



КОД
безопасности

КОНТИНЕНТ WAF

Защита веб-приложений и автоматизированный анализ их бизнес-логики

ПРЕИМУЩЕСТВА



ВИРТУАЛЬНЫЙ ПАТЧИНГ
И ЗАЩИТА ОТ АТАК 0-DAY



АВТОМАТИЗИРОВАННОЕ ИЗУЧЕНИЕ
БИЗНЕС-ЛОГИКИ ПРИЛОЖЕНИЙ



ПРОСТОТА МИГРАЦИИ
С БЕСПЛАТНОГО ПО ЗА СЧЕТ ПОДДЕРЖКИ
ПРАВИЛ MODSECURITY



НИЗКИЙ УРОВЕНЬ
ЛОЖНЫХ СРАБАТЫВАНИЙ



АНАЛИЗ ЗАШИФРОВАННОГО
АЛГОРИТМАМИ ГОСТ ТРАФИКА
БЕЗ ПОТЕРИ ПРОИЗВОДИТЕЛЬНОСТИ
(С ИСПОЛЬЗОВАНИЕМ КОНТИНЕНТ TLS)



ЭРГОНОМИЧНЫЙ
ГРАФИЧЕСКИЙ ИНТЕРФЕЙС



АНАЛИЗ ТРАФИКА

- 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
- Анализ отклонений поведения пользователя от стандартного сценария
- Анализ данных в SSL-туннеле
- Пакет преднастроенных сигнатур
- Поддержка правил формата ModSecurity

УПРАВЛЕНИЕ И МОНИТОРИНГ

- Графическое отображение модели разбора запросов и ответов веб-сервера
- Мониторинг и управление защитой нескольких приложений из единой консоли
- Графическое отображение и редактирование правил принятия решений
- Вывод обобщенной статистики в режиме реального времени
- Агрегирование и приоритизация данных о событиях ИБ
- Автоматическое оповещение оператора о событиях ИБ
- Ролевая модель доступа в консоль управления
- Аудит действий оператора WAF в консоли управления
- Интеграция в SIEM-систему по протоколу syslog

ОБНАРУЖЕНИЕ АТАК НА ВЕБ-ПРИЛОЖЕНИЯ

- Обнаружение специфических для веб-приложений атак
 - OWASP TOP 10
 - SQL-инъекции
 - Cross Site Scripting
 - Cross Site Request Forgery
- Обнаружение аномалий как в запросах, так и в ответах веб-сервера
- 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

РЕЖИМЫ РАБОТЫ

- Работа в режиме зеркалирования
- Работа «в разрыв»
- Работа в режиме аудита
 - Анализ логов активности веб-сервера



СЦЕНАРИИ ПРИМЕНЕНИЯ

ЗАЩИТА СЛОЖНЫХ ВЕБ-ПРИЛОЖЕНИЙ

Результат:

- Минимизированы затраты, связанные с атаками на веб-приложения
- Уменьшен риск репутационных потерь при взломе корпоративного сайта
- Повышена устойчивость веб-приложений к DoS-атакам
- Предотвращены попытки мошеннических действий злоумышленников
- Снижен уровень ложных срабатываний

ЗАЩИТА СЕТИ ОРГАНИЗАЦИИ ОТ КОМПРОМЕТАЦИИ ЧЕРЕЗ ВЕБ-САЙТ

Результат:

- Минимизирован риск взлома сайта
- Снижен риск атаки на корпоративную сеть через взломанный сайт

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

Результат:

- Информационная система приведена в соответствие требованиям приказа ФСТЭК России № 17 (ГИС)
- Минимизированы риски, связанные с невыполнением требований регуляторов



МОДЕЛЬНЫЙ РЯД

МОДЕЛЬ	IPC-1000L	IPC-3000L
		
Производительность, HTTP-запросов в секунду	до 1 000	до 3 000
Процессор	Intel Xeon E5-1275v6	Intel Xeon E5-2680v4
Оперативная память	Не менее 32 ГБ	Не менее 128 ГБ
Интерфейсы	8x 1000BASE-T Ethernet 10/100/1000 8x 1000BASE-X Ethernet SFP	1x 1000BASE-T Ethernet 10/100/1000 4x 10 Gigabit Ethernet SFP+

СЕРТИФИКАТЫ



ФСТЭК России

4-й класс защиты МЭ типа «Г»

Может применяться для защиты ИСПДн до УЗ1 включительно, ГИС до К1 включительно, АСУ ТП до К1 включительно, АС до класса 1Г включительно

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка продуктов линейки «Континент» может осуществляться как напрямую, силами специалистов компании «Код Безопасности», так и через авторизованных партнеров.

В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.

Существует несколько пакетов технической поддержки:



Базовый



Стандартный



Расширенный



VIP

КАТАЛОГ УСЛУГ	ПАКЕТ ПОДДЕРЖКИ			
	БАЗОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ	VIP
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О КОМПАНИИ «КОД БЕЗОПАСНОСТИ»

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

+7 (495) 982-30-20 (многоканальный)

info@securitycode.ru

www.securitycode.ru