Success story

GROUP-IB TDS AT THE FOREFRONT OF PROTECTING A TOP RUSSIAN BANK

БАНК СОЮЗ

Founded:

1993

Industry:

FINANCE AND BANKING

Main shareholder:

IPJSC INGOSSTRAKH

Main activities:

RETAIL, CORPORATE, AND INVESTMENT BANKING BUSINESS SERVICES; SERVICES FOR WEALTHY PRIVATE CLIENTS

SOYUZ BANK

Soyuz Bank has been operating for more than 25 years and offers a full range of banking products for both individuals and companies. The bank's regional network includes 30 branches and covers Russia's main industrial and cultural centres.

Customers of Soyuz Bank are able to quickly open business accounts, receive covered (deposited) letters of credit, and enter into bank account/bank deposit agreements, both in roubles and foreign currencies.

- Standard & Poor's rating agency assigned Soyuz Bank its long-term and short-term foreign currency "B" rating with a stable outlook.
- RAEX rating agency assigned Soyuz Bank its ruBB+ credit rating with a stable outlook.
- ACRA rating agency assigned Bank Soyuz its "BB+(RU)" credit rating on a national scale; the rating outlook is "Positive".

Introduction

Soyuz Bank has enjoyed its customers' trust for more than 25 years. In this time, technology has evolved drastically and bank has always been at the forefront of digitalisation, introducing technological solutions that are both convenient for customers and optimal for internal business processes.

Digitalisation increases the quality of banking services, but equally it increases the risk of cyberattacks. Soyuz Bank takes a serious approach to the security of its systems, service channels, and customers. Among other measures, the bank introduces innovative protection solutions and uses data on new threats to adapt its security tactics and strategies.

Challenges

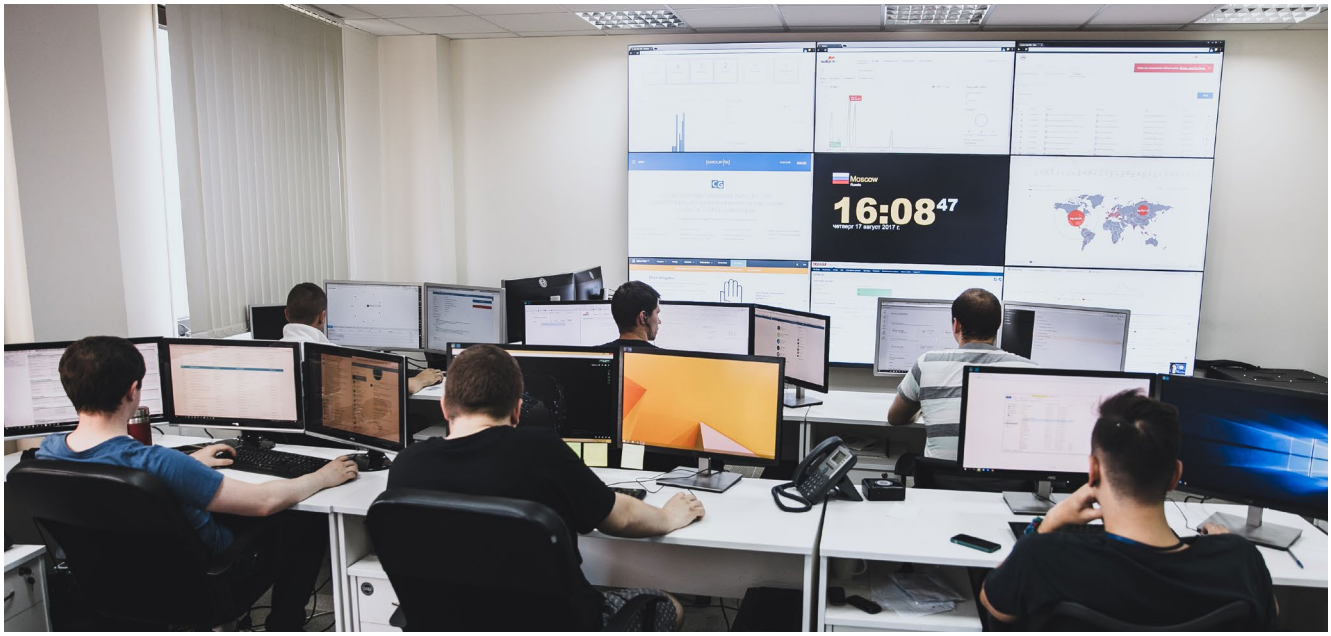
In light of the rapidly evolving threat landscape, Bank Soyuz decided that it needed a solution to protect the company against new threats. The established "traditional" security systems (antivirus software, IDS) were suitable for their main tasks, but they did not detect new types of attack. It was important that the bank's protection system be able to detect malicious activity even in cases where attackers used legitimate tools.

Group-IB's experience and expertise, proprietary Threat Intelligence system, and real-time data enrichment made the company stand out from its competitors. Group-IB TDS helped Soyuz Bank perform in-depth analysis of traffic and conduct behavioural analysis of files in an isolated environment in order to detect threats that were overlooked by traditional solutions.

> Effective detection of new threats combined with the solution's costs and implementation time (installation took about a week) make TDS a truly unique product.

Svyatoslav Berezin,
Head of Information Security
at Soyuz Bank

Success story: "Soyuz Bank"



Group-IB's solution

TDS Sensor for network traffic analysis and TDS Polygon for dynamic file analysis in an isolated environment

Use cases

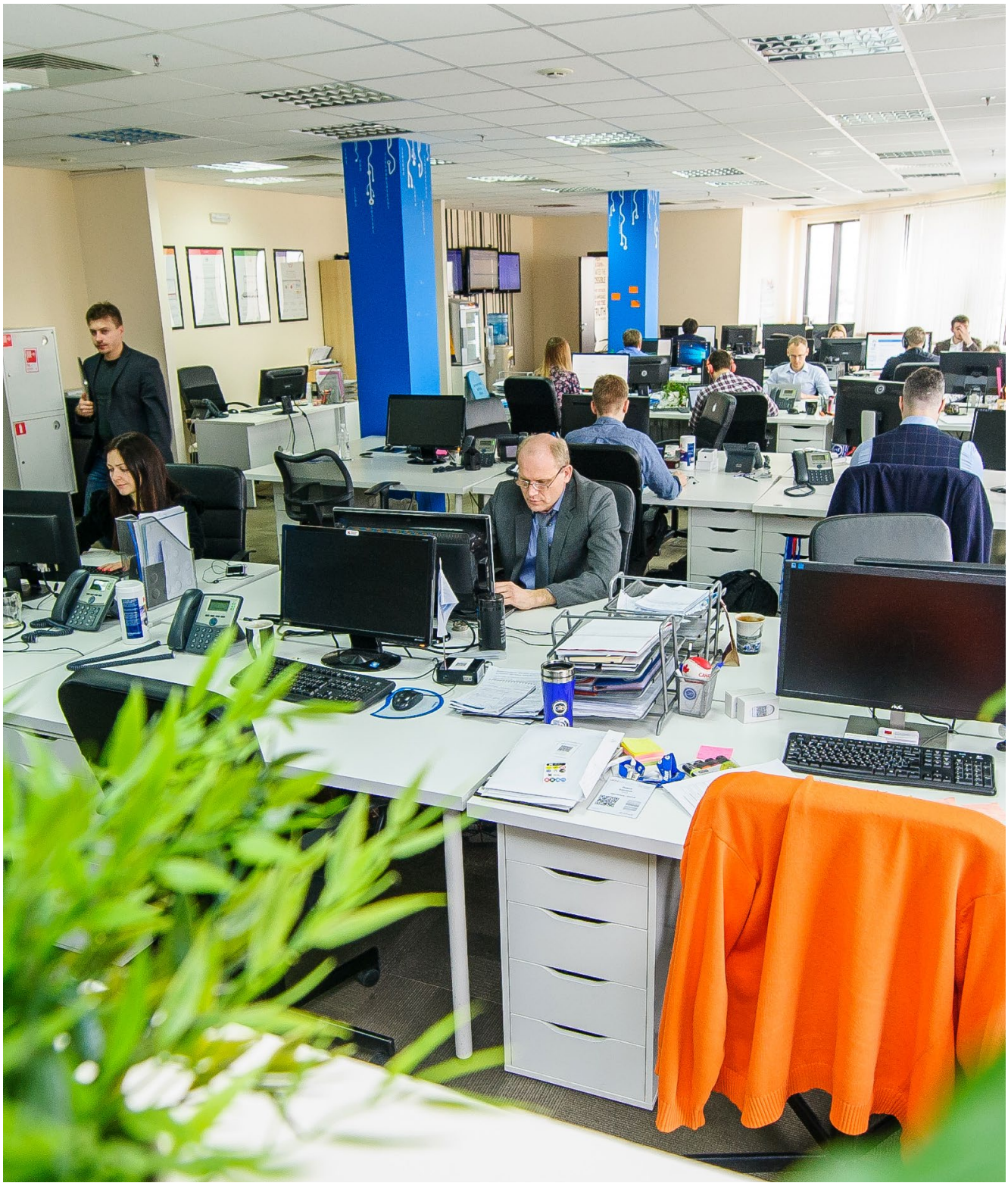
Soyuz Bank has created its own Security Operations Center (SOC), whose team is responsible for monitoring and responding to cybersecurity incidents. SOC specialists regularly use TDS to obtain valuable information about system failures, potential threats, and incidents, which is updated 24/7 in real time in the management console.

The bank's incident response team successfully counteracts current attacks. However, threats are often difficult to predict and the experience of other banks shows how important it is to work with external experts in the case of particularly complex incidents. Soyuz Bank has not yet faced such challenges, but it has prepared for them. Corresponding contractual relations have been established between the bank and Group-IB: in the event of an attack, the bank can promptly receive expert assistance in incident response and forensics to quickly prevent damage.

The bank's departments regularly report to senior management and the Supervisory Board. Some of the data obtained from TDS is included in regular reports and graphs that reflect the malicious activity dynamics and threat prevention results.

Results and prospects

The main criterion the bank uses to assess the solution's effectiveness is the quality and completeness of the detection of complex threats. Group-IB's system covers a wide range of security tasks and increases the security level of critical assets. The solution has been successfully used for 3 years and plays a key role in the first line of defence with regard to the bank's security.



Group-IB is one of the global leaders in detecting and preventing cybercrime, providing best-in-class anti-APT and anti-fraud solutions, and protecting intellectual property online.

According to **Gartner**, **IDC**, and **Forrester**, Group-IB is one of the key providers of Threat Intelligence in the world, with more than 100,000 profiles of cyber criminals in its database.

Group-IB's clients include top banks and financial organizations, business corporations and transport companies, IT companies and telecommunications service providers, and retail and FMCG brands in more than 60 countries

16 YEARS
of experience in cybercrime investigation and analysis

1000+
investigations worldwide

EUROPOL INTERPOL **Official partner**

OSCE **Recommended by the Organization for Security and Cooperation in Europe (OSCE)**

Find out more about Group-IB Threat Detection System

group-ib.ru/tds
demo@group-ib.com