SZCZEGÓŁY OFERTY

Najnowsze trendy w Przeciwdziałaniu praniu pieniędzy AI, DeFi, ESG, mikropłatności i globalne zagrożenia 2024–2025

Szkolenie prezentuje najnowsze typologie prania pieniędzy i finansowania terroryzmu odkryte przez FATF, Europol SOCTA, IMF i UNODC w latach 2024–2025.

Szczegółowo omawia nowe techniki prania używane w projektach ESG („AML greenwashing"), mikropłatnościach w gamingu i streaming, AI-wspierane fałszywe faktury, DeFi i stablecoiny oraz pranie przez nieruchomości i aktywa luksusowe. Uczestnicy dowiedzą się, jak instytucje compliance i FIU powinny odpowiednio zareagować — przejść od reaktywnego działania do inteligentnego zarządzania ryzykiem opartych na technologii i threat intelligence.

Adresaci

- compliance officers, analitycy AML w bankach, fintechach i VASP
- pracownicy FIU, nadzorcy i regulatorzy
- specjaliści bezpieczeństwa finansowego i cyberbezpieczeństwa
- zespoły prawne i audytowe działające w sektorze AML/CFT

Program szkolenia

Moduł 1: Najnowsze typologie AML 2024–2025 – ewolucja zagrożeń

1. **Zmienność metod – badania FATF**
   FATF wskazuje na coraz częstsze wykorzystanie projektów ESG do ukrywania przepływów ilicitnych; użycie sztucznej inteligencji do automatycznego tworzenia fałszywych dokumentów handlowych; a także rosnącą skalę prania przez crowdfunding i tokenizację aktywów.
2. **Nowa rzeczywistość finansowych przestępstw (Analiza SOCTA 2025 Europol)**
   Europol opisuje zorganizowane przestępstwa jako globalnie zintegrowane, napędzane przez AI-driven operacje, skalowalne transakcje DeFi i cyfrowe platformy, gdzie każdy etap — od rekrutacji po finansowanie — jest zautomatyzowany i trudny do wykrycia.
3. **Ryzyka regionalne: nieruchomości, hazard, luksusowe aktywa (IMF, UNODC)**
   Globalny wzrost prania przez rynku nieruchomości, kasyna online i tokenizację dzieł sztuki, jachtów czy nieruchomości komercyjnych – wykorzystywanie wartości realnych i wysokiej płynności do reintegracji środków.
4. **Kluczowe geografie ryzyka**
   Zwiększony przepływ transakcji z jurysdykcji o niskim nadzorze (np. niektóre kraje Afryki i Azji Południowej), pojawienie się shadow-fintechów i nielegalnych procesorów płatniczych operujących poza systemem licencyjnym.
5. **Technologia jako katalizator przestępstw**

Organizacje przestępcze korzystają z AI do tworzenia multijęzycznych oszustw, deepfake'ów i zarządzania operacjami w skali globalnej, czyniąc tradycyjne procedury analiz podejrzanych transakcji niewystarczającymi.
6. **Nowa lista wysokiego ryzyka (FATF Grey/Black list)**
   Wyznaczenie kolejnych państw (np. Liban, Wenezuela) jako jurysdykcji wysokiego ryzyka zmusza instytucje do stosowania EDD i pogłębionej analizy podmiotów z tych obszarów.

Moduł 2: Nowe schematy prania pieniędzy – metody 2024–2025

1. **AML greenwashing**
   Pranie pieniędzy pod płaszczykiem inwestycji ekologicznych i źródeł zrównoważonych; transfery jak leasing „zielonych projektów", gdzie kryminalne środki są przekształcane w środki pozornie legalne.
2. **Mikropłatności jako narzędzia layeringowe**
   Platformy gamingowe i streaming wykorzystują dziesiątki tysięcy mikropłatności, aby rozdzielić środki i utrudnić ich śledzenie – sam wolumen transakcji stanowi sposób maskowania.
3. **AI-wspierany trade-based money laundering**
   Wykorzystanie algorytmów do generowania faktur, kontraktów i dokumentów handlowych maskujących realne przepływy między państwami, utrudniając urzędową kontrolę trade-based transakcji.
4. **DeFi, stablecoiny i anonimowe transfery**
   Pranie przez zdecentralizowane giełdy (DEX), mosty cross-chain, miksery pozwala na szybki, pseudo-anonimowy przepływ środków bez wersji KYC i możliwości blokady transferu.
5. **Hazard online i tokenizacja dóbr luksusowych**
   Wartość aktywów jest przenoszona przez tokeny art, wirtualne kasyna czy nieruchomości – przestrzeń słabo nadzorowana, gdzie wysokie kwoty można łatwo przepuścić poza system bankowy.
6. **Sieci globalnych struktur prania**
   Zorganizowane grupy działające jako firmy-proxy państw, prowadzą hybrydowe operacje destabilizacyjne, kreując własne kanały finansowe i korzystając z politycznego parasola ochronnego.

Moduł 3: Technologie detekcji i compliance przyszłości

1. **Graph-network AI na blockchainie**
   Nowe architektury graph-network AI (jak GAT-ResNet) są w stanie wykrywać relacje i wzorce prania na blockchainach skuteczniej niż klasyczne narzędzia graph analytics.
2. **Deep learning dla mikropłatności mobilnych**
   Modele uczące się analizują miliardy transakcji generowanych przez urządzenia IoT i smartfony – eliminując fałszywe alarmy i zwiększając precyzję detekcji.
3. **Modele unsupervised dla cross-border AML**
   Analiza transakcji bez wcześniejszego treningu – adaptacyjne modele wykrywają anomalie w transferach międzynarodowych natychmiast, nawet przy niespójnych danych.
4. **Monitorowanie DeFi + mikropłatności z AI**
   Łączenie danych blockchain, zachowań użytkowników i mikropłatności jest analizowane za pomocą AI, identyfikując anomalie w czasie rzeczywistym.
5. **Explainable AI w compliance**
   Modele ML muszą być audytowalne, zgodne z GDPR – powodują, że wnioski detekcyjne są interpretowalne i mogą być poddane ocenie regulacyjnej.
6. **Cross-functional analityka zagrożeń**
   Połączenie zespołów fraud + AML + cybersecurity tworzy holistyczną warstwę threat intelligence zdolną do szybkiego reagowania na nowe schematy.

Moduł 4: Reakcja instytucji – praktyczne podejście

1. **EDD wobec ESG i greenwashing**
   Prowadzenie dogłębnej weryfikacji źródeł finansowania projektów ekologicznych, analiza dokumentacji, transparentność struktur właścicielskich i beneficjentów.
2. **KYC w erze mikropłatności**
   Budowanie profili użytkowników korzystających z platform gaming/streamingowych; threshold tuning i dynamiczne modele monitoringu zamiast jednorazowego CDD.
3. **AML w stablecoinach i DeFi**
   Włączanie blockchain analytics do systemów monitoringu; współpraca z VASP; raportowanie transakcji realizowanych poza centralizowanymi giełdami.
4. **Enhanced Due Diligence wobec krajów z list FATF**
   Weryfikacja struktur właścicielskich, potoków pieniężnych, pochodzenia środków dla kontrahentów z jurysdykcji grey/black list.

5. **Współpraca FIU i Europol**
   Integracja inteligencji z raportów SOCTA z analizą wnętrza institution; wymiana danych real-time; analiza globalnych zagrożeń w SAR reporting.
6. **Strategia compliance nastawiona na intelligence**
   Przekształcenie AML z reakcyjnego monitoringu do adaptacyjnego systemu opartego na threat intelligence, inteligentne zarządzanie ryzykiem i governance cross-funkcjonalne.

Warunki uczestnictwa i regulamin

Warunki uczestnictwa

po otrzymaniu zgłoszenia prześlemy potwierdzenie przyjęcia zgłoszenia, a na około 2 dni przed terminem szkolenia zostaną wysłane wiadomości organizacyjne wraz z linkiem do szkolenia oraz materiałami szkoleniowymi. Płatności po szkoleniu, zwykle w tym samym dniu po szkoleniu prześlemy do Państwa faktury do zapłaty wraz z zaświadczeniem drogą mailową.

Regulamin

rezygnację przyjmujemy najpóźniej na 3 dni przed szkoleniem w formie pisemnej. Rezygnacja w późniejszym terminie wiąże się z koniecznością pokrycia kosztów w 100%. Nieobecność na szkoleniu nie zwalnia z dokonania opłaty. W przypadku braku możliwości wzięcia udziału w danym terminie jest możliwość przesłania nagrania ze szkolenia online.

Promocja

490 + VAT
za każdą kolejną osobę z firmy

690 + VAT | za osobę

NADCHODZĄCE TERMINY