Nemesida WAF

комплексная защита сайта от хакерских атак 24/7

waf.pentestit.ru

info@pentestit.ru

О компании

Комплексный подход при оказании услуг позволяет избавить наших клиентов от всех вопросов, связанных с информационной безопасностью. Среди наших клиентов – крупнейшие компании из ИТ, телекоммуникационной, банковской, финансовой сфер, а также компании, специализирующиеся в области электронной коммерции.

Наши специалисты имеют опыт нахождения уязвимостей на самых защищенных ресурсах. 8 из 10 аудитов заканчивается обнаружением уязвимостей со статусом «Критичный».

Современные атаки

Рост количества атак на веб-сайты обусловлен:

- активным развитием и распространением веб-приложений, их сложностью;
- интеграцией сервисов;
- использованием сторонних модулей и решений;
- большим количеством инструментов взлома, описанием методов и векторов атак;
- координированием и кооперированием атак;
- снижением качества кода, способствующему появлению 0-day уязвимостей;
- легкой монетизацией результатов атак;
- недостаточной подготовкой систем и подразделений для противодействия таким атакам.

Современные атаки

Ежедневно мы блокируем следующие виды атак:

- попытки выявления критичных файлов и доступа к служебным скриптам;
- попытки выявления уязвимых плагинов/модулей;
- попытки эксплуатации «нашумевших» уязвимостей;
- попытки доступа к критичным зонам;
- использование autopwn-систем и ботов.

Nemesida WAF

Отличительные особенности Nemesida WAF:

- абсолютная точность выявления атак;
- уникальные алгоритмы выявления атак,
- механизмы предугадывания начала атаки;
- отсутствие периода обучения;
- «Standalone» и «Cloud» версии;
- удобный личный кабинет.

Nemesida WAF

Web Application Firewall — защитный экран уровня приложений, предназначенный для выявления и блокирования современных атак на веб-приложения, в том числе и с использованием уязвимостей нулевого дня:

- SQL Injection — sql инъекции;
- remote Code Execution (RCE) — удаленное выполнение кода;
- cross Site Scripting (XSS) — межсайтовый скриптинг;
- cross Site Request Forgery (CSRF) — межстайтовая подделка запросов;
- Remote File Inclusion (RFI) — удалённый инклуд;
- Local File Inclusion (LFI) — локальный инклуд;
- auth bypass — обход авторизации;
- Insecure Direct Object Reference — небезопасные прямые ссылки на объекты;
- bruteforce — подбор паролей.

Преимущество облачной версии Nemesida WAF – защита от DDoS-атак, как сетевых, так и уровня WEB-приложения. Нет необходимости использовать сторонние решения для защиты от подобных атак – Nemesida WAF обеспечивает комплексную защиту в круглосуточном режиме.

Обнаружение атак

В процессе систематического обновления базы сигнатур для Nemesida WAF используются следующие источники:

- атаки на защищаемые веб-приложения клиентов с общим трафиком 300-800 Mbps;
- атаки на инфраструктуру Pentestit;
- атаки на специализированные Honeypots с трафиком атак до 30 Mbps;
- база атак на веб-приложения отдела анализа защищенности Pentestit;
- поведенческий анализ пользователей сайта.

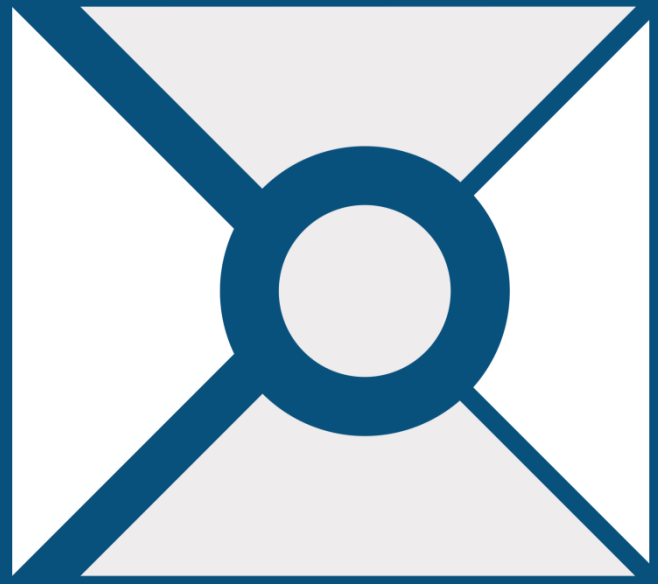
Обнаружение атак

Сигнатуры и анализ поведения:

- синтаксические сигнатуры;
- мутации и техники обхода;
- анализ действий пользователя;
- репутация.

Наши преимущества

- Полный цикл разработки: от составления математической модели угрозы до проверки методов обхода защитных средств.
- Простая установка и обслуживание: облачный сервис требует минимальных настроек на стороне клиента.
- Комбинированные методы обнаружение атак на основе сигнатур и машинного обучения.
- Блокирование атак «нулевого дня» - защита от «первой волны», таймаут для патч-менеджмента.
- Круглосуточный мониторинг и техническая поддержка.
- Удобство использования.
- Лояльная ценовая политика.
- Контроль качества.



Nemesida WAF -
спокойствие за безопасность