RansomLeak

Програма навчання з кібербезпеки

Усі вправи RansomLeak за категоріями та курсами, а також рекомендовані навчальні шляхи за ролями. Кожна вправа це інтерактивний модуль на 5-10 хвилин.

Оновлено листопад 2026 р. · ransomleak.com/uk/syllabus

Навчальні шляхи за ролями

Усі працівники

База, яку кожна людина в компанії має пройти першою: пошта, запит на вхід, завантаження файлу і кнопка «повідомити».

1. Фішинг
2. Цільовий фішинг
3. Квішинг (QR-фішинг)
4. Компрометація корпоративної електронної пошти (BEC)
5. Атака шквалом push-запитів
6. Звички з менеджером паролів
7. Безпечний перегляд і завантаження
8. Програми-вимагачі
9. Основи класифікації даних
10. Безпечне використання GenAI
11. Фішинг, написаний ШІ
12. Основи повідомлення про інциденти

Підкріплюють: Фішинг (email), Втома від MFA, Квішинг (QR-код), Підроблена сторінка входу, Шкідливе вкладення

Керівники

Керівників підробляють найчастіше. Цей шлях про дзвінки, винятки й погодження, на які зловмисники цілять саме їх.

1. Вейлінг із діпфейком
2. Імітація голосу керівника
3. Запити на винятки з вимог безпеки
4. Видавання себе за вас перед службою IT-підтримки
5. Ваш публічний цифровий слід
6. Злам делегованої поштової скриньки
7. Щоквартальна перевірка доступу
8. Погодження постачальника з урахуванням ризиків
9. Реагування керівника на фішинг у команді
10. Керівництво під час атаки програми-вимагача

Підкріплюють: Вішинг (дзвінок), Діпфейк, Соцмережі / OSINT, Чат (Teams / Slack)

Фінанси та бухгалтерія

Платіжне шахрайство рідко схоже на злам. Воно схоже на постачальника, який змінив реквізити, або директора, якому потрібен переказ сьогодні.

1. Шахрайство з рахунками та платежами
2. Компрометація корпоративної електронної пошти (BEC)
3. Процедури перевірки
4. Фішинг зі зворотним дзвінком
5. Двоетапний фішинг
6. Платіжне шахрайство з клонованим голосом
7. Виявлення діпфейк-аудіо
8. Supplier Bank Detail Fraud
9. Запити на винятки з вимог безпеки

Підкріплюють: Фішинг (email), Вішинг (дзвінок), Ланцюг атаки, Шкідливе вкладення, Діпфейк

HR і команди з персоналу

HR зберігає найбільше персональних даних і веде найризикованіші процеси: найм, звільнення та запити суб'єктів даних.

1. Діпфейк-шахрайство під час найму
2. Основи персональних даних
3. Збір даних працівників
4. Життєвий цикл доступу працівника
5. Обробка законних DSAR
6. Виявлення шахрайських DSAR
7. Запобігання крадіжці особистих даних
8. Надмірна відкритість у соцмережах
9. Fake Recruiter Approaches

Підкріплюють: Фішинг (email), Соцмережі / OSINT, Чат (Teams / Slack), Діпфейк

Рецепція та роздрібна торгівля

Дані пацієнтів і карток витікають біля стійки, а не в серверній. Побудовано навколо обов'язків HIPAA та PCI DSS для ролей, що працюють з клієнтами.

1. Workstation Screen Privacy
2. Incidental Verbal Disclosures
3. Identity Verification Before Disclosure
4. Card Terminal Tampering Checks
5. Unverified Terminal Servicing
6. Card Details Taken by Phone or Email
7. Card Numbers on Paper
8. Фальшивий технік
9. Незаблоковані робочі станції

Підкріплюють: Смішинг (SMS), Вішинг (дзвінок), Квішинг (QR-код)

Розробники

Експлуатуйте класичні вразливості вебу та API, а потім виправте їх. Завершується новими ризиками ШІ-асистентів для коду в репозиторії.

1. SQL-ін'єкція
2. Збережений XSS
3. Порушена авторизація на рівні об'єктів
4. Підробка запитів на боці сервера (SSRF)
5. Небезпечна десеріалізація
6. Секрети в історії Git
7. Шкідливі pull requests
8. Зловживання ланцюгом залежностей
9. Галюцинація ШІ в назві пакета
10. Неперевірене виправлення від ШІ
11. Отруєння файлу правил

Підкріплюють: Згода OAuth, Витік даних у ШІ-чаті, Підроблена сторінка входу, Чат (Teams / Slack)

Хмарні та платформні інженери

Акаунт, образ, кластер і пайплайн, кожен як межа безпеки, яку можна зламати, а потім закрити.

1. Надмірні дозволи IAM
2. Публічні бакети у сховищі
3. Довгоживучі ключі доступу
4. Зловживання метаданими інстансу
5. Секрети в шарах образу
6. Небезпечні конфігурації робочих навантажень у Kubernetes
7. Надмірно широкі дозволи в Kubernetes
8. Секрети в стані Terraform
9. Бар'єр політик як код
10. Небезпечна конфігурація системи в CI/CD

Підкріплюють: Згода OAuth, Втома від MFA, Підроблена сторінка входу

Команди, що створюють продукти зі ШІ

Для тих, хто випускає функції на LLM, агентів чи MCP-сервери. Спершу промпт-ін'єкція, далі автономність, інструменти й основи Закону ЄС про штучний інтелект.

1. Ін'єкція промптів в LLM
2. Розкриття чутливої інформації через LLM
3. Агент ШІ з надмірними дозволами
4. Перехоплення цілі агента
5. Зловживання інструментами агента та їх експлуатація
6. Отруєння інструментів MCP
7. Неналежне керування токенами й розкриття секретів у MCP
8. Класифікація ризиків ШІ
9. Упередженість і дискримінація в ШІ

Підкріплюють: Витік даних у ШІ-чаті, Згода OAuth, Діпфейк

Працівники чутливих технологій

Операційна безпека для тих, хто створює оборонні, подвійного призначення чи експортно контрольовані продукти. Що видає фото, виставка чи відвідувач.

1. Photo Location Leaks
2. Fitness App Location Leaks
3. Trade Show Elicitation
4. Production Floor Visitors
5. Giveaway USB Devices
6. Need to Know
7. Removable Media and Air Gaps
8. Data Spill Reporting

Підкріплюють: Соцмережі / OSINT, Смішинг (SMS), Чат (Teams / Slack)

Уся програма

Обізнаність з безпеки

Сформуйте культуру, де безпека на першому місці, за допомогою інтерактивних вправ із фішингу, соціальної інженерії, безпеки пристроїв та інших тем.

Фішинг та атаки з імітацією 17

Фішинг зі зворотним дзвінком
Розпізнайте фальшиве сповіщення про шахрайство, яке має змусити вас зателефонувати.

Фішинг
Розпізнайте фішинговий лист до того, як натиснете.

Вішинг
Витримайте реалістичний вішинговий дзвінок.

Смішинг
Виявіть шахрайство, приховане у ваших SMS.

Двоетапний фішинг
Розпізнайте пастку довіри з двох листів.

Компрометація корпоративної електронної пошти (BEC)
Зупиніть шахрайський переказ від імені гендиректора.

Соціальна інженерія
Розпізнайте маніпуляцію до того, як поступитеся.

Вейлінг із діпфейком
Розпізнайте згенерованого ШІ керівника на відеодзвінку.

Цільовий фішинг
Ваш публічний профіль — це їхній сценарій атаки.

Квішинг (QR-**фішинг**)
Цей QR-код обходить усі ваші поштові фільтри.

Соціальна інженерія у WhatsApp
Ваш «керівник» у WhatsApp — не ваш керівник.

Шахрайство від імені техпідтримки
Це попередження про вірус і є справжньою атакою.

Отруєння пошукової видачі
Перші результати пошуку не завжди надійні.

Шахрайство з рахунками та платежами
Виявіть підроблений рахунок постачальника через трибічне звірення, доки він не потрапив у платіжний файл.

Процедури перевірки
Зупиніть BEC зі зміною реквізитів постачальника: звіртеся з авторитетним довідником і передзвоніть незалежним каналом.

Виявлення діпфейк-аудіо
Розпізнайте клонований штучним інтелектом голос керівника в розмові, доки платіж не пішов.

Шахрайство із запрошеннями в календарі
Розпізнайте підроблене запрошення в календарі, доки фальшива сторінка зустрічі не зібрала ваші облікові дані.

Безпека пристроїв 10

Найкращі практики резервного копіювання
Складіть план резервного копіювання, який переживе програми-вимагачі.

Шифрування та дисципліна блокування
Відпрацюйте звички, що захищають пристрої, залишені без нагляду.

Оновлення ОС та основи патчів
Побачте, як пропущені оновлення відкривають реальні шляхи атаки.

Програми-вимагачі
Переживіть атаку програми-вимагача в реальному часі.

Атака через підкинутий USB
Подумайте двічі, перш ніж вставляти цю флешку.

Патчі кінцевих пристроїв і сповіщення EDR
Зрозумійте, що означає сповіщення EDR і що робити далі.

Обізнаність про розширення файлів
Виглядає як PDF. Запускається як шкідливе ПЗ.

Безпечне користування Bluetooth
Ваші навушники передають більше, ніж музику.

Безпека мобільних пристроїв
Одне підроблене SMS. Вісім годин викраденого доступу.

Дозволи мобільних застосунків
Назвіть функцію, яку вмикає кожен дозвіл, або відкличте його.

Паролі та безпека облікових записів 8

Безпека відновлення облікового запису
Захистіть відновлення облікових записів від соціальної інженерії.

Підстановка облікових даних (credential stuffing)
Побачте, як злиті паролі живлять автоматизовані атаки.

Життєвий цикл доступу працівника
Керуйте правами доступу під час зміни ролей.

Принцип найменших привілеїв
Тримайте доступ на мінімумі, якого вимагає ваша робота.

Налаштування MFA **та найкращі практики**
Налаштуйте багатофакторну автентифікацію правильно.

Атака шквалом push-запитів
Телефон вібрує тридцятий раз. А потім у Slack пишуть: підтвердіть.

Звички з менеджером паролів
Виробіть надійні звички роботи з менеджером паролів.

Основи привілейованого доступу
Дізнайтеся, чому адмінські облікові записи потребують особливого поводження.

Безпека в інтернеті та браузері 6

HTTPS і безпека вебсайтів
Дізнайтеся, чому замочок не доводить безпеку сайту.

Безпечний перегляд і завантаження
Помічайте шкідливі завантаження до їх запуску.

Тайпосквотинг
Викривайте доменні трюки, які використовують проти вас.

Ризики автозаповнення в браузері
Приховані поля непомітно крадуть ваші автозаповнені дані.

Безпека розширень браузера
Це корисне розширення може красти все підряд.

Зловживання сповіщеннями браузера
Та CAPTCHA була пасткою для push-спаму.

Повідомлення про інциденти 2

Основи повідомлення про інциденти
Знайте, коли і як повідомляти про інцидент безпеки.

Культура повідомлення
Створіть команду, яка повідомляє без страху.

Безпечне спілкування та обмін даними 7

Контроль спільного доступу в хмарі
Перевірте, хто бачить ваші спільні файли просто зараз.

Керування гостьовим доступом
Контролюйте, куди мають доступ зовнішні користувачі й на який термін.

Безпечне листування в месенджерах
Не дайте чутливим даним витекти через чати.

Політика щодо соцмереж
Дізнайтеся, чого не варто публікувати з корпоративних облікових записів.

Надмірна відкритість у соцмережах
Побачте, як зловмисники використовують ваші публічні профілі.

Ризики OAuth сторонніх застосунків
Перевірте, кому ви дали дозвіл на доступ.

Безпечні онлайн-зустрічі
Помітьте непроханого учасника, видаліть його, заблокуйте зустріч, подайте звіт.

Політики безпеки та ваша роль 5

Основи мислення аудитора
Мисліть як аудитор, щоб знаходити прогалини комплаєнсу.

Робота з порталом аудиту
Орієнтуйтеся в GRC-порталах і подавайте докази для аудиту.

Обов'язки працівника з безпеки
Знайте свої особисті обов'язки з безпеки на роботі.

Обізнаність про політики ISMS
Пов'яжіть політики ISO 27001 зі своєю щоденною роботою.

Правила користування інтернетом і поштою
Залишайтеся в межах корпоративних політик щодо інтернету й пошти.

Захист конфіденційної інформації 7

Основи класифікації даних
Маркуйте дані правильно за рівнем чутливості.

Запобігання крадіжці особистих даних
Помічайте прийоми крадіжки особистих даних, націлені на працівників.

Безпечний обмін файлами
Діліться файлами безпечно, не створюючи прогалин у захисті.

Витік даних
Не дайте чутливим даним залишити вашу організацію.

Чутливі дані в логах
У продакшн-логах є те, чого ви ніколи не надіслали б поштою.

Обізнаність про метадані
Чорний прямокутник поверх тексту не видаляє текст.

Безпечне використання GenAI
Використовуйте генеративний ШІ без витоку конфіденційних даних клієнтів.

Безпека на робочому місці 17

Внутрішня загроза (умисна)
Розпізнайте тривожні ознаки зловмисного інсайдера.

Тіньове IT
Дізнайтеся, що стається, коли команди користуються несхваленими застосунками.

Атаки через зображення (Stegosploit)
Цей файл зображення може нести більше, ніж пікселі.

Внутрішня загроза (випадкова)
Одне не те вкладення. Конфіденційні дані потрапили не в ту скриньку.

Гігієна інструментів співпраці
Одне спрощення в командному каналі — і облікові дані скрізь.

Безпечна утилізація документів
Дізнайтеся, куди насправді потрапляє викинута сторінка.

Основи чистого столу
Подивіться, що перехожий робить із записками на вашому столі.

Роздруківки без нагляду
Сторінка в лотку належить тому, хто дійде до неї першим.

Безпека адміністратора принтера
Офісний принтер досі відповідає на admin / admin.

Прогалини в реєстрації відвідувачів
Його ніхто не записав, але в нього зустріч о десятій.

Відвідувачі без супроводу
Бейдж пускає гостя всередину. Супровідник знає, де він зараз.

Проникнення через домофон
Кур'єр біля дверей — це ще не посвідчення.

Позичений бейдж
Позичте бейдж, і журнал дверей однаково запише вас.

Фальшивий технік
У нього ящик з інструментами, бейдж і дві хвилини. Перевірте все одно.

Підглядання через плече
Ваш екран видно з двох метрів за спиною.

Незаблоковані робочі станції
Активний екран — це відкритий сеанс із чиїмось ім'ям.

Badge Door Tailgating
Treat holding a badge door as an access decision.

Безпека віддаленої роботи та домашнього офісу 3

Користування VPN і безпека
Налаштуйте й використовуйте VPN, не залишаючи прогалин.

Безпека домашнього роутера
Дізнайтеся, хто ще сидить у вашій домашній мережі.

Безпека IoT і смарт-пристроїв
Ваша розумна камера набирає 28 балів зі 100.

Робота в громадських місцях 8

Фішинг через портал авторизації Wi-Fi
Більше часу в Wi-Fi за робочий пароль — не вигідна угода.

Небезпечна підробка мережі Wi-Fi
Назва мережі нічого не довела. Сумніваєтеся — підключайтеся через телефон.

VPN у публічному Wi-Fi
VPN, що відключився посеред завантаження, про це не повідомить. Аварійний вимикач повідомить.

Підмінені QR-коди
У QR-коду немає відправника, а замінити його можна наклейкою.

Джус-джекінг
Порт, що просить ваші файли, — не зарядний пристрій.

Підслуховування та крадіжка пристрою
Голос чути далі, ніж видно екран.

Boarding Pass Oversharing
See what a posted boarding pass hands a stranger.

Screen Privacy in Public
Keep your screen unreadable to the seat behind you.

Безпека для керівників і топменеджерів 10

Злам делегованої поштової скриньки
Пароль вашого асистента став ключем до вашої скриньки.

Щоквартальна перевірка доступу
«Схвалити все» — це підпис, а не спосіб спростити собі роботу.

Керівництво під час атаки програми-вимагача
Очолюйте, але не платіть.

Платіжне шахрайство на тлі угоди
Угода була в новинах. Саме тому шахрайство спрацювало.

Видавання себе за вас перед службою IT-підтримки
Службі IT-підтримки потрібне право відмовляти вам.

Запити на винятки з вимог безпеки
Дедлайн справжній. Прогалина, яку ви схвалюєте, теж.

Імітація голосу керівника
Звучить точнісінько як ваш генеральний директор. Це нічого не доводить.

Погодження постачальника з урахуванням ризиків
Ваш підпис вирішує, хто тримає дані ваших клієнтів.

Реагування керівника на фішинг у команді
Від вашої реакції залежить, коли повідомлять про наступний випадок.

Ваш публічний цифровий слід
Що незнайомець може дізнатися про вас за пів дня.

Privacy & Compliance Frameworks

Master GDPR compliance with hands-on exercises covering data protection, breach response, and privacy by design.

Основи ШІ для всіх 4

Що вважається ШІ
Автоматичне ще не означає ШІ. Вивчіть юридичний критерій.

Маркування ШІ-контенту та діпфейків
Якщо це можна прийняти за справжнє, потрібна позначка.

Використання ШІ в межах закону
Те, що ви вставляєте, публікуєте та вмикаєте, регулює закон.

Коли ШІ виходить боком
Штраф платить компанія. Але наслідки будуть і для вас.

Відповідність GDPR 18

Основи персональних даних
Розпізнавайте персональні дані, перш ніж із ними працювати.

Принципи та правові підстави
Оберіть правову підставу до початку роботи.

Повсякденні обов'язки щодо конфіденційності
Три рефлекси, які не дають малій проблемі вирости.

Збір даних працівників
Надішліть анкету працівникам двічі: спершу неправильно, потім законно.

Управління маркетинговою згодою
Будуйте законні opt-in-сценарії, які приймають регулятори.

Реагування на витік даних
Оцініть витік і встигніть повідомити за 72 години.

Перевірка конфіденційності за проєктуванням
Оцініть функцію продукту крізь призму конфіденційності.

Обробка законних DSAR
Опрацюйте запит суб'єкта даних на доступ від початку до кінця.

Редагування PII у документах
Вилучайте персональні дані з документів перед їх розкриттям.

Виявлення шахрайських DSAR
Виявляйте підроблені запити на доступ до даних, які використовують для соціальної інженерії.

Перевірка сторонніх обробників даних
Оцініть, як постачальник контролює обробку даних, до підписання договору.

Реагування на інциденти безпеки
Координуйте команди безпеки та конфіденційності під час активного витоку.

Транскордонна передача даних
Орієнтуйтеся в механізмах передачі даних за межі ЄЕЗ.

Оцінка впливу на захист даних
Проведіть DPIA для обробки даних із високим ризиком.

Картування даних та реєстр обробки
Побудуйте реєстр обробки за статтею 30 з нуля.

Управління згодою на файли cookie
Виправте банер cookie, до якого регулятор уже має претензії.

Дотримання строків зберігання даних
Вирішіть, що видалити, зберегти, заморозити або анонімізувати.

Штабна вправа з реагування на витік
Візьміть на себе роль відповідального за конфіденційність у штабі під час атаки програм-вимагачів.

Відповідність Закону ЄС про штучний інтелект 16

Основи грамотності з ШІ
Здобудьте грамотність з ШІ за статтею 4, перш ніж братися за корпоративні інструменти ШІ.

Класифікація ризиків ШІ
Розподіліть реальні впровадження ШІ за чотирма рівнями ризику Закону ЄС про штучний інтелект.

Заборонені практики ШІ
Зупиніть заборонені впровадження ШІ, доки вони не запрацювали.

ШІ високого ризику: обов'язки розгортача
Зупиніть запуск ШІ високого ризику, якщо є прогалини бодай в одній із семи областей вимог.

Постачальник чи розгортач: хто відповідає?
Відповідний вимогам продукт вендора не робить відповідним ваше впровадження.

Прозорість і розкриття щодо ШІ
Правильно маркуйте ШІ-чат-боти та синтетичні медіа за статтею 50.

Змістовний людський нагляд
Скасуйте кредитну рекомендацію ШІ, коли докази їй не відповідають.

Управління даними для ШІ
Зупиніть навчання моделі на наборі даних із витоками, упередженнями чи зайвими даними.

ШІ та захист даних
Проведіть медичну систему ШІ одразу через Закон ЄС про штучний інтелект і GDPR.

Упередженість і дискримінація в ШІ
Знайдіть проксі-змінні, приховані в моделі відбору резюме.

Оцінка впливу на основоположні права
Проведіть FRIA, перш ніж ШІ для соціального житла ухвалить перше рішення про допомогу.

Звітування про інциденти з ШІ
Повідомте про дискримінаційну модель відмов ШІ за статтею 73.

Управління ШІ у вашій організації
Побудуйте реєстр систем ШІ й покладіть край тіньовому ШІ в компанії.

Обов'язки для моделей ШІ загального призначення
Розберіть обов'язки постачальника GPAI та розгортача далі в ланцюгу для моделей системного ризику.

Відповідальне використання інструментів ШІ на роботі
Ухвалюйте рішення щодо ШІ за правилами протягом звичайного робочого дня.

Штрафи та правозастосування Закону ЄС про штучний інтелект
Співвіднесіть трирівневу шкалу штрафів із реальними випадками правозастосування.

OWASP Top 10 ризиків конфіденційності 10

Порушення конфіденційності через вразливості вебзастосунків
Дійсний вхід — це ще не ключ до записів усіх клієнтів.

Витік даних на боці оператора
Витік стався через вашу власну консоль підтримки.

Недостатнє реагування на витік даних
Без журналу читань правильних людей не повідомити.

Згода на все
Рекламний піксель спрацював, перш ніж хтось сказав «так».

Непрозорі політики
Повідомлення казало «ніколи». Карта даних показала «щоночі».

Insufficient Deletion of User Data
The delete button removed one copy out of six.

Недостатня якість даних
Те саме ім'я, інша людина, один обліковий запис.

Відсутнє або недостатнє завершення сесії
Вона натиснула «Вийти». Кіоск залишив її в системі.

Неможливість доступу до даних і їх зміни
Вона попросила всі свої дані. Отримала чотири поля.

Збір даних, не потрібних для мети, на яку погодився користувач
Реєстрація хотіла знати її дату народження, друзів і місцезнаходження.

Робота з контрольованою інформацією 8

CMMC Level 2 in Practice
Answer a CMMC assessor from what you actually do.

BYOD and Controlled Data
Keep controlled documents off a personal phone.

Need to Know
Share the pages someone needs, not the whole package.

Secure Printing and Disposal
Number, collect and shred every controlled copy.

Removable Media and Air Gaps
Cross an air gap the approved way, not with a personal USB stick.

Export-Controlled Data Sharing
Learn why showing a drawing can be an export.

Data Spill Reporting
Report a misdirected controlled file in the first minute.

Controlled Document Marking
Keep each customer's marking on what you write.

Відповідність HIPAA 6

Workstation Screen Privacy
Keep patient records off a screen the waiting room can read.

Incidental Verbal Disclosures
Confirm patient details without the queue hearing them.

Identity Verification Before Disclosure
Verify a caller before sharing anything about a patient.

Shared Workstation Logins
Never work in a session logged in as someone else.

Paper PHI Handling and Disposal
Keep printed patient records out of trays and bins.

Facility Access Control
Stop a stranger with a toolbox at the staff door.

PCI DSS для персоналу на касі 6

Card Terminal Tampering Checks
Check the card machine for tampering at the start of a shift.

Unverified Terminal Servicing
Verify a technician before they touch the card machine.

PIN Capture by Hidden Camera
Find the hidden camera watching customers type their PIN.

Card Numbers on Paper
Never write a customer's card number down.

Card Details Taken by Phone or Email
Keep card numbers out of the inbox and off the phone notes.

Rogue Devices on the Payment Network
Notice the extra device plugged into the payment network.

Безпека ШІ та LLM

Підготуйтеся до загроз на основі ШІ: промпт-ін'єкцій, діпфейк-атак і маніпуляцій LLM.

ШІ на роботі 15

Фішинг, написаний ШІ
Розпізнайте фішинговий лист з бездоганним правописом і назвою вашого проєкту.

Вішингові дзвінки від ШІ
Прийміть шахрайський дзвінок від ШІ, який відповідає на будь-яке запитання.

Платіжне шахрайство з клонованим голосом
Відреагуйте на запит про платіж, надісланий голосовим повідомленням вашого керівника.

Клонування вашого голосу
Розберіться з наслідками, коли клон вашого голосу телефонує колезі.

Діпфейк-шахрайство під час найму
Проведіть перевірку живості віддаленого кандидата під час співбесіди.

Шахрайський ШІ-чат підтримки
Розпізнайте підроблений ШІ-чат підтримки, який просить ваш код входу.

Несанкціоновані ШІ-нотатники
Знайдіть ШІ-нотатник на конфіденційній HR-зустрічі.

Промпт-ін'єкція в документах
Знайдіть прихований текст у PDF, що стоїть за ШІ-підсумком.

Неперевірена чернетка від ШІ
Приберіть внутрішні подробиці з відповіді клієнту, яку склав ШІ.

Інструменти тіньового ШІ
Сфотографуйте дорожню карту в безкоштовний ШІ-застосунок, а потім виправте ситуацію.

Шахрайський платіж агента ШІ
Подивіться, як вебсторінка перенаправляє платіж, який здійснює ваш агент ШІ.

Надмірний доступ ШІ-асистента
Перевірте джерело, коли асистент відповідає зарплатами колег.

Спільний агент — спільний доступ
Поділіться асистентом на своїх файлах і побачте, як він відповідає вашим доступом.

Витік даних через браузерного агента
Він діє від вашого імені на кожному сайті, куди ви ввійшли.

Агент натиснув «Дозволити»
Він схвалив екран дозволу, якого ви навіть не бачили.

OWASP Top 10 для LLM-застосунків 10

Ін'єкція промптів в LLM
Зупиніть прихований промпт, що перехоплює вашого ШІ-асистента посеред завдання.

Розкриття чутливої інформації через LLM
Подивіться, що стається, коли конфіденційні дані потрапляють у споживчий інструмент ШІ.

Ланцюг постачання ШІ
Розгорніть плагін ШІ, який ховає бекдор на видноті.

Отруєння даних і моделей ШІ
Подивіться, як отруєні документи в реальному часі псують відповіді вашого ШІ.

Небезпечна обробка виводу ШІ
Проексплуатуйте ШІ, чиї відповіді без перевірки йдуть у робочі системи.

Агент ШІ з надмірними дозволами
Змусьте ШІ-асистента зловжити власними дозволами.

Розкриття прихованого контексту
Витягніть приховані інструкції з клієнтського чат-бота на ШІ.

Вразливості векторів і ембедингів
Проексплуатуйте конвеєр RAG, щоб дістатися документів поза вашим рівнем доступу.

Хибна інформація від ШІ
Спіймайте вигадану статистику та фальшиві посилання у звіті від ШІ.

Атака на відмову в обслуговуванні ШІ
Запустіть атаку на спустошення гаманця проти незахищеного API ШІ.

OWASP Top 10 для агентних застосунків 10

Перехоплення цілі агента
Помітьте момент, коли мету агента ШІ тихо переписують.

Зловживання інструментами агента та їх експлуатація
Спіймайте шахрайські записи, які інструменти агента підкидають у вашу чергу.

Зловживання ідентичністю й привілеями агента
Знайдіть агента, який тихо розширює собі доступ.

Вразливості ланцюга постачання агентних систем
MCP-сервер із бекдором дублює кожен запит ваших агентів.

Неочікуване виконання коду ШІ-агентами
Прочитайте pull request від ШІ, перш ніж схвалити reverse shell.

Отруєння пам'яті й контексту агента
Один отруєний запис у пам'яті тижнями керує агентом.

Незахищена взаємодія між агентами
Підробіть одне повідомлення в шині агентів без автентифікації, і агент підкориться.

Каскадні збої в мультиагентних системах
Один хибний запис, п'ять агентів і поданий регулятору звіт.

Зловживання довірою людини до агента
Тижні бездоганних погоджень — це підготовка пастки, а не привід заспокоїтися.

Неконтрольовані ШІ-агенти
Нормальні метрики, чистий вивід і один агент, що діє на власний розсуд.

OWASP MCP Top 10 10

Отруєння інструментів MCP
Агенти читають описи інструментів як інструкції, а не як документацію.

Ін'єкція та виконання команд через MCP
Крапка з комою в аргументі інструмента стає командою оболонки.

Підрив потоку намірів у MCP
Текст, який агент прочитав, не є командою, яку він має виконувати.

Тіньові сервери MCP
Список серверів у вашому клієнті — не те саме, що насправді слухає мережу.

Втручання в ланцюг постачання й залежності MCP
Встановлення сервера MCP запускає його код ще до того, як ви його прочитаєте.

Відсутність аудиту й телеметрії MCP
Журналювання, увімкнене сьогодні, не поверне вчорашній день.

Недостатня автентифікація й авторизація в MCP
Схвалити сервер — не те саме, що автентифікувати його.

Підвищення привілеїв у MCP через розширення дозволів
Агент дотягується так далеко, як дозволяє його токен, а не завдання.

Неналежне керування токенами й розкриття секретів у MCP
Токен у вашій конфігурації MCP — це токен, який читає ваш асистент.

Ін'єкція контексту й надмірне розкриття даних у MCP
Коли один агент обслуговує багатьох клієнтів, його контекст — це дані.

Безпечна розробка з ШІ-помічниками 12

Галюцинація ШІ в назві пакета
Помічник назвав пакет. Ніхто не перевірив, що він справжній.

Неперевірене виправлення від ШІ
Помічник сказав, що все безпечно. Це було не так.

Витік секрету через контекст ШІ
Помічник прочитав файл, якого ви йому не давали.

Отруєння файлу правил
Правило скидалося на примітку. Помічник його виконав.

Промпт-ін'єкція через задачі
Звіт про помилку міг подати будь-хто. Бот його злив.

Порожні тести від ШІ
Дванадцять зелених тестів. Жоден не перевіряв випадок, через який стався витік.

Хмарні облікові дані, доступні автоматично
Помічник виконав видалення з ключем продакшну, що стояв на вашому ноутбуці.

Застосунок від ШІ без рев'ю
Його за вихідні написав помічник. Ніхто не переглянув.

Небезпечний згенерований IaC
Plan пройшов без помилок. У продакшн вийшов публічний бакет.

Ліцензійне зараження коду від ШІ
Написав помічник. Належить комусь іншому.

Необмежений доступ помічника до файлів
Ваш проєкт закінчується на корені робочої області. Доступ помічника — ні.

Вимкнені запобіжники ШІ
Три запобіжники вимкнено. Решту зробила одна залежність.

Реальні інциденти

Учіться на справжніх інцидентах безпеки. Пройдіть крок за кроком атаку на MGM Resorts, випадки BEC-шахрайства та інші.

Розбори інцидентів 4

Поштова атака через OneNote
Простежте реальну BEC-схему, побудовану на тижнях стеження за поштовою скринькою.

HTTP2Shell RCE
Один стиснутий запит. Жодного входу. Оболонка на вашому сервері.

PHP2Shell RCE
Один запит, жодного входу — і командна оболонка на вашому сервері.

Злам MGM Resorts
Переживіть 10-хвилинний дзвінок у службу підтримки, що коштував $100 млн.

OPSEC

Операційна безпека для працівників, які створюють чутливі технології. Помічайте, що видають фото, застосунки, виставки, відвідувачі та дружні запитання, закривайте кожну прогалину й повідомляйте про неї.

Основи OPSEC 5

Linked Device Takeover
See what one tap on Link hands a stranger.

Fitness App Location Leaks
Stop a fitness app from mapping where you live and work.

Group Chat Membership
Check who is really in the work group chat.

Photo Location Leaks
Check what a photo gives away before you post it.

Fake Recruiter Approaches
Spot a friendly approach that is really elicitation.

OPSEC для промисловості 10

Demo Unit Tampering
Check a demo unit after strangers have been near it.

Exhibitor Badge Sharing
Keep your exhibitor badge on you, even for ten minutes.

Family and Home Oversharing
Find what family posts reveal about your work.

Giveaway USB Devices
Leave the free USB stick from the show unplugged.

Overnight Stand Security
Close a trade-show stand so nothing walks overnight.

Prototype Photos and Video
See what a short test-range clip tells strangers.

Supplier Bank Detail Fraud
Verify a supplier's new bank account before paying.

Trade Show Elicitation
Answer friendly questions at the stand without oversharing.

Unattended Demo Laptop
Lock the demo laptop every time you step away.

Production Floor Visitors
Challenge a visitor nobody is escorting.

Безпека застосунків

Проексплуатуйте вразливості з OWASP Top 10 для вебу, API та мобільних застосунків, а потім випустіть виправлення. Практика безпечного кодування для розробників.

OWASP Top 10 для вебзастосунків 26

Клікджекінг
Викрадіть клік на кнопці підтвердження в банку.

Ін'єкція команд
Допишіть другу команду до серверної утиліти.

Компоненти з відомими вразливостями
Отримайте виконання коду через застарілу бібліотеку.

Підробка міжсайтового запиту (CSRF)
Переказуйте гроші зі сторінки, якій жертва ніколи не довіряла.

Обхід каталогів
Прочитайте системні файли через посилання на завантаження.

DOM XSS
Запустіть XSS, якого сервер ніколи не побачить.

Примусовий перегляд
Витягніть експорт персональних даних із маршруту, на який немає посилань.

Горизонтальне підвищення привілеїв
Змініть одну цифру й прочитайте дані іншого клієнта.

Ін'єкція заголовка Host
Переспрямуйте лист про скидання пароля на схожий домен.

Небезпечне перенаправлення URL
Сховайте фішингову сторінку за справжнім входом.

Залишений код налагодження
Витягніть продакшн-секрети із забутого маршруту налагодження.

Персональні дані в URL
Дістаньте персональні дані просто з посилання.

Відображений XSS
Складіть шкідливе посилання, яке спрацьовує щойно його відкрили.

Підробка запитів на боці сервера (SSRF)
Змусьте сервер витягнути власні хмарні облікові дані.

Фіксація сесії
Підкиньте ідентифікатор сесії й успадкуйте вхід жертви.

SQL-ін'єкція
Викачайте базу даних через одну незахищену форму пошуку.

Збережений XSS
Підкиньте скрипт у коментар і подивіться, як він спрацює.

Розкриття токена в URL
Повторно застосуйте сесійний токен, зібраний із логу реферерів.

Перебір користувачів
Зберіть перевірений список клієнтів із форми входу.

Вертикальне підвищення привілеїв
Підробіть роль у токені й станьте адміністратором.

Слабка випадковість
Передбачте токен скидання пароля й заберіть акаунт.

XXE-ін'єкція
Прочитайте файл паролів через завантажений XML.

Слабке хешування паролів
Викрадена таблиця хешів безпечна, лише якщо безпечне саме хешування.

Обхід кроків оформлення замовлення
Пропустіть оплату — і замовлення все одно піде на склад.

Небезпечна десеріалізація
Завантажена копія, що запускає код зловмисника.

Відмова із відкриттям доступу в перевірці повернень
Змусьте перевірку дати збій — і повернення буде виплачене.

OWASP Top 10 для безпеки API 10

Порушена авторизація на рівні функцій
Викличте ендпоінти для персоналу з акаунта лише для читання.

Порушена авторизація на рівні об'єктів
Підмініть ідентифікатор і прочитайте дані іншого пасажира.

Порушена автентифікація в API
Підберіть шестизначний код входу.

Надмірне розкриття даних
Прочитайте поля, яких інтерфейс ніколи не показує.

Неналежне управління інвентарем
Прочитайте записи через виведену з експлуатації версію API.

Ін'єкція
Перетворіть поле пошуку на читання всієї бази даних.

Недостатнє логування й моніторинг
Подивіться дані клієнта й не залиште жодного сліду.

Масове присвоєння
Намалюйте собі бонусний баланс двома зайвими ключами.

Неправильна конфігурація безпеки
Прочитайте дані авторизованого акаунта з будь-якого сайту.

Необмежене споживання ресурсів
Викачайте каталог одним завеликим запитом.

OWASP Mobile Top 10 13

Неправильне використання облікових даних у мобільних застосунках
У кожній копії застосунку був ключ SMS-шлюзу компанії.

Недостатня безпека ланцюга постачання в мобільних застосунках
Оновлення SDK, яке команда не обирала, потрапило до її застосунку.

Непідписані оновлення по повітрю
Оновлення, яке ніхто не підписав, потрапило до кожного користувача під час запуску.

Біометричне розблокування без криптографії
Перевірка відбитка пальця сказала «так», хоча до сенсора ніхто не торкався.

Незахищена автентифікація та авторизація в мобільних застосунках
Застосунок сказав, що він працівник, і API повірив.

Недостатня перевірка вхідних і вихідних даних у мобільних застосунках
Посилання вирішило, кому підуть гроші, а користувач цього навіть не побачив.

Відкритий доступ до моста WebView
Віджет у статті довідки міг прочитати сесію користувача.

Незахищений обмін даними в мобільних застосунках
Застосунок довіряв будь-якому сертифікату, тож будь-хто в тій самій мережі Wi-Fi міг прочитати його трафік.

Недостатні заходи захисту приватності в мобільних застосунках
Дані користувачів про здоров'я лежали на панелі збоїв.

Недостатні заходи захисту бінарного коду в мобільних застосунках
Хтось перезібрав застосунок і видав собі безкоштовні нагороди.

Неправильна конфігурація безпеки в мобільних застосунках
Випускова збірка досі постачалася з меню налагодження.

Незахищене зберігання даних у мобільних застосунках
Вживаний планшет досі зберігав робочу сесію.

Недостатня криптографія в мобільних застосунках
Резервні копії зашифрували ключем, спільним для кожної копії застосунку.

Безпека Git і CI/CD

Розглядайте репозиторій і конвеєр як межі безпеки. Витягніть секрети з історії комітів, отруїть збірку, зловживіть раннером, а потім захистіть гілку за замовчуванням і шлях розгортання.

Безпека Git і репозиторіїв 8

Секрети в історії Git
Відновіть чинний ключ API з того коміту, що його видалив.

Відкритий каталог .git
Відновіть увесь код проєкту з однієї публічної URL-адреси.

Закомічені файли з секретами
Клонуйте публічний репозиторій і прочитайте закомічений .env.

Підміна автора коміту
Протягніть бекдор під іменем мейнтейнера.

Обхід захисту гілки
Перезапишіть main через force-push, оминувши код-рев'ю і CI.

Витік токенів доступу
Клонуйте приватні репозиторії токеном із публічного gist.

Шкідливі pull requests
Помітьте бекдор, схований у безневинному виправленні тесту.

Розкриття секретів у CI/CD
Дістаньте ключ розгортання просто з публічного логу збірки.

OWASP Top 10: ризики безпеки CI/CD 10

Недостатні механізми контролю потоку в CI/CD
Захист гілки нічого не дає, якщо розгортання оминає конвеєр.

Недостатнє керування ідентичністю та доступом у CI/CD
Вихід підрядника оформили, а токен CI лишився чинним.

Зловживання ланцюгом залежностей
Назва була цілком правильна. А реєстр, з якого прийшов пакет, — ні.

Отруєне виконання конвеєра
Workflow був правильний. Код зловмисника запустила конфігурація лінтера.

Недостатні механізми контролю доступу на рівні конвеєра
Секрет репозиторію є в кожному завданні, зокрема й у пул-реквесті сторонньої людини.

Недостатня гігієна облікових даних у CI/CD
Один ключ усюди, і ніхто не може сказати, що зламає його ротація.

Небезпечна конфігурація системи в CI/CD
Друге завдання успадковує все, що перше залишило на диску ранера.

Неконтрольоване використання сторонніх служб
Пробний період дворічної давності досі читає кожен приватний репозиторій.

Неналежна перевірка цілісності артефактів
Розгорнуто не той артефакт, який було зібрано.

Недостатнє журналювання та видимість у CI/CD
Конвеєр — це місце, де код стає продакшном, а журналів він майже не вів.

Безпека хмари

Розглядайте акаунт, образ і кластер як межі безпеки. Прочитайте бакет, який ніхто не збирався публікувати, втечіть із привілейованого пода, захопіть кластер через RBAC, а потім перевіряйте Terraform політиками як кодом.

Безпека хмарної інфраструктури 9

Публічні бакети у сховищі
Перелічіть вміст бакета без облікових даних і заберіть клієнтський експорт.

Надмірні дозволи IAM
Перетворіть непримітні облікові дані збірки на повноцінного адміністратора.

Довгоживучі ключі доступу
Скористайтеся ключем, який витік місяці тому й досі проходить автентифікацію.

Зловживання метаданими інстансу
Перетворіть функцію завантаження за URL на крадіжку хмарних облікових даних.

Відкрита хмарна мережа
Підключіться напряму до продакшн-бази даних, оминаючи застосунок.

Захоплення субдомену
Роздавайте власну сторінку входу з домену, який справді належить компанії.

Прогалини в журналах аудиту
Розслідуйте інцидент, де журнал охоплював один регіон, а решту зловмисник видалив.

Надмірні привілеї в serverless
Перетворіть публічний URL функції на роль з доступом до всього акаунта.

Межі між акаунтами
Проведіть облікові дані з пісочниці в продакшн, а потім поставте стелю над акаунтом.

Безпека контейнерів та образів 8

Секрети в шарах образу
Прочитайте живий токен із шару, який збірка намагалася підчистити.

Привілейовані контейнери
Перетворіть shell у контейнері на root на хості.

Відкритий Docker-демон
Захопіть продакшн-хост через Docker API без автентифікації.

Вразливі базові образи
Проексплуатуйте CVE у шарі ОС, який ніхто не перевіряє.

Шкідливі базові образи
Простежте криптомайнер до одного рядка в Dockerfile.

Відкритий реєстр контейнерів
Завантажте приватний образ, а потім підмініть тег, який вони розгортають.

Відкрита мережа контейнерів
Один мапінг портів виставляє продакшн-базу даних в інтернет.

Мінімальні образи контейнерів
Урізьте 412-мегабайтний runtime до того, без чого справді не обійтися.

OWASP Kubernetes Top Ten 13

Небезпечні конфігурації робочих навантажень у Kubernetes
Один привілейований под — і весь вузол відкритий.

Надмірно широкі дозволи в Kubernetes
Одна тимчасова прив'язка до cluster-admin — і підрядник читає зарплати.

Помилки керування секретами в Kubernetes
Секрет був надійно захищений. Його значення лежало в журналі збою.

Брак примусового застосування політик на рівні кластера
Перемістіть тег — і продакшн сам його завантажить.

Відсутня сегментація мережі в Kubernetes
Достатньо одного вебпода, щоб дістатися до кожного внутрішнього сервісу.

Надмірно відкриті компоненти в Kubernetes
Облікові дані не потрібні: кластер відповідає всім.

Хибно налаштовані й вразливі компоненти кластера
Сервер API був під замком. А kubelet — ні.

Горизонтальне переміщення з кластера в хмару
Под бере хмарну ідентичність вузла й виходить за межі кластера.

Порушена автентифікація в Kubernetes
Под, що ніколи не звертається до API, усе одно несе ключ до нього.

Застарілі та вразливі надбудови кластера
Контролер входу, який ніхто не оновлював, читає всі секрети.

Недостатнє логування та моніторинг у Kubernetes
Майнер працював тижнями, бо за кластером ніхто не стежив.

Непідписані образи контейнерів
Усі бар'єри пройдено. Жоден не перевірив базовий образ.

Відкриті резервні копії etcd
Один знімок — і секрети всього кластера можна прочитати.

Безпека інфраструктури як коду 7

Бар'єр політик як код
Або бар'єр, який ніхто не обійде, або лише порада.

Радіус ураження в Terraform
Перейменування дає в plan один рядок про знищення, і apply його виконує.

Дрейф у Terraform
Закрийте порт у консолі — і наступний запуск apply відкриє його знову.

Витоки через Terraform plan
Plan вивів пароль до бази даних у публічному коментарі.

Секрети в стані Terraform

Пароля немає в жодному файлі .tf. Але у файлі стану він є.

Недовірені модулі Terraform

Модуль, прив'язаний до гілки, може змінитися за вашої спини.

Недовірений Terraform plan

Plan запускає код, а CI запускає plan з повними обліковими даними.

Підкріплено мікронавчанням

Між модулями короткі мікровправи тримають ті самі навички в тонусі. Кожна це атака на 2-4 хвилини в реальному форматі, яка надходить за розкладом або одразу після кліку на симуляцію.

Фішинг (email) 2 хв
Помітьте ознаки листа для крадіжки облікових даних, перш ніж клікнути.

Смішинг (SMS) 2 хв
Знайдіть SMS від «кур'єра» серед звичайних повідомлень у телефоні.

Вішинг (**дзвінок**) 3 хв
Вислухайте того, хто просить ваш код MFA, і вирішіть, коли покласти слухавку.

Чат (Teams / Slack) 3 хв
Прочитайте повідомлення від стороннього акаунта, що видає себе за внутрішню підтримку.

Втома від MFA 2 хв
Підтвердьте або відхиліть потік MFA-запитів, яких ви не надсилали.

Квішинг (QR-**код**) 2 хв
Вирішіть, чи сканувати QR-код «оплатити тут», наклеєний на паркомат.

Підроблена сторінка входу 2 хв
Роздивіться точну копію сторінки входу Microsoft, перш ніж щось вводити.

Витік даних у ШІ-чаті 3 хв
Скористайтеся публічним ШІ-асистентом, не вставляючи дані, яких він не повинен бачити.

Ланцюг атаки 4 хв
Простежте одну BEC-аферу, що переходить з листа в SMS, а далі в дзвінок.

Згода OAuth 2 хв
Прочитайте екран згоди, перш ніж дати застосунку повний доступ до пошти.

Шкідливе вкладення 2 хв
Перевірте вкладення з простроченим рахунком, перш ніж його відкрити.

Соцмережі / OSINT 3 хв
Знайдіть, що радісний пост про перший робочий день дарує зловмиснику.

Діпфейк 3 хв
Відрізніть справжній запис керівника від згенерованого ШІ. Незабаром.

І двохвилинний урок у Slack або Teams щоробочого дня

Мікровправи вчать помічати атаку. Чат-уроки підтримують цю звичку. Короткі уроки й 30-секундні перевірки приходять у месенджер, який команда вже тримає відкритим, і там же завершуються: без входу в систему й без відкриття курсу.

За вашим розкладом. Щоробочого дня, двічі на тиждень чи щомісяця, у часовому поясі кожної людини, з денними й тижневими лімітами.

Саме вчасно. Клікнули на фішингову симуляцію? За кілька хвилин приходить 60-секундний урок саме про цю приманку.

Повідомити службу безпеки. Один клік на будь-якому підозрілому повідомленні, і воно вже в команди безпеки.

Враховується як будь-яка вправа. Проходження видно у звітах та експортах, і воно впливає на Human Risk Score.