ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

АКЦИОНЕРНОЕ ОБЩЕСТВО «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ»

(АО «ПМ»)

СИСТЕМА ВЫЯВЛЕНИЯ И ПРЕДУПРЕЖДЕНИЯ АТАК НА ВЕБ-РЕСУРСЫ «AML WEB PROTECTION»

Функциональные характеристики

На 12 листах

Москва 2025

Аннотация

Настоящий документ описывает функциональные характеристики Системы выявления и предупреждения атак на веб-ресурсы «AML Web Protection» (далее – «AML», Система).

Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

АО «ПМ»	–	Акционерное общество «Перспективный мониторинг»
«AML»	–	Система выявления и предупреждения атак на веб-ресурсы «AML Web Protection»
СЗИ	–	Система защиты информации
ИБ	–	Информационная безопасность

1 Общие сведения

Основным направлением деятельности АО «ПМ» является оценка практической защищенности информационных систем, выявление их уязвимостей при помощи средств инструментального и ручного анализа, реагирование на инциденты безопасности, разработка программных продуктов в области информационной безопасности. Система выявления и предупреждения атак на веб-ресурсы «AML Web Protection» также является разработкой компании.

Задача «AML» – защитить внутренние и внешние веб-ресурсы организации от компьютерных атак. Для решения данной задачи Система взаимодействует напрямую с журналами веб-сервера и не анализирует содержимое сетевого трафика. «AML» использует алгоритмы поведенческого анализа для выявления атакующих сессий по записям журнала веб-сервера и синхронизируется с веб-сервером для блокировки вредоносной активности.

2 Функциональное назначение

«AML» использует в качестве входных данных необработанные журналы событий от веб-серверов. Система группирует события в сессии и с помощью алгоритмов поведенческого анализа определяет, являются ли указанные сессии атакующими или пользовательскими. Анализ может выполняться в двух режимах:

– пакетный режим обработки журналов – способ обработки журнала, при котором пользователь загружает журнал веб-ресурса вручную, а система анализирует данный файл и выдает результат;

– потоковый режим обработки журналов – способ обработки журнала, при котором пользователь выбирает журнал, для которого система автоматически отслеживает изменения, анализирует их по мере поступления новых событий и определяет атакующие и пользовательские сессии.

Для потокового режима обработки журналов может быть активирована функция блокировки атакующих сессий, которая ограничивает доступ к веб-ресурсу для атакующих IP-адресов и User Agent.

2.1 Функциональные возможности

К функциональным возможностям «AML» относятся:

1) пакетная обработка журналов веб-серверов, применяемая для разового проведения анализа журнала событий. В рамках данного режима можно получить результат анализа журнала за конкретный, интересующий пользователя, временной период;

2) потоковая обработка журналов веб-серверов, применяемая для постоянного мониторинга журналов событий. В рамках данного режима пользователь может наблюдать за результатами анализа в режиме реального времени, оперативно детектируя атакующие сессии;

3) создание белых списков из IP-адресу и User-Agent – исключение доверенных ресурсов из блокируемых во избежание блокировки легитимной активности;

4) блокировка атакующих сессий – автоматический механизм, ограничивающий доступ к веб-ресурсу для атакующих сессий путем отправки на веб-сервер команды о блокировке нарушителей по IP-адресу и User-Agent;

5) добавление парсера – сущности системы, которая содержит регулярное выражение, позволяющее провести синтаксический анализ записей журнала событий веб-ресурсов и привести их в структурированный формат, удобный для дальнейшей обработки и анализа моделью. При добавлении парсера у пользователя имеется возможность на реальных данных (строке из своего журнала событий) проверить корректность работы добавляемого парсера;

6) подтверждение или опровержение результата работы модели – указанные данные учитываются в итоговой статистике и позволяют оценить точность работы модели;

7) просмотр результатов анализа журналов событий, позволяющий проводить ретроспективу проведенных работ и оценить уровень защищенности веб-ресурса. Ознакомиться с результатами анализа можно тремя способами:

– на странице журнала событий выводится полная и подробная информация о проведенной обработке;

– на главной странице сайта можно ознакомиться со сводной информацией по всем доступным ресурсам в визуальном формате – на диаграммах и графиках;

– в разделе «Отчеты» можно выгрузить результат анализа журнала событий в документе формата PDF.

3 Используемые технические средства и дополнительное программное обеспечение

Клиентская часть (портал для пользователя) функционирует в веб-браузере. Рекомендованные веб-браузеры для использования: Яндекс.Браузер и Google Chrome.

Для входа в «AML» компьютер пользователя должен отвечать следующим требованиям:

– 512 МБ свободного дискового пространства на жестком диске;

– открытые порты 443 (HTTPS) и 80 (HTTP);

– монитор, поддерживающий разрешение экрана 1024x768;

– Intel Pentium 1 ГГц (или совместимый аналог) для 32-разрядной операционной системы;

– Intel Pentium 2 ГГц (или совместимый эквивалент) для 64-разрядной операционной системы;

– 1 ГБ свободной оперативной памяти.

Язык разработки – Python 3.11. Использованные библиотеки из официального репозитория пакетов с открытым исходным кодом (https://pypi.org):

– Django (https://pypi.org/project/Django);

– Django REST framework (https://pypi.org/project/djangorestframework);

– Celery (https://pypi.org/project/celery);

– Scipy (https://pypi.org/project/scipy/);

– Sqlalchemy (https://pypi.org/project/SQLAlchemy/);

– Scikit-learn (https://pypi.org/project/scikit-learn/);

– Pandas (https://pypi.org/project/pandas/);

– Numpy (https://pypi.org/project/numpy/);

– Redis (https://pypi.org/project/redis).

Язык разработки – JavaScript. Использованные библиотеки из официального репозитория пакетов с открытым исходным кодом (https://npmjs.org):

– Vue (https://www.npmjs.com/package/vue);
– Pinia (https://www.npmjs.com/package/pinia);
– Axios (https://www.npmjs.com/package/axios);
– Vuetify (https://www.npmjs.com/package/vuetify).

Используемые форматы данных – JSON, YAML.

4 Входные данные

В качестве входных данных в «AML» передаются необработанные журналы событий веб-сервера, на основе которых свою работу последовательно выполняют два алгоритма. Параметризуемый алгоритм группировки событий объединяет записи журнала событий в сессии по IP-адресу или IP-адресу и User-Agent. Сформированные им сессии передаются в алгоритм выявления атакующих сессий, который оценивает каждую из выявленных сессий и как атакующую или пользовательскую, а также определяет уровень риска для атакующих сессий.

5 Выходные данные

Система предоставляет данные о результатах анализа журналов событий, включая количество, распределение сессий на атакующие и пользовательские, уровень риска для атакующих сессий. Также в «AML» можно ознакомиться со сведениями о заблокированных по результатам анализа атакующих сессиях и временных метках – когда была произведена блокировка, сколько длилась данная сессия и какие запросы совершались атакующим.

На основе предоставленных системой данных строятся информационные диаграммы и отчеты, которые позволяют владельцу веб-сервера сделать выводы об уровне защищенности ресурса и необходимости проведения мероприятий по улучшению защиты.

6 Загрузка Системы

Загрузка Системы производится согласно документу «Инструкция по установке AML».