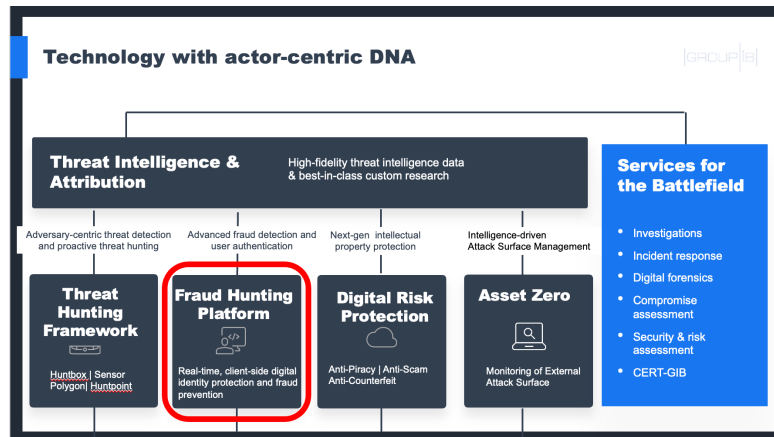
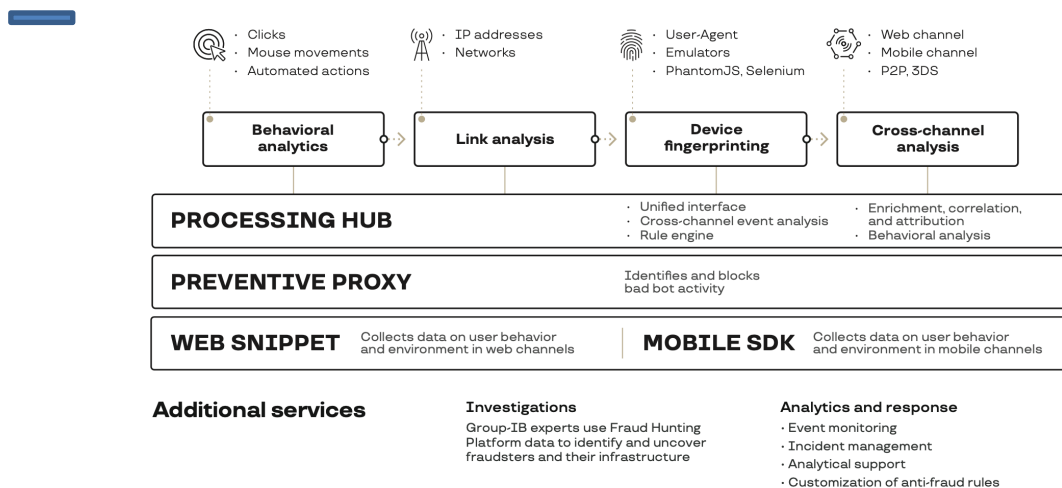


FRAUD HUNTING PLATFORM (FHP) - proaktywna ochrona tożsamości cyfrowej użytkownika w czasie rzeczywistym i zapobieganie oszustwom internetowym



- Wczesne wykrywanie i blokowanie nieuczciwych działań
- Bezproblemowa i bezpieczna obsługa klienta
- Kompleksowa platforma zapobiegająca oszustwom
- Identyfikacja infrastruktury podmiotów stanowiących zagrożenie

Group-IB Fraud Hunting Platform architecture



Web Snippet - Zbiera dane na temat zachowań użytkowników i środowiska w kanałach internetowych

Mobile SDK - Zbiera dane na temat zachowań użytkowników i środowiska w kanałach mobilnych

Zapobieganie wielokanałowym i między-klienckim atakom i oszustwom



Wykrywanie oszustw płatniczych Ochrona użytkowników przed oszustwami związanymi z kartami płatniczymi, przejmowaniem kont, socjotechniką i złośliwym oprogramowaniem.

Wykrywanie prania brudnych pieniędzy Analiza powiązań między kontami użytkowników i innymi podmiotami w celu wykrycia podejrzanych transakcji.

Zdemaskowanie oszustów Wykrycie infrastruktury podmiotów stanowiących zagrożenie, aby ustalić ich tożsamość.

Blokowanie złośliwych botów Ochrona przed wszystkimi rodzajami złośliwych botów, w tym tych które potrafią naśladować ludzkie zachowanie.

Zapobieganie oszustwom związanym z programami lojalnościowymi Wykrywanie oszustwa związanego z milami podróży lub programami bonusowymi sklepów internetowych.

Ochrona interfejsów API Blokowanie nieautoryzowanego użycie interfejsów API przez złośliwe boty.

Zwiększona wykrywalność oszustw Wykrywanie nowych schematów inżynierii społecznej, niesankcjonowanego zdalnego dostępu, oszustw związanych z kontami użytkowników, złośliwego oprogramowania, przeciwdziałania praniu brudnych pieniędzy oraz ataków wielokanałowych.

Blokowanie złośliwych botów Dedykowany moduł blokuje boty typu shell, boty emulujące zachowanie użytkownika, boty mobilne.

Poprawa funkcjonalności od strony użytkownika końcowego Usunięcie dodatkowych kroków przy uwierzytelnianiu klienta, rozszerzenie limitów transakcji, brak fałszywych blokad konta.



Optymalizacja kosztów biznesowych Obniżenie kosztów powiadomień SMS, tokenów, kart zdrapek, połączeń z klientami

Ułatwienie zachowania zgodności z przepisami Pomoc firmom w zachowaniu zgodności z lokalnymi regulacjami dotyczącymi ochrony danych w zakresie zapewnienia bezpieczeństwa środowiska płatniczego (np. PSD2).

Opcje wdrożenia

Moduł Secure Bank FHP jest automatycznie uruchamiany na urządzeniach klientów końcowych. Zbiera on dane kontrolne w celu stworzenia unikalnego profilu każdego klienta i wykorzystania go do szczegółowej analizy zachowań. Analiza ta może być wykonana zarówno w chmurze Group-IB, w chmurze AWS innej firmy lub w ramach infrastruktury lokalnej banku. Niezależnie od metody wdrożenia, gromadzenie danych odbywa się bezproblemowo dla klienta końcowego.