История успеха

GROUP-IB И ТИНЬКОФФ

Усиление «эшелона» Тинькофф за счет Group-IB TDS Polygon

Тинькофф

20-40% в год
Потенциал роста
чистой прибыли

507,6 млрд
Совокупные активы
на 30 сентября 2019 года

10 млн
Клиентов

ЭКОСИСТЕМА ТИНЬКОФФ

Тинькофф — финансовая онлайн-экосистема, выстроенная вокруг потребностей клиента.

Экосистема Тинькофф предоставляет полный спектр финансовых услуг для частных лиц и для бизнеса. Особое внимание Тинькофф уделяет развитию лайфстайл-банкинга: экосистема дает клиентам возможность анализировать и планировать личные траты, инвестировать сбережения, получать бонусы в рамках программ лояльности, бронировать путешествия, покупать билеты в кино, бронировать столики в ресторанах и многое другое.

Все сервисы Тинькофф доступны через мобильные приложения и сайт Tinkoff.ru.

Тинькофф не имеет отделений: сеть из 2500 представителей позволяет доставлять продукты компании в любой регион страны в кратчайшие сроки, а клиенты обслуживаются через онлайн-каналы и контакт-центр. Во всех коммуникациях Тинькофф активно использует технологии искусственного интеллекта и машинного обучения, более 35% обращений клиентов в чатах обрабатывается без участия сотрудников банка.

Все продукты и большинство внутренних ИТ-систем Тинькофф разработаны самой компанией. 70% сотрудников штаб-квартиры — ИТ-специалисты.

Ядром экосистемы является основанный в 2006 году Тинькофф Банк — крупнейший независимый онлайн-банк в мире, обслуживающий 10 миллионов клиентов. Банк был признан журналом Global Finance “Лучшим розничным онлайн-банком мира“ (2018), “Лучшим розничным онлайн-банком России” (2015, 2016, 2018 и 2019 г.), журналом The Banker - “Банком Года России” (2013, 2017 г).

Материнская компания банка TCS Group Holding PLC торгуется на Лондонской бирже с октября 2013 года и на Московской бирже с октября 2019 года.

Год основания:
2006

Отрасль:
ФИНАНСЫ

Деятельность:
ДИСТАНЦИОННОЕ БАНКОВСКОЕ И ФИНАНСОВОЕ ОБСЛУЖИВАНИЕ

Количество сотрудников:
> 10 000

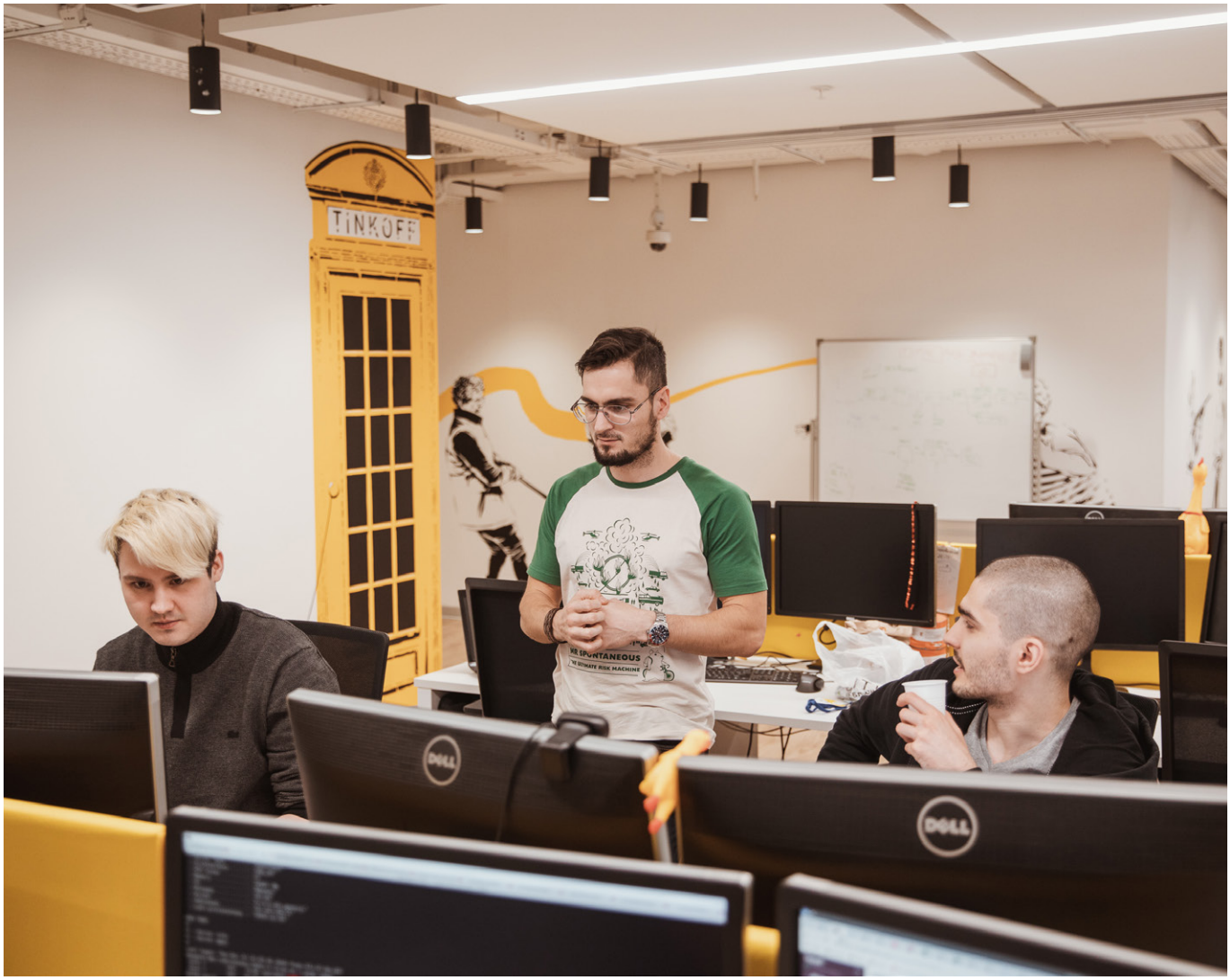
Описание ситуации

Тинькофф — финансовая экосистема, выстроенная вокруг Тинькофф Банка, первого и единственного в России полностью онлайн-банка, обслуживающего свыше десяти миллионов клиентов дистанционно через онлайн-каналы и контакт-центр. Уникальная структура банка накладывает высокие требования к уровню информационной безопасности как внутренних ИТ-систем, так и финансовых продуктов и сервисов.

В этом контексте ключевыми приоритетами для Тинькофф являются стабильное бесперебойное функционирование операционных процессов и превентивная защита от широкого спектра киберугроз, несущих потенциальные риски для ежедневной работы банка.

Несмотря на широкое распространение антивирусных средств, зачастую они оказываются бессильны перед целевыми атаками хакерских групп, эпидемиями вирусов-шифровальщиков, атаками на платежную инфраструктуру с использованием методов социальной инженерии, нелегитимным использованием ресурсов компаний для криптомайнинга и др.

Ключевую роль в выявлении угроз, относящихся к категории «нулевого дня» (т.е. ранее неизвестных) играют продукты класса Anti-APT (англ. Advanced Persistent Threat — «развитая устойчивая угроза», целевая кибератака), позволяющие проводить многосторонний анализ вредоносных файлов в, так называемой, «песочнице» — изолированной от основной сети банка среде.



Поставленные задачи

В качестве «песочницы» в Тинькофф использовалось решение одного из ведущих международных вендоров. Однако, практика показала, что уществующей конфигурации недостаточно.

Банк принял решение усилить качество детектирования, сделав ставку на эшелонированную защиту, основу которой составили сразу несколько «песочниц».

По итогам продолжительного тестирования различных продуктов в стэк решено было включить высокотехнологичную систему раннего выявления кибератак Group-IB Threat Detection System Polygon.

> Нам важно заранее узнавать о появлении новых типов угроз и оперативно реагировать на них, минимизируя возможные риски. Мы решили развернуть «эшелон песочниц», сделав упор на обнаружение, прежде всего, угроз «нулевого дня». Именно они являются наиболее опасными и могут быть выявлены только умными системами поведенческого анализа, позволяющими изучить файл до того, как он попадет на компьютер пользователя.
>
> **Дмитрий Гадарь,**
> Руководитель Департамента информационной безопасности Тинькофф

Решение Group-IB

Высокотехнологичная система раннего выявления кибератак Group-IB Threat Detection System Polygon

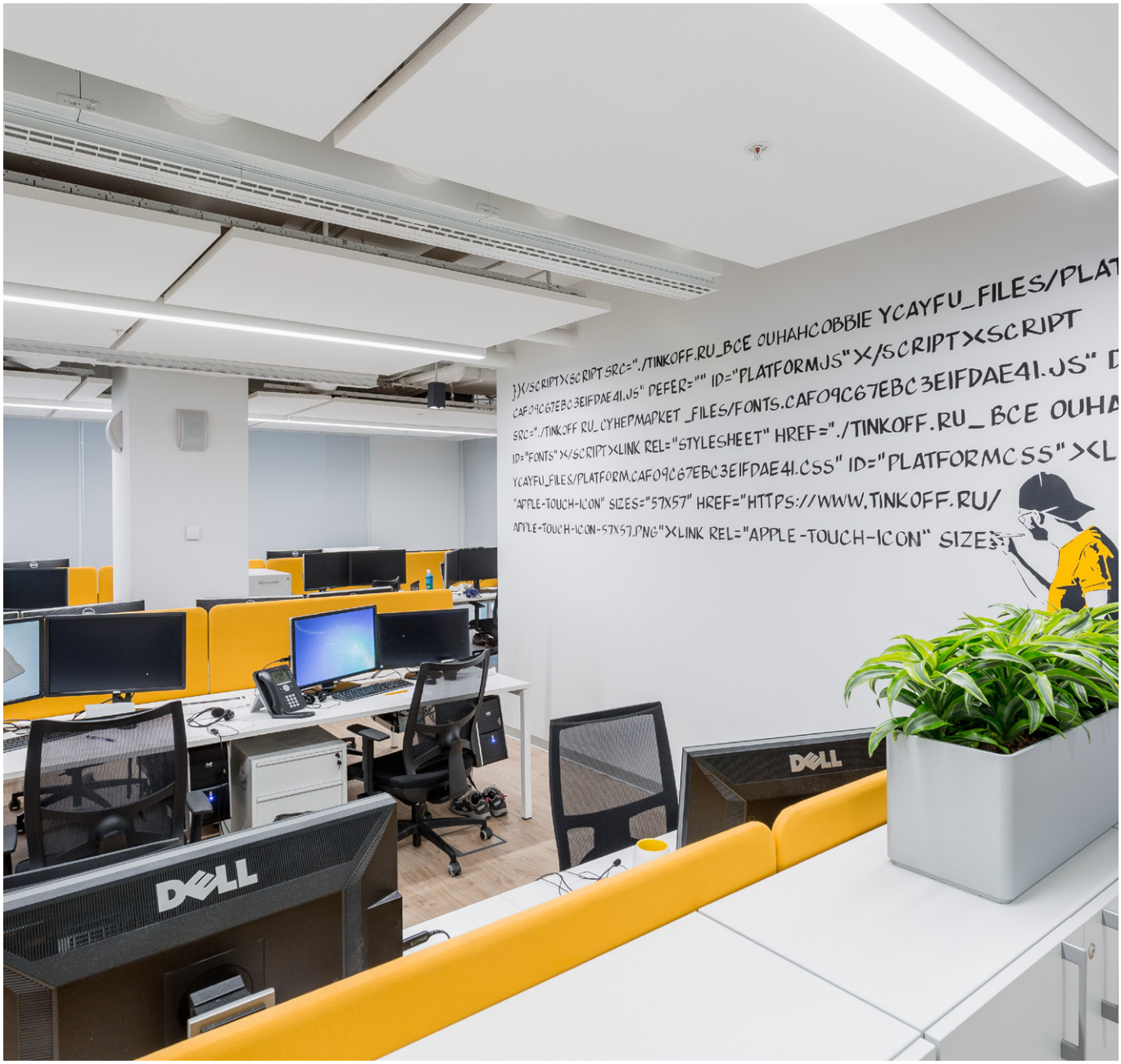
Описание решения Group-IB

Group-IB TDS — комплексное решение, предназначенное для выявления целевых атак и неизвестных угроз, охоты за угрозами как внутри защищаемого периметра, так и за его пределами, реагирования на инциденты и их расследования.

Применение Group-IB TDS позволяет определять заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений.

Group-IB TDS Polygon представляет собой модуль для детонации файлов в изолированных средах, извлечения индикаторов и обогащения их. Главной задачей Group-IB TDS Polygon является всеми возможными способами обнаружить вредоносный код в почтовых вложениях, скачиваемых файлах и ссылках.

> Эффективные Anti-APT решения должны не просто осуществлять статический и динамический анализ файлов, но и противостоять множеству техник, позволяющих злоумышленникам обнаруживать виртуализацию ОС и обходить технологию детектирования угроз другими, довольно разнообразными, способами.
>
> Дьявол всегда в деталях: даже такие, казалось бы, простые вопросы как анализ ссылок, поддержка сотен форматов файлов, изменяющие во времени свое состояние ссылки, — все это серьезный вызов для вендоров, разрабатывающих продукты этого класса.
>
> Немаловажна и полнота предоставляемых поведенческих отчетов: детальный разбор действий объекта анализа и наступающих в системе изменений позволяют аналитику, работающему с системой, сделать свой экспертный независимый вывод о правильности вердикта и степени угрозы, который несет данный файл. Эти задачи решает TDS Polygon, что и было продемонстрировано в ходе успешного пилота на реальных кейсах Тинькофф.
>
> **Никита Кислицин,**
> Руководитель Департамента сетевой безопасности Group-IB



Результаты работы

Совместно со специалистами Тинькофф было инициировано пилотное тестирование Group-IB Threat Detection System Polygon исключительно на реальных данных, с учетом специфики банка, объемов обрабатываемой информации, типичных сценариев работы и других характеристик реального ИТ-ландшафта компании.

«Пилотный» проект подтвердил качество поведенческих отчетов TDS, позволяющих оценить степень критичности угрозы для банка, а также показал высокую эффективность при выявлении ранее неизвестных векторов хакерских атак.

> В рамках тестирования TDS Polygon показал высокую эффективность работы и правильность выбранной нами стратегии. Сейчас продукт успешно используется в «боевом» режиме.
>
> **Дмитрий Гадарь,**
> Руководитель Департамента информационной безопасности Тинькофф

Group-IB — одна из ведущих международных компаний по детектированию и предотвращению кибератак, выявлению фрода и защиты 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.

60 000+
часов реагирования

1000+
успешных расследований по всему миру

EUROPOL INTERPOL **Официальный партнер**

OSCE **Рекомендована Организацией по Безопасности и Сотрудничеству в Европе (ОБСЕ)**

Узнать больше о тестировании на проникновение от Group-IB

group-ib.ru/audit
ac@group-ib.com