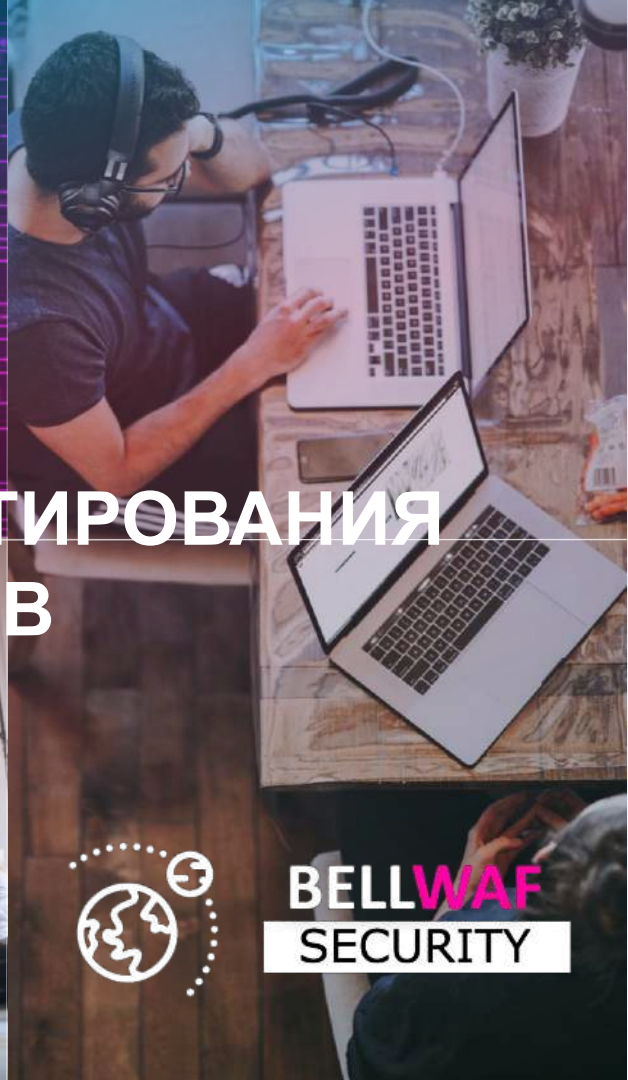
РЕШЕНИЯ ДЛЯ ЗАЩИТЫ И ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ WEB-РЕСУРСОВ



Bellintegrator

BELLWAF SECURITY

Новые технологии и цифровизация приносят не только реальные преимущества для компаний и их клиентов, но и новые риски кибербезопасности.

Немаловажным являются требования регулирующих органов к финансовым организациям и госорганам в части защиты информации.

ОСНОВНЫЕ СТАНДАРТЫ, РЕГУЛИРУЮЩИЕ ЗАЩИТУ

- **СТО БР ИББС-1.0-2014**
- **Письмо Банка России от №49-Т** «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности»
- **Положение Банка России № 382-П** «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств» (Положение Банка России №719-П от 04.06.2020 вступило в силу с 01.01.2022г. вместо №382-П (утратило силу))
- **Положение Банка России №552-П** "О требованиях к защите информации в платежной системе Банка России
- **ГОСТ Р 57580.1-2017** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер».
- **63-ФЗ** «Об электронной цифровой подписи»
- **98-ФЗ** «О Коммерческой тайне»
- **149-ФЗ** «Об информации, информационных технологиях и о защите информации»
- **152-ФЗ** «О персональных данных»
- **187-ФЗ** «Критическая информационная инфраструктура»
- **PCI DSS**
- **ПП № 1119** «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПОВЫШЕНИЕ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ:

- Защитит ценную интеллектуальную собственность и данные клиентов от киберпреступников
- Позволит разработать стратегии, направленные на обеспечение более строгого соблюдения требований в сфере финансовых услуг при одновременном снижении давления со стороны регулирующих органов
- Расширит набор навыков и возможностей персонала в области ИТ и кибербезопасности
- Усилит мониторинг и скорость принятия мер противодействия кибератакам
- Сократит время, необходимое для реагирования на угрозы

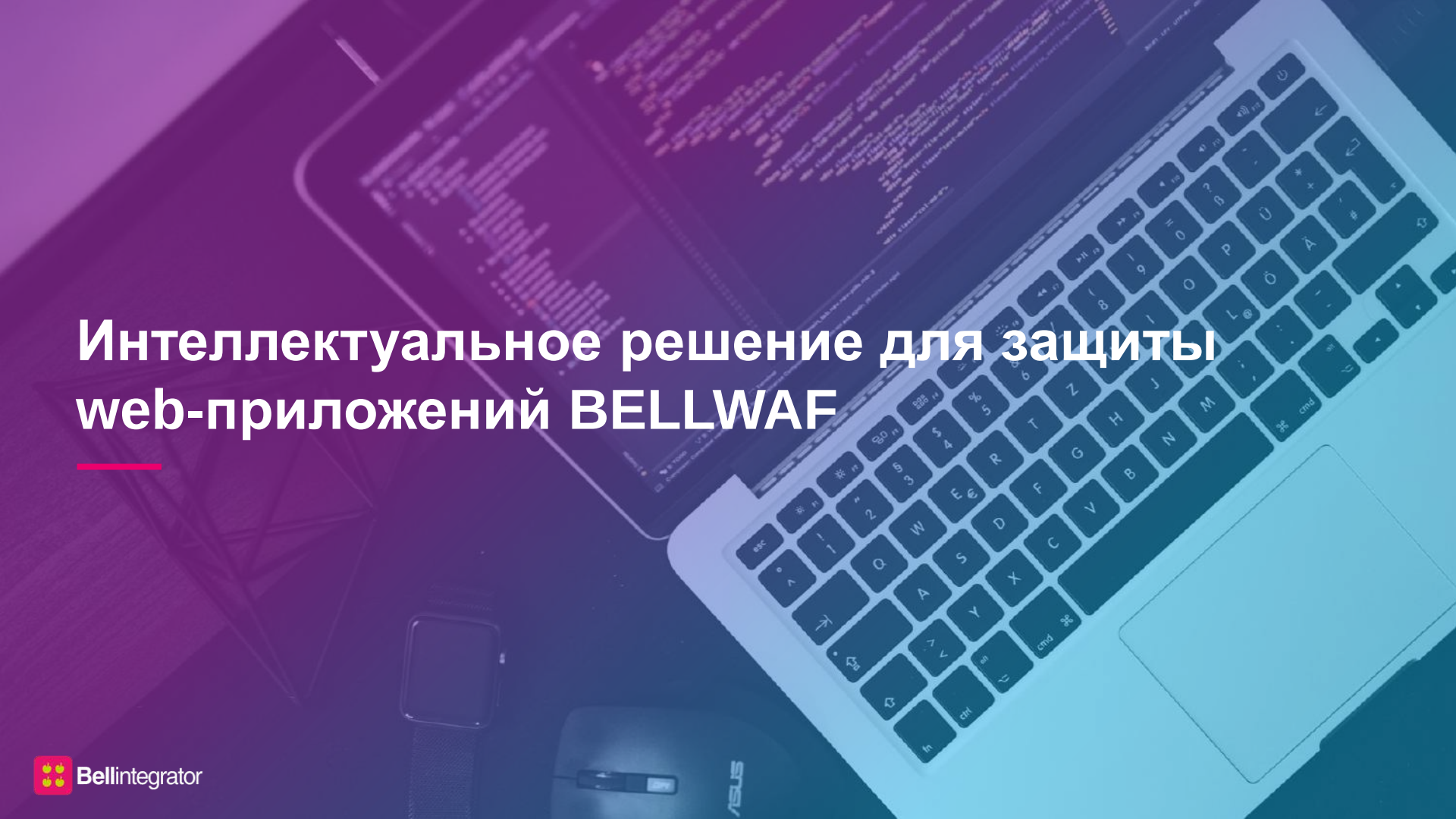
КАК ОБЕСПЕЧИТЬ КИБЕРБЕЗОПАСНОСТЬ КОМПАНИЙ

- **Регулярные ИБ тренинги** — для повышения осведомленности персонала в вопросах информационной безопасности
- **Аудит информационной безопасности и инструменты сканирования сети** для обнаружения и предотвращения эксплуатации уязвимостей, своевременного патчинга
- **Корректная сегментация сети** — для лучшего контроля сетевого трафика и повышения эффективности систем кибербезопасности
- **NTA (Network Traffic Analysis)** — для обнаружения аномалий в трафике и выявления кибератак на ранних этапах
- **Межсетевые экраны и системы обнаружения и предотвращения вторжений (IDS/IPS)** — для защиты периметра сети, блокировки несанкционированного доступа и обнаружения потенциально вредоносного трафика
- **WAF (Web Application Firewall)** — для защиты веб-ресурсов с помощью межсетевых экранов приложений от таких атак, как межсайтовая подделка запроса (CSRF), межсайтовый скриптинг (XSS), SQL-инъекция и других угроз
- **Защита конечных точек** для снижения риска заражения программами и вирусами, шифрования информации, соблюдения соответствия политикам и регламентам ИБ
- **Организация безопасного удаленного доступа к сети и создания зашифрованного канала связи** с помощью средств криптографической защита информации (СКЗИ) и VPN

КАК ОБЕСПЕЧИТЬ КИБЕРБЕЗОПАСНОСТЬ КОМПАНИЙ

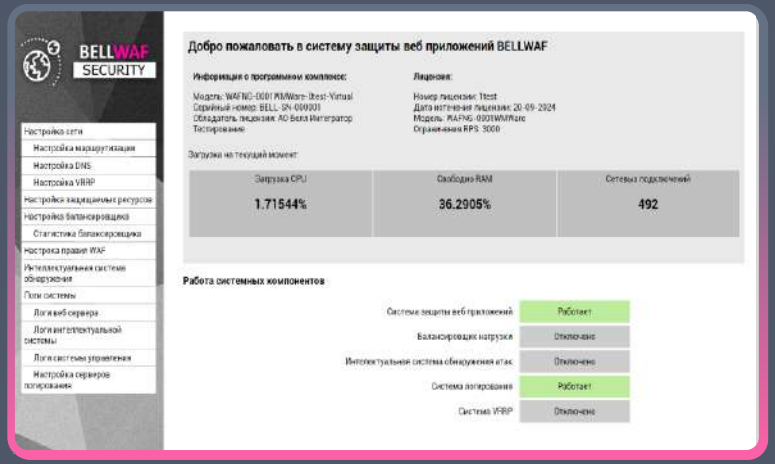
- **СЗИ от НСД** — для защиты стационарных и мобильных устройств от несанкционированного доступа, а также обеспечения соответствия требованиям регуляторов
- **DLP-системы** — для предотвращения утечки конфиденциальных материалов, а именно: анализа и блокировки данных, передаваемых с помощью электронной почты, мессенджеров, интернет-ресурсов и других источников
- **Системы управления доступом (IDM, PIM)** — для контроля жизненного цикла учетных записей и разграничения прав доступа к сегментам сети
- **Решения для управления сетевым доступом (NAC)** — для инвентаризации устройств, обеспечения видимости и контроля подключений к корпоративной сети
- **Системы классификации данных** — для повышения безопасности конфиденциальной информации путем классификации, определения пользователей, взаимодействовавших с документами, упрощения доступа, поиска и отслеживания данных, а также устранения дублирований
- **Использование интерактивных ловушек** для эффективного обнаружения APT-атак
- **Threat Intelligence** — для система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры на основании данных о тактиках, инструментах и активности злоумышленников
- **Антифрод-решения** — для проактивной защиты цифровой личности, предотвращения мошенничества и бот-атак на всех устройствах, платформах и сессиях пользователя в режиме реального времени

Интеллектуальное решение для защиты web-приложений BELLWAF



Bellintegrator

BELLWAF SECURITY



Решение основано на передовых технологиях и регулярных исследованиях экспертов, чтобы обеспечить высочайший уровень безопасности и непрерывность бизнес-процессов организации.

BellWAF — это мощный инструмент защиты от веб-угроз. Используя инновационные технологии и глобальную аналитику, WAF непрерывно осуществляет проактивную защиту веб-приложений от большинства атак, включая OWASP Top 10, автоматизированные атаки, атаки на стороне клиента и атаки нулевого дня.

Другой отличительной особенностью является **простота внедрения и использования**. Благодаря интуитивному интерфейсу и высокому уровню автоматизации BellWAF понятен специалистам даже без глубоких технических знаний.

Bellintegrator

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

МАШИННОЕ ОБУЧЕНИЕ ПРОТИВ АТАК НУЛЕВОГО ДНЯ

Передовые техники машинного обучения **позволяют мгновенно и точно определять атаки**, включая атаки нулевого дня. Они также обеспечивают высокий уровень автоматизации продукта, включая способность к самообучению, что минимизирует ручной труд.

МЕХАНИЗМЫ КОРРЕЛЯЦИИ ДЛЯ ТОЧНОГО ОПРЕДЕЛЕНИЯ ОСНОВНЫХ УГРОЗ

Механизмы корреляции **проводят тщательный анализ данных** (поведения пользователей, уязвимостей и др.) и **выстраивают цепочки атак**. Это позволяет с высокой точностью определять только основные угрозы при минимуме ложных срабатываний.

АВТОМАТИЧЕСКОЕ ПРОФИЛИРОВАНИЕ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ

Благодаря непрерывному профилированию поведения пользователей на базе машинного обучения WAF проактивно **защищает от DDoS-атак уровня приложений и автоматизированных атак**, осуществляемых с целью кражи уникального контента или размещения несанкционированного контента на защищаемом сайте. Постоянно обучаясь на реальных данных, продукт создает профиль нормального пользовательского поведения и сравнивает его с остальными действиями, которые могут отличаться и, следовательно, быть опасными. В результате алгоритм машинного обучения может предсказывать возможные атаки, а сама система — заранее предупредить офицера информационной безопасности о таких обнаружениях. При этом WAF не оказывает влияние на активность пользователей и «хороших» программ-роботов.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

ШИРОКИЕ ВОЗМОЖНОСТИ ИНТЕГРАЦИИ ДЛЯ МНОГОУРОВНЕВОЙ ЗАЩИТЫ

WAF можно **интегрировать с другими системами** (Check Point, Arbor, Cisco ASA) для блокировки подозрительной активности пользователей в рамках всей инфраструктуры организации. Интеграция с **SIEM-системами**, такими как ArcSight (Micro Focus), QRadar, Check Point SmartCenter, PT SIEM — также обеспечивает защиту по всему периметру, синхронизируя все события безопасности в едином интерфейсе.

ПРЕИМУЩЕСТВА ДЛЯ ОРГАНИЗАЦИЙ. ЭКСПЕРТНАЯ ЗАЩИТА В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Исследовательский центр Bell Integrator **анализирует данные** со всего мира в режиме реального времени. На базе этой аналитики и с учетом постоянно улучшаемых технологий продукт регулярно автоматически обновляется. Это обеспечивает проактивную защиту от самых современных угроз.

ДОСТУПНОСТЬ

BellWAF можно **развернуть как аппаратное или виртуальное устройство**. Продукт также полностью готов для работы в качестве **облачного сервиса** в моделях SaaS, VAS и MSS.

ПОМОЩЬ В СОБЛЮДЕНИИ СТАНДАРТОВ

BellWAF помогает **выполнять требования PCI DSS**, приказов и требований **ФСТЭК России**, а так же для финансовых организаций соблюдение **ГОСТ 57580** и других международных, государственных и корпоративных стандартов безопасности.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

ВЫСОКАЯ ПРОДУКТИВНОСТЬ

BellWAF значительно упрощает повседневное управление безопасностью приложений. Удобство интерфейса, автоматизированные процессы управления и защиты и точное определение самых важных рисков существенно улучшают производительность сотрудников ИБ, помогая им сконцентрироваться на решении действительно значимых задач.

БЫСТРЫЙ И ПРОСТОЙ ЗАПУСК

Благодаря высокому уровню автоматизации **продукт можно быстро установить и настроить даже без глубоких технических знаний**. Это позволяет существенно сэкономить время и ресурсы на внедрение вне зависимости от количества и сложности приложений.

ГИБКОСТЬ УПРАВЛЕНИЯ ДЛЯ НАСТРОЙКИ ПРОДУКТА НА ЛЕТУ

В BellWAF предусмотрено **множество опций для детальной настройки системы**. Готовые шаблоны политик безопасности можно мгновенно применить для любого количества защищаемых приложений или их отдельных частей.

ПРОСТОТА ВНЕДРЕНИЯ И ИСПОЛЬЗОВАНИЯ. ИНТУИТИВНО ПОНЯТНЫЙ ИНТЕРФЕЙС

BellWAF можно быстро развернуть в режиме «прозрачный прокси-сервер, обратный прокси-сервер, режим мониторинга или расследований». При этом он готов обслуживать до 160 000 rps обращений без отказа в обслуживании и выполнять функцию балансировщика нагрузки.

Bellintegrator

КОНКУРЕНТЫ

GROUP-IB

УШЛА С РЫНКА

BI.ZONE Cybersecurity

РЕШЕНИЕ УЖЕ БОЛЬШЕ ГОДА **НАХОДИТСЯ В РАЗРАБОТКЕ**

solidwall

РЕШЕНИЕ РАБОТАЕТ В ПОЛНОМ ОБЪЕМЕ **ТОЛЬКО В ОБЛАКЕ**

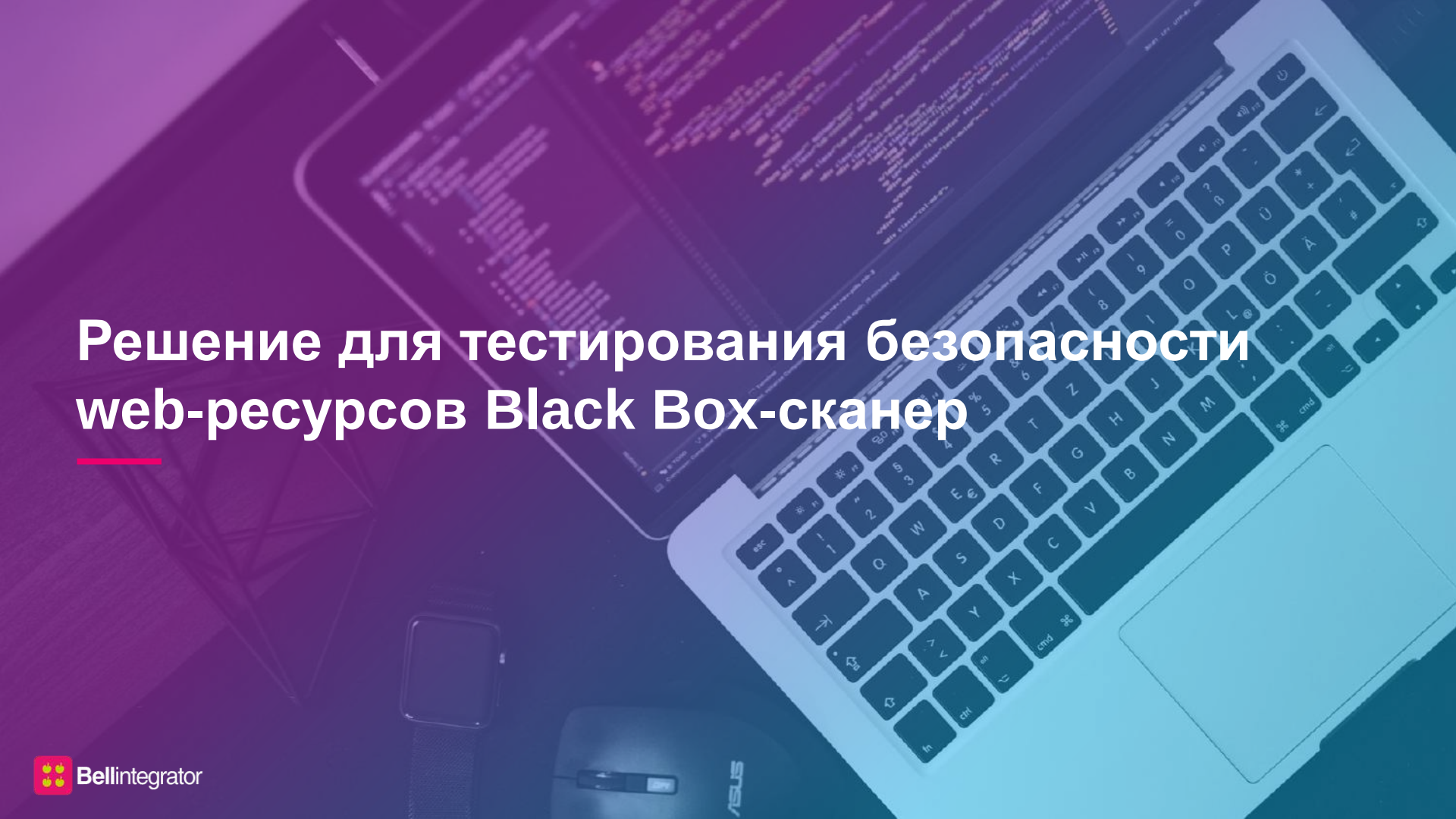
wallarm

УШЛА С РЫНКА

BI.ZONE Cybersecurity

Мы пошли дальше. И на основе WAF создали собственную систему комплексного сканирования и тестирования веб-приложений на уязвимости.

Решение для тестирования безопасности web-ресурсов Black Box-сканер



Bellintegrator

Black Box-сканер

Мы разработали свой продукт, который позволяет анализировать защищенность приложений, выявлять и устранять уязвимости в них на ранней стадии разработки.

Чтобы выявить уязвимости, Black Box-сканер использует метод черного ящика при сканировании приложений — имитирует поведение злоумышленника, у которого нет знаний о внутреннем устройстве приложения. Это позволяет оценивать защищенность веб-приложения без использования каких-либо исходных данных, кроме адреса веб-цели. Такой динамический анализ помогает своевременно находить уязвимости приложений и предотвращать реализацию угроз безопасности, которые могут негативно сказаться на деятельности компании.

КАК ЭТО РАБОТАЕТ?

1›

Мы либо берем готовые коллекции postman, либо запускаем сканирование сайта по адресу, и система начинает пассивное сканирование.

В результате пассивного сканирования создается карта сайта, загружается его содержимое, система начинает смотреть на различные формы и поля, через которые можно совершить то или иное действие (например, подменить значение или попробовать перехватить токен пользователя), а также анализировать адреса и контент всех имеющихся запросов.

Во время прохода пассивным сканером мы смотрим сообщения WAF и анализируем их на предмет возможных уязвимостей.

2›

На втором этапе запускается активный сканер, который благодаря полученной информации начинает пенетрировать приложение.

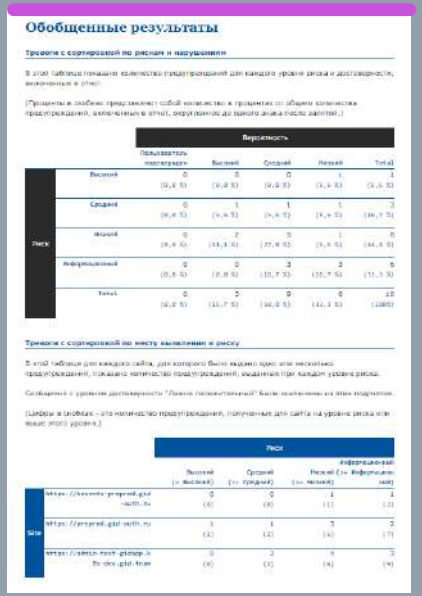
Когда активное сканирование заканчивается, и система понимает, что сайт на самом деле не такой простой, то запускается AJAX-сканер, который, исполняя в песочнице код сайта, компилирует необходимые данные, исследует полученный код и пытается взломать наше веб-приложение.

РЕЗУЛЬТАТ РАБОТЫ СКАНЕРА

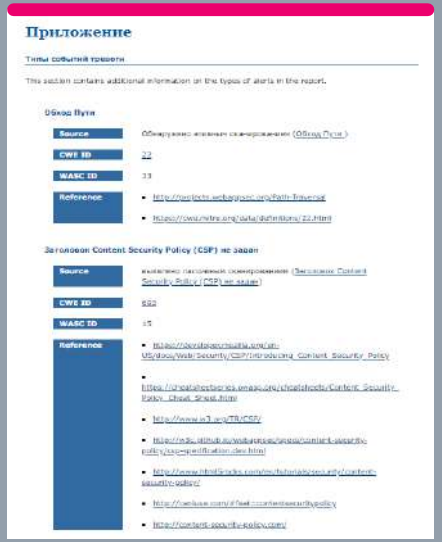
Результатом работы сканера является сводка по возможным уязвимостям, степени риска, а главное возможности эксплуатации той или иной уязвимости. А собранная база данных уязвимостей при ознакомлении с ними в отчете несет в себе информацию по их устранению.


Отчет о Комплексном Инструментальном Сканировании Безопасности

Содержание


Обобщенные результаты


Тревоги


Приложение

ПРЕИМУЩЕСТВА BLACK BOX-СКАНЕРА

УНИВЕРСАЛЬНОСТЬ

Black Box-сканер может быть использован для тестирования безопасности любого веб-приложения, независимо от его типа или размера.

ТОЧНОСТЬ

Black Box-сканер обеспечивает высокую точность результатов тестирования, что позволяет выявить все уязвимости в веб-приложении.

ЭКОНОМИЯ ВРЕМЕНИ

Black Box-сканер позволяет быстро и точно определить все уязвимости в веб-приложении, что значительно экономит время на тестирование безопасности.

АВТОМАТИЗАЦИЯ

Black Box-сканер позволяет автоматизировать процесс тестирования безопасности, что значительно экономит время и ресурсы.

ПРОСТОТА ИСПОЛЬЗОВАНИЯ

Black Box-сканер имеет интуитивно понятный интерфейс и не требует специальных знаний или навыков для работы с ним.

НАДЕЖНОСТЬ

Black Box-сканер является надежным инструментом, который может работать в любых условиях и не требует особого обслуживания.

Black Box-сканер для web-приложений полностью закрывает потребности информационной безопасности по безопасной разработке.

Он позволяет быстро и точно определить все уязвимости в web-приложениях.

В Bell Integrator Black Box-сканер применяется для проверки ВСЕХ приложений, доходящих до стадии публикации в релиз.

Другие ИБ-решения от компании Bell Integrator

Bellintegrator

НОВОЕ РЕШЕНИЕ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОНТЕЙНЕРОВ

(CSP) Container Security Platform

Container Security Platform (CSP) - это платформа для обеспечения безопасности контейнеров. Она предоставляет инструменты и сервисы для защиты контейнеров от различных угроз, таких как вредоносное ПО, хакерские атаки и другие виды кибератак. CSP позволяет автоматизировать процесс обеспечения безопасности контейнеров, что значительно экономит время и ресурсы, и обеспечивает высокую точность результатов тестирования, что позволяет выявить все уязвимости в контейнерах. CSP имеет интуитивно понятный интерфейс и не требует специальных знаний или навыков для работы с ним. CSP является надежным инструментом, который может работать в любых условиях и не требует особого обслуживания.

РЕШЕНИЯ В ПРОЦЕССЕ РАЗРАБОТКИ

Bell NGFW

Файрвол с возможностью интеллектуальной защиты сети до уровня L7, а также возможностью интеграции с внешними IRP-системами, работы с SIEM-системами

Bell Web/Mail Scanner

Обеспечивает защиту электронной почты с помещением вредоносной корреспонденции в отдельную защищенную песочницу (sandbox) и предотвращает проникновение в защищенный периметр вредоносного кода

Bell IDS/IPS

Анализатор трафика для обнаружения и принятия решений по блокировке выявленного вредоносного трафика как в режиме мониторинга бриджа, так и в качестве маршрутизатора

SIEM (Security information and event management)

Решение для мониторинга событий безопасности в реальном времени, а также долгосрочного хранения и анализа данных с различных объектов инфраструктуры организации

СПАСИБО!

Сергей Головашов

+7(999) 964-00-34

SGolovashov@bellintegrator.ru

BELLWAF

BLACKBOX

Москва, 2-й Южнопортовый проезд 18, стр. 2

тел.: +7 (495) 980-6181
факс: +7 (495) 980-6183

info@bellintegrator.ru
www.bellintegrator.ru