

Еволюція антифроду:

як синергія IBM Trusteer та IBM Safer Payments зупиняє шахрайство

Компанія Solidity пропонує два інструменти, які разом захищають клієнта і його кошти.

Схеми інтернет-шахрайства змінюються швидше, ніж традиційні системи захисту встигають на них реагувати. Згідно з останніми аналітичними даними IBM Trusteer, класичні атаки із захопленням акаунтів (Account Takeover), які здійснювалися з пристроїв зловмисників, відходять у минуле. Це створює запит на принципово нові інструменти моніторингу та захисту платіжних операцій.

Нові загрози: коли ворог усередині

Статистичні показники свідчать, що шахрайство через довірені пристрої наразі є головною загрозою для світового корпоративного та роздрібного банкінгу. Про що говорять цифри аналітики?

- 2 з 3 шахрайських транзакцій сьогодні здійснюються безпосередньо з пристроїв самих жертв (Scam/соціальна інженерія).

- 61% підтвердженого фроду відбувається через довірені пристрої, які клієнти раніше неодноразово використовували для легітимних операцій.

Зловмисникам більше не потрібно викрадати паролі чи клонувати пристрої — вони маніпулюють діями користувачів за допомогою методів соціальної інженерії безпосередньо під час сесії або використовують інструменти віддаленого доступу.

Подвійний ешелон захисту від Solidity

Для ефективної протидії цим загрозам компанія Solidity впроваджує комплексний підхід, що поєднує два потужні рішення від IBM: сесійний антифрод IBM Trusteer та транзакційний антифрод IBM Safer Payments.

IBM Trusteer — це SaaS-платформа сесійного антифроду, яка безперервно аналізує поведінку користувача та оточення його пристрою (мобільний застосунок чи веб-ресурс) у реальному часі. Система здатна виявляти активні дзвінки під час сесії, наявність шкідливого ПЗ, ознаки віддаленого контролю та аномалії на етапі онбордингу.

IBM Safer Payments — це інтелектуальна система протидії фінансовому шахрайству в режимі реального часу, що використовує передові алгоритми машинного навчання та гнучкий модуль правил для перевірки кожної фінансової транзакції.

Сила інтеграції: єдине вікно прийняття рішень

Найбільшу ефективність демонструє саме крос-канальна інтеграція цих двох систем. Контекст сесії та поведінкові маркери, які збирає IBM Trusteer, передаються в транзакційне ядро IBM Safer Payments. На основі цих зведених даних приймається остаточне рішення щодо безпеки платежу.

«Скам у класичному вигляді стрімко росте, адже людина — це найпростіше місце для компрометації. Раніше ми закривали багато кейсів лише на базі IBM Safer Payments. Проте клієнти запропонували інтегрувати обидва рішення в єдину систему прийняття фінального рішення, і ми це реалізували. Завдяки такій синергії та крос-канальній інтеграції рівень виявлення шахрайства сягає 90% при утриманні помилкових сповіщень (fraud alerts) нижче 0,05%. У класі сесійного антифроду це дійсно найкращі показники в галузі на сьогодні».



Сергій СОПРОНЮК,
керівник антифрод-департаменту компанії Solidity

Така архітектура дозволяє не просто точково фіксувати підозрілі дії на пристрої, а миттєво зупиняти виведення коштів у момент спроби проведення платежу.

«У сучасному цифровому світі довіра клієнтів та фінансова стійкість бізнесу безпосередньо залежать від швидкості та точності реагування на загрози. Впровадження передових антифрод-рішень, таких як IBM Safer Payments та IBM Trusteer, дозволяє фінансовим інституціям не просто захищати транзакції в реальному часі, а й будувати проактивну систему управління ризиками, яка адаптується до нових викликів за лічені дні».



Юрій ФЕДЕЦЬ, CEO компанії Solidity

Поєднання сесійного та транзакційного ешелонів захисту від компанії Solidity дає українському фінансовому сектору змогу випереджати технології шахраїв та гарантувати безпеку клієнтських коштів навіть у випадках складного таргетованого скаму.

Щоб дізнатися більше,
зверніться до фахівців **Solidity** —
офіційного **IBM Gold Partner** в Україні.

SOLIDITY

info@solidity.com.ua, <https://solidity.com.ua>