

Континент WAF



Континент WAF обеспечивает защиту веб-приложений за счет фильтрации трафика на прикладном уровне. За счет понимания контекста работы приложения, Континент WAF обеспечивает более высокую эффективность защиты веб-приложений по сравнению с традиционными средствами защиты ИТ-инфраструктурами – межсетевыми экранами и средствами обнаружения вторжений.

Возможности продукта включают в себя следующие функции:

- 1) Анализ трафика:
 - Гибкая настройка моделей работы приложений
 - Автоматическое построение модели работы приложения
 - Анализ отклонений поведения пользователя от стандартного сценария
 - Анализ данных в SSL-туннеле
 - Пакет преднастроенных сигнатур
 - Поддержка правил формата ModSecurity
- 2) Обнаружение атак на веб-приложения:
 - Обнаружение специфических для веб-приложений атак
 - Обнаружение аномалий как в запросах, так и в ответах веб-сервера
 - Обнаружение аномалий на основе модели работы приложения
 - Обнаружение аномалий внутри вложенных данных, передаваемых по протоколу HTTP/HTTPS Обнаружение bruteforce-атак
- 3) 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
- 4) Режимы работы:
 - Работа в режиме зеркалирования
 - Работа «в разрыв»
 - Работа в режиме аудита
 - Анализ логов активности веб-сервера

Наши контактные данные:

ул. Ленина, д.20, (четвертый этаж), каб. 422, 423. Остановка "Яблонька".
e-mail: info@ooo-skb.ru(ссылка для отправки email), тел. 53-20-18