GROUP-IB AND TINKOFF

A stronger defense shield thanks to Group-IB’s Threat Hunting Framework, Polygon module
TINKOFF ECOSYSTEM

Tinkoff is an online financial ecosystem centered around the needs of its customers.

Tinkoff offers a comprehensive range of financial services for both individuals and businesses. With a focus on lifestyle banking, the Tinkoff ecosystem helps customers assess and plan personal spending, invest savings, earn loyalty program rewards, book trips, buy movie tickets, make restaurant reservations, and much more.

All Tinkoff services are accessible via its mobile application and the Tinkoff.ru website.

The Tinkoff ecosystem is branchless. Its proprietary network made up of 2,500 smart couriers delivers the company’s products anywhere in Russia in the shortest time possible, and customer services are handled online and via the company call center. Tinkoff actively uses AI and machine learning technologies to streamline communication: more than 35% of customer chat queries are resolved with no staff involvement.

All Tinkoff products and most of its IT systems have been developed in-house. More than 70% of the bank’s HQ staff are IT specialists.

At the core of the ecosystem is Tinkoff Bank, which was founded in 2006 and has since become one of the world’s largest independent direct banks, with more than 10 million customers. In recent years, Global Finance has named Tinkoff Bank the world’s Best Consumer Digital Bank (2018), the Best Consumer Digital Bank in Russia (2015, 2016, 2018, 2019), and the Best Consumer Digital Bank in Central and Eastern Europe (2019). The Banker recognized Tinkoff Bank as the Bank of the Year in Russia on two occasions, in 2013 and 2017.

The bank’s parent company, TCS Group Holding PLC, is listed on the London Stock Exchange (since October 2013) and the Moscow Exchange (since October 2019).
Background

Tinkoff is a financial ecosystem built around Tinkoff Bank, Russia’s first and only 100% online bank serving more than ten million customers remotely through online channels and a contact center. The bank’s unique structure imposes high requirements on the level of information security for both internal IT systems and financial products and services.

In light of this, Tinkoff’s key priorities are twofold: stable uninterrupted operational processes combined with preventive protection against a wide range of cyberthreats that endanger the bank’s daily operations.

Despite the popularity of anti-virus software, it is often ineffective against targeted attacks, ransomware outbreaks, attacks on payment infrastructure using social engineering techniques, illegitimate use of company resources for crypto mining, and similar threats.

Anti-APT products play a key role in identifying zero-day threats (previously unknown ones). Such products allow for multilateral analysis of malicious files in a “sandbox”, i.e. an environment isolated from the bank’s main network.
Challenge

Initially, Tinkoff used a sandbox designed by a leading international vendor. However, practice showed that the existing configuration was not enough.

The bank decided to improve its detection capabilities by focusing on a layered defense involving several sandboxes.

After testing many products, the bank decided to include Group-IB’s Threat Hunting Framework (THF), Polygon module in the stack.

“It is crucial that we identify new types of threats as quickly as possible and respond to them promptly all the while limiting potential risks. As such, we decided to develop our range of sandboxes and to focus on detecting zero-day threats.

Zero-day attacks are arguably the most dangerous. They can be detected only through intelligent behavioral analysis systems that examine files before they reach a user’s computer.”

Dmitry Gadar,
Head of Information Security at Tinkoff
Group-IB’s solution
Group-IB Threat Hunting Framework, Polygon module

Description
Group-IB THF is a comprehensive solution that helps identify targeted attacks and unknown threats, hunt for threats within the protected perimeter and beyond, and perform incident response and investigation.

Group-IB THF identifies infections that are usually overlooked by typical security tools such as anti-virus software, firewalls, and intrusion prevention systems.

Group-IB Polygon is designed as a module for detonating files in isolated environments, extracting indicators of compromise, and enriching them. The main purpose of Group-IB Polygon is to detect malicious code in email attachments, files being downloaded, and links — by any means possible.

“Effective anti-APT solutions should not only perform static and dynamic file analysis, but also counter various techniques used by attackers to detect OS virtualization and bypass threat detection solutions in other, relatively diverse, ways. The devil is in the detail. Even seemingly simple issues (such as link analysis, support for hundreds of file formats, links that change their state over time) are serious challenges for vendors of anti-APT products. It is also important that behavioral reports are complete and comprehensive. A detailed analysis of the object’s actions and changes that occur in the system help the analyst working with the system determine independently whether the verdict is accurate and how dangerous the file is. Polygon successfully solves such tasks, which was demonstrated during a pilot project involving real-life Tinkoff cases.”

Nikita Kislitsin,
Head of the Network Security Department at Group-IB
Results

Pilot testing of Group-IB’s Polygon was launched together with Tinkoff specialists. It was based on real-life data alone, taking into account the bank’s specific characteristics, the amount of processed information, typical work scenarios, and other features of the company’s real IT landscape.

The pilot project confirmed the high quality of THF behavioral reports, which allowed for accurate assessments of threat levels. It also showed solution to be highly efficient when identifying previously unknown vectors of hacker attacks.

”During testing, Polygon proved to be highly effective and confirmed that we chose the right security strategy. We are now using the product in «combat» conditions, with excellent results.

Dmitry Gadar,
Head of Information Security at Tinkoff
Group-IB is an international leader in detecting and preventing cyberattacks, identifying fraud, and protecting intellectual property online.

According to Gartner, IDC, and Forrester, Group-IB is one of the world’s key providers of Threat Intelligence, with a database containing more than 100,000 cybercriminals’ profiles.

Group-IB’s clients include major banks, financial organizations, industrial and transport corporations, IT and telecommunications providers, and retail and FMCG companies in 60 countries.

Learn more about Group-IB’s Threat Hunting Framework

65 000+
hours of incident response

1200+
investigations worldwide

Official partner

EUROPOL
INTERPOL

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

OSCE

Learn more about Group-IB’s Threat Hunting Framework

group-ib.com/thf
thf@group-ib.com