INFERA SECURITY

безопасность встроенная в ДНК

www.InfEraSecurity.ru

тел.: +7 915 234 9900

почта: info@InfEraSecurity.ru

INFERA Security. О компании

новая Эра информационной безопасности

экспертиза людей сильнее «возраста компании»

«Наша команда — это не стартап без опыта - 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.»

Игорь Бирюков
Генеральный директор InfEra Security

15+ лет в ИБ

- ex-руководитель Киберхаба «Сколково»
- автор статей для ведущих СМИ, спикер и модератор крупнейших ИБ-конференций
- амбассадор клуба резидентов «Кибердома», член клуба КУБИТ
- реализовывал государственные проекты по ИБ, руководил отделами технической защиты и ИБ-консалтингом в ведущих компаниях
- большой опыт получения лицензий ФСТЭК и ФСБ, знание законодательства и нормативных документов ФСТЭК России, ФСБ России, Минцифры

INFERA Security. Продуктовый портфель

безопасность встроенная, а не прикрученная

INFERA SECURITY

добавляем экспертизу ИБ в R&D без посредников

защищаем ИИ-модели и бизнес-данные

INFERA AI.SafeCode

ВСТРОЕННЫЙ AI.SECURITY АГЕНТ В ПРОЦЕССЫ РАЗРАБОТКИ

ИИ-платформа для ИБ-анализа исходного кода с целью обнаружения уязвимостей и аномалий в режиме реального времени, внедрения подхода Security by Design в R&D, в процессы разработки ПО и использования open-source компонентов

INFERA AI.Firewall

ЗАЩИТА ИИ-МОДЕЛЕЙ И ИХ БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ

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

КОНСАЛТИНГ И УСЛУГИ

подготовка документации и внедрение процесса DevSecOps, определение метрик, настройка и интеграция DevSecOps инструментов, настройка Security Gates, разработка стратегии защиты LLM

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

- стандартная 8x5
- расширенная 24x7

INFERA AI.SafeCode

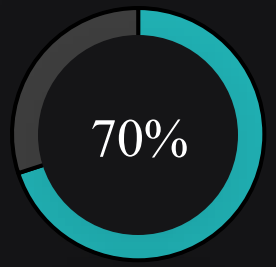
встроенный AI.SECURITY агент в процессы разработки

ИИ-платформа для ИБ-анализа исходного кода с целью обнаружения уязвимостей и аномалий в режиме реального времени, внедрения подхода Security by Design в R&D, в процессы разработки ПО и использования open-source компонентов

Почему нужен DevSecOps?

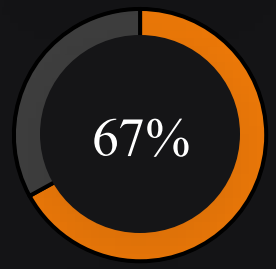
IN{ERA} SECURITY

классический подход безопасности не работает в современных скоростях DevOps



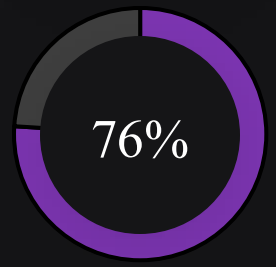
времени уходит на ручную проверку уязвимостей и багов без DevSecOps у безопасников и разработчиков

GitLab DevSecOps Survey



разработчиков отмечают рост числа уязвимостей в ПО за последний год

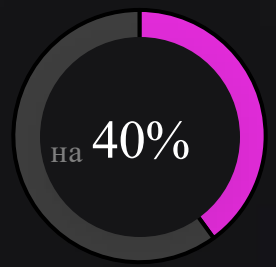
GitLab Global DevSecOps Report 2024



CISO признают, что текущие процессы безопасности не успевают за DevOps-циклами и остаются «заплаточными»

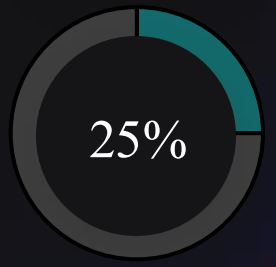
Gartner Research

только автоматизация и Shift Left Security позволяют командам безопасно выпускать ПО в высоком темпе



к 2027г. увеличится количество команд R&D, использующих ИИ

Gartner



дефектов ПО, попавших в производство, будут вызваны отсутствием контроля за кодом, сгенерированным ИИ

Gartner

ГОСТ Р 56939-2024, GDPR, ISO 27001, PCI DSS

все требуют, чтобы безопасность была встроена в процесс разработки, а не добавлялась постфактум

INFERA AI.SafeCode

анализ кода в реальном времени

— INFERA AI.SafeCode анализирует код программы на наличие уязвимостей в процессе его написания разработчиком

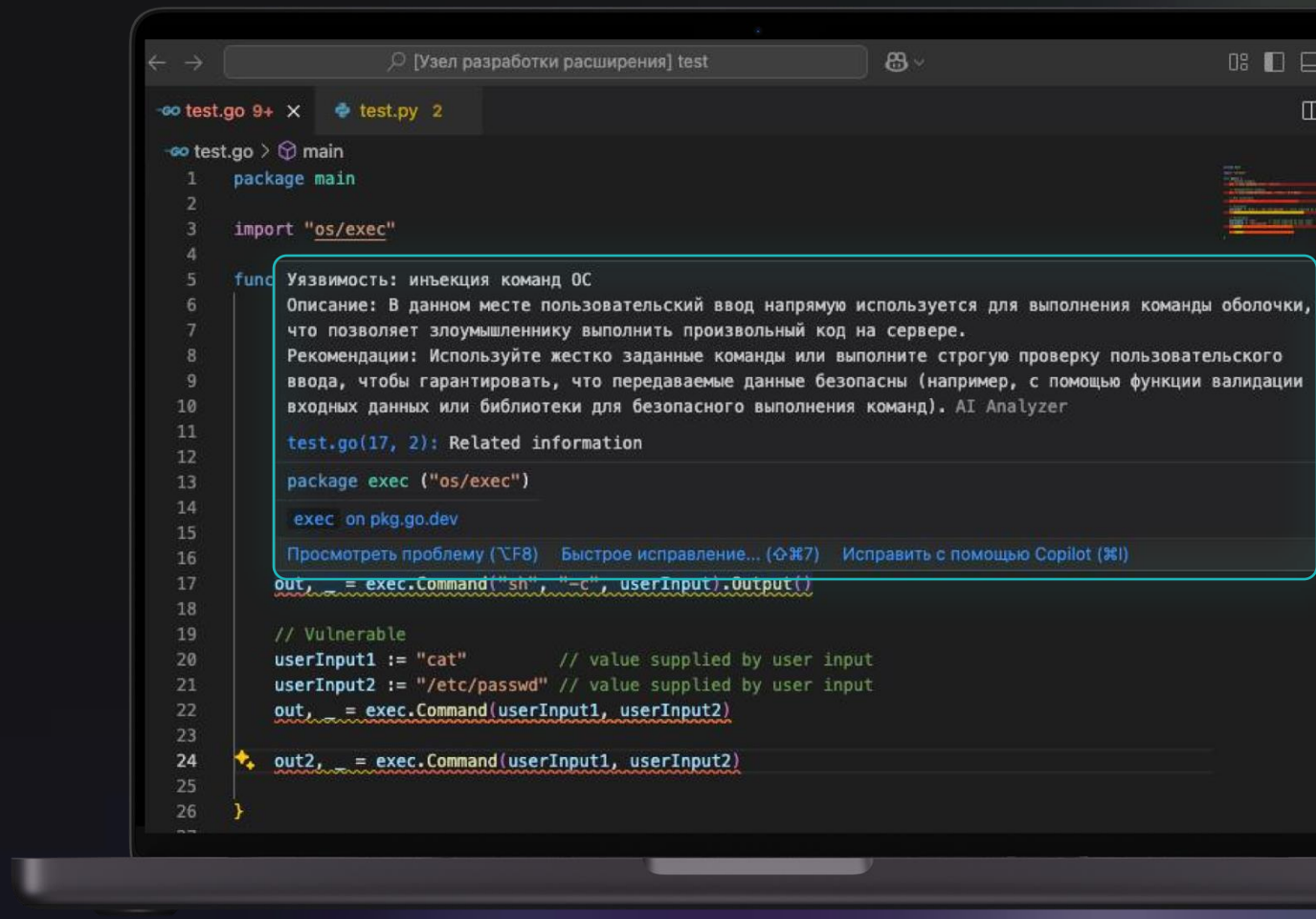
— в том числе осуществляется проверка кода open-source компонентов перед их использованием в отношении ПО, поставляемого на объекты КИИ

ИИ-подход

— LLM распознает сложные паттерны и предлагает варианты исправления

широкая поддержка языков программирования

Python, Java, JavaScript, C++, C#, Typescript, SQL, C, Go, PHP и других



INFERA AI.SafeCode

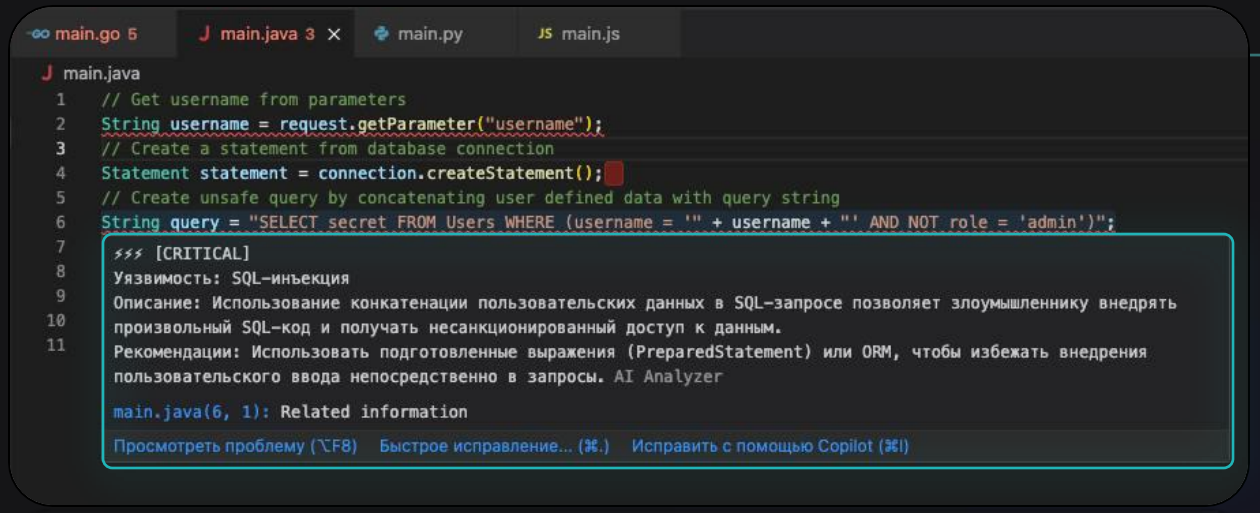
поиск уязвимостей в runtime режиме

в процессе написания кода

интеграция с IDE

— установка плагина занимает считанные минуты

— бесшовно встраивается в процесс разработки и поддерживает распространённые IDE



поддерживаемые платформы

— LPT сервер работает на Linux

— Клиент-серверная модель

LLM-интеграция

возможность размещения в открытом облаке и в on-premise

результат

— безопасный код уже на этапе разработки — никаких сюрпризов на стадии тестирования и эксплуатации

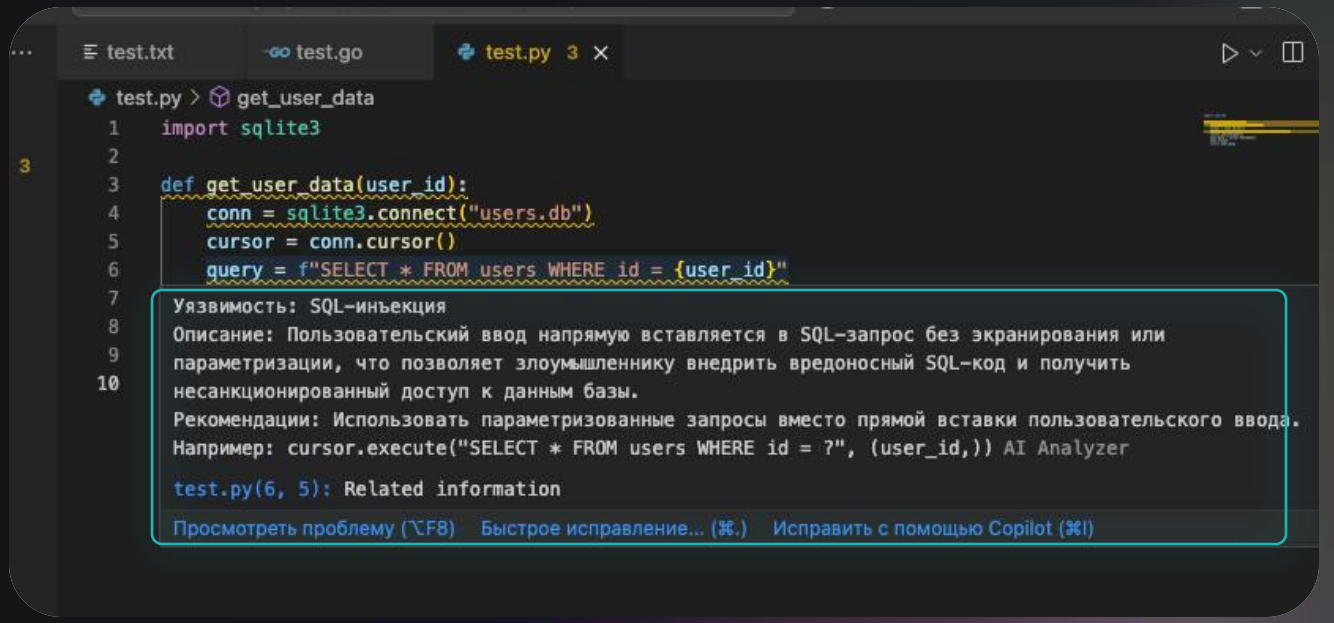
— безопасный код без замедления релизов

— выпуск ПО для КИИ в соответствии с требованиями регуляторов

INFERA AI.SafeCode. ИИ-модель

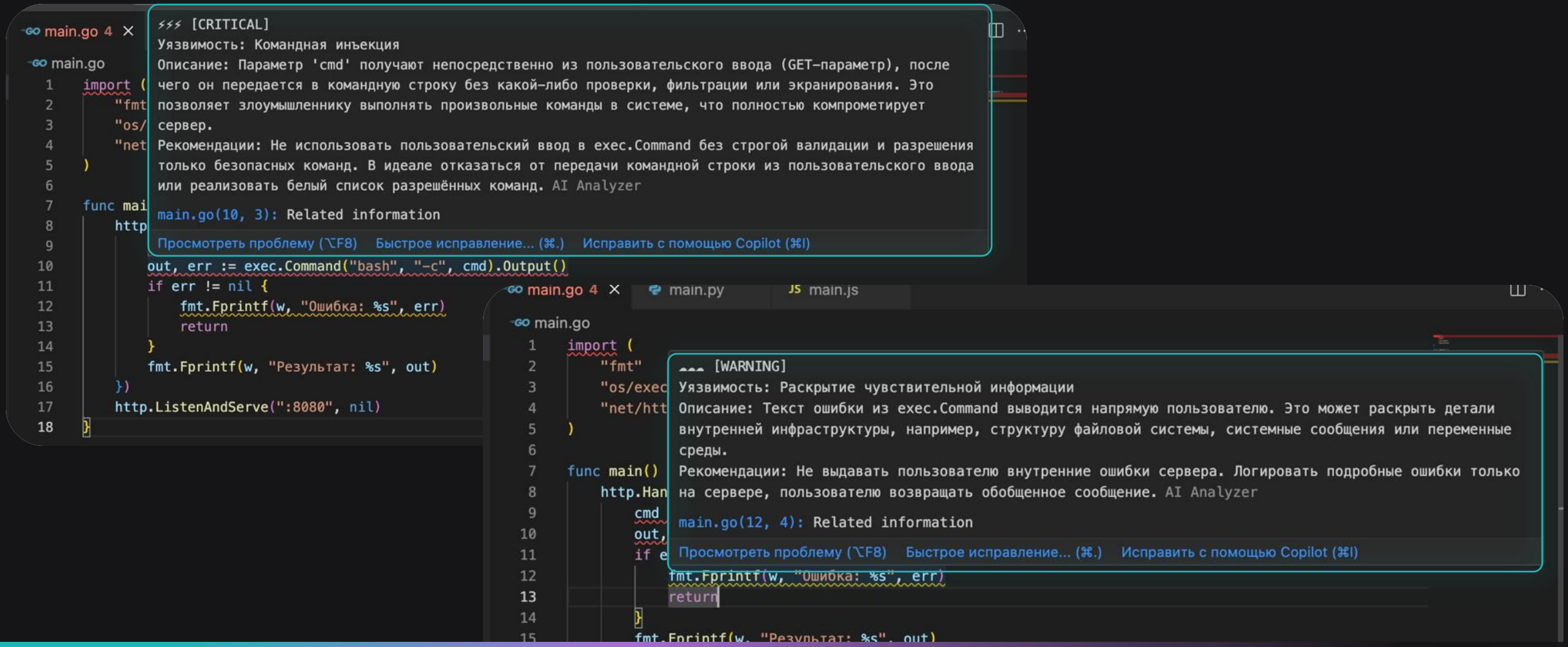
подход на основе ИИ включает:

- контроль уязвимостей на основе анализа исходного кода с помощью ИИ
- отображение разработчику ПО уязвимого участка кода, описание типа уязвимости, а также варианта для устранения
- факт обнаружения уязвимости отправляется в систему учёта уязвимостей
- при исправлении уязвимость перестаёт отображаться
- при необходимости, возможно добавить перечень ложных срабатываний для последующей фильтрации



в INFERA AI.SafeCode машинное обучение и искусственный интеллект используются для улучшения обнаружения уязвимостей и эффективной расстановки приоритетов

INFERA AI.SafeCode



добавляем экспертизу ИБ в R&D без посредников

Соответствие требованиям законодательства

INFERA SECURITY

DevSecOps помогает автоматизировать выполнение требований:

- ГОСТ Р 56939-2024
- ФЗ-152, ФЗ-187
- ISO 27001, PCI DSS, GDPR

ГОСТ Р 56939-2024 — это не просто compliance-документ, а фундамент для внедрения DevSecOps-подхода в российском контексте. Он задаёт минимальный уровень зрелости безопасной разработки и побуждает автоматизировать, моделировать и интегрировать ИБ в каждую фазу разработки ПО

DevSecOps — это лучший способ выполнить требования ФСТЭК к безопасной разработке, сопровождению и реагированию на угрозы

связь ГОСТ Р 56939-2024 с DevSecOps

элемент DevSecOps	ГОСТ Р 56939-2024
Shift Left	требование начинать ИБ с первых этапов проекта
CI/CD Security	контроль сборки, статический и динамический анализ
Security as Code	использование IaC + политик как код
SBOM и supply chain	учет происхождения компонентов, требования к цепочке поставок
Автоматизация ИБ	рекомендуется в тестировании, сопровождении, мониторинге
Моделирование угроз	обязательный элемент проектирования
DevSecOps-чемпионы	ГОСТ требует наличия ответственных за ИБ в проектных ролях

INFERA AI.SafeCode. Преимущество использования

обеспечение безопасности на всех этапах разработки и эксплуатации ПО

ускорение выпуска ПО без жертв для ИБ

- продукт выходит быстрее и безопаснее
- ИИ встроенная в среду разработки позволяет делать проверки автоматически
- команда R&D не ждёт согласований от InfoSec

уменьшение затрат на устранение уязвимостей

- исправление бага на стадии продакшена может стоить в 10–30 раз дороже, чем на стадии разработки
- сокращение числа инцидентов безопасности до 40–50% при грамотной автоматизации тестов и проверки кода

устойчивость к supply chain атакам

- снижается киберриск атаки на цепочку поставок (проверка интеграций и подключений)
- безопасная интеграция с другими системами

соблюдение требований регуляторов

- ГОСТ Р 56939-2024, ФЗ-152, ФЗ-187 и др.

обнаружение уязвимостей в open-source

- безопасность должна быть встроена в процесс разработки и в проверку используемых компонентов

безопасное ПО для КИИ

- независимая проверка исходного кода open-source решений перед их использованием в отношении критически важного ПО

INFERA AI.SafeCode — это инвестиции в снижение рисков, ускорение релизов и цифровую устойчивость бизнеса

INFERA SECURITY

безопасность встроенная в ДНК

спасибо за внимание

www.InfEraSecurity.ru

тел.: +7 915 234 9900

почта: info@InfEraSecurity.ru