КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ WAF

О КОМПАНИИ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ФАКТЫ О КОМПАНИИ

Компания «Код Безопасности» - российский разработчик программных и аппаратных средств, обеспечивающих защиту информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

Более 20 лет на страже безопасности крупнейших предприятий России. Ведет свою деятельность на основании **9 лицензий ФСТЭК, ФСБ и Минобороны РФ**.

Технологии защиты обеспечивают безопасность **1 200 000 компьютеров** в **32 000 организаций.**
3 центра разработки: Москва, Санкт-Петербург, Пенза.

Более **300 квалифицированных специалистов R&D**, имеющих уникальные компетенции.

Более **50 разработанных СЗИ и СКЗИ.**

Более **60 действующих сертификатов** соответствия подтверждают высокое качество продуктов.

Партнерская сеть компании насчитывает **более 900 авторизованных партнеров.**

Компетентность «Кода Безопасности» подтверждена независимыми аналитиками:

- **«Крупнейшие производители высокотехнологичного оборудования»: №1** («Эксперт РА»), **№3** («Коммерсант»).
- **«Крупнейшие разработчики программного обеспечения»: №7** («Эксперт РА»), **№9** («Коммерсант»).
- **«Крупнейшие ИТ-компании России»: №30** («Коммерсант»), **№47** (TAdviser).

КОД БЕЗОПАСНОСТИ

ЦЕЛОСТНЫЙ ПОДХОД К ИБ

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

ЗАЩИТА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

ЗАЩИТА ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

КОД БЕЗОПАСНОСТИ

НАМ ДОВЕРЯЮТ

ГОСУДАРСТВЕННЫЕ ОРГАНИЗАЦИИ:

- Федеральное казначейство России
- Федеральная налоговая служба России
- Федеральная таможенная служба России
- Федеральный Фонд обязательного медицинского страхования
- Центральная избирательная комиссия Российской Федерации
- Министерство юстиции Российской Федерации

СИЛОВЫЕ СТРУКТУРЫ:

- Министерство внутренних дел Российской Федерации
- Министерство обороны Российской Федерации
- Федеральная служба безопасности Российской Федерации
- Федеральная служба охраны Российской Федерации

ТЕЛЕКОММУНИКАЦИОННЫЕ КОМПАНИИ:

- ПАО «Ростелеком»
- ФГУП «Почта России»
- ГК «АКАДО Телеком»
- АО «Военелеком»

ФИНАНСОВЫЕ ОРГАНИЗАЦИИ:

- ПАО «Сбербанк»
- Центральный банк Российской Федерации
- ГК «Внешэкономбанк»
- АО «Газпромбанк»
- АО «Страховая группа МСК»
- ПАО «ВТБ24»
- ПАО «Банк «Возрождение»

ПРОМЫШЛЕННЫЕ ПРЕДПРИЯТИЯ:

- ГК «Ростех»
- АО «Российские космические системы»
- ПАО «ГМК «Норильский никель»
- ГКНПЦ им. М.В. Хруничева

ПРЕДПРИЯТИЯ ТЭК:

- Государственная корпорация по атомной энергии «Росатом»
- ПАО «Газпром»
- ОАО «АК «Транснефть»
- ОАО «НК «Роснефть»

О ПРОДУКТЕ

КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ WAF

КОНТИНЕНТ WAF

Защита веб-приложений и автоматизированный анализ их бизнес-логики

Предназначен для решения следующих задач:

- **Защита веб-приложений от специфических угроз (OWASP TOP 10*)**
- **Защита от ошибок в логике приложения**
- **Защита от DoS-атак уровня приложения**

*OWASP TOP 10 – список 10 наиболее критичных угроз веб-приложений по версии международной некоммерческой организации The Open Web Application Security Project

КОД БЕЗОПАСНОСТИ

СЕРТИФИКАТЫ

КОНТИНЕНТ WAF

ФСТЭК России

- **4 класс по РД МЭ 2016, тип Г**

Продукт сертифицирован для защиты

- **автоматизированных систем (АС) до класса защищенности 1Г включительно**
- **государственных информационных систем (ГИС) до К1 включительно**
- **информационных систем персональных данных (ИСПДн) до УЗ1 включительно**

КОД БЕЗОПАСНОСТИ

КОНЦЕПЦИЯ ПАК «КОНТИНЕНТ WAF»

Гибкая архитектура

Многоуровневая защита веб-приложений

Низкая стоимость владения

Континент WAF

ВАРИАНТЫ ПРИМЕНЕНИЯ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

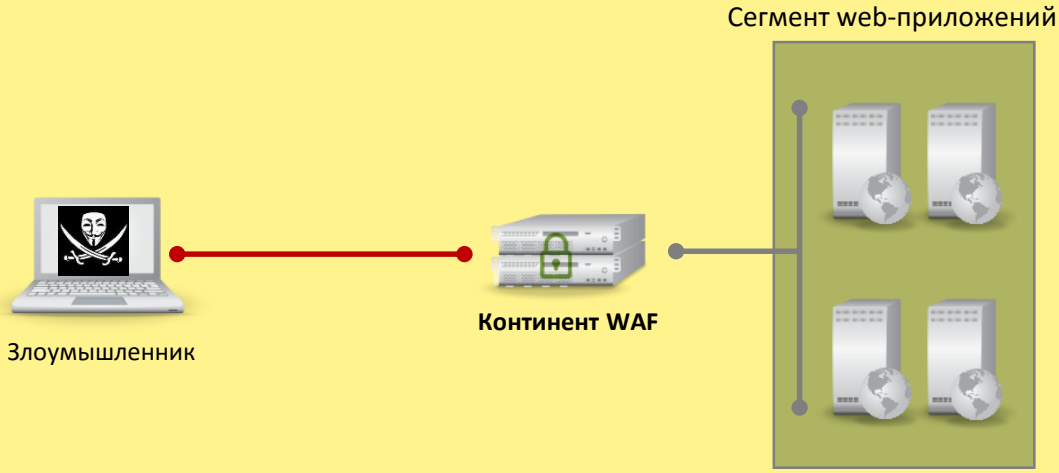
ЗАЩИТА WEB-ПРИЛОЖЕНИЯ

Сценарии использования:

- Защита публичных веб-приложений
- Защита личного кабинета пользователя
- Защита систем межведомственного взаимодействия
- Защита мобильных приложений
- Защита веб-интерфейсов критичных систем

Компоненты:

- Континент WAF



КОД БЕЗОПАСНОСТИ

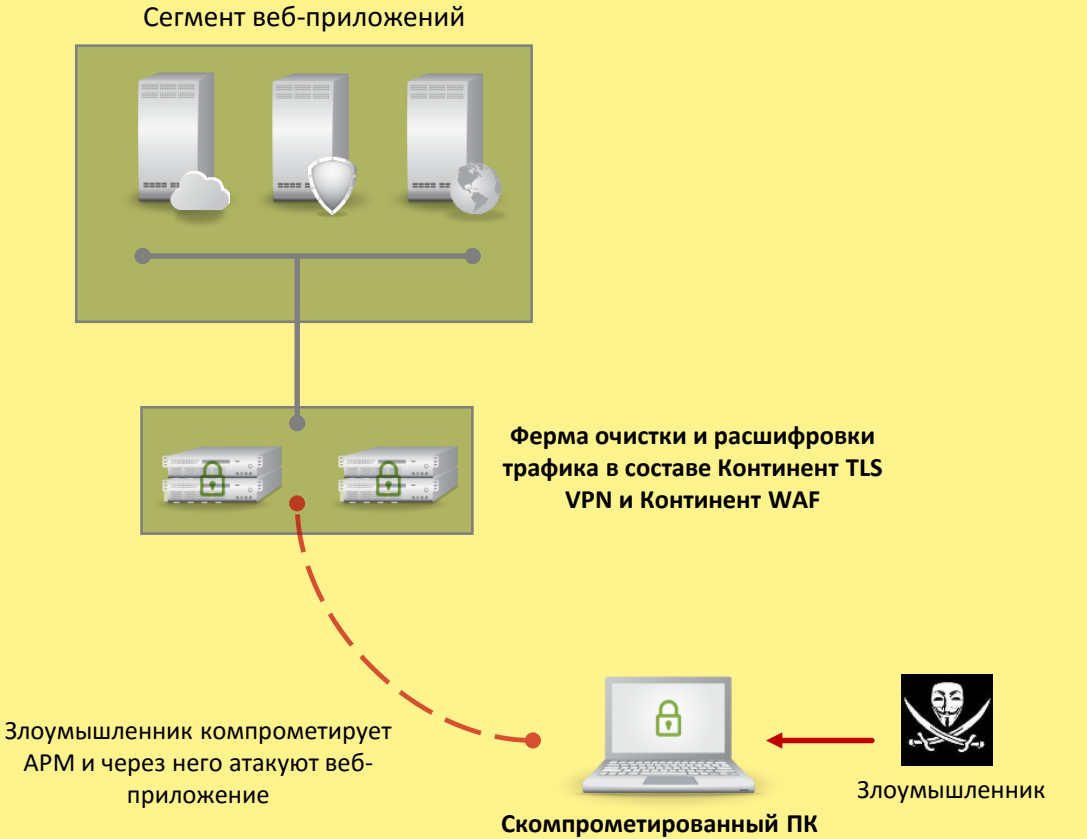
ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ С ШИФРОВАНИЕМ ГОСТ 28147-89

Сценарии использования :

- Защита систем дистанционного банковского обслуживания для юр. лиц
- Защита порталов гос. ведомств

Компоненты:

- Континент WAF
- Континент TLS VPN



ВОЗМОЖНОСТИ

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

АНАЛИЗ ТРАФИКА

КОНТИНЕНТ WAF

Аппаратно-программный комплекс, предназначенный для защиты веб-приложений

Гибкая настройка моделей работы приложений

- **Валидация протокола HTTP**
- **Синтаксический анализ запросов и ответов**
- **Определение бизнес-логики приложения**
- **Идентификация, аутентификация пользователей и контроль сессий**

Автоматическое построение модели работы приложения (профилирование)

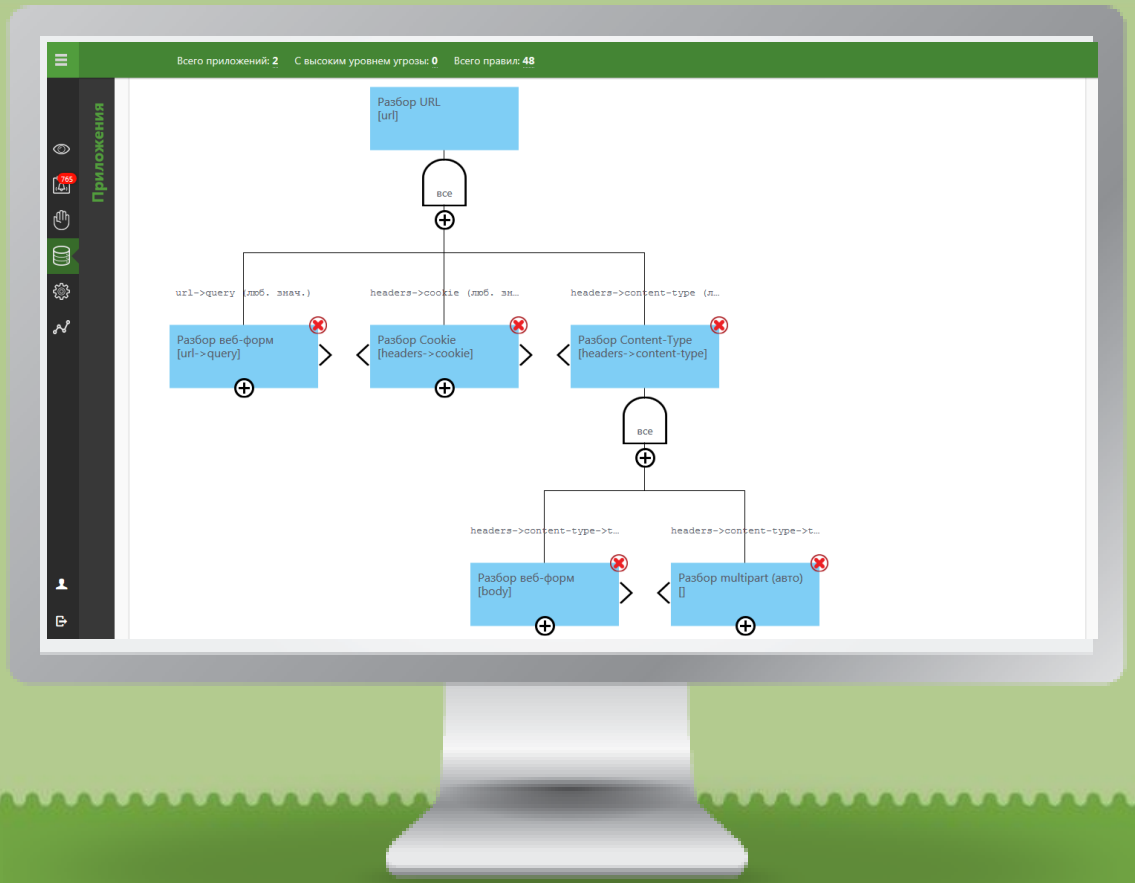
Анализ соответствия поведения пользователя позитивной модели работы приложения (запрещено всё, что явным образом не разрешено)

Расшифровка SSL-трафика (MitM)

Пакет преднастроенных сигнатур

КОД БЕЗОПАСНОСТИ

ГРАФИЧЕСКОЕ ОТОБРАЖЕНИЕ ВСЕХ ВОЗМОЖНЫХ HTTP-ЗАПРОСОВ И ОТВЕТОВ



Дерево разбора HTTP- запросов и ответов веб-приложения для построения модели работы и правил принятия решений

КОД БЕЗОПАСНОСТИ

ОБНАРУЖЕНИЕ АНОМАЛИЙ

КОНТИНЕНТ WAF

Аппаратно-программный комплекс, предназначенный для защиты веб-приложений

Обнаружение аномалий как в HTTP-запросах, так и в ответах

Обнаружение аномалий на основе модели работы приложения

- **Совпадение с моделью**
- **Отклонение от модели**

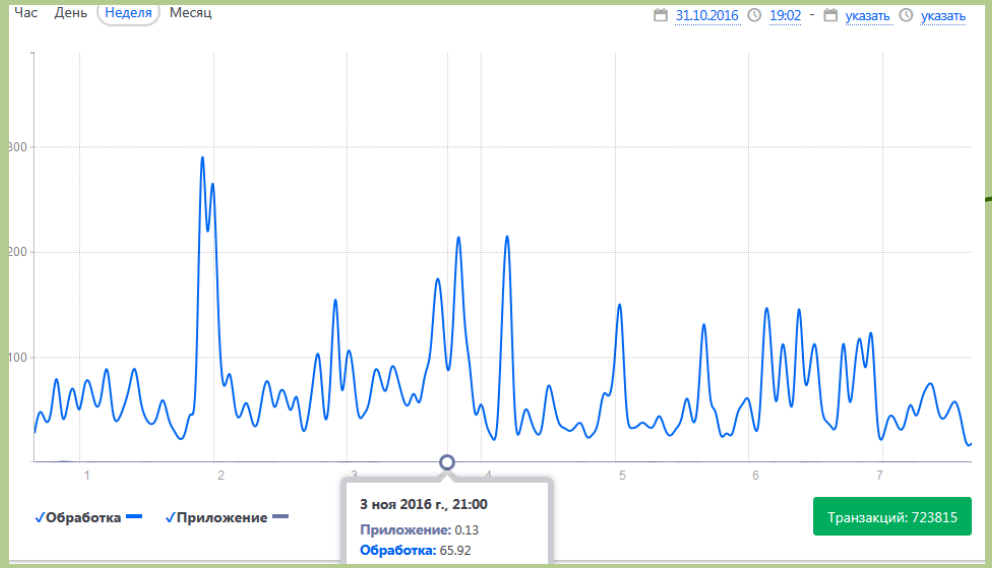
Обнаружение аномалий внутри вложенных данных, передаваемых по протоколу HTTP

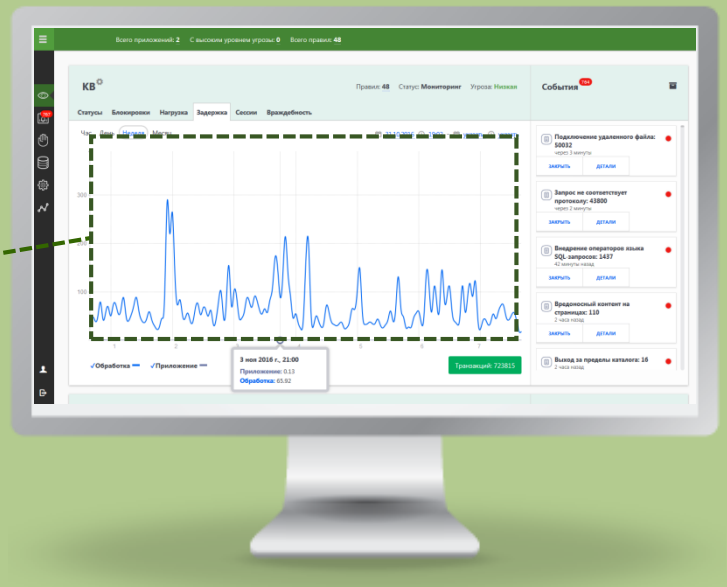
Обнаружение Bruteforce-атак

КОД БЕЗОПАСНОСТИ

ИНФОРМАЦИЯ ОБ АНОМАЛИЯХ

Статистика задержек ответов веб-сервера

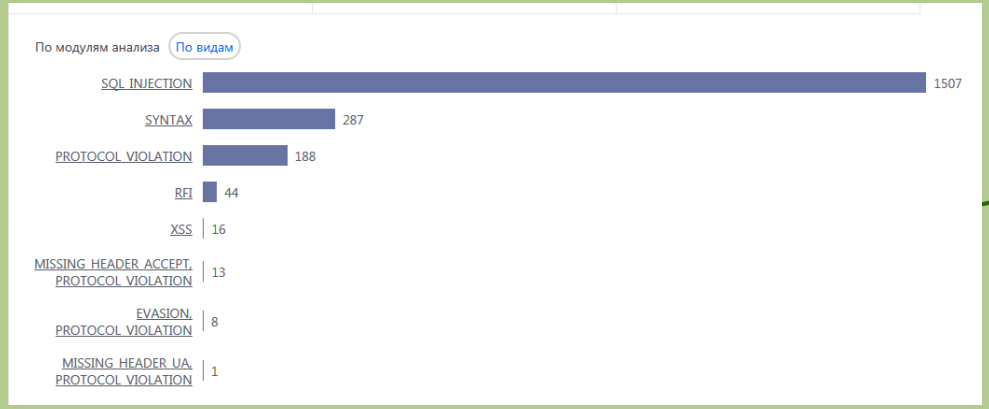


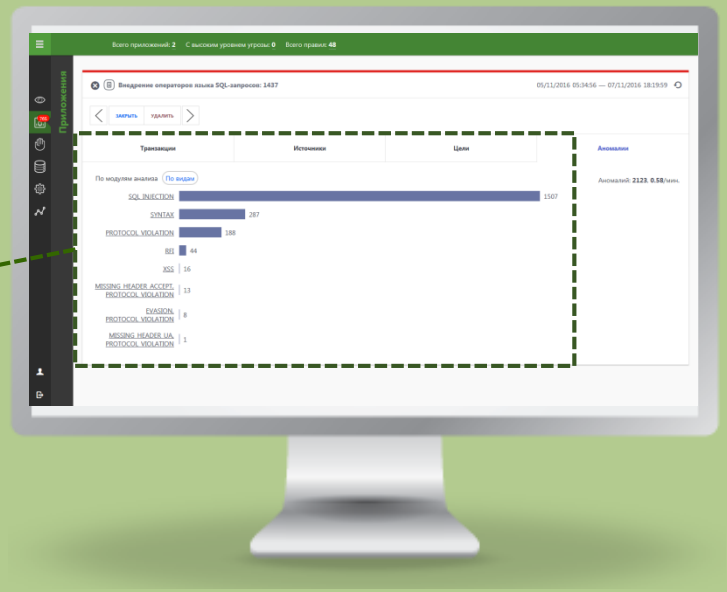


КОД БЕЗОПАСНОСТИ

ИНФОРМАЦИЯ ОБ АНОМАЛИЯХ

Распределение по видам аномалий для сработавшего правила





КОД БЕЗОПАСНОСТИ

ИНТЕРФЕЙС УПРАВЛЕНИЯ

КОНТИНЕНТ WAF

Аппаратно-программный комплекс, предназначенный для защиты веб-приложений

Графическое отображение модели разбора запросов и ответов веб-сервера

Графическое отображение моделей функционирования веб-приложений

Ролевая модель доступа в систему управления

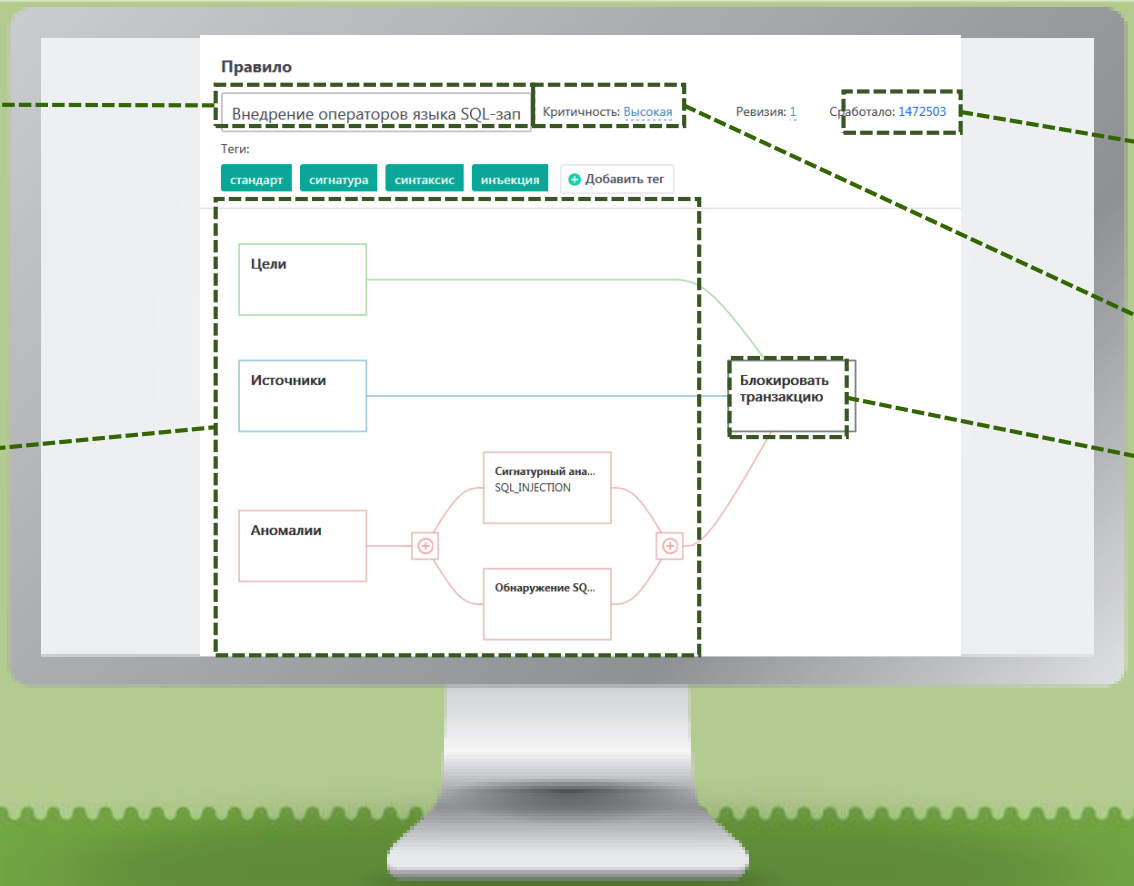
Аудит действий оператора Континент WAF

КОД БЕЗОПАСНОСТИ

УДОБНЫЙ ИНТЕРФЕЙС РЕДАКТИРОВАНИЯ ПРАВИЛ ПРИНЯТИЯ РЕШЕНИЙ

Название правила

Условия активации правила



Число срабатываний правила

Критичность правила

Решение

КОД БЕЗОПАСНОСТИ

МОНИТОРИНГ И АУДИТ СОБЫТИЙ

КОНТИНЕНТ WAF

Аппаратно-программный комплекс, предназначенный для защиты веб-приложений

Вывод обобщенной статистики в режиме реального времени

Агрегирование и приоритизация данных о событиях ИБ

Автоматическое оповещение оператора Континент WAF по электронной почте

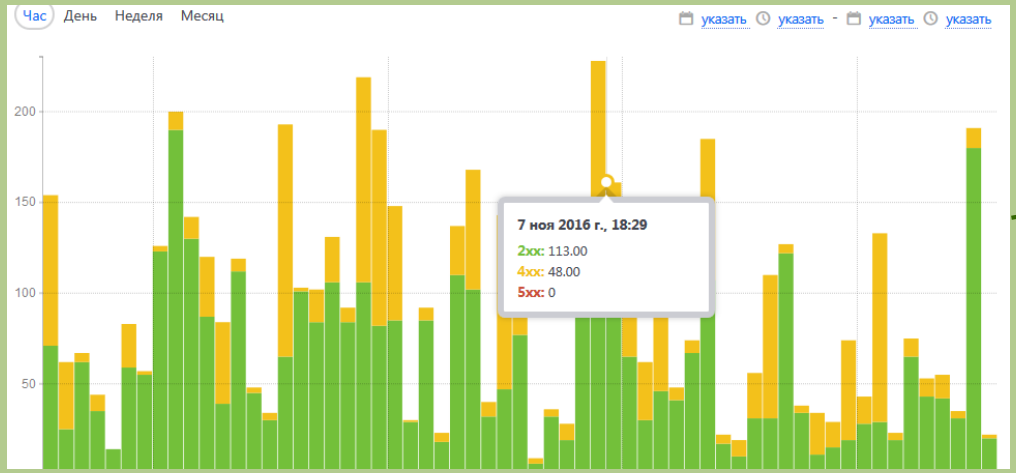
Генерация и регулярная рассылка отчетов в формате PDF по электронной почте

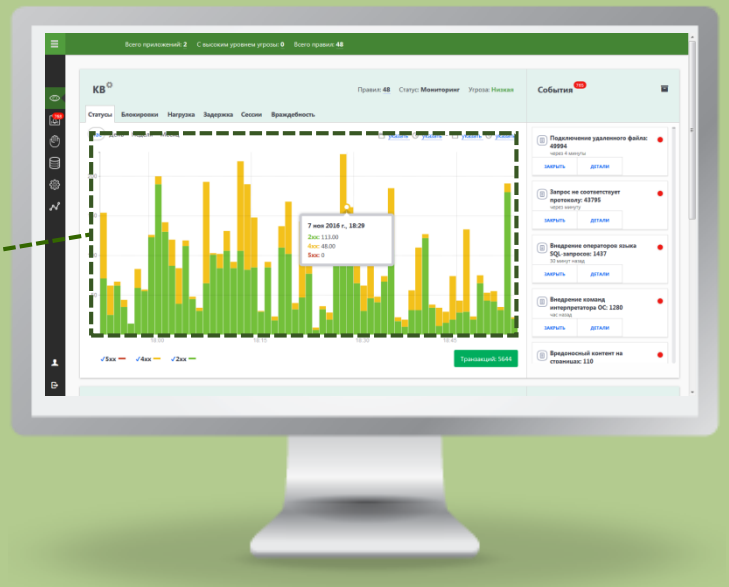
Интеграция с SIEM-системами через протокол syslog

КОД БЕЗОПАСНОСТИ

СОСТОЯНИЕ ВЕБ-ПРИЛОЖЕНИЙ

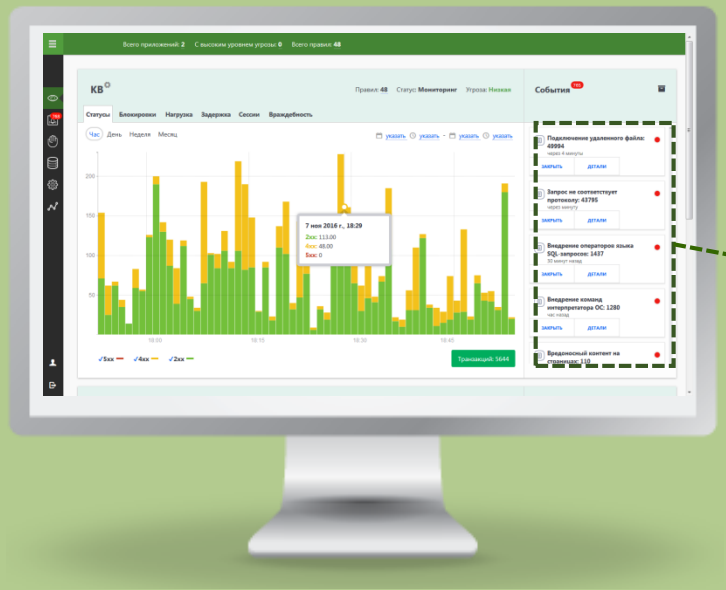
Статистика HTTP-ответов





КОД БЕЗОПАСНОСТИ

СОСТОЯНИЕ ВЕБ-ПРИЛОЖЕНИЙ



Последние сработавшие правила

Подключение удаленного файла: 49994
через 4 минуты
ЗАКРЫТЬ ДЕТАЛИ

Запрос не соответствует протоколу: 43795
через минуту
ЗАКРЫТЬ ДЕТАЛИ

Внедрение операторов языка SQL-запросов: 1437
30 минут назад
ЗАКРЫТЬ ДЕТАЛИ

Внедрение команд интерпретатора ОС: 1280
час назад
ЗАКРЫТЬ ДЕТАЛИ

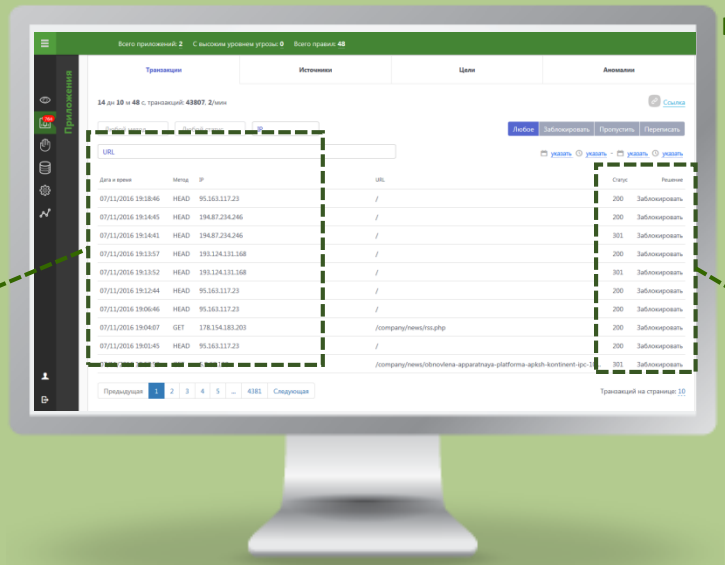
Вредоносный контент на страницах: 110

КОД БЕЗОПАСНОСТИ

СТАТИСТИКА СРАБАТЫВАНИЯ ПРАВИЛА

Дата и время события, метод, IP-адрес источника атаки

Дата и время	Метод	IP
07/11/2016 19:18:46	HEAD	95.163.117.23
07/11/2016 19:14:45	HEAD	194.87.234.246
07/11/2016 19:14:41	HEAD	194.87.234.246
07/11/2016 19:13:57	HEAD	193.124.131.168
07/11/2016 19:13:52	HEAD	193.124.131.168
07/11/2016 19:12:44	HEAD	95.163.117.23
07/11/2016 19:06:46	HEAD	95.163.117.23
07/11/2016 19:04:07	GET	178.154.183.203
07/11/2016 19:01:45	HEAD	95.163.117.23
07/11/2016 18:57:59	GET	5.9.62.130



Реакция веб-сервера на запрос и решение о блокировке

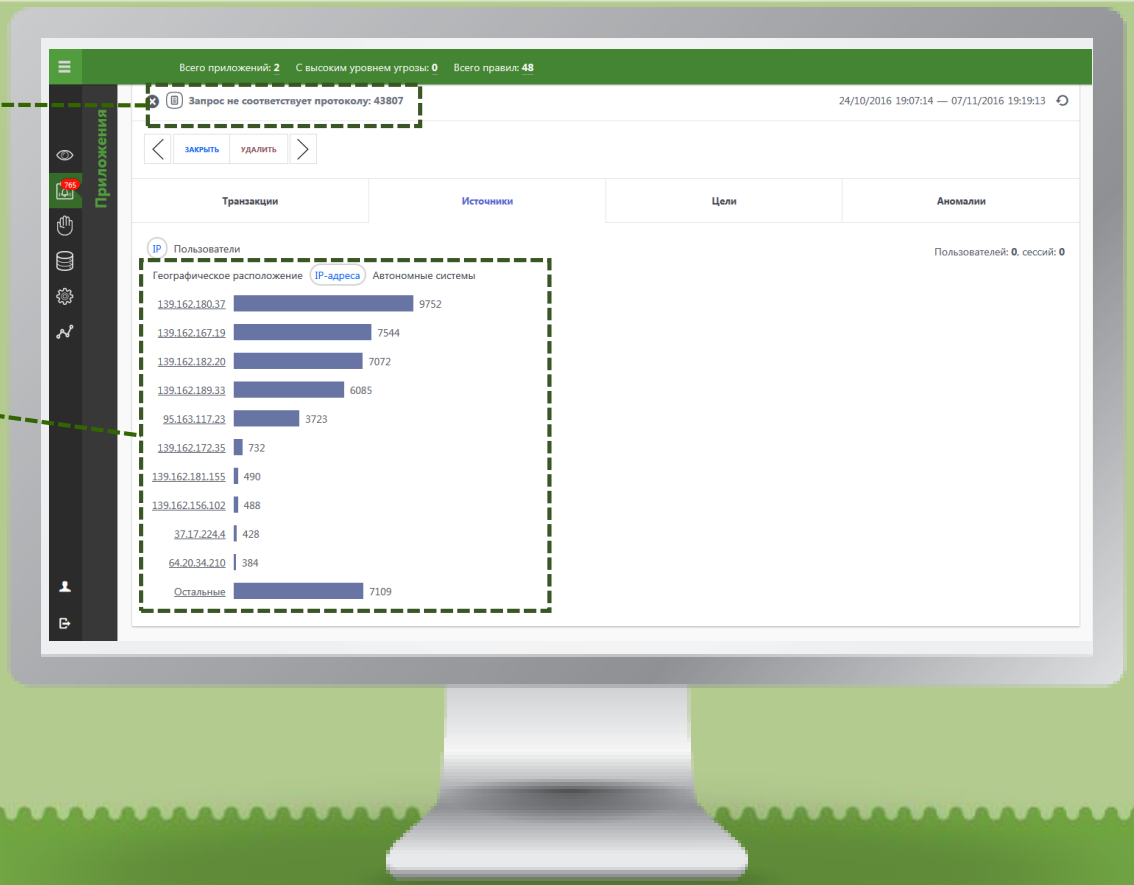
Статус	Решение
200	Заблокировать
200	Заблокировать
301	Заблокировать
200	Заблокировать
301	Заблокировать
200	Заблокировать
200	Заблокировать
200	Заблокировать
200	Заблокировать
301	Заблокировать

КОД БЕЗОПАСНОСТИ

СТАТИСТИКА ИСТОЧНИКОВ АТАК ПО ПРАВИЛУ

Название правила и число срабатываний

Список источников атак



РЕЖИМЫ РАБОТЫ И АППАРАТНАЯ ПЛАТФОРМА

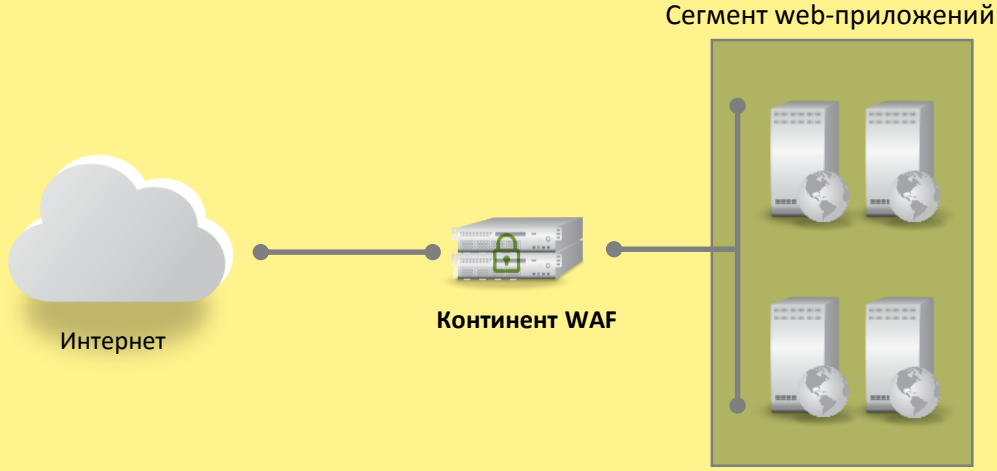
КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ WAF В РЕЖИМЕ INLINE

КОНТИНЕНТ WAF

Блокировка атак и несанкционированной активности

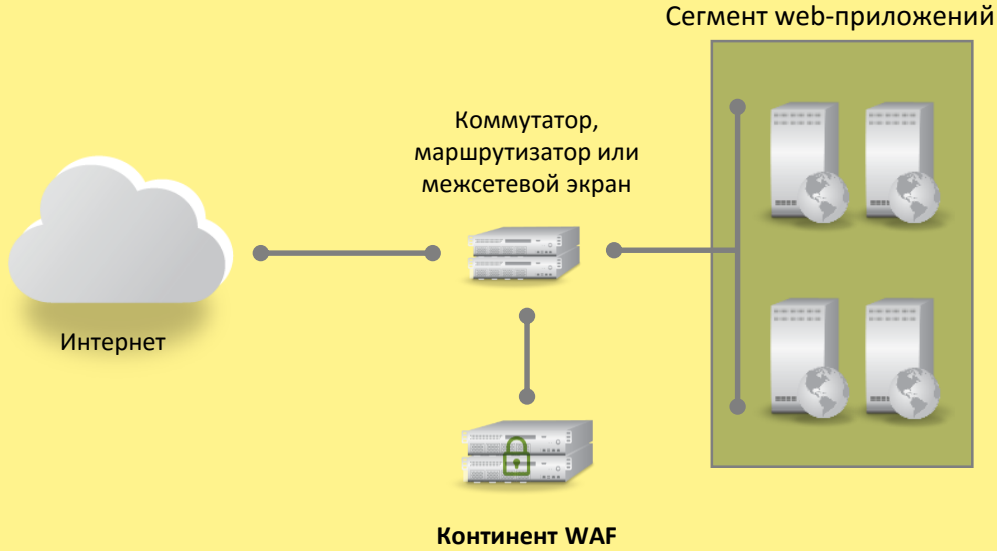


КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ WAF
В РЕЖИМЕ ЗЕРКАЛИРОВАНИЯ

КОНТИНЕНТ WAF

Обнаружение атак с информированием оператора

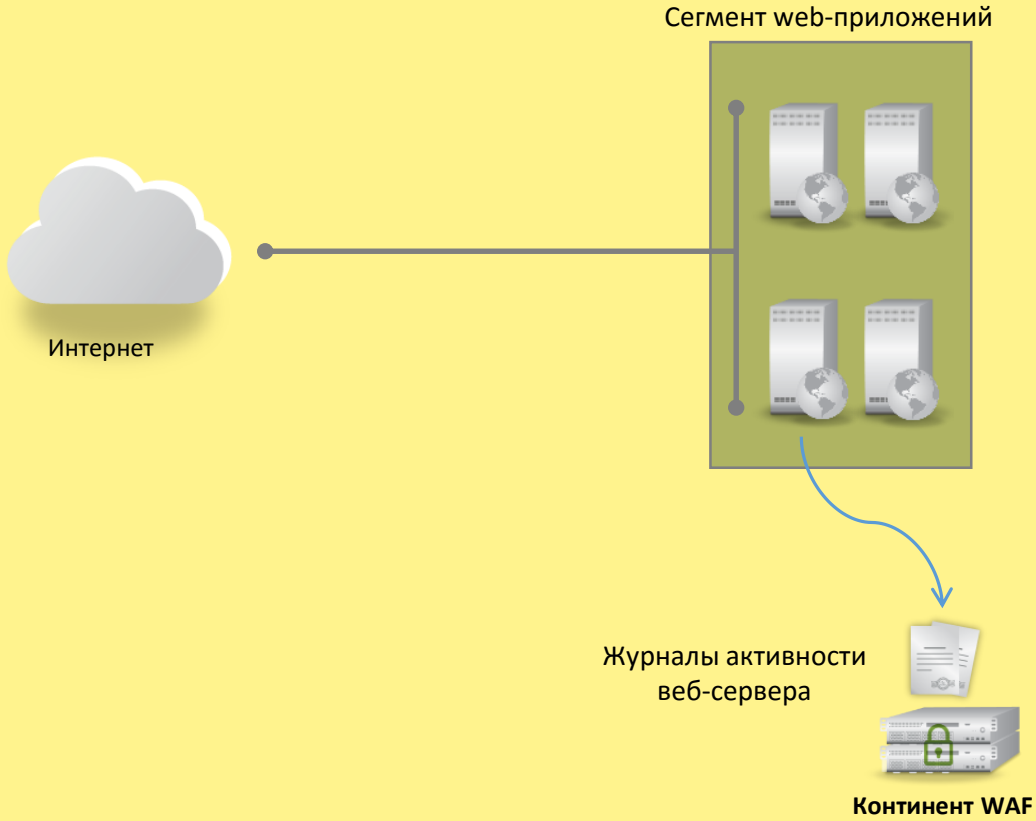


КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ WAF В РЕЖИМЕ АУДИТА

КОНТИНЕНТ WAF

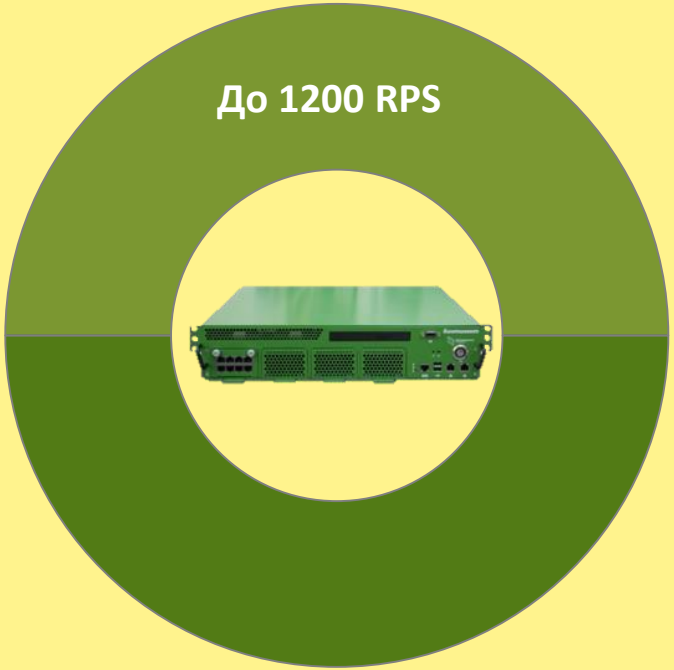
Обнаружение атак, осуществленных до внедрения Континент WAF



КОД БЕЗОПАСНОСТИ

КОНТИНЕНТ WAF IPC-1000

Производительность, HTTP-запросов в секунду



Процессор

- 2x Intel Xeon

Оперативная память

- 16 GB DDR3

Сетевые интерфейсы

- 10x Ethernet 10/100/1000

ПРЕИМУЩЕСТВА

КОД БЕЗОПАСНОСТИ

КОД БЕЗОПАСНОСТИ

ПРЕИМУЩЕСТВА КОНТИНЕНТ WAF

- Адаптация под сложные веб-приложения
- Обнаружение атак на бизнес-логику веб-приложений
- Низкий уровень ложных срабатываний
- Преднастроенные сигнатуры и модели валидации HTTP
- Реализация в виде физического или виртуального устройства
- Интеграция с SIEM-системами

КОД БЕЗОПАСНОСТИ

ТЕХПОДДЕРЖКА

	Пакет поддержки			
Каталог услуг	**VIP**	**Расширенный**	**Стандартный**	**Базовый**
Доступность услуги	24x7, e-mail, телефон	24x7, e-mail, телефон	8x5, e-mail, телефон	8x5, e-mail, телефон
Приоритет	*Самый высокий приоритет обслуживания*	*Высокий приоритет обслуживания*	*Средний приоритет обслуживания*	*Низкий приоритет обслуживания*
Выделенный инженер (для проведения работ)	●			
Присутствие инженера на площадке заказчика	●			
Консультирование по дополнительному функционалу продукта	●	●		
Консультирование по установке и использованию продукта	●	●	●	●
Регистрация обращений на веб-портале	●	●	●	
Специальные условия на приобретение новых версий продукта	●	●	●	●
Доступ на форум по продукту и базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Личный кабинет на веб-портале	●	●	●	●
Информирование о доступных обновлениях продукта по запросу	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●

СПАСИБО!

КОНТАКТЫ:

+7 (495) 982-30-20

info@securitycode.ru

www.securitycode.ru

КОД БЕЗОПАСНОСТИ