ISSP

АНТИФРОД ДЛЯ БАНКІВ І НЕ ТІЛЬКИ

eCommerce | Процесінгові Центри |
Мікрофінансові організації та інші небанківські установи

ISSP Antifraud допоможе виявити та усунути різні види фінансового та банківського шахрайства при обробці великих обсягів даних.

РІВЕНЬ ПЛАТІЖНИХ ШАХРАЙСТВ СЯГНУВ БЕЗПРЕЦЕДЕНТНОГО РІВНЯ

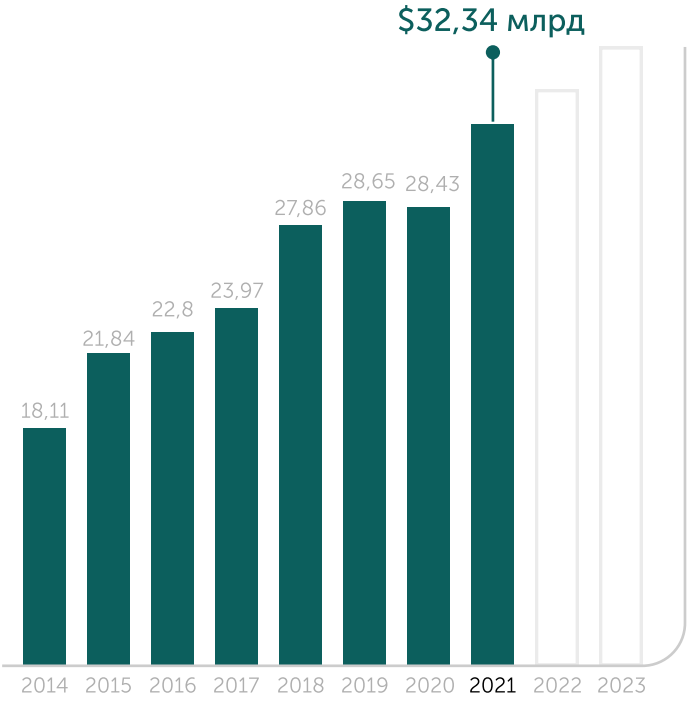
За оцінками НБУ, кіберризики входять в трійку найбільших ризиків для банківської системи України.

Найбільш поширеними кіберзагрозами для фінустанов залишаються DDoS атаки та атаки на інформаційну інфраструктуру.

20тис Зафіксовано фішингових доменів з початку 2022 року.

90% Доля інтернет шахрайств в структурі сукупних збитків від незаконних дій у 2022 році.

Протягом останніх десяти років, рівень платіжних шахрайств з використанням банківських карток у світі збільшився зі $18,11 млрд у 2014 році до вражаючих $32,34 млрд у 2021 році ->



Джерело: Nilson Report, 2022

ПОСИЛЕННЯ КОНТРОЛЮ З БОКУ РЕГУЛЯТОРА: ПОСТАНОВА НБУ №58

Постанова Правління Національного банку України від 03 травня 2023 року № 58 "Про затвердження Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку" дозволить банкам ефективно боротися з різними видами фінансового шахрайства, сприятиме розвитку галузі антифрод-технологій та підвищенню ефективності заходів безпеки.

- Необхідність додаткових інвестицій на антифрод-проєкти
- Часові обмеження до кінця 2025 року
- Підвищена відповідальність банків за дотримання нових вимог та стандартів

РІШЕННЯ ВІД ISSP

ISSP пропонує сучасні антифрод рішення, які допоможуть виявити та усунути різні види фінансового та банківського шахрайства при обробці великих обсягів даних.

Наші продукти включають системи аналізу, які в режимі реального часу створюють моделі поведінки користувачів платіжних сервісів. Вони оперативно виявляють будь-які аномалії, що можуть свідчити про можливе шахрайство, та вживають проактивних заходів для його запобігання.

Тісна співпраця з визнаними лідерами галузі, такими як D8 Corporation та OpenText, створює можливості для реалізації проєктів будь-якої складності із урахуванням специфіки роботи наших клієнтів.

10+ років — Впровадження інноваційних рішень провідних вендорів з персоналізованим підходом

32 країни — Визнають наш комулятивний досвід у розробці, впровадженні та підтримці складних антифрод рішень і платформ

ДЛЯ КОГО?

- Банки
- Процесінгові Центри
- eCommerce платформи
- Мікрофінансові організації
- Небáнківські фінáнсові устáнóви

КОМПЛЕКСНИЙ ПІДХІД

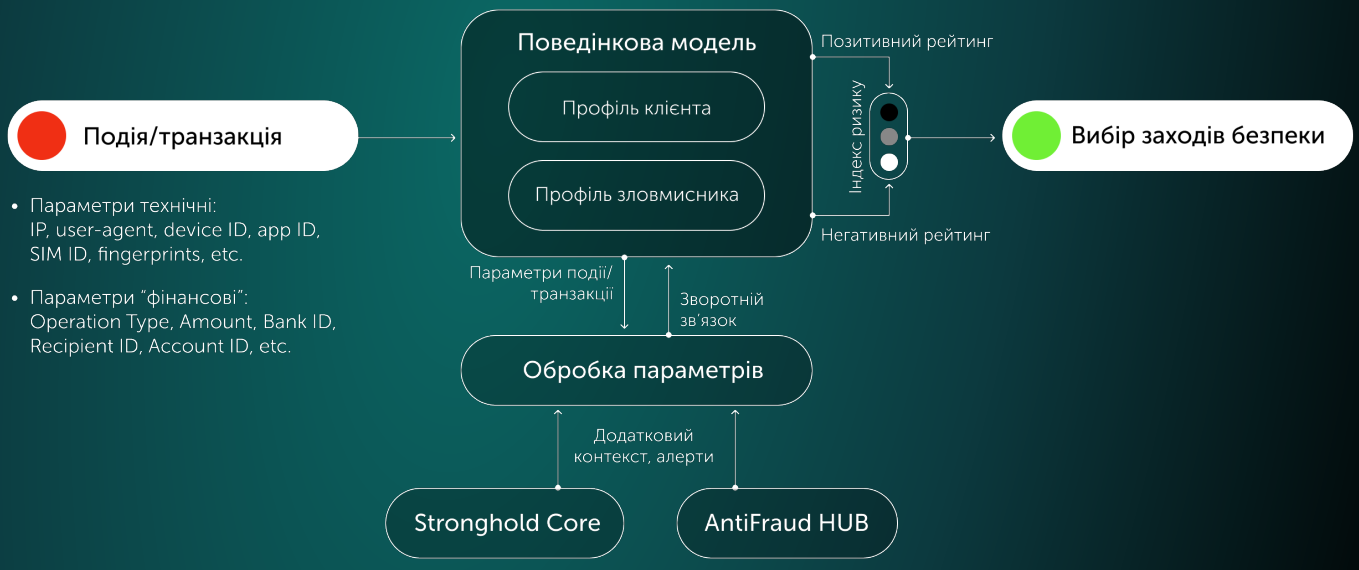
ISSP + ЄМА + D8 Corporation

Для покращення безпеки банківських операцій та подальшого підвищення кіберзахисту банківських установ ISSP та D8 розпочали тісну співпрацю з Асоціацією Учасників Міжбанківських Платіжних Систем України «ЄМА».

ЯК ПРАЦЮЮТЬ НОВІТНІ АНТИФРОД РІШЕННЯ

Наша ціль - це протидія платіжному шахрайству, вровадження нових норм регуляції, підвищення рівня кіберстійкості та посилення взаємодії у фінансовій сфері.

Сучасні антифрод рішення від ISSP та D8 відповідають всім ключовим технічним вимогам нормативних актів регуляторів щодо посилення протидії платіжному шахрайству (Постанова НБУ № 58 про запровадження посиленої автентифікації платіжних операцій)



ПЛАТФОРМА STRONGHOLD

D8 Corporation

Платформа Stronghold використовує моделювання поведінки та аналізує активність споживачів у реальному часі на основі встановлених параметрів для виявлення аномалій. Коли система виявляє відхилення від звичайної поведінки, вона автоматично надсилає повідомлення або виконує попередньо налаштовані дії.

Автоматична реакція на підозрілу активність підвищує рівень безпеки операцій та дозволяє виявляти навіть надскладні патерни, які неможливо відстежити вручну.

D8 Stronghold має універсальну архітектуру, спеціально розроблену під потреби банків та процесингових центрів. Вона повністю відповідає вимогам RFP та не потребує тривалого часу для налаштування.

ПЕРЕВАГИ

Швидка реакція
Зі швидкістю реакції менше 20 мс навіть на складні математичні моделі, платформа оперативно реагує на всі події та виявляє потенційні загрози в реальному часі.

Висока ефективність
Показник виявлення шахрайських дій складає більше 90%, що забезпечує безпеку ваших операцій та знижує ризик фінансових втрат.

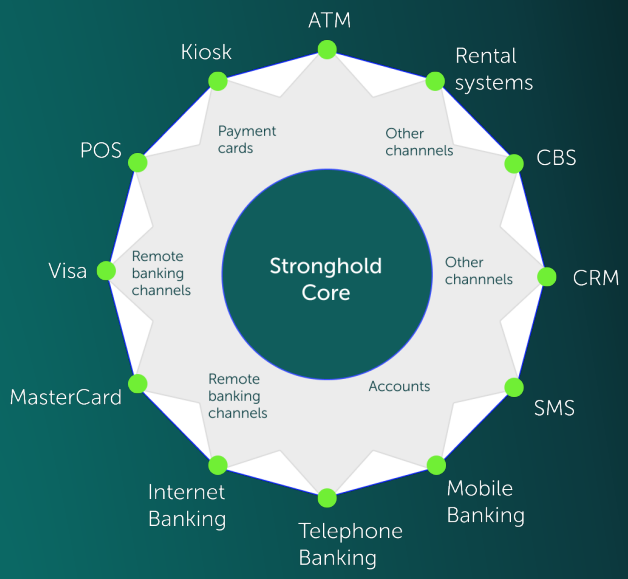
Гнучкість та адаптивність
Платформа дозволяє налаштовувати її під власні потреби організації. StrongHold надійно адаптується до будь-якого середовища, незалежно від складності, будь-то інтеграція з сучасними веб-системами чи застарілою інфраструктурою.

Оптимальне співвідношення «ціна-якість»
Платформа пропонує ефективні рішення по запобіганню платіжного шахрайства за розумні гроші. Впровадження антифрод рішень не стане фінансовим тягарем для вашої організації.

Комплексна підтримка під ключ
Платформа надає комплексну підтримку, супроводжуючи організації під час всього періоду впровадження та обслуговування.

ФУНКЦІОНАЛЬНІ ОСОБЛИВОСТІ

- Безперешкодна інтеграція з різноманітними джерелами даних.
- Архітектура Multi-Tenant: Підтримує мультикористувацький режим для масштабування моніторингу та оцінки.
- Аналіз поведінки даних: Збагачення інсайтів за допомогою аналізу користувацької поведінки.
- Оцінка ризиків: Вбудовані засоби для надійної оцінки ризиків уже доступні в платформі.
- Використання моделей штучного інтелекту та машинного навчання.
- Гнучка настроювана звітність, адаптована під запит конкретної організації.
- Відповідність стандартам AML: Повністю відповідає стандартам PCI DSS 3.2



Шахрайство призводить не лише до фінансових втрат, але й шкодить репутації фінансової установи та підриває довіру з боку клієнтів.

Тому для організацій важливо впровадити ефективні антифрод рішення.

ПЛАТФОРМА ARCSIGHT

OpenText

Антифрод система ArcSight служить додатковим рівнем безпеки системи авторизації і захищає від шахрайських дій, під час яких можуть використовуватися втрачені, викрадені або підроблені картки. Вона моніторить різні види операції систем Дистанційного банківського обслуговування.

Система ґрунтується на аналізі поведінки власників банківських рахунків та оперативно виявляє та надійно блокує будь-які аномальні патерни поведінки.

Платформа аналізує профілі клієнтів і створює "чорні" та "білі" списки отримувачів платежів. Вона безперешкодно інтегрується з системою авторизації обробки данних банку, підвищуючи свою ефективність завдяки постійному оновленню інформації про шахрайські дії.

Кожного разу, коли фіксується "підозріла" транзакція, система негайно сповіщає персонал банку та вживає заходів для блокування подальших транзакцій.

ПЕРЕВАГИ

Автоматизоване виявлення аномалій
Для запобігання внутрішньому шахрайству ArcSight Antifraud використовує строгий контроль процесів – порівнює фактичні процеси із попередньо визначеними моделями.

Моніторинг транзакцій в реальному часі
Система гарантовано оброблює тисячі транзакцій за секунду. Це дозволяє фінансовим установам виявляти та реагувати на шахрайські дії негайно, зменшуючи ризик фінансових втрат.

Відповідність стандартам безпеки
ArcSight Antifraud дозволяє банкам налаштовувати процеси відповідно до міжнародних та галузевих стандартів безпеки, таких як PCI DSS. Дотримуючись цих стандартів, банки можуть забезпечити безпеку своїх інформаційних систем, мереж та даних клієнтів.

Аналіз поведінки та профілювання
Система створює та постійно оновлює профілі клієнтів, шахраїв та отримувачів платежів на основі атрибутів транзакцій. Цей аналіз дозволяє виявляти будь-які незвичайні патерни чи відхилення від нормальної поведінки, полегшуючи виявлення потенційних шахрайств.

КЛІЄНТИ, ЯКІ ВЖЕ КОРИСТУЮТЬСЯ АНТИФРОД РІШЕННЯМИ ВІД D8 ТА ARCSIGHT

ПУМБ · LIBERTY · ProCredit Bank · CREDO BANK · Halyk

МИ ГОТОВІ ВАМ ДОПОМОГТИ

info@issp.com