PENTESTIT
Cybersecurity services and software
+7 (495) 204-19-72 || info@pentestit.ru

ОБЗОР ОСНОВНЫХ ВОЗМОЖНОСТЕЙ, ОСОБЕННОСТЕЙ И ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК ПО «NEMESIDA WAF»

> Особенностью «Nemesida WAF» является точность выявления атак при минимальном количестве ложных срабатываний, наличие системы виртуального патчинга, качественно подобранная база сигнатур, масштабируемость и ценовая политика, позволяя обеспечивать безопасность интернет-магазинов, порталов, API и прочих веб-приложений на предприятиях любого масштаба.

Общая информация

Язык интерфейса	Английский
Язык документации	Русский, английский
Наличие исследовательского центра в России	lab.pentestit.ru
Режим работы	IPS, IDS, Combined
Вид поставки	• В виде установочного дистрибутива • В виде образа виртуальной машины • В виде облачного сервиса
Правовая информация	«Nemesida WAF» внесен в реестр отечественного ПО и имеет все необходимые свидетельства.

Кластеризация, SSL, стандарты

- Терминация SSL
- Пассивное декодирование SSL
- Поддержка сессий, установленных на клиентских сертификатах
- Поддержка Active-Active кластеризации
- Поддержка Active-Passive кластеризации
- Поддержка балансировки нагрузки между защищаемыми веб-приложениями
- Поддержка WebSockets

- Поддержка XML
- Поддержка JSON

Выявление атак

Класс блокируемых атак	• Injection (RCE, SQLi, OS command и т.д.) • XSS • Information Leakage • Path Traversal • Open Redirect • Web Shell • HTTP Response Splitting • RFI/LFI • Server-Side Request Forgery
Наличие репутационной базы	Собственная репутационная и GeoIP база.
Обнаружение ботов на основе значений полей запроса	На основе их сигнатур и поведенческого анализа.
• Защита от атаки на XML • Блокировка отдельного запроса • Временное блокирование запросов от источника по IP-адресу • Проверка HTTP-транзакций на соответствие RFC и лучшим практикам контроля • Категоризация по типу активности (типу атаки) источников • Создание правил сигнатур и их исключений на основе задаваемого набора критериев (например: метод, URL, значение параметра, заголовок) и регулярных выражений	

Машинное обучение («Nemesida AI»)

Точность выявления атак	«Nemesida AI» на ~30% эффективнее сигнатурного анализа.
Метод машинного обучения	Используется классический алгоритм машинного обучения. Ключевыми особенностями «Nemesida AI» являются точность выявления

	аномалий, минимальное количество ложных срабатываний и отсутствие высоких требований к аппаратным ресурсам.

- Адаптация WAF к изменяемому приложению
- Автоматическое создание поведенческих моделей
- Выявление аномалий и оценка их уровня критичности
- Выявление новых признаков атак, в том числе выявление атак «нулевого дня»
- Интерфейс управления поведенческими моделями (дообучение моделей)

Атаки методом перебора

«Nemesida WAF» способен выявлять атаки методом перебора (brute-force), в том числе распределенные (с использованием распределенных вычислительных сетей). При обнаружении такого вида атак используется расстояние Левенштейна и нечеткая логика.

Дополнительные возможности

- Интеграция со сканерами уязвимостей, в том числе с «Nemesida WAF Scanner»
- Антивирусный анализ
- Интеграция с системами класса SIEM
- Интеграция с межсетевыми экранами
- Отсутствие ограничений по количеству трафика и виртуальным хостам для Standalone-версии

Вспомогательные модули

- Личный кабинет «Nemesida WAF»
- «Nemesida WAF Scanner»
- Virtual patching
- «Signtest»

Фильтрация и уведомления

- Личный кабинет для работы с инцидентами
- Гибкая фильтрации записей журнала безопасности по заданным критериям
- Ручной и автоматическая агрегации записей журнала безопасности по типу атаки, имени параметра, URL, IP-адресу
- Верификация атаки с использованием встроенного динамического сканера
- Автоматическая агрегация событий с интенсивным характером
- Наличие возможности настройки отчетности для получения сводной информации по событиям безопасности
- Наличие интерфейса с информацией о сетевой загрузке WAF
- Зафиксированные события содержат запрос в полном объеме (целиком)
- Зафиксированные события содержат описание сработавшего правила политики безопасности
- Экспорт и импорт журнала событий безопасности в полном объеме
- E-mail и Syslog уведомления