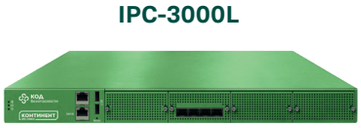
КОД безопасности

Континент WAF 2

Система защиты веб-приложений с автоматизированным анализом бизнес-логики

- Виртуальный патчинг и защита от атак 0-day
- Автоматизированное изучение бизнес-логики приложений
- Простота миграции с бесплатного ПО за счет поддержки правил Modsecurity
- Поддержка протокола WebSocket на уровне бизнес-логики
- Низкий уровень ложных срабатываний
- Эргономичный графический интерфейс
- Анализ зашифрованного алгоритмами ГОСТ трафика без потери производительности (с использованием Континент TLS)

Модельный ряд

Характеристики	IPC-R1000	IPC-3000L
		
Производительность, HTTP-запросов в секунду	до 1 000	до 3 000
Процессор	Intel Xeon E-2276G	Intel Xeon E5-2680v4
Оперативная память	Не менее 32 ГБ	Не менее 128 ГБ
Интерфейсы	8 x 10/100/1000BASE-T RJ45 4 x 10G SFP+	1 x 10/100/1000BASE-T RJ45 4 x 10GB SFP+

Возможности

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.
- Расширение доступных для разбора структур передаваемых данных.
- Возможность выбора различных объектов в качестве источника анализа данных (IP-адрес, сессионный идентификатор и т.д.).
- Проверка успешности действий пользователя и контроль последовательности действий (уровень бизнес-логики).

Режимы работы

- Работа в режиме мониторинга.
- Работа «в разрыв» (Reverse Proxy).
- Работа в режиме аудита:
  - Анализ логов активности веб-сервера.

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 с SIEM-системой по протоколу syslog.
- Обновление правил ModSecurity в соответствии с OWASP Top 10.
- Возможность создания списков объектов для дальнейшего использования в правилах.

Обнаружение атак на веб-приложения

- Обнаружение специфических для веб-приложений атак:
  - OWASP TOP 10;
  - Bruteforce-атаки;
  - DoS на уровне приложений;
  - Атаки на механизмы авторизации и аутентификации;
  - Автоматизированные атаки.
- Обнаружение аномалий в запросах и 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.

Сценарии применения

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.

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.

Сертификаты

ФСТЭК России

- МЭ Г4 сертификат

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