ІНТЕРАКТИВНЕ НАВЧАННЯ З КІБЕРБЕЗПЕКИ

Навчання з кіберобізнаності, яке запам'ятовується

RansomLeak — це інтерактивна 3D-платформа навчання з кібербезпеки, де співробітники навчаються на практиці, а не переглядаючи відео. Захопливі симуляції тривалістю від 5 до 10 хвилин охоплюють фішинг, програми-вимагачі, соціальну інженерію, загрози ШІ та відповідність нормативним вимогам, формуючи стійку зміну поведінки в усій вашій організації.

100+	4	3D	100%
Інтерактивних вправ	Навчальні категорії	Захопливі симуляції	Сумісність зі SCORM

Навчальні категорії

Кіберобізнаність

Різновиди фішингу (цільовий, вішинг, смішинг, BEC, QR-коди, зворотний дзвінок), аудіо-діпфейки, втома від MFA, менеджери паролів, підкинуті USB-носії, програми-вимагачі, безпека браузера, ризики OAuth, тіньове IT та внутрішні загрози.

Приватність і відповідність вимогам

GDPR (обробка DSAR, реагування на витоки, DPIA, ROPA, транскордонна передача даних, згода на маркетинг), CCPA/CPRA, HIPAA та Закон ЄС про ШІ (прозорість, врядування, класифікація ризиків, FRIA).

Безпека ШІ та LLM

Пряме й непряме впровадження запитів (prompt injection), атаки з діпфейками, розкриття конфіденційних даних, ризики ланцюга постачання моделей, надмірна автономність та OWASP Top 10 для LLM і агентних застосунків.

Реальні інциденти

Розбір справжніх зламів: атака програм-вимагачів на MGM Resorts, зброєзовані вкладення OneNote та нові інциденти, що додаються щомісяця.

НЕЗАБАРОМ

Безпека застосунків

OWASP Top 10, безпечне програмування, гігієна залежностей.

Безпека API

OWASP API Top 10, BOLA, обмеження частоти запитів.

Хмарна безпека

IAM, відкриті S3, Kubernetes, керування секретами.

Мікротренування

Короткі повторювані вправи, які співробітники проходять наживо, прямо в браузері. Кожне тренування відпрацьовує один шаблон атаки за дві-три хвилини, а потім відстежує, кому потрібне ще одне повторення.

Тренування з фішингу

Розпізнавайте ознаки соціальної інженерії в атаках через пошту: скидання облікових даних, шахрайство з рахунками через схожі домени та шкідливі вкладення.

Тренування з діпфейків

Відрізняйте справжній запис керівника від синтетичного й виробляйте звичку перевіряти через незалежний канал, перш ніж діяти.

Тренування в месенджерах

Виявляйте видавання себе за іншу особу та шахрайство з подарунковими картками в месенджерах на кшталт WhatsApp, Slack і Teams, де запити здаються неформальними та терміновими.

Тренування з MFA

Протистійте бомбардуванню push-запитами через втому від MFA: відхиліть запит, який ви не ініціювали, змініть пароль і повідомте про інцидент.

Незабаром більше форматів мікронавчання

Нові формати тренувань виходять щомісяця й налаштовані на шаблони атак, що з'являються на поверхнях загроз клієнтів.

Створюйте власні тренування у своєму середовищі. Кожен клієнт отримує необмежену кількість тренувань, налаштованих під власну поверхню загроз.

Симуляції

Доступні як додаткові модулі

ДОДАТКОВО

Симуляції фішингу

Реалістичні поштові атаки, що доставляються через пряму інтеграцію M365 Graph і Google Workspace, повз спам-фільтр, із кнопками звітування та автоматизованим усуненням наслідків.

- Наскрізна аналітика за 8 етапами
- Відстеження повторних порушників
- Контроль за статтею 88 GDPR і вимогами виробничих рад

ДОДАТКОВО

Симуляції смішингу

Перевірте, як співробітники реагують на SMS-фішинг — канал, перед яким немає поштового шлюзу. Реальна доставка SMS на тій самій платформі, що й ваша поштова програма.

- Доставка в робочі години кожного часового поясу
- Відстеження натискань і REPORT для кожного отримувача
- Відмова через STOP і REPORT, автоматичне усунення наслідків

НЕЗАБАРОМ

Симуляції вішингу

Симуляції голосових дзвінків, що перевіряють, чи звіряють співробітники особу перед тим, як діяти за терміновим телефонним запитом. У стадії активної розробки; приєднається до пошти й SMS, коли канал запуститься.

- Сценарії з підробкою ідентифікатора абонента
- Перевірка зворотним дзвінком через незалежний канал
- Єдине звітування з поштою та SMS

Управління людськими ризиками

Оцінка людського ризику

Надайте кожному співробітнику оцінку від 0 до 100, що показує ймовірність піддатися атаці соціальної інженерії. Вона побудована на реальній поведінці в симуляціях, навчанні та усуненні наслідків, а не на опитувальнику, і пояснюється аж до подій, що стоять за нею.

- Рівні від низького до критичного, кожен із рейтингом достовірності
- 90-денний період напіврозпаду, тож недавня поведінка важить найбільше
- Захист від нестачі даних, тож тихий новачок ніколи не вважається безпечним

Автоматизація на основі ризику

Перетворюйте оцінки на дії. Автоматично записуйте співробітників із високим ризиком на усунення прогалин, сповіщайте їхніх керівників і реагуйте на провалену симуляцію в мить, коли вона стається. Кожне правило спершу виконується в режимі пробного запуску й фіксує кожну свою дію.

- Попередній перегляд у режимі пробного запуску на вашій реальній команді
- Обмеження радіуса впливу, індивідуальний період очікування, перевірка відновлення
- Повний журнал аудиту, який аудитор може підтвердити

Можливості платформи

Інтерактивні 3D-симуляції

Співробітники практикуються всередині реалістичних сценаріїв, а не дивляться пасивні відео. Навчання на практиці формує стійку м'язову пам'ять.

SCORM 1.2 і 2004

Експортуйте вправи як пакети SCORM для будь-якої LMS. Відстежуйте завершення, бали та витрачений час напряму.

Аналітика в реальному часі

Відстежуйте прогрес співробітників, виявляйте прогалини в знаннях і формуйте звіти про відповідність для аудиторів.

Управління кампаніями

Створюйте власні навчальні шляхи, плануйте кампанії та призначайте вправи командам або відділам.

SSO, MFA і SCIM

Входьте через SAML 2.0 або OIDC з будь-яким постачальником ідентифікації, забезпечуйте багатофакторну автентифікацію та автоматично надавайте доступ користувачам із вашої HRIS через SCIM 2.0.

Гейміфікація

Бали, значки та таблиці лідерів стимулюють залученість. Співробітники змагаються й навчаються водночас.

Інтеграції

Підключіть навчання до вашого стека

Вбудуйте навчання й дані про людський ризик в інструменти, якими ваша команда безпеки вже користується. Призначайте навчання із заявки, інциденту чи виявлення, стежте за людським ризиком на дашбордах і доводьте відповідність автоматично.

Сервісдеск

Автоматично призначайте навчання із заявки про безпеку й записуйте завершення назад. Застосунки для Jira Service Management, Freshservice та ManageEngine ServiceDesk Plus.

SOAR та інциденти

Призначайте відповідний урок просто з плейбука чи інциденту. PagerDuty, Cortex XSOAR і Tines — усе через один API призначень.

Спостережуваність

Будуйте оцінку людського ризику, завершення й результати фішингу на ваших дашбордах. Джерело даних Grafana, quickstart для New Relic і Datadog.

Докази відповідності

Завершення автоматично надходять як докази контролю. Живі синхронізації Vanta й Drata для SOC 2, ISO 27001, HIPAA, PCI DSS, GDPR і NIS2.

Чат і сповіщення

Сповіщення про завершення, нагадування про прострочення та персональні нагадування. Застосунок Slack і вебхуки каналів, а застосунок Microsoft Teams уже в дорозі.

SIEM та експорт даних

Витягуйте події як JSON чи CSV або передавайте їх через підписані вебхуки, тож ваш SIEM приймає дані про обізнаність поряд з усім іншим.

Побудовано на платформі для розробників. REST API з токен-автентифікацією та довідником OpenAPI, одинадцять підписаних подій вебхуків (HMAC-SHA256, із журналами доставок і автоматичними повторами) та токени з обмеженим доступом для кожного тенанта лежать в основі кожної інтеграції вище.

Підключені платформи

- Jira Service Management
- Freshservice
- ServiceDesk Plus
- PagerDuty
- Cortex XSOAR
- Tines
- Grafana
- New Relic
- Datadog
- Vanta
- Drata
- Slack
- Microsoft Teams
- Okta
- Microsoft Entra ID

Технічні характеристики

РОЗГОРТАННЯ

- Хмарна SaaS-платформа
- Експорт SCORM 1.2 / 2004
- Багатоорендна архітектура
- SSO (SAML 2.0, OIDC)
- Надання користувачів через SCIM 2.0
- REST API та webhooks
- Сервісдеск, SOAR та SIEM конектори

ІНТЕГРАЦІЯ З LMS

- Будь-яка LMS із підтримкою SCORM
- Cornerstone OnDemand
- SAP SuccessFactors
- Workday Learning
- Moodle, Canvas, Docebo

КОНТЕНТ

- 100+ інтерактивних вправ
- Модулі по 5–10 хвилин
- Щомісячні випуски нового контенту
- Англійська, українська, нідерландська, італійська, німецька (інші — за запитом)
- Брендування під білою етикеткою та власний контент

Сценарії використання

Навчання з кіберобізнаності | Навчання з відповідності (GDPR, HIPAA) | Стійкість до фішингу | Адаптація нових співробітників | Тренування з реагування на інциденти | Навчання щодо ризиків ШІ

Звітність про відповідність

- SOC 2
- ISO 27001
- GDPR
- NIS2
- HIPAA
- PCI DSS
- DORA

Готові побачити це в дії?

Замовте демо або спробуйте бібліотеку вправ безкоштовно на ransomleak.com.

Замовити демо

info@ransomleak.com

ВЕБСАЙТ
ransomleak.com

EMAIL
info@ransomleak.com

LINKEDIN
ransomleak