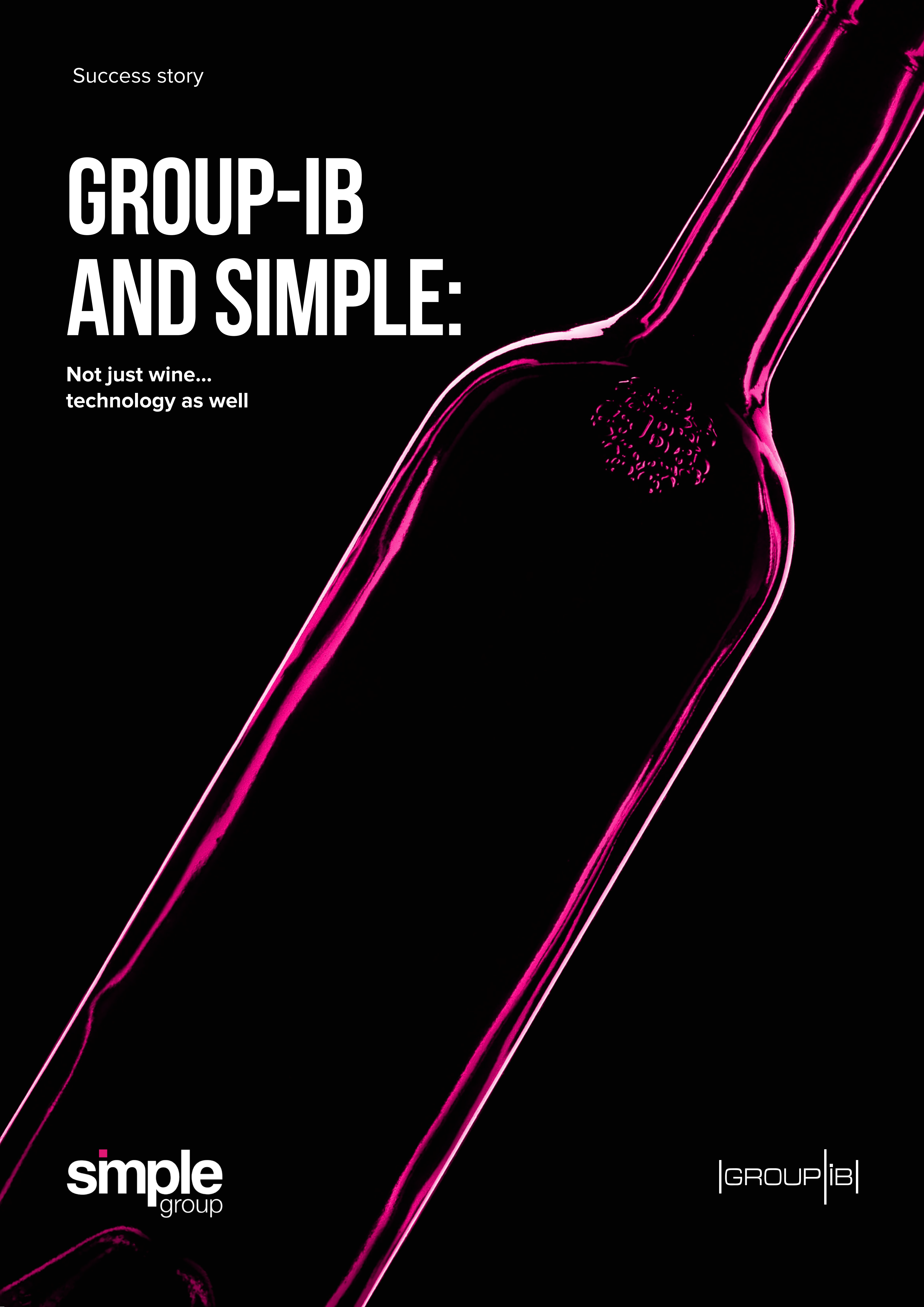
Success story

GROUP-IB AND SIMPLE:

Not just wine... technology as well



simple group

GROUP IB

GROUP IB

80+
cities and towns
in Russia

2,000+
highly skilled
employees

>500
exclusive
suppliers

Simple Group

Simple Group is one of Russia’s leading wine importers. The national distributor and retailer boasts a dynamically developing network of wineries. Its online store operates under the retail brand SimpleWine.

For more than 25 years, Simple has gained the trust of the most prestigious wineries across the globe.

Simple’s mission is to raise people’s quality of life by reviving the wine culture in Russia.

An integrated business approach gradually transforms this goal into practice, from wine restaurants and bars (Grand Cru and Simple Bar) to the Simple Media publishing house (Simple Wine News, swn.ru) and the Enotria wine school.

Founded:
1994

Industry:
ALCOHOL

Activity:
IMPORT AND DISTRIBUTION OF HIGH-QUALITY ALCOHOL PRODUCTS IN RUSSIA, RETAIL

Employees:
2,000+

simple
group

Background

Simple’s mission is to enhance people’s quality of life by reviving the wine culture in Russia.

An integrated business approach gradually transforms this goal into practice, from wine restaurants and bars (Grand Cru and Simple Bar) to the Simple Media publishing house (Simple Wine News, Wine Stage) and the Enotria wine school. An integral part of Simple’s success lies in its advanced IT infrastructure. Thanks to unique IT systems and stringent requirements when it comes to information security, Simple guarantees its partners and customers reliable, high-quality services.

As any business grows, it becomes more vulnerable to attacks. In turn, software and hardware solutions become increasingly difficult to manage, and monitoring updates in a timely manner becomes a true challenge.

What’s more, the retail industry faces additional threats in the form of vulnerabilities in cash register equipment, which often lacks the latest software.

> We used several traditional security tools at the same time, yet we still came across false positives and undetected malware. One of the weakest links in our infrastructure is cash registers. Operating system manufacturers rarely provide updates and the OS versions themselves are outdated. The products we used to protect against complex threats in the past were ineffective and unable to solve the tasks required. That is why we decided to look for a more efficient, easy-to-manage, and scalable solution.
>
> **Vladimir Bondarev,**
> Head of the Infrastructure and Support Division, IT Department at Simple

Why Group-IB

Simple's Security Department was tasked with finding a comprehensive and high-quality solution that would better protect the company's corporate network and identify malicious files more effectively. The company needed a solution that could both detect abnormal traffic within the network and analyze the behavior of infected files in an isolated environment.

Candidates for a pilot project included several companies whose anti-APT solutions analyzed malicious file behavior in a "sandbox", i.e. an environment isolated from the main network.

Group-IB's solution stood out from the rest thanks to its innovative technologies and tools used for file analysis.

During testing, Group-IB's software detected several malicious files that were overlooked by the other solutions. The latter failed to identify emails with password-protected archives and files with malware that runs pending tasks.

Another factor that played a key role in Simple's supplier selection process was Group-IB's extensive experience in investigating cybercrimes, tracking threat actors, and analyzing related information.

> For large companies like Simple, a high-quality solution against complex attacks is essential. Modern APT groups use various techniques to infect corporate networks, which can lead to customer data and money being stolen and can inflict reputational and financial damage on the company. Together with Simple's own specialists, we implemented a comprehensive project designed to detect modern attacks and defend against them. The collaboration between Group-IB's experts and Simple's incident response specialists helped achieve an unparalleled level of security.
>
> **Anton Fishman,**
> Head of the System Solutions
> Department at Group-IB

Group-IB's solution

Group-IB Threat Hunting Framework (THF):
Sensor and Polygon modules

Description of Group-IB's solution

Group-IB THF is a comprehensive solution designed to identify targeted attacks and unknown threats, hunt for threats within the protected perimeter and beyond, and carry out incident response and investigation.

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

Sensor is a THF module for analyzing incoming and outgoing data packets. Sensor uses Group-IB THF's own signatures and behavioral analysis rules to detect common network anomalies, abnormal device behavior, and interactions between infected devices and hackers' C&C servers. Moreover, the module extracts objects from various sources and sends them to Polygon for analysis.

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

> Thanks to its technology allowing for in-depth file analysis and detonation of malicious payloads, Group-IB Polygon significantly increases any organization's level of protection against key initial infection vectors. We are delighted that our solution, delivered as a cloud service through Polygon Cloud, was appreciated and adopted by such a valued client as Simple.
>
> **Nikita Kislitsin,**
> Head of the Network Security
> Department at Group-IB

Results

Group-IB's solution met the customer's expectations in every aspect. Integrating it into the wine merchant's existing infrastructure took only a week thanks to the joint efforts of both companies' employees.

The number of false positives has plummeted, and Simple's Security Department now promptly receives a comprehensive analysis of any incidents identified. THF also displays a summary of information on the system's current state on a TV screen to ensure faster incident response.

Sensor detects suspicious events and additionally examines them on related systems such as firewalls and web mail gateways. Any malicious files detected are sent for analysis to Polygon. Polygon then runs the infected files in an isolated environment for the purpose of malware analysis. If the file does not run in the selected environment, it is restarted in another environment.

The module uses various methods to hide the virtualization. After the object is placed in the selected virtual environment, the solution emulates a wide range of real-user actions, from mouse movements and keystrokes to clicking on links and downloading, opening, and running files. Moreover, it logs the file execution in full and records a video.

> The number of false positives is now so low that we sometimes even forget that we're using THF! We would like to express our sincere thanks for such a well thought-out user interface. Barely any effort is required to learn how to manage the system, which is incredibly user-friendly. In the months that we've been using THF, the solution has saved our security specialists considerable amounts of time, which they can now spend on developing infrastructure, introducing new technologies, and taking part in training courses.
>
> **Vladimir Bondarev,**
> Head of the Infrastructure and Support Division, IT Department at Simple

|GROUP|iB|

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.

65 000+
hours of incident response

1200+
investigations worldwide

EUROPOL INTERPOL **Official partner**

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

Learn more about Group-IB's Threat Hunting Framework

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