GROUP-IB

AVO

ИСТОРИЯ УСПЕХА

GROUP-IB × AVO BANK

Эшелонированная защита клиентов нового цифрового банка Узбекистана

О «AVO bank»

Отрасль	Финансы
Основан	2023
География	Узбекистан
Решения GROUP-IB	Threat Intelligence, Attack Surface Management, Managed Extended Detection and Response (Managed XDR), Fraud Protection

AVO bank – это высокотехнологичный банк Узбекистана, который прошел процедуру ребрендинга и перезапустился в 2024 году. Ключевым продуктом банка стала кредитная карта AVO platinum, доступная в том числе полностью в цифровом формате через мобильное приложение.

1 Миллион пользователей

Скачали приложение AVO за первые три месяца

Контекст

Количество попыток атак постоянно увеличивается: чем больше развивается AVO bank, тем больше появляется угроз. Сегодня это десятки тысяч предотвращенных негативных событий в месяц, что делает оперативное и качественное реагирование на них критически важным.

Перед AVO bank стояла амбициозная задача: в кратчайшие сроки запустить цифровые сервисы и обеспечить комплексную защиту информационной безопасности клиентов и сотрудников. При этом банк стремился сохранить удобство, скорость и качество оказываемых услуг. Для решения этой задачи требовались системы с гибкой моделью лицензирования, которые можно было развернуть в сжатые сроки.

С развитием цифровой экономики и соответственно увеличением киберугроз в Узбекистане всё больше внимания уделяется вопросам информационной безопасности. Финансовые организации, такие как AVO bank, сталкиваются с необходимостью соответствовать требованиям регуляторов, направленных на повышение уровня защищенности в финансовых учреждениях. Поэтому выбор поставщика решений также зависел от возможности соответствовать регуляторным требованиям по внедрению антифрод-решений и предоставлению отчетности о выявленных мошеннических ресурсах.

Проблемы и задачи

Необходимость комплексной защиты клиентов и сотрудников нового банка на фоне растущих угроз

Поиск решений в SaaS-формате из-за ограниченных ресурсов и амбициозных сроков запуска коммерческой деятельности

Потребность в специалистах SOC для мониторинга сложных инцидентов

Необходимость соответствовать требованиям регулятора

Почему выбрали Group-IB?

> Наша команда давно знакома с качеством решений Group-IB и считает их одними из лучших на международном рынке. Гибкие возможности развертывания решений в формате SaaS и партнерство Group-IB с Центральным банком Узбекистана также послужили убедительными аргументами для нас. А одним из решающих факторов стало наличие у Group-IB собственного центра реагирования на инциденты информационной безопасности (SOC) и возможность его подключения к мониторингу инцидентов банка.

ЕВГЕНИЙ АРТЮХИН,

руководитель службы безопасности AVO bank

Group-IB — один из ведущих мировых поставщиков решений в области кибербезопасности. Компания давно представлена на рынке Центральной Азии, а в августе 2023 года Group-IB подписала Меморандум о сотрудничестве с Центральным банком Узбекистана. В декабре 2023 года в Ташкенте был открыт центр по противодействию цифровой преступности Group-IB. Это стратегическое решение было направлено на повышение кибербезопасности в Узбекистане и в целом в Центральной Азии. В центре работают опытные специалисты по защите от мошенничества, анализу угроз, расследованию инцидентов и разработке программного обеспечения.

Платформа

Unified Risk Platform

Продукты

- Threat Intelligence
- Fraud Protection
- Business Email Protection
- Digital Risk Protection
- Managed XDR
- Attack Surface Management

Услуги

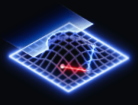
- Реагирование на инциденты и цифровая криминалистика
- Исследование высокотехнологичных преступлений
- Аудит и консалтинг
- Образовательные программы

Решения Group-IB

AVO bank сразу внедрил три решения Group-IB – Attack Surface Management, Threat Intelligence и Managed Extended Detection and Response. Параллельно банк запустил пилотное тестирование продуктов Digital Risk Protection и Fraud Protection. По итогам тестирования обе системы доказали свою эффективность и сейчас успешно используются банком.

Threat Intelligence

дает AVO bank уникальные данные киберразведки по всем атакующим, нацеленным на организацию, индустрию и регион. Стратегические, операционные и тактические сведения об угрозах позволяют подготовиться к атакам заранее и повысить эффективность всей инфраструктуры ИБ.



Attack Surface Management

представляет собой основанное на данных киберразведки SaaS-решение, отслеживающее все доступные извне цифровые активы AVO bank для выявления любых неконтролируемых рисков. Решение обнаруживает широкий спектр угроз для любых типов ресурсов, включая веб-сайты, домены, приложения, оборудование, программное обеспечение, среды разработки, открытые порты, формы авторизации и облачные решения.

Managed XDR

это комплексное решение для обнаружения и устранения киберугроз, включающее сервисную составляющую. Поддержка ведущих аналитиков Центра кибербезопасности SOC позволяет существенно расширить возможности внутренней команды ИБ в сфере обнаружения и проактивного поиска угроз, а также реагирования на инциденты кибербезопасности.

Digital Risk Protection

это платформа автоматического управления цифровыми рисками, нацеленными на бренд, на основе искусственного интеллекта. Она позволяет выявлять и устранять нарушения за пределами периметра AVO bank, включая фишинг, утечки данных и поддельные аккаунты компании в соцсетях.

Fraud Protection

это инновационное решение с применением современных технологий искусственного интеллекта, а также уникальных запатентованных технологий, которое предотвращает онлайн-мошенничество в реальном времени во всех цифровых каналах. Система защищает AVO bank от мошенничества с банковскими картами, атак с использованием социальной инженерии, ботов и вредоносных программ.

Результаты

30

Мошеннических ресурсов

имитирующих бренд банка, было заблокировано за 1 неделю использования DRP

1 700+

Событий

среднего и высокого уровня опасности обнаружено с помощью Managed XDR за 10 месяцев

30 000

Подписчиков

нелегитимного Telegram-канала, использующего бренд банка, были защищены от мошенничества

1

Минута

в среднем требуется для реагирования на угрозу

0

Фишинговых писем

попадает в почту сотрудников банка

В том числе благодаря внедрению решений Group-IB в марте 2024 г. банк успешно прошел процедуру сертификации по соответствию требованиям международного стандарта безопасности данных в индустрии платежных карт — PCI DSS (Payment Card Industry Data Security Standard).

Решения полностью оправдали ожидания AVO bank. Быстрая интеграция позволила обеспечить комплексную защиту инфраструктуры и клиентов в кратчайшие сроки. Банк отметил несколько значительных результатов внедрения:

Снижение внутренних рисков

Человеческий фактор нельзя полностью устранить, однако Group-IB Managed Detection and Response (Managed XDR) позволяет минимизировать такие угрозы. Даже если сотрудник банка случайно скачает вредоносный файл или запустит полученную по почте вредоносную программу, такие файлы блокируются до того, как какой-либо ущерб будет нанесен.

Защита средств и данных клиентов

Решение Fraud Protection позволило AVO bank более эффективно выявлять случаи сессионного мошенничества и предотвращать хищение средств клиентов в режиме реального времени.

> Продукты Group-IB защищают наш банк от разных типов угроз: от фишинга, скама и вредоносного ПО до сложных атак с использованием шифровальщиков. Анализируя информацию в интерфейсах решений, мы не только контролируем безопасность наших клиентов, но и можем управлять внутренними ресурсами, перераспределяя нагрузку на наших сотрудников, что также повышает качество нашей работы и обеспечивает спокойствие клиентов.

ЕВГЕНИЙ АРТЮХИН,

руководитель службы безопасности AVO bank

Отслеживание целевых угроз на этапе подготовки

С помощью Group-IB Threat Intelligence (TI) AVO bank оперативно узнает о готовящихся атаках, нацеленных на индустрию, регион и клиентов банка. Наличие матрицы MITRE ATT&CK® позволяет команде ИБ отслеживать и анализировать все актуальные угрозы в едином интерфейсе и сразу получать информацию о техниках, тактиках и процедурах атакующих. Также TI позволяет AVO bank анализировать информацию об утекших данных банковских карт и отслеживать упоминания банка на андеграундных форумах.

Расширение возможностей мониторинга и детектирования

Наличие команды экспертов SOC позволило банку усилить отслеживание и реагирование на инциденты информационной безопасности. Group-IB Managed Detection and Response (Managed XDR) обнаруживает и блокирует все найденные вредоносные файлы до того, как они попадают во внутренние решения банка. Это также позволяет сократить расходы на антивирусные программы и другие стандартные решения, не обеспечивающие необходимый уровень защищенности.

Мгновенное реагирование

Managed XDR позволяет оперативно реагировать на угрозы, изолируя зараженные хосты и устраняя все следы вредоносной активности. С момента обнаружения угрозы до момента реагирования проходит не больше одной минуты.

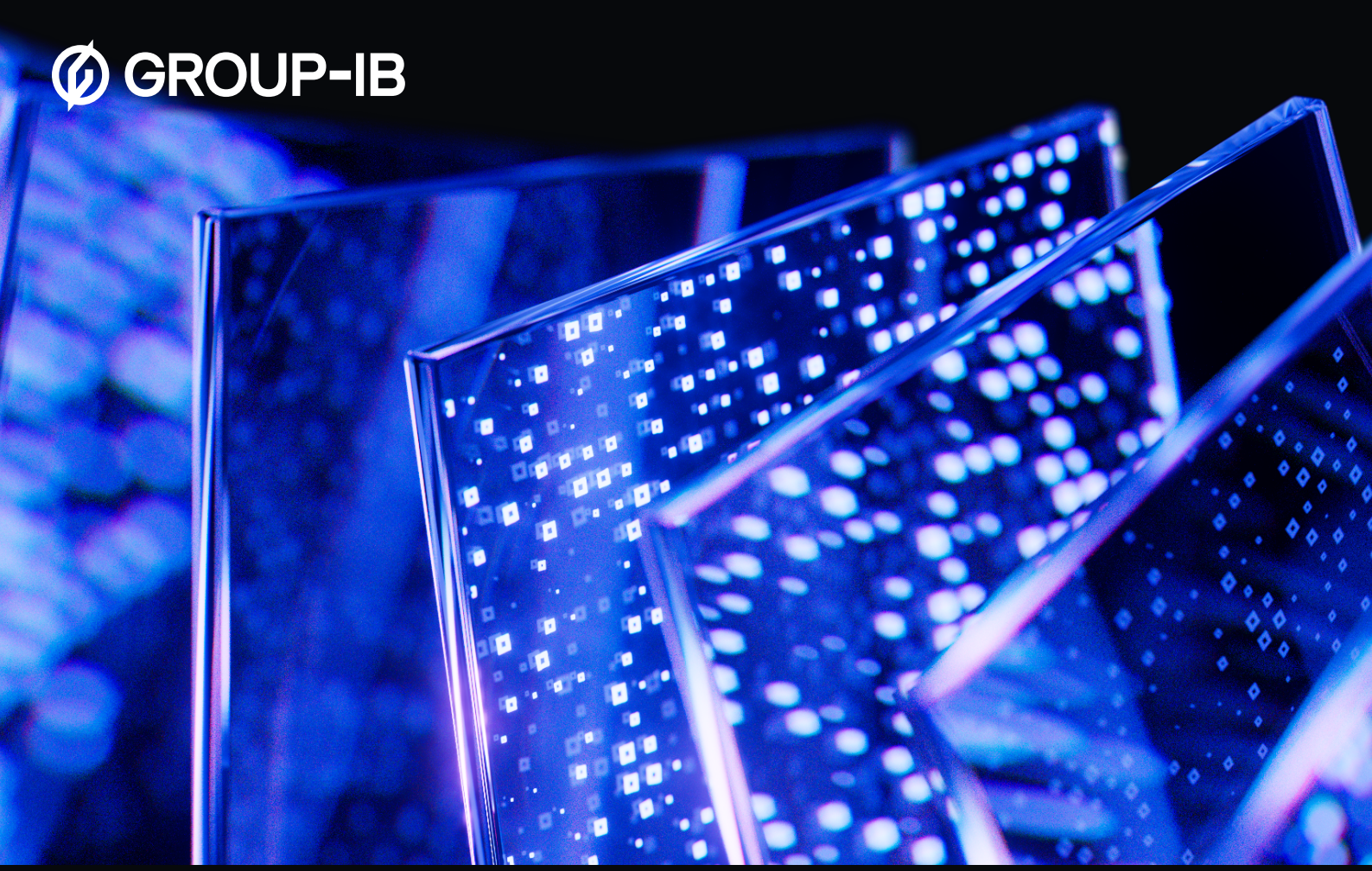
Устранение угрозы фишинга и скама

Благодаря внедрению Managed XDR банку удалось свести количество фишинговых писем к нулю. А с помощью решения Digital Risk Protection (DRP) AVO bank выявляет и блокирует 90% мошеннических ресурсов. Благодаря решениям Group-IB банк выявляет и устраняет угрозы, которые не удавалось обнаружить раньше, например, мошеннические каналы в Telegram. С помощью Group-IB банк также оперативно выявляет и блокирует фишинговые атаки, нацеленные на топ-менеджмент компании.

Сканирование внешнего периметра в режиме реального времени

Attack Surface Management (ASM) позволяет снизить нагрузку на ИБ-команду, выступая в качестве первого эшелона защиты. Банк контролирует все новые цифровые активы и теневые ИТ, отслеживая любые доступные извне ресурсы и оперативно устраняя критические риски.

GROUP-IB



Предотвращаем и исследуем киберпреступления с 2003 года

77 тыс.

часов реагирования
на инциденты

1,5 тыс.

успешных исследований
киберпреступлений
по всему миру

Group-IB — одна из ведущих международных компаний по детектированию и предотвращению кибератак, выявлению фрода и защите интеллектуальной собственности в сети.

По версии Gartner, IDC и Forrester, Group-IB является одним из ключевых поставщиков Threat Intelligence в мире, в базе которой хранится 100 000+ профайлов киберпреступников.

Клиентами Group-IB являются крупнейшие банки и финансовые организации, промышленные и транспортные корпорации, ИТ и телеком провайдеры, ритейл и FMCG компании в 60 странах мира.