

Information Security

ENSURING CYBERSECURITY IN THE DIGITAL AGE: THE FUND'S ROLE AND RESPONSIBILITY

Information security is an integral part of stable operation of the information network, protection of national interests and maintenance of trust on the part of society and partners. With the development of digital technologies, Samruk-Kazyna JSC constantly increases the level of information security to prevent cyber threats, as

well as brings information security requirements in line with legislative norms.

The Fund's key strategic objectives in this area are to ensure accessibility, integrity, confidentiality and sustainability.

CREATING A CULTURE OF SAFETY

As part of strengthening information security in accordance with the requirements of the international standard ISO 27001, work was carried out to analyse and optimise the IT infrastructure.

According to the conducted maturity assessment of information security processes, in which 11 domains were assessed according to CobiT 4.1 DS5 (Deliver and Support), the information security management system corresponds to a "certain level" of maturity.

The Fund implements best practices, defines processes, policies, procedures, and documents key actions in the field of information security. Responsibility and accountability are defined, process owners are appointed. There is formalised and structured communication of information to the Fund's management.

Physical Infrastructure.

The comprehensive survey identified existing problems, potential points of failure and vulnerabilities in the IT infrastructure.

Detailed documentation of the changes made and recommendations for a smooth transition to the updated configuration with minimal risk and disruption were prepared.

As a result of this work, the reliability, security and efficiency of the IT infrastructure have been significantly improved, which will ensure its stable functioning and compliance with modern requirements.

Training.

Training sessions and testing using specialised software are conducted to develop cyber hygiene skills among the Fund's employees.

SHAPING EFFECTIVE INFORMATION SECURITY POLICIES

The Fund's Group of Companies implemented the Corporate Information Security Standard regulating the general set of rules for ensuring information security and managing the process of coordination of activities. The Fund implemented the requirements of the "Basic Rules of Information Security" and the relevant rules and regulations.

Within the framework of effective management of the process of categorisation of the Fund's

information assets, establishment of information security requirements for protected information assets, as well as assignment of access levels to employees, the development of the methodology of classification of information assets in Samruk-Kazyna JSC was initiated. It is planned to implement the process of establishing gradations of importance of information and assigning specific information resources to the appropriate categories according to the degree of their confidentiality.

PROTECTING CRITICAL INFRASTRUCTURE

Server and network equipment placement was optimised to improve performance and serviceability.

Modern software products for monitoring, preventing information leakage, scanning and obtaining operational information on vulnerabilities have been implemented.

COUNTERING CYBERATTACKS

In the conditions of the Fund, a monitoring centre operates to maintain information security systems and promptly respond to external and internal threats to the IT infrastructure.

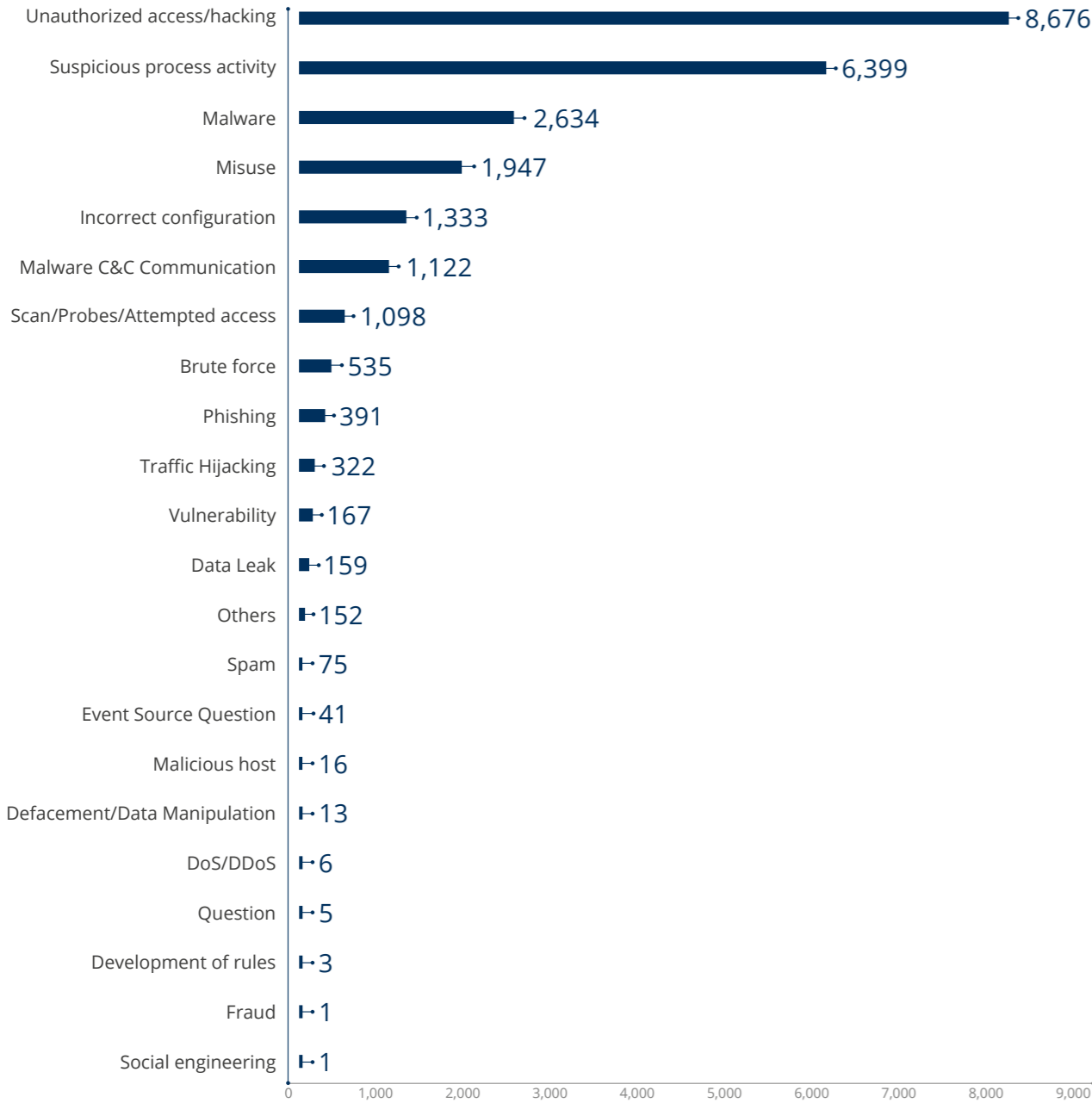
In accordance with the requirements of the Fund's internal documents and applicable information security standards, scans were performed using specialised software at least 6 times during the reporting period

In 2024, audits of the Fund's portfolio companies for compliance with the information security

requirements were conducted, based on the results of which recommendations were developed to improve the level of information security

To identify cybersecurity risks, a list of risk sources and events is compiled to assess the negative impact on the Fund's activities. Quarterly risk reports are also generated.

INCIDENT STATISTICS BY THREAT TYPE FOR 2024 IN THE FUND GROUP



INCIDENT STATISTICS ACROSS THE GROUP, 2024

