INFOWATCH APPERCUT

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

УПРАВЛЕНИЕ КАЧЕСТВОМ ИСХОДНОГО КОДА БИЗНЕС-ПРИЛОЖЕНИЙ

InfoWatch Appercut — система автоматизированного контроля исходного кода бизнес-приложений на соответствие требованиям, предъявляемым к заказной разработке.

90% компаний дорабатывают бизнес-приложения* с помощью штатных программистов или отдают эту задачу на аутсорсинг

75% новых атак происходят на уровне бизнес-приложений*. Однако на рынке существуют решения, закрывающие угрозы небезопасного кода

Исправление ошибки в коде, найденной ***на этапе разработки, обходится в 10 раз дешевле,*** чем на этапе приемки готового продукта

INFOWATCH APPERCUT: ПРОВЕРЯТЬ «СВОИХ», ЗАЩИЩАТЬ ОТ «ЧУЖИХ»

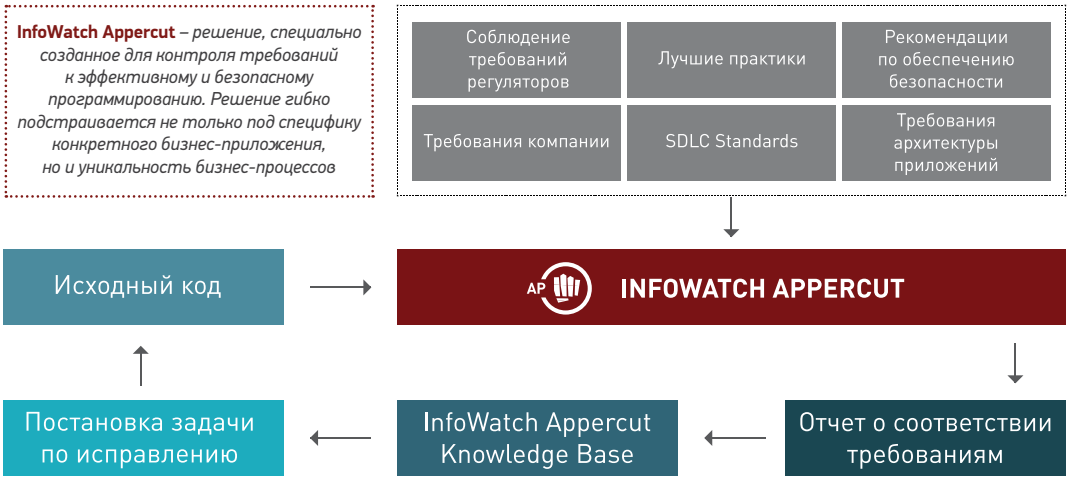
InfoWatch Appercut создан для принимающей стороны или заказчиков программного обеспечения, и его использование не требует специальных знаний в области программирования или аудита кода.

Код приложения в целом, его обновления или модули приложения за секунды сканируются на соответствие требованиям, автоматически создается описание несоответствий, а также выдаются рекомендации для их устранения.

В сравнении с ручной проверкой кода InfoWatch Appercut на порядок повышает скорость и результативность анализа и значительно сокращает расходы на оплату услуг сторонних аудиторов.

Кейс

Программист внедрил закладку в приложение для обработки операций с ценными бумагами. Она незаметно списывала со счетов клиентов определённое количество акций, «прокручивала» их на фондовой бирже и возвращала обратно, перечисляя прибыль на счёт мошенника.
В результате афёры ему удалось реализовать 110 тыс. акций и заработать 5,7 млн руб. Ущерб репутации его работодателя не оценивался. Мошенническую схему раскрыли только через год, программист осужден на 5 лет.



ТЕХНОЛОГИИ APPERCUT

Метод статического анализа кода (SAST**), используемый в InfoWatch Appercut, позволяет проводить проверки качества кода еще на этапе программирования, когда ошибку проще и дешевле исправить. Реализованные в InfoWatch Appercut лексерный, семантический анализы и анализ потоков данных обеспечивают полноту и скорость поиска небезопасных конструкций при приемлемом уровне ложноположительных срабатываний. Опасность использования конкретных конструкций детектируется буквально в момент их сохранения в программном проекте благодаря лексерному и семантическому анализу. Технология анализа потоков данных повышает качество поиска за счет точного обнаружения реальных угроз.

** Gartner Research*
*** Static Application Security Testing*

INFOWATCH APPERCUT

5 ПРИЧИН ИСПОЛЬЗОВАТЬ INFOWATCH APPERCUT

Не требует специальных навыков
Результат анализа кода приложения или его фрагмента представляет собой отчет с рекомендациями по исправлению ошибок. Специальные знания и навыки программирования для получения и последующей интерпретации результатов анализа не нужны.

Учитывает требования международных стандартов и специфику бизнеса
В базе InfoWatch Appercut заложены требования международных стандартов PCI DSS и HIPAA, лучшие практики CERT и OWASP, рекомендации SDLC, а также рекомендации производителей платформ 1С, SAP, Oracle, Microsoft. Пользователи InfoWatch Appercut могут добавлять в базу данных некорректных программных конструкций собственные шаблоны, отражающие специфику бизнес-процессов организации.

Легко масштабируется и поддерживает более 20 языков программирования
Лицензия InfoWatch Appercut позволяет исследовать любое количество приложений бесконечное количество раз. Поддерживает наиболее популярные языки разработки бизнес-приложений, в том числе 1С и ABAP4, а также языки веб-программирования.

Обеспечивает непрерывность бизнес-процессов
Нет необходимости останавливать исполнение критичных для бизнеса приложений для трудоемкой и длительной ручной проверки кода или внешнего аудита.

Подходит для использования на любом этапе цикла разработки ПО
Интерфейс командной строки позволяет встраивать вызов InfoWatch Appercut и запускать процесс анализа исходного кода в любой процедуре жизненного цикла разработки ПО – от программирования до приемки.

ИНТЕГРАЦИЯ С WEB APPLICATION FIREWALL И ANTI-DDOS ДЛЯ ЗАЩИТЫ ВЕБ-ИНФРАСТРУКТУРЫ

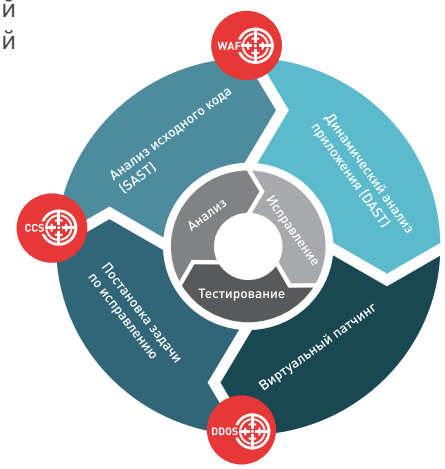
InfoWatch Attack Killer – непрерывная, активная и автоматизированная защита веб-инфраструктуры от внешних атак.

Синергия 4 технологий (SAST, DAST, WAF и Anti-DDoS) обеспечивает высокий уровень защиты, недостижимый при использовании подобных технологий по отдельности.

CCS **InfoWatch Attack Killer Custom Code Scanner (CCS)** – поиск уязвимостей приложений на основе технологии анализа исходного кода InfoWatch Appercut

WAF **InfoWatch Attack Killer WEB Application Firewall (WAF)** – защита от хакерских атак на веб-приложения и обнаружение уязвимостей веб-инфраструктуры на основе технологий компании Wallarm

DDOS **InfoWatch Attack Killer AntiDDoS** – гарантированное предотвращение DDoS-атак на основе технологии Qrator Labs



Технологии статического анализа исходного кода используются в рамках комплексного продукта для защиты веб-инфраструктуры от внешних атак InfoWatch Attack Killer. Модуль InfoWatch Attack Killer Custom Code Scanner, разработанный на базе Appercut, интегрирован с модулем InfoWatch Attack Killer WAF. Синергия технологий позволяет автоматизировать процесс безопасной разработки веб-приложений и сократить время выхода обновлений до 10 раз. InfoWatch Attack Killer обеспечит непрерывную и активную защиту критичного для бизнеса веб-ресурса.

INFOWATCH ® +7 (495) 22-900-22 sales@infowatch.ru www.infowatch.ru