Як український банк підвищив кіберстійкість

завдяки автоматизації перевірок засобів кібербезпеки

Сервіс Security Control Validation від Netwave забезпечує постійну перевірку ефективності захисту і його відповідності сучасним викликам.

З початком повномасштабної війни кількість кібератак на Україну зросла більш ніж утричі, і у 2025 році вона продовжує стрімко збільшуватися. При цьому близько 90% хакерських груп, що атакують Україну, контролюються силовими структурами РФ. Суттєво зросла складність хакерських кампаній, які з кримінального бізнесу перетворилися на інструмент гібридної війни. Для українського фінансового сектору це означає постійну протидію кіберпідрозділам країни-агресора: банки опинилися серед пріоритетних цілей поруч з іншими об'єктами критичної інфраструктури.

Виклик № 1: IT-інфраструктура як головна ціль атак

Сучасна банківська інфраструктура охоплює численні інформаційні системи, сервіси, пристрої та мережеві компоненти. З розвитком технологій зростає і кількість потенційних точок входу для атак. Цифрова трансформація підвищує ефективність бізнесу, але водночас ускладнює підтримку стабільного рівня безпеки: постійні зміни, оновлення та інтеграції створюють ризики появи вразливостей — як технічних, так і конфігураційних.

При цьому банківський сектор залишається однією з пріоритетних цілей для зловмисників, оскільки успішна атака на фінансову установу може призвести не лише до прямих фінансових втрат, але й до підриву довіри клієнтів та дестабілізації економіки загалом. В умовах війни кібератаки на банки стали повноцінним елементом агресії.

Виклик № 2: гонитва озброєнь у кіберпросторі

Швидкість еволюції кіберзагроз вражає — нові зразки шкідливого програмного забезпечення з'являються щотижня, а методи обходу захисту постійно ускладнюються. Зловмисники використовують різноманітні підходи: від соціальної інженерії та автоматизованих атак до застосування легітимних інструментів зі злочинною метою (тактики Living off the Land), уникаючи детектування традиційними засобами.

Щоб утримувати належний рівень кіберстійкості, недостатньо вчасно оновлювати сигнатури, правила виявлення та політики безпеки. Вкрай важливо регулярно перевіряти їх актуальність у контексті поточного ландшафту кіберзагроз. Для цього необхідні безперервний моніторинг і використання ефективних інструментів розвідки загроз (threat intelligence).

Виклик № 3: ілюзія безпеки від пентестів

Тестування на проникнення залишається важливою практикою оцінки захисту, але його результати відображають стан лише на момент перевірки: нові ризики можуть з'явитися одразу після завершення тестування.

З огляду на ці виклики, провідний український банк вирішив переосмислити підхід до оцінювання ефективності захисних систем. У відповідь на потреби Клієнта наша команда запропонувала доповнити традиційний пентестинг нашим сервісом Security Control Validation (SCV).

Security Control Validation: безперервна перевірка ефективності засобів захисту

У співпраці з командою Netwave Банк упровадив Сервіс Security Control Validation — інноваційне рішення, що поєднує потужну технологічну базу вендора (Picus Security) з експертизою Netwave у локальній адаптації, сервісному супроводі та методології аналізу результатів. SCV базується на автоматизованому моделюванні реальних векторів атак і забезпечує постійну оцінку спроможності захисних систем протистояти актуальним технікам зловмисників.

Кожен тест структурується відповідно до фреймворку MITRE ATT&CK, що дає змогу не лише виявляти слабкі місця, а й розуміти, які саме етапи ланцюга атаки потребують посилення.

Що зробило сервіс Netwave унікальним

Команда Netwave не лише впровадила технологічну платформу, а й побудувала повноцінний сервіс на її основі — з урахуванням вимог банківського сектору та операційних реалій великих IT-ландшафтів. Завдяки цьому SCV перетворився для Банку на інструмент постійного контролю кіберстійкості, а не просто на технологічний продукт.

Операційні переваги для банківських установ

- **Постійність і безпечність:** технічні спеціалісти компанії Netwave проводять регулярні автоматизовані перевірки без впливу на продуктивне середовище, що дає банкам змогу підтримувати цілодобову операційну діяльність і водночас мати поточну картину ефективності захисту.

➢ **Актуальність:** база сценаріїв атак оновлюється щоденно, забезпечуючи тестування щодо найновіших технік кіберзлочинців, серед яких тактики Living-off-the-Land.
➢ **Адаптація до контексту клієнта:** Netwave налаштовує сценарії з урахуванням особливостей архітектури та пріоритетів безпеки Банку.
➢ **Економічна ефективність сервісної моделі:** упровадження SCV у форматі сервісу дає банкам змогу отримати доступ до кращого у своїй ніші enterprise-рішення без значних капітальних інвестицій. Орех-модель забезпечує гнучкість бюджетування та можливість масштабування функціональності відповідно до потреб клієнта.
➢ **Експертний супровід:** спеціалісти Netwave надають консультації щодо побудови стратегії симуляцій, пріоритизації виявлених проблем і правильної інтерпретації результатів.

Security Control Validation: досвід банку

Банк розпочав співпрацю з Netwave із пілотного проєкту, який дав змогу швидко оцінити реальну ефективність захисних систем у різних сегментах інфраструктури.

Фокусні напрями тестування: спільно з командою кібербезпеки Банку було визначено пріоритетні вектори перевірок, які покривають найкритичніші точки фінансової установи. Особливу увагу приділено безпеці електронної пошти (як основному вектору фішингових атак), мережі та захисту кінцевих точок (більшою мірою — робочих станцій співробітників).

Трансформація операційних процесів: ключовим досягненням стала інтеграція регулярної перевірки засобів безпеки в щоденні операційні процеси Банку й можливість оперативного поліпшення контролів безпеки. Команда Netwave, використовуючи аналітичні можливості платформи, готує звіти з конкретними рекомендаціями щодо усунення недоліків та індикаторами компрометації для оновлення сигнатурних баз і правил детектування. Це дало Клієнту змогу перейти від реактивного до проактивного управління кіберризиками.

Результат: Банк отримав обґрунтовану, об'єктивну картину поточного стану безпеки, можливість вчасно усувати виявлені недоліки й підтримувати відповідність регуляторним вимогам (зокрема, постановам НБУ №95, №178).

Сучасні виклики кіберзагроз потребують принципово нового підходу до оцінювання ефективності систем захисту. Доповнення традиційних пентестів сервісом SCV дає змогу своєчасно виявляти «сліпі зони» у захисті, підвищуючи кіберстійкість фінансових установ, і забезпечує прозору доказову базу для контролюючих органів.
*Якщо ви прагнете перетворити перевірку безпеки на системний процес — фахівці **Netwave** допоможуть це реалізувати: налаштувати регулярні перевірки та забезпечити постійний контроль ефективності захисту.*

38 (044) 359 05 50,
team@netwave.ua,
https://netwave.ua/