Краткое описание компании для сайта партнера:

INFERA Security – российский разработчик решений кибербезопасности на основе AI и для защиты LLM-моделей.

Продукты INFERA Security охватывают ключевые задачи ИБ.

INFERA AI.Firewall – решение для защиты и безопасного использования LLM-моделей, включая контроль доступа и защиту конфиденциальных данных, фильтрацию вредоносных запросов и аудит взаимодействия с ИИ.

INFERA AI.SafeAgent – решение для защиты, безопасного использования и контроля работы ИИ-агентов с учетом привилегий и политик, анализа промптов, цепочек рассуждений и действий.

INFERA AI.SafeCode – платформа для анализа исходного кода и open-source компонентов с целью обнаружения уязвимостей и аномалий в режиме реального времени, внедрения методологии DevSecOps / MLSecOps в процессы разработки ПО.

INFERA AI.Platform – AI Security Operations платформа обеспечивает сквозную видимость всего жизненного цикла использования ИИ в реальном времени: от промпта и ИИ-сгенерированного кода до поведения автономных агентов и передачи обогащённых данных в SOC с приоритезацией по бизнес-рискам.

Подробнее на www.InfEraSecurity.ru

Краткое описание компании (1 276 символов с пробелами):

INFERA Security – российский разработчик решений кибербезопасности на основе AI и для защиты LLM-моделей.

Создаём будущее, в котором безопасность встроена в продукт с первой строки кода, искусственный интеллект усиливает R&D команды, а DevSecOps становится не просто методом, а культурой мышления.

Продукты INFERA Security охватывают ключевые задачи современной ИБ:

- **INFERA AI.Firewall** – решение для защиты и безопасного использования LLM-моделей, включая контроль доступа и защиту конфиденциальных данных, фильтрацию вредоносных запросов и аудит взаимодействия с ИИ.
- **INFERA AI.SafeAgent** – решение для защиты, безопасного использования и контроля работы ИИ-агентов с учетом привилегий и политик, анализа промптов, цепочек рассуждений и действий.
- **INFERA AI.SafeCode** – платформа для анализа исходного кода и open-source компонентов с целью обнаружения уязвимостей и аномалий в режиме реального времени, внедрения методологии DevSecOps / MLSecOps в процессы разработки ПО.
- **INFERA AI.Platform** – AI Security Operations платформа обеспечивает сквозную видимость всего жизненного цикла использования ИИ в реальном времени: от промпта и ИИ-сгенерированного кода до поведения автономных агентов и передачи обогащённых данных в SOC с приоритезацией по бизнес-рискам.

Мы строим экосистему, в которой ИИ помогает защищать, а безопасность становится умной, предиктивной и встроенной во всё, что вы создаёте.

Краткое описание компании с продуктами (471 символов с пробелами)

INFERA Security – российский разработчик решений кибербезопасности на основе AI и для защиты LLM-моделей. Продукты INFERA Security: **AI.Firewall** – для защиты и безопасного использования LLM-моделей; **AI.SafeAgent** – для аудита, мониторинга и контроля работы ИИ-агентов; **AI.SafeCode** – платформа для анализа исходного кода с целью обнаружения уязвимостей и аномалий в режиме реального времени; **AI.Platform** – сквозная видимость всего жизненного цикла использования ИИ в компании.

Краткое описание компании общее (243 символов с пробелами)

INFERA Security – российский разработчик решений кибербезопасности на основе AI и для защиты LLM-моделей. Мы строим экосистему, в которой ИИ помогает защищать, а безопасность становится умной, предиктивной и встроенной во всё, что вы создаёте.

О компании

INFERA Security – российский разработчик решений кибербезопасности на основе AI и для защиты LLM-моделей

Компания ООО «ИнфЭра Секьюрити» создана в 2025 году, является резидентом «Сколково», имеет статус МТК. Продукты прошли независимые экспертизы в государственных центрах, получили положительные экспертные заключения и соответствующие статусы.

Продукты включены в Реестр отечественного ПО:

- INFERA AI.SafeCode номер в реестре №31051
- INFERA AI.Firewall номер в реестре №31595

INFERA Security обладает уникальной экспертизой в области информационной безопасности и предлагает инновационные решения для безопасного применения искусственного интеллекта на предприятиях любых отраслей экономики и на объектах критической информационной инфраструктуры (КИИ). Наши решения обеспечивают внедрение подхода безопасной разработки программного обеспечения, соответствуют российским и международным стандартам безопасности.

Эксперты INFERA Security готовы делиться опытом и участвовать в создании совместных ИИ-платформ, способствующих устойчивому развитию цифровых экосистем и повышению киберустойчивости ключевых предприятий.

Наша миссия: формируем новую эру безопасности, где защита вшита в продукт с момента его создания, AI становится союзником, а DevSecOps культурой мышления.

Мы создаём будущее, в котором безопасность встроена в продукт с первой строки кода, искусственный интеллект усиливает R&D команды, а DevSecOps становится не просто методом, а культурой мышления.

Наш подход

Строим Security by Design среду нового поколения – не надстройку над устаревшими системами, а платформу, изначально созданную с учетом современных рисков: AI-угроз, Zero-Day, атак на LLM и сложных целевых атак.

Наша философия строится на 4 ключевых принципах:

- **Resilience by Design** – устойчивость по умолчанию, заложенная в архитектуру и код.
- **Integrated Security** – безопасность как неотъемлемая часть Dev, Ops и AI.
- **Predictive Defense** – проактивная защита, предотвращающая угрозы до их реализации.
- **Root-first Thinking** – акцент на устранение корневых причин, а не последствий.

Мы верим в **AI Security**, когда ИИ становится инструментом защиты, ускоряя процессы, обеспечивая прозрачность, снижая риски и издержки.

Почему INFERA Security

- **Автоматизация и скорость**. Создали платформу, которая позволяет безопасно использовать ИИ-модели и ИИ-агентов без потери контроля, обеспечивает сквозную видимость в реальном времени всего жизненного цикла использования ИИ: от промпта и ИИ-сгенерированного кода до поведения автономных агентов и передачи обогащённых данных в SOC с приоритезацией по бизнес-рискам.
- **Открытость и доверие**. Прозрачная архитектура, открытый road-map и регулярный аудит кода. Мы готовы показать, как работают ключевые модули наших продуктов, как и где используются LLM.
- **Экономическая эффективность**. Интеграция ИИ и ИБ-автоматизация с продуктами INFERA Security позволяют компаниям повышать производительность до 20% и снижать затраты на безопасность до 30%.
- **Реальная экспертиза**. Наша команда – это консолидация лучших практик, которые мы десятилетиями оттачивали в крупных ИБ-компаниях, проектах для госструктур и корпораций. Наши ключевые эксперты 15+ лет решают реальные ИБ-кейсы – от защиты крупнейших компаний России до развития ИБ-продуктов и ИБ-направлений в ведущих интеграторах и вендорах.

INFERA Security: создаём умную, предиктивную и встроенную безопасность, делаем это с пониманием архитектуры, угроз и будущего, которое уже наступило.

Описание продуктов

INFERA AI.Firewall

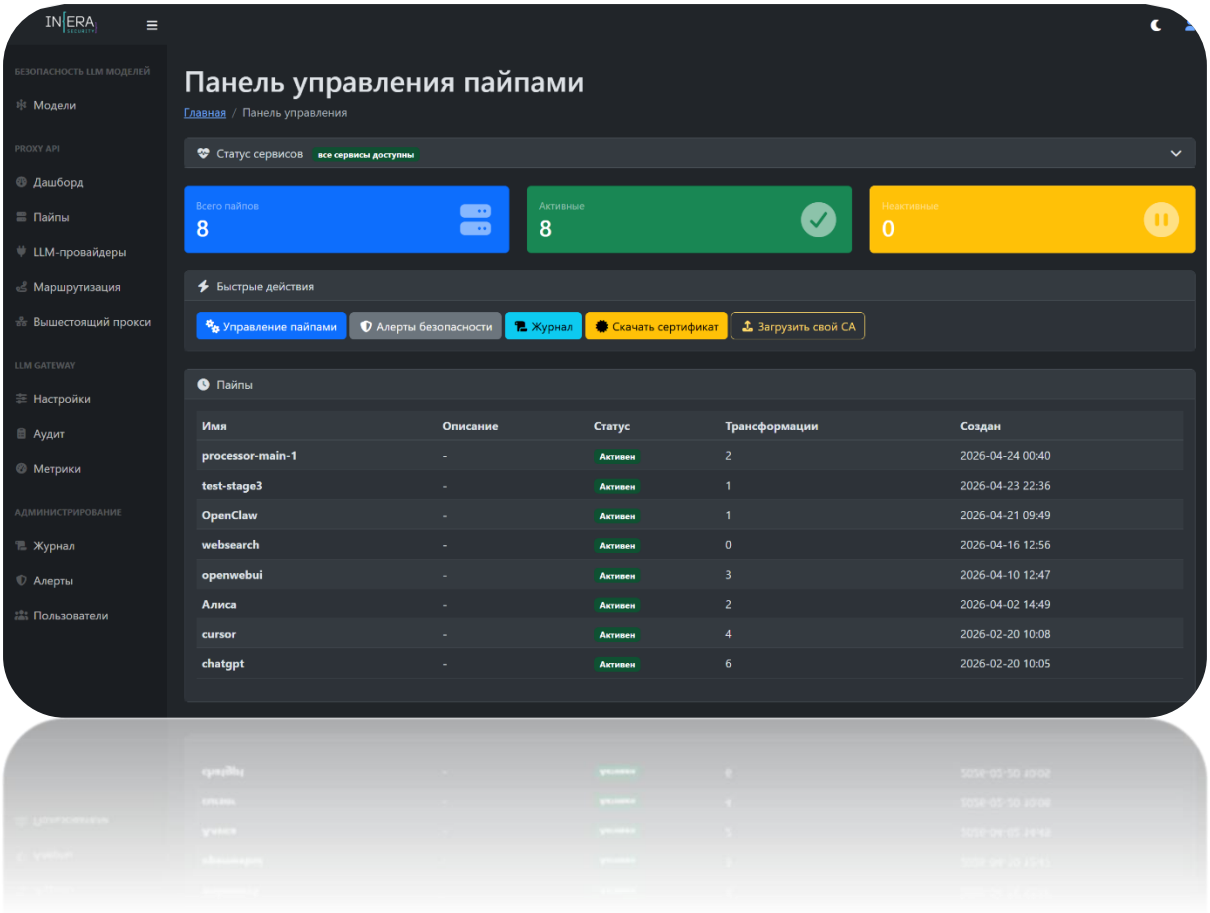
INFERA AI.Firewall – решение для защиты и безопасного использования LLM-моделей, включая контроль доступа и защиту конфиденциальных данных, фильтрацию вредоносных запросов и аудит взаимодействия с ИИ.

Позволяет выстраивать безопасность ИИ как часть архитектуры цифровых продуктов: от контроля доступа и защиты данных до тестирования устойчивости моделей к современным атакам.

Возможности INFERA AI.Firewall:

- маскирование данных, контроль доступа, защита от утечек и манипуляций
- сканер MLRed Teaming
- аудит всех взаимодействий с ИИ, контроль и фильтрация запросов, выявление любых аномалий и потенциальных угроз
- защита от угроз OWASP Top 10 for LLM Applications, OWASP Top 10 for Agentic Applications
- схемы подключения через Proxy, API Gateway, Guardrails, единое окно подключения пользователей
- безопасность vibe coding и контроль использования LLM-моделей в процессах разработки ПО
- различные режимы реагирования, включая блокировку сообщения, маскирование и демаскирование чувствительной информации или запрет доступа
- контроль расхода LLM-токенов, перераспределение задач и полная детализация
- поиск и блокировка секретов (API-ключей, токенов, паролей) в промптах и ответах
- возможность обучения на документах и данных организации
- гибкая настройка, ролевая модель, и разграничение прав доступа, аутентификация пользователей через keycloak

Запрос от пользователя проходит через решение. Автоматически производится проверка прав доступа через интеграцию с системой управления доступом. INFERA AI.Firewall анализирует и фильтрует запросы и ответы ИИ-модели, маскируя конфиденциальные данные, блокируя опасные или запрещённые. После прохождения всех проверок запрос передаётся LLM, а ответ пользователю. Если у пользователя нет прав доступа, то система выдаёт сообщение об этом и блокирует действие. Все этапы фиксируются в аудит-логе.



INFERA ML Red Teaming + AI.Firewall это одна связанная система: нашли уязвимость и сразу применили защиту (фильтрация, блокировка, маскировка данных, контроль доступа). Результат работы сканера ML Red Teaming отправляется в SOC или ASOC/ASPM, в зависимости от того, в каком подразделении компания использует ИИ. Отчёт содержит: тип атаки, название техники, текст атаки и ответ модели. Эти данные напрямую используются для донастройки AI.Firewall, обновления правил и политик. Модуль INFERA автоматически сканирует модели на этапах разработки, внедрения и эксплуатации без постоянного участия специалистов по ML.

Плюсы:

- поддержка облачных и корпоративных LLM-платформ, контроль нескольких LLM одновременно
- собственные модели для выявления атак и ПДн со скоростями задержки порядка 100 мс для средних запросов
- гибкая настройка фильтров и политик под конкретные бизнес-процессы
- MLSecOps: контроль использования LLM-моделей в процессах разработки и безопасность Vibe Coding
- сканер ML Red Teaming для автоматизированного тестирования, выявления и устранения уязвимостей в AI- и ML-моделях на всех этапах их жизненного цикла
- возможность работы в облачной, локальной и гибридной инфраструктуре

Для кого

- CISO, CIO, директора по цифровизации и внедрению ИИ
- ИБ-инженеры, Prompt-инженеры
- DevSecOps и AppSec специалисты
- CTO и руководители разработки
- компании, внедряющие AI в SDLC
- команды, использующие Cursor, GitHub Copilot, Tabnine или Codeium

Результат от использования INFERA AI.Firewall:

- безопасное и контролируемое использование ИИ в продуктах и сервисах компании
- устойчивость к атакам на ИИ-модели, фильтрация и блокировка вредоносных запросов, защита от угроз OWASP TOP 10 LLM и Agentic Applications
- защита данных от утечки и манипуляций, контроль доступа к данным и защита конфиденциальности
- аудит всех взаимодействий с ИИ, контроль запросов, выявление любых аномалий и потенциальных угрозы
- контроль Shadow AI и расхода токенов
- внедрение концепции MLSecOps, контроль использования ИИ в процессах разработки
- соответствие стандартам безопасности и улучшение прозрачности взаимодействий с ИИ (приказ 117, приказ 21, ФЗ об ИИ, ФЗ-152, ГОСТ Р 56939-2024, отраслевые регламенты и ГОСТы)

Ссылка на описание: https://www.inferasecurity.ru/ai_firewall/

INFERA AI.SafeAgent

INFERA AI.SafeAgent – решение для защиты, безопасного использования и контроля работы ИИ-агентов с учетом привилегий и политик, анализа промптов, цепочек рассуждений и действий.

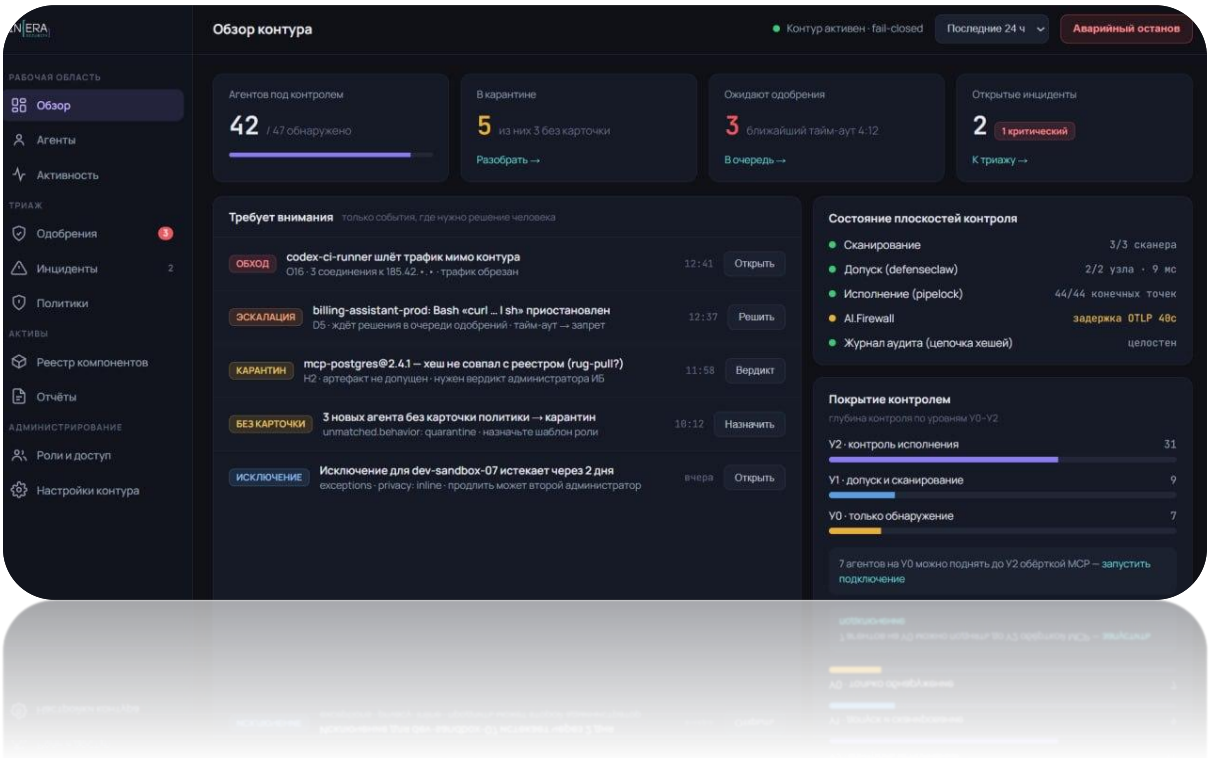
Реализован контроль на уровне всех точек взаимодействия: LLM → агент → инструменты. INFERA AI.SafeAgent контролирует трафик, действия, делает инспекцию входных и выходных данных, проверку до запуска агента и до исполнения им какого-либо действия, контролирует опасные команды и инъекции, изолирует агента в случае необходимости. Обеспечивается полная видимость и контроль над действиями агентов с предсказуемыми затратами и минимальным влиянием на бизнес-процессы компании.

INFERA AI.SafeAgent представляет собой runtime-слой контроля агентов:

- единый список всех обнаруженных агентов с фильтрами по среде, уровню контроля и статусу;
- перехват вызова инструментов (tool calls) с проверкой полномочий и аргументов;

- профили доступа с deny-by-default и least privilege;
- обнаружение Shadow AI с возможностью карантина;
- очередь HITL-одобрений и аварийный останов (Kill Switch);
- полный след сессии для расследования инцидентов;
- режим fail-closed: всё, что явно не разрешено политикой, автоматически запрещено;
- управление ролями (администратор / оператор SOC / аудитор), пользователями и настройками контура.

Система работает совместно с INFERA AI.Firewall как единая платформа, обеспечивая сквозную видимость использования ИИ в корпоративной инфраструктуре компании: от промпта до реального действия ИИ-агента.



В INFERA AI.SafeAgent в карточке агента представлена вся информация по агенту: метаданные, активность, инциденты, полномочия, доступы, белые списки MCP, криминалистический снимок и т.д.

Единая приборная панель даёт ключевые показатели: агенты под контролем, в карантине, ожидающие одобрения, открытые инциденты, покрытие уровнями контроля, аварийный останов.

Конструктор политик позволяет гибко настраивать правила рисков, полномочия, DLP, сетевые ограничения, MCP-реестр, предохранители, HITL (Human-in-the-Loop) и бюджеты. Система умеет останавливать агента целиком, детектировать зацикливание, работать в fail-closed режиме для необратимых действий и изолировать код в песочнице. Параллельно контролируются затраты через квоты и ML-роутинг.

Решение позволяет закрывать все ключевые угрозы OWASP Top 10 for Agentic Applications 2026 – от Tool Misuse и Privilege Compromise до Rogue Agents.

В INFERA AI.SafeAgent реализована контроль Shadow AI через многоуровневую проверку на хосте пользователя, выявление и блокировка неавторизованного использования ИИ-инструментов и агентов. Осуществляется сетевой анализ трафика, контроль запущенных процессов, анализ артефактов браузера, обнаружение сохранённых ключей и токенов в файловой системе. Решение автоматически различает корпоративно-утверждённые ИИ-инструменты от запрещённых и блокирует последние.

Для кого

- CISO, CIO, директора по цифровизации и внедрению ИИ
- ИБ-инженеры, Prompt-инженеры
- DevSecOps и AppSec специалисты
- CTO и руководители разработки
- компании, внедряющие AI в SDLC

Результат от использования INFERA AI.SafeAgent

- безопасное и контролируемое использование ИИ-агентов в корпоративной среде
- устойчивость к атакам на ИИ-агентов и через них, фильтрация и блокировка вредоносных запросов, защита от угроз OWASP TOP 10 for Agentic Applications
- защита данных от утечки и манипуляций, контроль доступа к данным и защита конфиденциальности
- аудит всех взаимодействий с ИИ-агентами, контроль запросов, выявление любых аномалий и потенциальных угрозы
- контроль Shadow AI
- соответствие стандартам безопасности и улучшение прозрачности взаимодействий с ИИ (приказ 117, приказ 21, ФЗ об ИИ, ФЗ-152, ГОСТ Р 56939-2024, отраслевые регламенты и ГОСТы)

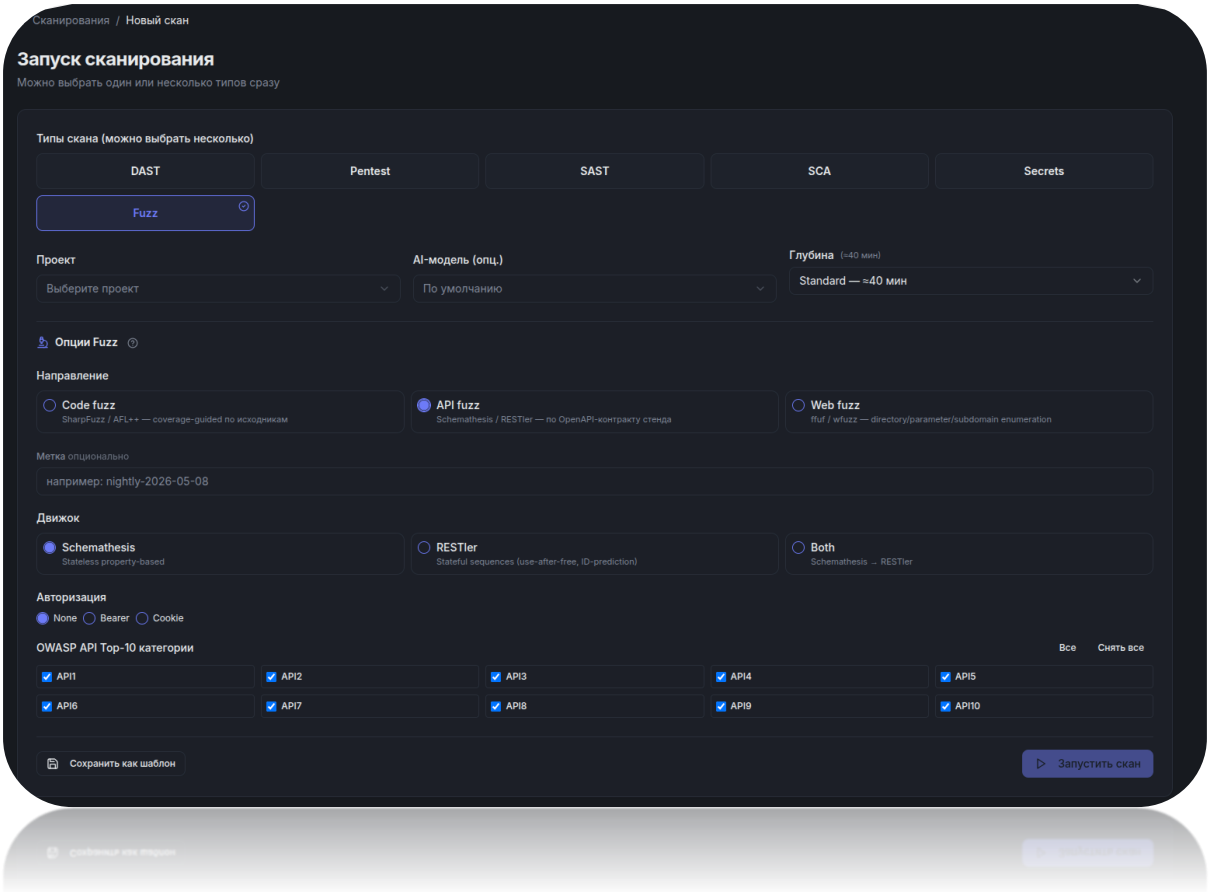
Ссылка на описание: https://inferasecurity.ru/ai_safeagent/

INFERA AI.SafeCode

INFERA AI.SafeCode – платформа для анализа исходного кода и open-source компонентов с целью обнаружения уязвимостей и аномалий в режиме реального времени, внедрения подхода DevSecOps / MLSecOps в процессы разработки ПО.

Помогает выявить и предотвратить уязвимости ещё на стадии проектирования и кодирования, а не находить их после развертывания и сборки ПО.

Платформа объединяет SAST, SCA, Secrets, DAST, Pentest, Code Fuzzing и API Fuzzing в единый DevSecOps / MLSecOps-контур.



— SAST – анализ исходного кода в реальном времени прямо в среде разработки;

— SCA – анализ open-source зависимостей;

— Secrets – поиск и верификация секретов;

— DAST– динамический анализ работающего приложения;

— Pentest – AI-агент для имитации ручного пентеста;

— Code Fuzzing – поиск crash и edge-case уязвимостей;

— API Fuzzing – анализ REST, GraphQL, gRPC и WebSocket API.

Все сканеры работают как единая система, а не как набор отдельных инструментов.

INFERA AI.SafeCode не просто показывает список подозрений, а подтверждает найденные уязвимости. К каждой подтвержденной уязвимости прилагается рекомендация с исправлением, а проблема подсвечивается прямо во время написания кода. Комментарии отображаются на проблемных строках с доказательством и кнопкой «применить AutoFix».

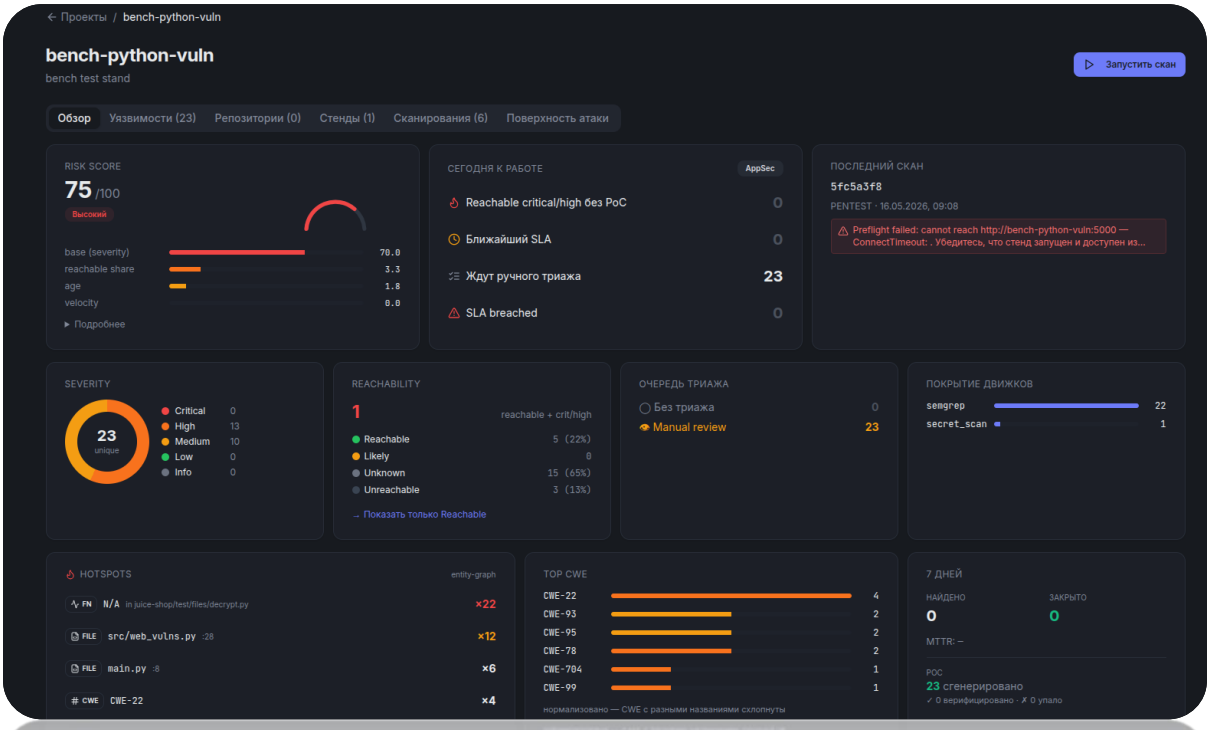
Преимущества INFERA AI.SafeCode:

— анализ кода программы на наличие уязвимостей в процессе его написания разработчиком в среде IDE

— выявление уязвимостей сразу в момент разработки ПО и подтверждение их доказательствами

— 7 сканеров в едином DevSecOps / MLSecOps-контуре: SAST, SCA, Secrets, DAST, Pentest, Code Fuzzing и API Fuzzing

- автоматическое распределение high/critical-уязвимостей в понятные задачи для разработчика с объяснениями, доказательствами и рекомендациями по исправлению
- единая картина рисков по коду, API, компонентам и зависимостям
- обнаружение сложных паттернов, которые могут быть пропущены традиционными инструментами
- контроль vibe coding и анализ кода, сгенерированного ИИ, через INFERA AI.Firewall контроль всех взаимодействий с ИИ в департаменте разработки
- проведение оценки качества разрабатываемого кода и ПО
- качество выявления уязвимостей: TPR (True Positive Rate) – 94%, FPR (False Positive Rate) < 8%, точность достижимости (reachability precision) – 91%
- добавление в систему базы уязвимостей от Заказчика
- использование облачных или локальных серверов



INFERA AI.SafeCode обнаруживает следующие типы уязвимостей: инъекция команд ОС, секреты в коде, отсутствие защиты от XSS, SQL- инъекции, командные инъекции, некорректная обработка входных данных, раскрытие чувствительной и конфиденциальной информации, использование MDS для хеширования, слабая криптографическая стойкость и/или шифрование, обработка файлов и т.д.

Реализована широкая поддержка языков программирования: Python, JavaScript/TypeScript, Java, C#/.NET, Go, Rust, PHP, Ruby, C/C++, Swift и других.

Для кого

- команды разработки (Backend / Frontend / Fullstack)
- CISO, DevSecOps и AppSec специалисты
- CTO и руководители разработки
- компании, внедряющие AI в SDLC
- команды, использующие Cursor, GitHub Copilot, Tabnine или Codeium

Результат от использования INFERA AI.SafeCode:

- безопасный код уже на этапе разработки – никаких сюрпризов на стадии тестирования и эксплуатации
- безопасный код без замедления релизов: сокращение времени исправления уязвимостей в проде до минут
- доказательная приоритезация: критичная уязвимость всегда имеет доказательство и объяснение
- управляемый DevSecOps / MLSecOps-процесс
- единая платформа вместо набора разрозненных инструментов
- единая картина риска по коду, API, компонентам и зависимостям
- выпуск ПО для КИИ в соответствии с требованиями регуляторов
- взращивание Security Champions
- снижение стоимости устранения уязвимостей
- легкое внедрение Security в DevOps-процессы
- устойчивость к supply chain атакам
- соблюдение требований регуляторов к процессам безопасной разработки

INFERA Security позволяет внедрить MLSecOps и масштабировать AI-разработку с соблюдением требований безопасности (приказ 117, приказ 21, ФЗ об ИИ, ФЗ-152, ГОСТ Р 56939-2024, отраслевые регламенты и ГОСТы).

Ссылка на описание: https://www.inferasecurity.ru/ai_safecode/

INFERA AI.Platform *MVP

INFERA AI.Platform – AI Security Operations платформа обеспечивает сквозную видимость всего жизненного цикла использования ИИ в реальном времени: от промпта и ИИ-сгенерированного кода до поведения автономных агентов и передачи обогащённых данных в SOC с приоритезацией по бизнес-рискам.

Платформа объединяет выводы и аналитику из трех продуктов AI.Firewall, AI.SafeAgent, AI.SafeCode и предоставляем сквозную видимость всего жизненного цикла использования ИИ: при работе с ИИ-моделями, использовании ИИ-агентов для решения бизнес-задач и автоматизации сервисов, при разработке собственного ПО и интеграций.

1. архитектурная связка всех продуктов по безопасному использованию ИИ в корпоративной инфраструктуре

2. защита и расследование инцидентов в реальном времени на уровне промптов, кода и действий агентов
3. сквозная аналитика по использованию ИИ в компании, контроль расхода токенов, эффективное перераспределение задач на ИИ-модели
4. едина платформа контроля за рисками использования ИИ во всех подразделениях
5. end-to-end расследование AI-инцидентов
6. compliance и аудит использования ИИ, включая контроль действий ИИ-агентов
7. выявление и управление Shadow AI
8. проактивное выявление и защита от новых атак на И-модели и агентные системы
9. интеграция с SOC и SOAR
10. метрики и отчётность для руководства и регуляторов

Источник данных для AI.Platform	Кросс-платформенные задачи
AI.Firewall	— comliance-аудит использования ИИ во всех департаментах — детекция и блокировка атак на ИИ-модели и ИИ-агентов — корреляция событий — threat hunting по атакам на LLM — обогащение инцидентов контекстом — выявление и блокирование утечек конфиденциальных данных и секретов — аудит доступа к генеративному ИИ, контроль использования и расходов — защита от утечек конфиденциальной информации и секретов
AI.SafeAgent	— end-to-end расследование AI-инцидентов — форензика и root-cause анализ — compliance и аудит решений агента — корреляция событий через единую платформу — управление Shadow AI — приоритизация инцидентов — защита от атак на агентные системы
AI.SafeCode	— предотвращение попадания уязвимого кода в прод — контроль всех взаимодействий с ИИ в разработке — выявление Shadow AI в разработке — улучшение DevSecOps-метрик — анализ, контроль и предотвращение рискованного использования vibe coding

	— поиск и блокировка секретов (API-ключей, токенов, паролей) в промптах и ответах — защита от атак на цепочку поставок
AI.Platform (кросс-продуктовая)	— сквозная видимость всего цикла использования ИИ — комплексные многоэтапные расследования — dashboards, визуализация и аналитика из трех систем по безопасному использованию ИИ — приоритизация по бизнес-рискам — отчётность для руководства и регуляторов — повышение ROI использования ИИ во всех подразделениях, контроль расходов и эффективное использование — улучшение политик и моделей — планирование автоматизации и ресурсов — переход SOC от «реагируем на инцидент» к «понимаем и предотвращаем риски на всём пути использования ИИ»