Уважаемые коллеги!

Приглашаем Вас принять участие в онлайн-мероприятии, посвящённом самой актуальной теме в области информационной безопасности – безопасное использование искусственного интеллекта и контроль работы ИИ-агентов.

В настоящее время компании массово переходят от простых чат-ботов к автономным ИИ-агентам. При этом агенты не просто отвечают, а выполняют реальные действия: работают с почтой, базами данных, API, кодом и даже запускают цепочки задач в мультиагентных системах. Вместе с возможностями пришли новые риски.

Переход к агентам кардинально меняет поверхность атаки. Если раньше угрозы ограничивались генерацией вредоносного текста или утечкой через промпт, то теперь агент может выполнить действия с реальными последствиями (отправить деньги, изменить данные в CRM, запустить код на сервере), получить отравленные данные через RAG или ответы инструментов (indirect prompt injection), отклониться от изначальной цели пользователя, «заразить» соседние агенты или создать каскадные отказы.

Согласно данным OWASP Top 10 for Agentic Applications за 2026 год, среди ключевых угроз для ИИ-агентов выделяются злоупотребление инструментами и компрометация привилегий, отравление памяти агента и отравление данных в RAG-системах, подмена идентичности агентов и отравление их межагентных коммуникаций, появление агентов-изгоев вместе с каскадными отказами в системе, а также нарушение исходного намерения пользователя и манипуляция целями агента.

Не упустите шанс узнать о самых передовых решениях в этой области и обсудить актуальные вызовы с ведущими ИБ-экспертами!

ПРОГРАММА ОНЛАЙН-МЕРОПРИЯТИЯ

INFERA AI.SafeAgent – аудит, мониторинг и контроль работы ИИ-агентов

- **Agent Runtime Security**
- **Контроль работы ИИ-агентов: кто отвечает, когда агент принимает решение, влияющее на технологические и бизнес-процессы компании**
- **INFERA AI.SafeAgent. Безопасное использование ИИ-агентов и что важно контролировать уже сейчас**
- **Кейсы и ответы на вопросы**

Ссылку на подключение пришлем за час до мероприятия