SOLIDWALL AI SECURITY GATEWAY

ИНТЕЛЛЕКТУАЛЬНЫЙ СЕТЕВОЙ ЭКРАН ДЛЯ ЗАЩИТЫ AI-ПРИЛОЖЕНИЙ И API

Решение разработано на базе технологий Yandex Cloud с учетом экспертизы SolidLab и доступно для развертывания как в контуре клиента, так и по облачной модели

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

- Защита от основных видов атак на AI-приложения из перечней OWASP LLM Top-10 Risks и OWASP Top-10 for Agentic Applications, в том числе от атак инъекций запросов к LLM (prompt injection), нарушения ограничений LLM (jailbreak), утечек чувствительной информации
- Защита от основных видов атак на веб-приложения из перечня OWASP Top-10, от логических атак на AI-приложения
- Полнофункциональная защита API (функционал API Gateway) с возможностью создания и корректировки моделей
- Отражение переборных атак и ботов, сочетающее позитивную модель, рейт-лимитинг, анализ поведения пользователей при обращении к AI-специфичной функциональности приложения
- Противодействие «умному DoS-у», учитывающее особенности функционирования больших языковых моделей
- Контроль действий пользователей на основе анализа и хранения легитимных транзакций, а также использования механизмов контроля бизнес-логики

ПРЕИМУЩЕСТВА

- Механизмы интерпретируемого машинного обучения с возможностью анализа и ручной корректировки полученных моделей, минимизирующие затраты ресурсов на настройку
- Адаптивные страницы блокировок, затрудняющие использование AI/LLM для реализации атак на AI-приложения
- Использование негативных методов обнаружения атак на AI-приложения
- Противодействие переборным атакам и повторяющимся запросам
- Работа на основе позитивных моделей приложения
- Возможность обнаружения аномалий и значимых событий
- Функции упрощенного («быстрого») подавления ложных срабатываний оператором SolidWall AI Security Gateway, а также возможность тонкой настройки в привязке к отдельным параметрам
- Управление правилами принятия решений на основе данных об источнике и цели HTTP-транзакции, а также обнаруженных в ней аномалиях или значимых данных
- Возможность мониторинга и аудита событий информационной безопасности в формате статистики, оповещений, с функцией выгрузки данных в отчет
- Встраивание в корпоративную инфраструктуру доставки приложений

РЕЖИМЫ РАБОТЫ

Возможность работы узлов анализа в активном режиме защиты AI-приложения по схеме «в разрыв» между клиентами приложения и самим приложением с возможностью быстрого включения или выключения режима блокировки

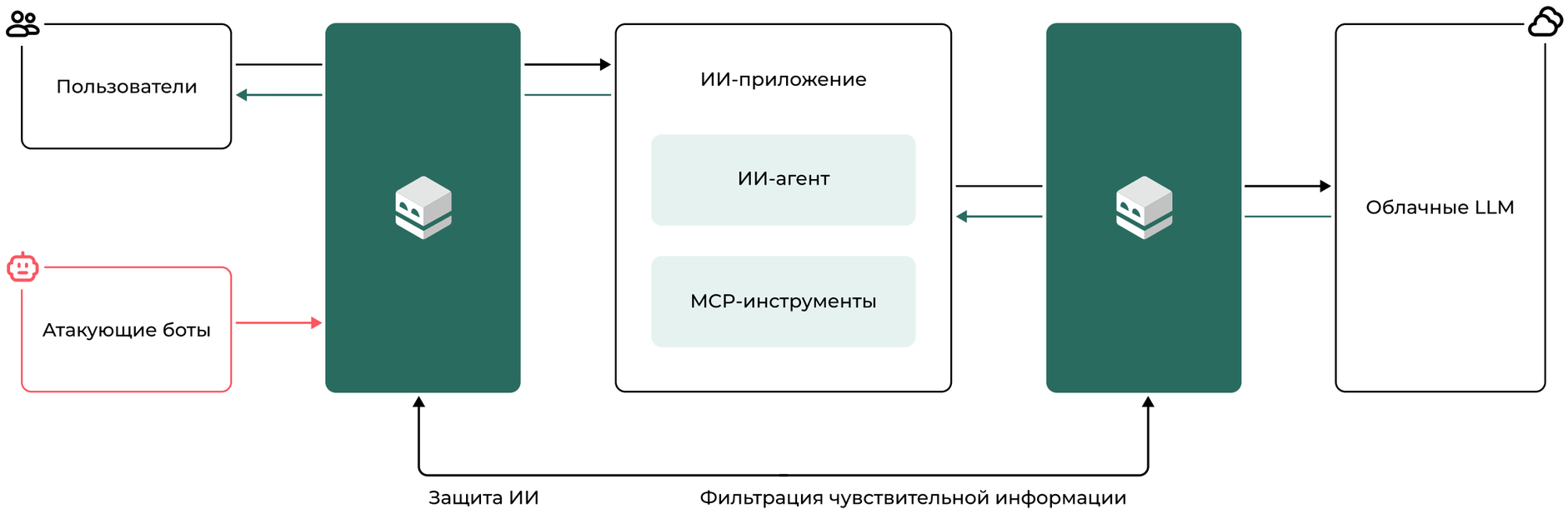
Возможность работы узлов анализа в активном режиме защиты чувствительной информации по схеме «в разрыв» между AI-приложением и внешним провайдером LLM-моделей с возможностью фильтрации запросов в сторону внешнего провайдера LLM-моделей, содержащих чувствительную информацию

ОТКАЗОУСТОЙЧИВОСТЬ

- Возможность построения кластерных конфигураций «Active/active» или «Active/passive» для узлов анализа, «Active/passive» с репликацией для системы управления
- Поддержка программного режима «bypass» и выполнения действия по умолчанию без проверки в случае локальных сбоев или резких скачков нагрузки

ИНТЕГРАЦИЯ С ВНЕШНИМИ СИСТЕМАМИ

- Возможность интеграции с SIEM-системами
- Возможность интеграции с другими системами с помощью механизмов Syslog, SQL, REST API
- Возможность загружать спецификации OpenAPI в качестве действий модели Бизнес-логики (в частности, как один из инструментов встраивания в CI/CD)
- Модуль интеграции со сканером защищенности приложений SolidPoint для раннего выявления недостатков и уязвимостей AI-приложения в соответствии с перечнем OWASP LLM Top-10 Risks
- Предоставление API для отправки данных во внешние системы
- Возможность мониторинга работоспособности программных и аппаратных компонентов с использованием систем мониторинга Zabbix и Prometheus
- Возможность загружать спецификации OpenAPI в качестве действий модели бизнес-логики



125040, г. Москва, ул. Вавилова, д. 47А +7 (499) 705-76-57 info@solidlab.ru

Группа компаний SolidLab работает в области информационной безопасности более 15 лет, защищая организации от киберугроз, предупреждая атаки, минимизируя риски финансовых и репутационных потерь. SolidLab предлагает полный комплекс услуг: от пентестов до защиты приложений, реагирования на инциденты и организации процессов SDLC.