АТАКИ НА ВАШУ ОРГАНИЗАЦИЮ – ПОД ПРИЦЕЛОМ НАШЕЙ ЗАЩИТЫ

INFOWATCH ATTACK KILLER

ВЫСОКАЯ БОЕВАЯ ЭФФЕКТИВНОСТЬ В БОРЬБЕ С МНОГОВЕКТОРНЫМИ ЦЕЛЕНАПРАВЛЕННЫМИ АТАКАМИ

INFOWATCH ATTACK KILLER

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

НЕПРЕРЫВНАЯ АКТИВНАЯ БЕЗОПАСНОСТЬ ПОСТОЯННО ИЗМЕНЯЮЩИХСЯ ОБЪЕКТОВ, КРИТИЧЕСКИ ВАЖНЫХ ДЛЯ БИЗНЕСА

Удобный инструмент, обеспечивающий непрерывную активную защиту от большинства видов таргетированных атак без дополнительных действий со стороны пользователя.

ЭВОЛЮЦИЯ ЗАЩИТЫ

1998	2005	2007	2009	2012	2015
Включил и работает. **Использование базовых методов защиты**: антивирусы, фаерволы и др.	**Усложнение** корпоративной инфраструктуры **и перенесение бизнес-процессов** в плоскость ИТ	**Уход от активной защиты**: ложные срабатывания – страшней инцидента	**Ответственность за инциденты** на офицерах безопасности: настроить, поддерживать, оценивать,реагировать – вовремя!	**Неготовность к новым видам атакам**: защита от угроз, о которых еще не известно	Включил – работает и защищает: **Continuous Security** – ответ на современные угрозы

- Вирусы, трояны
- Утечки информации
- Хакерские взломы, DDoS
- Таргетированные атаки
- Многовекторные таргетированные атаки

Сегодня действия злоумышленников становятся всё более изощренными. Используя уже ставшие традиционными методы атак, хакеры могут достичь своих целей – например, кражи данных или денежных средств – благодаря комплексному воздействию и тщательной подготовке кампании, направленной против конкретной организации.

МНОГОВЕКТОРНЫЕ ТАРГЕТИРОВАННЫЕ (ЦЕЛЕНАПРАВЛЕННЫЕ) АТАКИ

- это организованный комплекс действий злоумышленников против конкретной организации.

Отдельными элементами цепи спланированных действий становятся известные угрозы:

- внедрение специализированного вредоносного программного обеспечения
- эксплуатация уязвимостей веб-инфраструктуры и исходного кода бизнес-приложений
- методы социальной инженерии
- DDoS-атаки

Чаще всего целью хакеров является воровство платежных данных и коммерческих секретов, хищение средств, а также вывод из строя критически важных объектов инфраструктуры.

ТИПОВОЙ СЦЕНАРИЙ АТАКИ

РАЗВЕДКА

1. Сканирование веб-инфраструктуры жертвы на уязвимости
2. Разведка в части внутренней защиты компании

ОТВЛЕЧЕНИЕ ВНИМАНИЯ

DDoS-атака

ВХОД В СИСТЕМУ

1. Уязвимости веб-инфраструктуры и бизнес-приложений
2. Фишинг
3. Социальная инженерия

ЗАКРЕПЛЕНИЕ В ИТ-СИСТЕМЕ И ДОЛГОСРОЧНОЕ НАХОЖДЕНИЕ В КОМПАНИИ

1. Заказное вредоносное ПО, не детектируемое базовыми средствами защиты
2. Уязвимости приложений

СОКРЫТИЕ СЛЕДОВ

DDoS-атака

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

УЩЕРБ ДЛЯ БИЗНЕСА ОТ ТАРГЕТИРОВАННЫХ АТАК

1. **Нарушение доступности** вследствие DDoS
2. **Нарушение целостности** вследствие хакерского взлома
3. **Нарушение конфиденциальности** вследствие кражи конфиденциальной информации

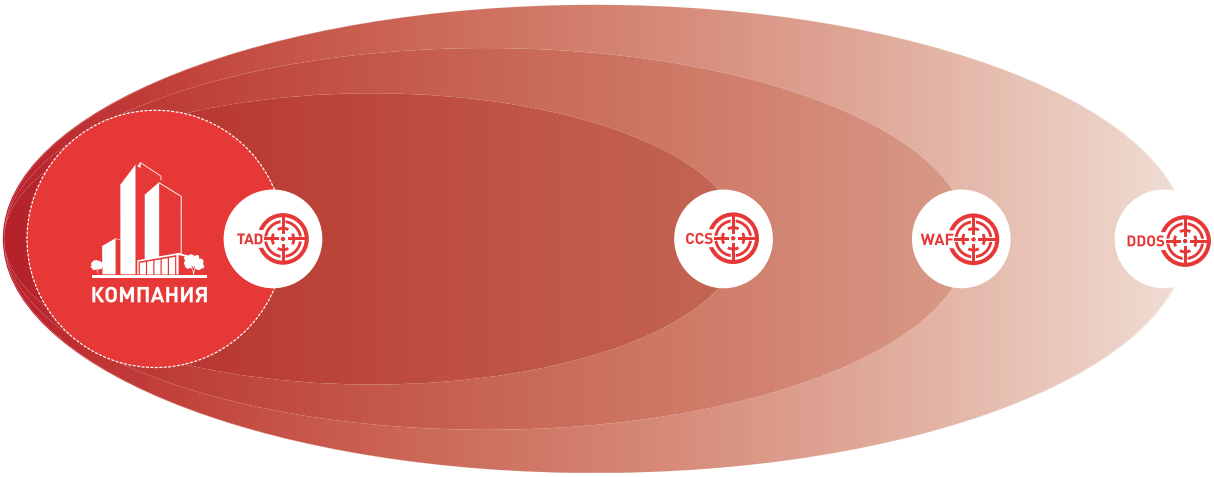
Прямые финансовые потери и репутационный ущерб

- Вывод из строя объектов, критически важных для бизнеса
- Прямой финансовый ущерб из-за дестабилизации работы веб-ресурсов
- Репутационные потери
- Утечка платежных данных, конфиденциальной информации, ноу-хау, коммерческой тайны
- Перенаправление счетов, воровство и мошенничество
- Компрометация персональных и финансовых данных

CONTINUOUS SECURITY - ОТВЕТ НА СОВРЕМЕННЫЕ УГРОЗЫ

Успешная защита от многовекторных таргетированных атак возможна только при комплексном подходе, закрывающем наиболее популярные методы проникновения злоумышленников. С одной стороны, чаще всего заказное зловредное ПО попадает в организацию через уязвимости веб-инфраструктуры, с другой – в компании всегда может оказаться сотрудник, который случайно или намеренно запустит специализированную троянскую программу, например, с флеш-накопителя.

Подход InfoWatch представляет собой комплексную защиту как на уровне рабочих станций и серверов, так и на уровне веб-инфраструктуры.



TAD *InfoWatch Attack Killer Targeted Attack Detector (TAD)*

WAF *InfoWatch Attack Killer WEB Application Firewall (WAF)*

CCS *InfoWatch Attack Killer Custom Code Scanner (CCS)*

DDOS *InfoWatch Attack Killer AntiDDoS*

При этом, безопасность веб-приложений усложняется тем фактором, что они постоянно изменяются – а значит, изменяются и настройки, тонкость и точность которых обеспечивает свободный доступ к сайту легитимных пользователей. Заказное зловредное ПО, оказавшееся внутри компании, не детектируется антивирусными программами и другими базовыми средствами защиты – обнаружить его можно только с помощью непрерывного мониторинга состояния ИТ-инфраструктуры и обнаружения в ней системных аномалий.

Для защиты от многовекторных таргетированных атак компания InfoWatch создала уникальный продукт класса Continuous Security.

Отличительной особенностью данного комплекса является непрерывность защиты, а также способность автоматически адаптироваться к изменяющимся объектам, критически важным для бизнеса. Постоянное машинное самообучение системы позволяет минимизировать участие офицера безопасности в процессе защиты и настройки.

INFOWATCH ATTACK KILLER

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

ЗАЩИТА ОТ СЛОЖНЫХ АТАК: ПРОСТО КАК «РАЗ-ДВА-ТРИ»

ШАГ 1 | ДИНАМИЧЕСКОЕ ОБНАРУЖЕНИЕ ТАРГЕТИРОВАННЫХ АТАК ВНУТРИ КОМПАНИИ

Модуль InfoWatch Attack Killer Targeted Attack Detector предназначен для обнаружения таргетированных атак или их следов на рабочих станциях и серверах.

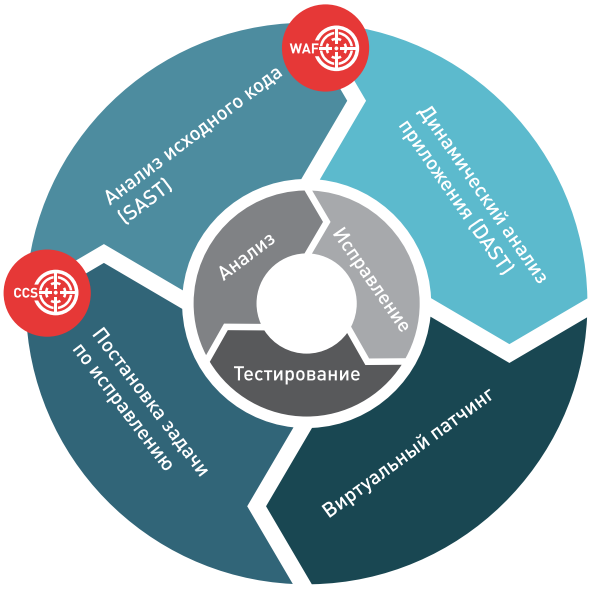
Самообучающаяся экспертная облачная система проводит непрерывный мониторинг ИТ-инфраструктуры и анализирует полученные данные на наличие в ней аномальных активностей. Решение постоянно выполняет сканирование с целью сбора и классификации широкого спектра характеристик объектов системы. Результатом сканирования является срез системы (slice), который подвергается нескольким видам анализа.

Использование различных видов анализа обеспечивает высокую точность классификации аномалий. Решение поможет выявить вредоносное ПО, которое было внедрено в компанию даже до начала эксплуатации решения InfoWatch Attack Killer TAD.

ШАГ 2 | ВНЕДРЕНИЕ БЕЗОПАСНОЙ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЙ

Безопасный выпуск обновлений для веб-приложений возможен благодаря совместному использованию модулей InfoWatch Attack Killer CCS и InfoWatch Attack Killer WAF. Статический анализ кода, проводимый модулем CCS, детектирует уязвимости, а затем передает их на модуль WAF. Встроенный динамический сканер в модуле WAF определяет уровень критичности найденных уязвимостей, подтверждая их выпуском эксплойтов.

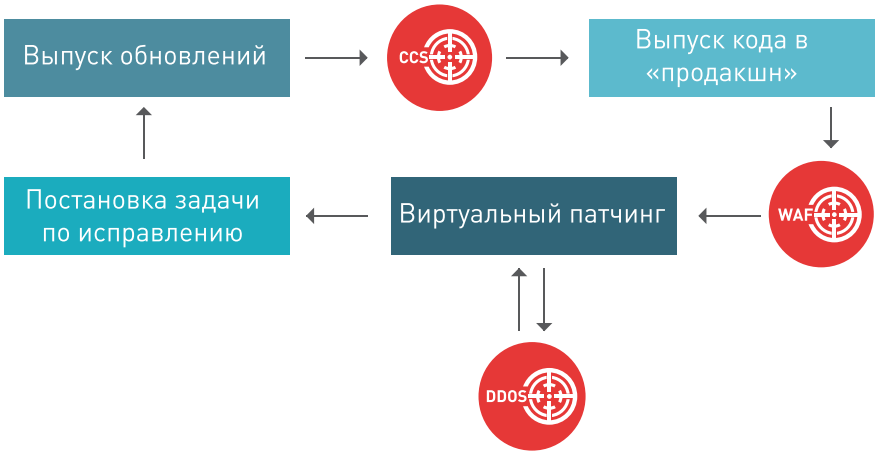
Подтвержденные уязвимости автоматически закрываются виртуальными патчами до их исправления разработчиками. Совместное использование CCS и WAF позволит повысить полноту обнаруженных ошибок в коде, вместе с тем, минимизируя количество ложных срабатываний практически до нуля. Такой подход к разработке дает возможность выпускать безопасные обновления сайта с уникальными возможностями для посетителей быстрее конкурентов.



ШАГ 3 | КОМПЛЕКСНАЯ ЗАЩИТА ВЕБ-ИНФРАСТРУКТУРЫ

Даже при частых обновлениях сайт останется под надежной защитой InfoWatch Attack Killer. После подтверждения гипотез об уязвимостях, найденных модулем CCS, WAF передает информацию на модуль AntiDDoS, который блокирует зловредные запросы на уровне узлов фильтрации, расположеные на магистралях крупнейших интернет-провайдеров.

Уникальная архитектура системы узлов фильтрации обеспечивает защиту от DDoS-атак и хакерских взломов на начальном этапе. Приятным бонус для владельцев сайтов станет снижение нагрузки на веб-приложение и увеличение его быстродействия, благодаря фильтрации зловредных запросов на максимальном «расстоянии» от периметра сети.



INFOWATCH ATTACK KILLER

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

InfoWatch Attack Killer – объединяет четыре технологии, разработанных лидерами своих продуктовых ниш. Глубокая взаимная интеграция и синергия всех используемых технологий позволяют добиться высокого уровня защищенности, недостижимого при использовании технологий соответствующих классов по отдельности.

TAD

InfoWatch Attack Killer Targeted Attack Detector (TAD) – модуль обнаружения вредоносного программного обеспечения на рабочих станциях и серверах посредством статического и динамического анализа аномалий.

- С помощью анализа аномалий выявляет таргетированные атаки, реализуемые злоумышленниками с использованием специализированного программного обеспечения
- Осуществляет непрерывный мониторинг изменений состояния ИТ-системы и позволяет обнаружить замысел противника
- Благодаря самообучающимся алгоритмам экспертная облачная система с высокой точностью классифицирует обнаруженные аномалии
  - при необходимости к анализу подключаются аналитики InfoWatch

CCS

InfoWatch Attack Killer Custom Code Scanner (CCS) – модуль выявления уязвимостей в коде веб-приложений.

- Обнаруживает ошибки в исходном коде с учетом требований по безопасному программированию PCI DSS, OWASP, рекомендаций SDLC, а также производителей платформ
- Поддерживает все самые известные языки программирования (Java, PHP, JavaScript, C# и др.)

WAF

InfoWatch Attack Killer WEB Application Firewall (WAF) – модуль для предотвращения хакерских атак на веб-приложения и обнаружения уязвимостей веб-инфраструктуры.

- Автоматически непрерывно изучает веб-инфраструктуру компании
  - отправляет на анализ в облачную экспертную систему поведенческую статистику пользователей, результаты динамического сканирования ресурсов
  - на основе информации об уязвимостях, найденных модулем CCS, WAF выявляет какие из них могут стать реальными инцидентами ИБ
- Экспертная система WAF на основе всей собранной информации определяет «норму» работы веб-инфраструктуры и блокирует все аномальные действия (отличные от нормы)
  - выпускает виртуальные патчи для блокировки аномальных запросов до исправления уязвимостей разработчиками
  - анализируя аномалии в неструктурированных событиях находит логику и объединяет их в инцидент, определяя вектор атаки

DDOS

InfoWatch Attack Killer AntiDDoS – модуль позволяет выявлять и гарантированно предотвратить масштабные DDoS-атаки.

- Блокирует масштабные DDoS-атаки на начальном этапе благодаря распределенной системе узлов фильтрации
  - отказ любого из узлов не вызовет изменений в качестве обслуживания (BGP Anycast)
- Защищает ресурс непрерывно и в автоматическом режиме сразу после подключения
  - в случае атаки от клиента не потребуется дополнительных действий
- Обеспечивает защиту для большинства протоколов (HTTP, HTTPS, DNS, SIP и др.)

INFOWATCH ATTACK KILLER

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

ПОЧЕМУ?

ЕДИНСТВЕННОЕ В МИРЕ РЕШЕНИЕ

InfoWatch Attack Killer реализует многоуровневый подход к обнаружению и защите от большинства видов таргетированных атак

НЕПРЕРЫВНАЯ АКТИВНАЯ ЗАЩИТА, НИВЕЛИРУЮЩАЯ ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Активы компании находятся под непрерывной защитой с момента подключения. Пользователи InfoWatch Attack Killer узнают о попытках атак только из отчетов

АВТОМАТИЧЕСКАЯ АДАПТАЦИЯ К ОБЪЕКТАМ ЗАЩИТЫ И ИХ ИЗМЕНЕНИЯМ

Внедрение всего комплекса займет от нескольких часов до нескольких дней. При этом, активная защита начнется сразу, с момента подключения

УДОБНОЕ УПРАВЛЕНИЕ ЧЕРЕЗ ЕДИНЫЙ ВЕБ-ИНТЕРФЕЙС

Решение управляется из единой консоли и создает детализированные отчеты о зафиксированных таргетированных атаках, найденных уязвимостях и попытках их эксплуатации, аномальной активности приложений и DDoS-атаках

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ

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

РЕШЕНИЕ-КОНСТРУКТОР

Позволяет использовать каждый модуль по отдельности, в любых сочетаниях, а также быстро расширить используемый комплекс до полного комплекта

СОЮЗ ЛУЧШИХ В СВОЕМ КЛАССЕ!

ГК InfoWatch объединила передовые технологии лучших производителей средств защиты для эффективной безопасности бизнеса

О ГК INFOWATCH

Группа компаний InfoWatch объединяет ряд российских и зарубежных разработчиков программных продуктов и решений для обеспечения информационной безопасности организаций, противодействия внешним и внутренним угрозам. InfoWatch обладает обширной экспертизой и опытом реализации проектов информационной безопасности любой сложности в государственном секторе, ТЭК, финансовой, телекоммуникационной и многих других отраслях экономики.

cezurity — ГК InfoWatch является стратегическим инвестором компании **Cezurity**, разрабатывающей технологии и решения для защиты от широкого круга вредоносных программ и хакерских атак.

APPERCUT — **Appercut** входит в ГК InfoWatch и с 2011 года предлагает решение для поиска уязвимостей в исходном коде бизнес–приложений.

QRATOR — Компания **Qrator Labs*** с 2009 года занимается противодействием самым сложным и комплексным DDoS-атакам благодаря собственной инновационной сети фильтрации.

wallarm — Компания **Wallarm*** разрабатывает продукты, совмещающие в себе функции защиты веб-приложений от хакерских атак и поиска уязвимостей

** Компании Qrator Labs и Wallarm являются технологическими партнерами InfoWatch*

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