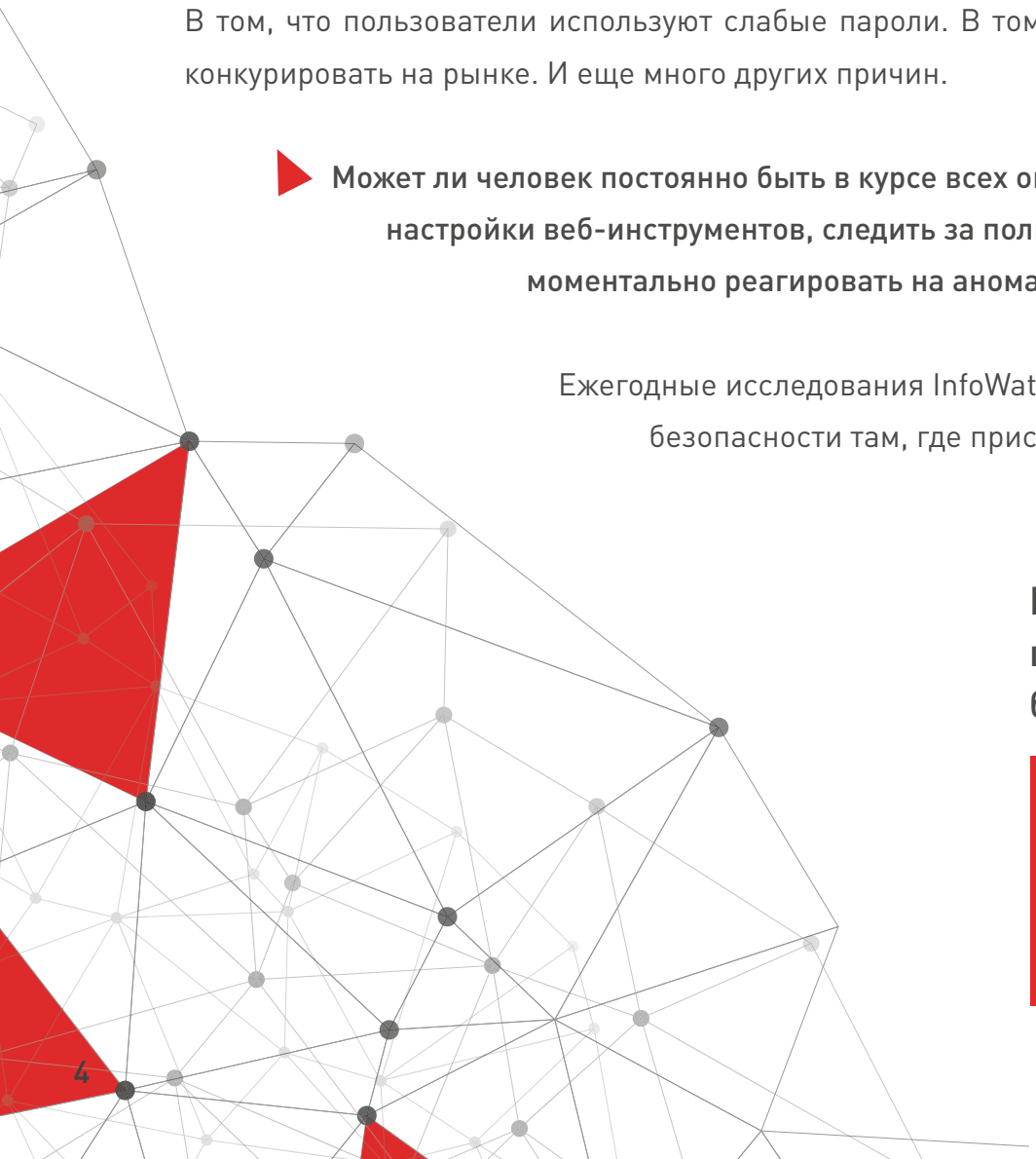
В ТАКИХ УСЛОВИЯХ ПРОЦЕСС ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ ДОЛЖЕН БЫТЬ АВТОМАТИЗИРОВАН И ВСТРОЕН НЕПОСРЕДСТВЕННО В ВЕБ–РАЗРАБОТКУ.

...И НЕ ПРЕРЫВАЕТСЯ

Ежедневно новостные заголовки пестрят сообщениями о взломах, хакерах, украденных данных или DDoS-атаках. Дело не в том, что программисты пишут «плохой» код, а в том, что многие сайты содержат стандартные ошибки, заложенные в веб-платформах. В том, что пользователи используют слабые пароли. В том, что «положить» сайт конкурента значительно дешевле, чем честно конкурировать на рынке. И еще много других причин.

Может ли человек постоянно быть в курсе всех опубликованных уязвимостей, безупречно контролировать настройки веб-инструментов, следить за пользовательским контентом, проверять все возможные векторы атак, моментально реагировать на аномальный трафик?

Ежегодные исследования InfoWatch подтверждают, что самое «узкое» место в корпоративной безопасности там, где присутствует человеческий фактор.



Подход InfoWatch к обеспечению безопасности критичной веб-инфраструктуры базируется на «3 китах»:

- непрерывность
- адаптивность
- максимальное исключение человеческого фактора

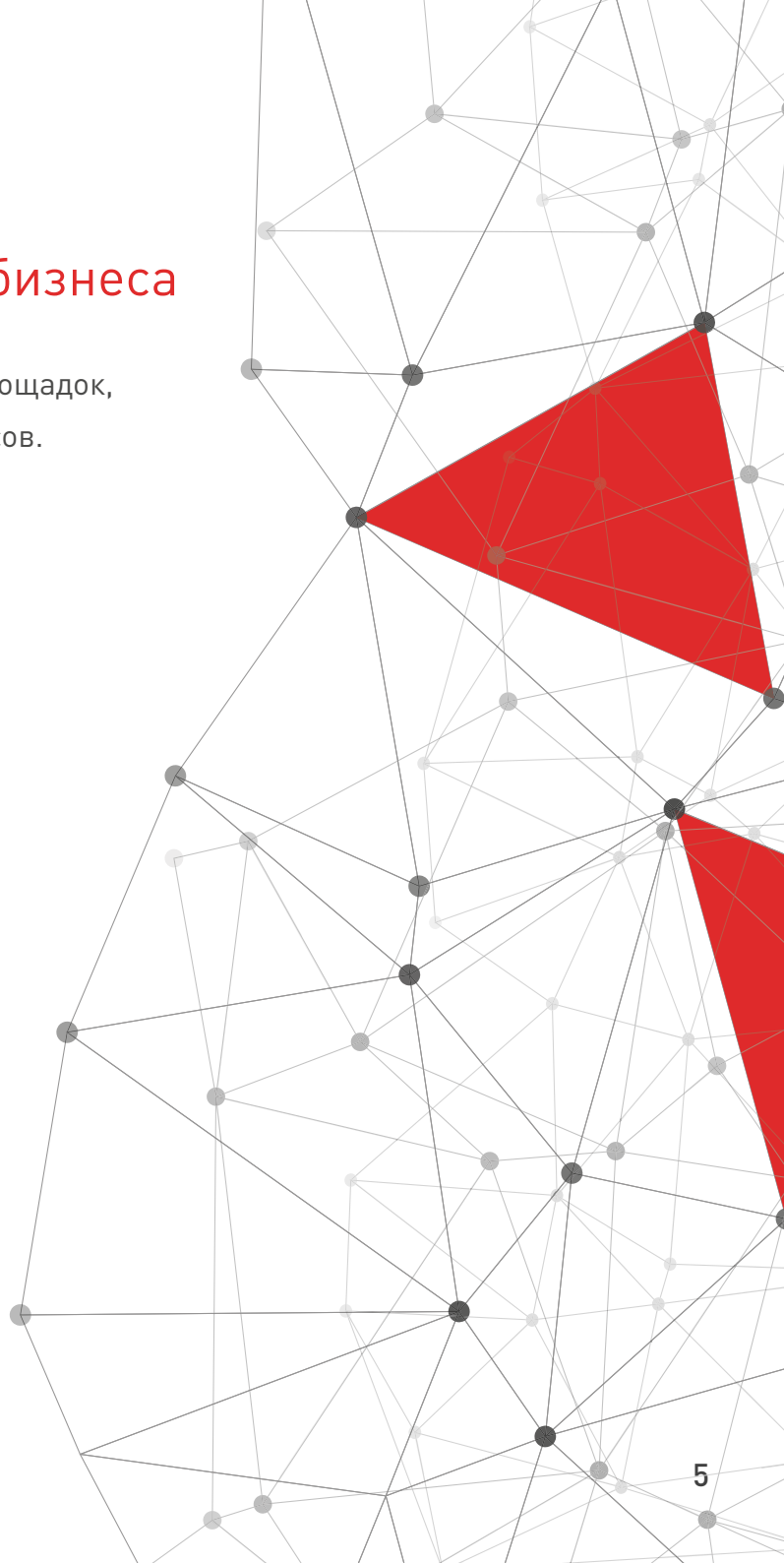
INFOWATCH ATTACK KILLER

непрерывная активная защита веб-приложений, критически важных для бизнеса

Решение будет особенно полезно для защиты систем интернет-банкинга, торговых площадок, порталов госуслуг, систем групповой работы, интернет-магазинов и других веб-ресурсов.

БЫСТРОЕ РЕШЕНИЕ КРИТИЧНЫХ ЗАДАЧ

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

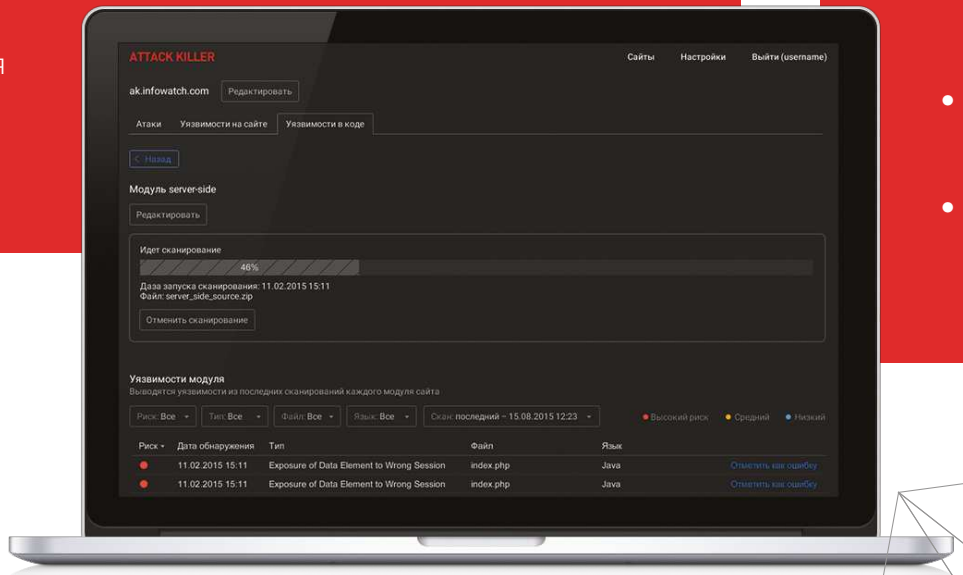


АРХИТЕКТУРА INFOWATCH ATTACK KILLER

INFOWATCH ATTACK KILLER CUSTOM CODE SCANNER (CCS)

технология статического анализа для поиска уязвимостей исходного кода приложений.

- Обнаруживает ошибки в исходном коде с учетом требований безопасного программирования: PCI DSS, OWASP, а также производителей платформ
- Поддерживает все самые известные языки программирования (Java, PHP, JavaScript, C# и др.)
- Для интерпретации отчетов не требуется специальной квалификации



INFOWATCH ATTACK KILLER WEB APPLICATION FIREWALL (WAF)

непрерывный поиск уязвимостей приложений и активная защита от хакерских атак в автоматическом режиме.

- Совмещает функции обнаружения уязвимостей приложения и активной защиты от хакерских взломов
- Благодаря алгоритмам самообучения автоматически адаптируется к изменениям ресурса
- Не требует ручной переконфигурации при каждом обновлении
- Выявляет многоступенчатые атаки из множества событий безопасности
- Формирует простые и наглядные отчеты и графики

INFOWATCH ATTACK KILLER ANTIDDOS

непрерывная защита веб-ресурса от DDoS-атак на основе облачной географической распределенной сети фильтрующих узлов.

- С момента подключения ресурс находится под непрерывной и активной защитой
- Автоматическая защита моментально реагирует на опасные аномалии
- Защищает даже самые нагруженные веб-проекты 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

КАК ЭТО РАБОТАЕТ

1

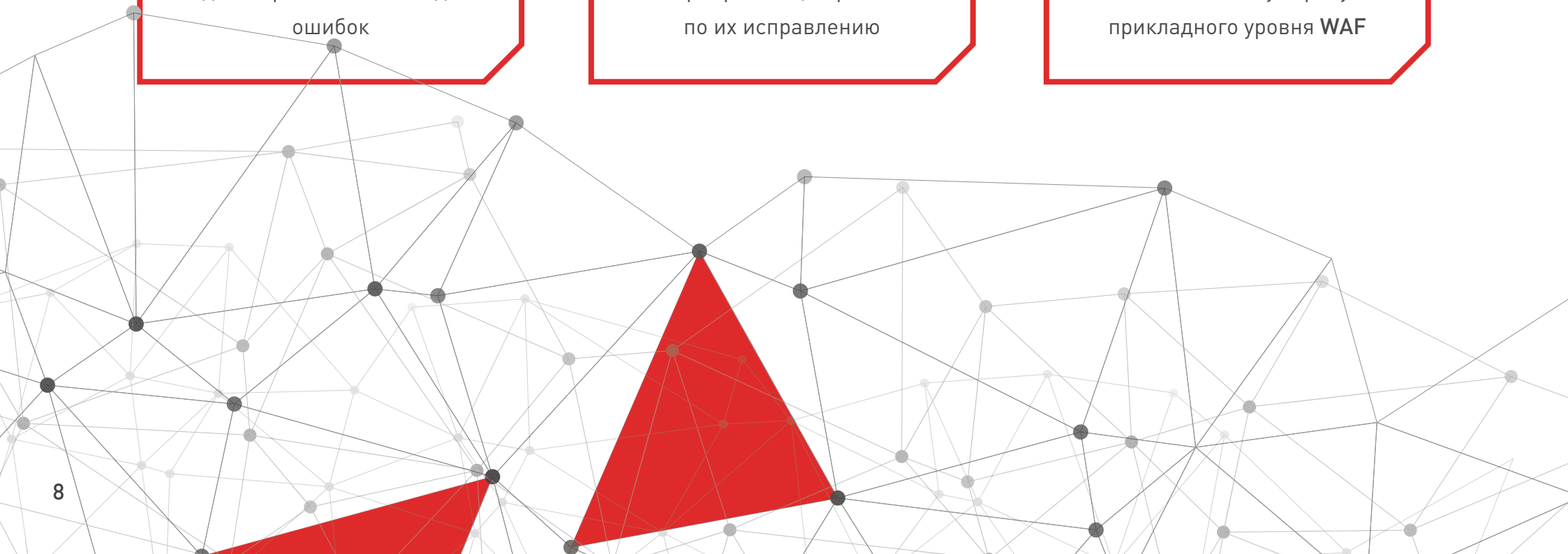
Статический сканер **CCS** находит уязвимости и выпускает рекомендации по их исправлению. Однако с **InfoWatch Attack Killer** приложение готово к релизу даже при наличии в коде ошибок

2

Работающее приложение проверяется динамическим сканером, встроенным в модуль **WAF**, для выявления среди всех уязвимостей реально опасных для конкретного приложения и приоритезации работы по их исправлению

3

Найденные уязвимости и способы их эксплуатации автоматически передаются от пассивных средств (статического и динамического сканера) к активным – **DDoS** – фильтрам модуля **AntiDDoS** и межсетевому экрану прикладного уровня **WAF**



4

AntiDDoS и **WAF** автоматически адаптируют свои настройки и добавляют правила фильтрации – «виртуальные патчи», не пропускающие опасные запросы к уязвимому функционалу

5

С момента подключения ресурс находится под непрерывной защитой от **DDoS**-атак. Весь трафик постоянно проходит через распределенную систему фильтрующих узлов

6

Пока программисты исправляют найденные уязвимости, **InfoWatch Attack Killer** закрывает возможные векторы атак в автоматическом режиме, а выпущенные обновления проходят весь цикл проверки

Непрерывная безопасность обеспечит партнерство между бизнес-заказчиком, разработчиком и сотрудником ИБ, где каждый получит желаемое: первый - оперативно запущенный функционал, лояльных клиентов и прибыль, второй – время на исправление ошибок без давления со стороны, а третий – безопасно эксплуатируемую систему

НЕПРЕРЫВНАЯ БЕЗОПАСНОСТЬ ДЛЯ НЕПРЕРЫВНОСТИ БИЗНЕСА

Безопасность – как фича и конкурентное преимущество вашего бизнеса

Надежный фундамент, заложенный в приложении на стадии разработки, гарантирует стабильную работу ресурса, а также безопасность проведения финансовых транзакций и хранения конфиденциальной информации.

С **InfoWatch Attack Killer** защита начинается на стадии разработки. Уверенность пользователей ресурса в его надежности повышает лояльность клиентов и привлекает новую аудиторию.

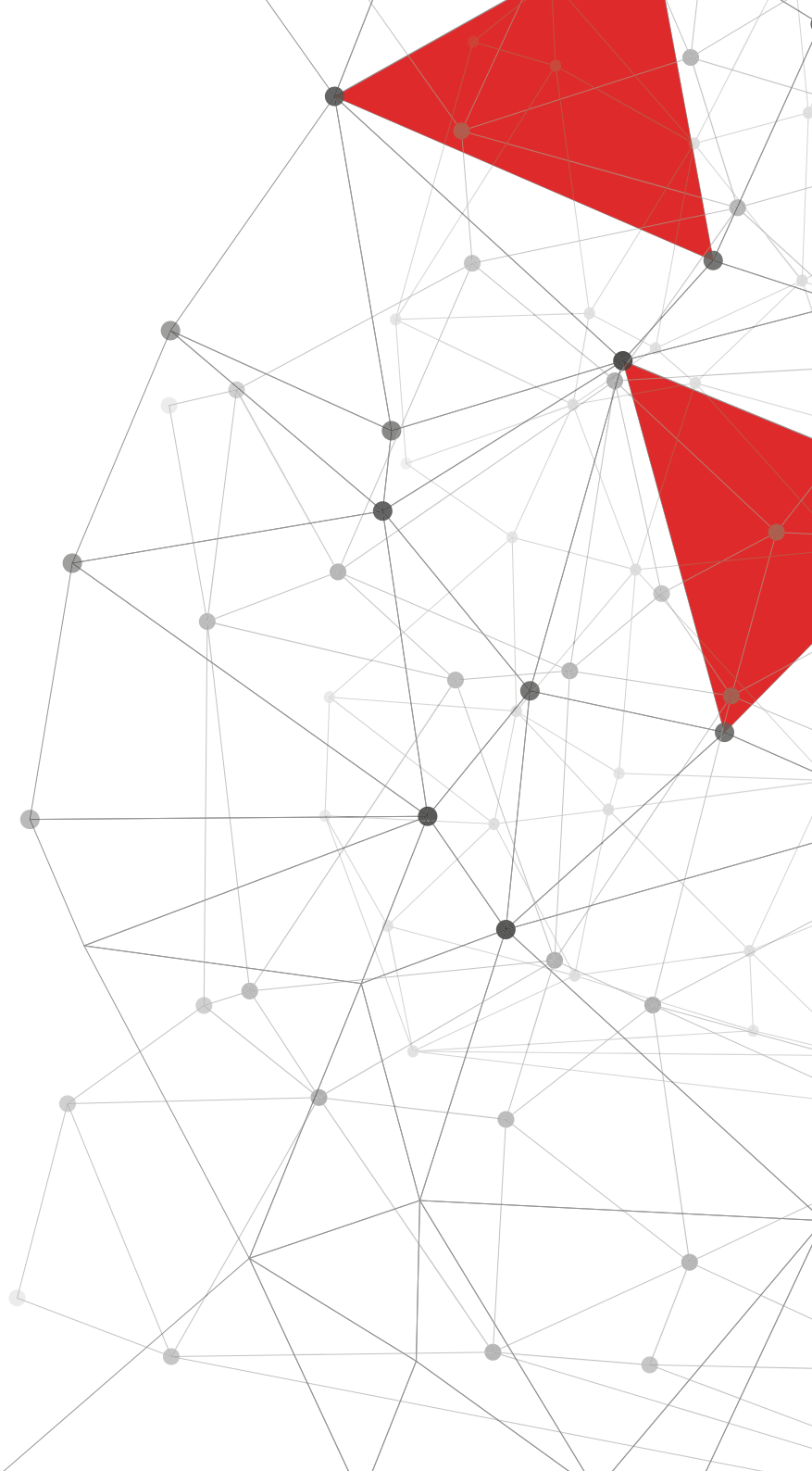
Даже уязвимые обновления – безопасны и готовы к выпуску

Самые простые обновления ресурса могут содержать в себе угрозу безопасности, поэтому приложение необходимо регулярно сканировать.

При частых обновлениях ручная проверка замедляет выпуск кода. Оперативное внедрение нового функционала возможно благодаря непрерывному поиску уязвимостей и их автоматическому устранению **InfoWatch Attack Killer** до исправления программистами.

Стабильность ресурса не зависит от человеческого фактора

Недоступность ресурса для клиентов приводит к репутационному и финансовому ущербу. Однако скорость реагирования на инциденты зачастую зависит от реакции оператора систем безопасности. **InfoWatch Attack Killer** мгновенно реагирует на аномальные активности, при этом алгоритмы самообучения исключают ложные срабатывания, и для легитимных пользователей ресурс будет доступен всегда .



ПОЧЕМУ INFOWATCH ATTACK KILLER?

Одно решение для защиты от любых веб-угроз

И выгодный компромисс между безопасностью, разработкой и бизнесом

Модульная схема подключения

Начните использовать защиту с любого из модулей

Единый веб-интерфейс и единые отчеты

Наглядные графики и отчеты о зафиксированных попытках атак на всех уровнях защиты

Союз лучших российских технологий

ГК InfoWatch объединила лучшие технологии, зарекомендовавшие себя на рынке

Помощь в соответствии требованиям регуляторов

Приказ ФСТЭК России №21 и №17, ФЗ-№152, PCI DSS, СТО БР ИББС, НДВ4, SDLC

Включен в реестр отечественного ПО

INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

www.infowatch.ru

+7 (495) 22-900-22
+7 (499) 37-251-74

sales@infowatch.ru