Table of contents

4.........................NAIIS

8.........................KOMIB

10.......................Angara Security

16.......................Security Code

20.......................Cryptography Museum

22.......................Cyberus

26.......................CyberED

34.......................Cyberdom

34.......................CyberQ

38.......................Security Vision

NAIIS

National Association for International Information Security (NAIIS) – a non-profit organization established in 2018 on the initiative of the Security Council of the Russian Federation to coordinate the activities of the Association's members to promote the implementation of the state policy of the Russian Federation in the field of international information security. (IIS).

The main objectives of NAIIS activities include:

- assistance in promoting Russian initiatives in the field of IIS provision;
- assistance to Federal legislative and executive authorities of the Russian Federation in their activities to implement state policy in the field of information security, to ensure the national interests of the Russian Federation in the information sphere, as well as to Russian commercial and non-profit organizations, and citizens involved in the implementation of state policy in this area in accordance with the legislation of the Russian Federation;
- contributing to the formation of a system for ensuring the sustainable functioning of global and national information infrastructures for the safe use of information and communication technologies in all spheres of society and public administration.

The founders of the Association are:

Lomonosov Moscow State University,
MGIMO University,
RANEPA,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
Editorial Board of the International Affairs Journal.

The Chairman of the Supervisory Board of the Association:

Oleg V. Khramov,
Deputy Secretary of the Security Council of the Russian Federation.

> «...in the effective implementation of the state policy outlined in the new edition of the Fundamentals of State Policy in the field of International Information Security, it is necessary to make more active use of the capabilities of scientific and expert circles, the business community, including, of course, the National Association for International Information Security.»
>
> **Russian President Vladimir Putin**

Russia-Africa Partnership Forum, 2024

Core areas

- proactive study of problematic issues of ensuring the IIS in the interests of forming the negotiating positions of government agencies; organization of interaction with the Ministry of Foreign Affairs of the Russian Federation and interested federal legislative and executive authorities with commercial and non-profit organizations and citizens contributing to the implementation of state policy in the field of IIS;

- participation within the Russian delegation in the preparation and conduct of expert consultations on the formation of the IIS system in the format of international organizations (UN, OSCE, SCO, CIS, CSTO, BRICS, APEC, G20, etc.), as well as bilateral, multilateral and regional consultations of the Russian Federation with other states;

- preparation, together with interested organizations and federal executive authorities, of proposals to strengthen international cooperation aimed at facilitating the successful implementation of the national project «Data Economy» in terms of information security issues.

Main events and projects

- Annual International Forum «Partnership of State Authorities, Civil Society and the Business Community in ensuring International Information Security». XIX Forum will be held in Moscow on September 16-18, 2025 in a hybrid (live and on-line) format.

- International Conference on the problems of ensuring the International Information Security System (according to the plan of the International Information Security Research Consortium).

▷ NAIIS is accredited to the UN Open-ended Working Group on International Information Security.

▷ The Association acts as a Contact Point for direct interaction between scientific and academic organizations of the BRICS member countries on International Information Security issues.

Publishing activities

- Collections of reports of the XVII and XVIII International Forums «Partnership of State Authorities, Civil Society and the Business Community in ensuring International Information Security»

- The specifics of the policy of the BRICS member states in the field of ICT development, ensuring national and international Information Security

- Collection of materials on the issues of information security of the member States of the League of Arab States

XII 2024
Кластер информационной безопасности
23-25 апреля
Выставочный комплекс ЭКСПОФОРУМ
Санкт-Петербург
МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
СБОРНИК ДОКЛАДОВ УЧАСТНИКОВ XVIII МЕЖДУНАРОДНОГО ФОРУМА
ПАРТНЕРСТВО ГОСУДАРСТВА, БИЗНЕСА И ГРАЖДАНСКОГО ОБЩЕСТВА ПРИ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
16-18 СЕНТЯБРЯ 2024 г.,
Г. МОСКВА, РОССИЯ

See also:

KOMIB

— a time-proven tool for creating a fair, reliable and sustainable International Cybersecurity System.

"Partnership for International Information Security Coordination Centre" (KOMIB) was established by the National Association for International Information Security with the support of the Security Council of the Russian Federation to increase the effectiveness of public-private partnership in international cyber security economic activity.

KOMIB:

- consults foreign partners in the development of state programs for the creation of integrated cyber security systems based on solutions offered by Russian companies;
- recommends foreign partners relevant Russian companies for the implementation of cyber security projects;
- provides necessary approvals for the execution of international cyber security projects;
- assists foreign partners to carry out an independent audit of ongoing complex cyber security projects with Russian companies.

The activities of KOMIB in the G2B format are focused on the needs and interests of Russian telecom operators, IT service providers, as well as manufacturers of cyber security goods and services.

More about us

KOMIB performs both representative and service functions for companies operating in the cyber security market:

- provides business consulting;
- represents the interests of entrepreneurs in government relations;
- provides assistance in the formation of legal environment and business infrastructure;
- facilitates Russian entrepreneurs in establishing business relations with foreign partners.

KOMIB

- has sufficient technical competence;
- possesses the necessary international relations expertise to participate in the creation negotiating positions for consultations in the G2G format;
- analyzes professionally the current situation on international markets and is able to provide reliable predictive assessments for the development of the situation on international cyber security markets;
- has established working relationships with commercial companies for involving concerned organizations in execution projects in the context of the G2G agreements.

АНО КОМИБ
KOMIB.RU
Информационная безопасность России:
суверенитет, проверенный временем.
Russian Cybersecurity:
Sovereignty Approved by Time
Ciberseguridad de Rusia:
Soberanía Confirmada por el Tiempo
Cybersécurité Russe:
une Souveraineté Confirmée par le Temps

ANGARA SECURITY

Angara Security — a group of companies that creates advanced solutions and services in the field of cybersecurity and provides a full range of information security services:

- design, implementation and maintenance of both integrated information security systems (ISMS) and individual solutions;
- cyber resilience management services at all stages of Cyber Kill Chain®, as well as identifying, responding to, and preventing cyber incidents, and analyzing the security of information infrastructures.
- secure development services, consulting and auditing, and more.

Cybersecurity services

Cyber incident monitoring and management (SOC and MDR)

Round-the-clock monitoring of cyber incidents at all stages - from prevention and detection of cyber incidents to response and elimination of consequences.

A software product stack based on SOAR, SIEM, and EDR class systems, as well as proprietary ML scripts, is used to provide the service.

Digital forensics and cyber incident response

Responding to cyber incidents, eliminating their consequences, and examining samples of malicious software.

We provide a detailed response report, reconstruction of the incident events, and recommendations for improving the security of the information infrastructure to prevent similar incidents in future.

Digital footprint analysis and DRP

Collection and analysis of information from open sources in both indexed and non-indexed segments of the Internet (including messengers, social networks, etc.), which may indicate

- an accomplished or planned computer attack on the organization;
- theft and/or sale of confidential information;
- the use of the company's branding for phishing purposes.

Attack Surface and Internal Assets Mar

The service allows you to receive data on the current stat
and internal perimeter, as well as all the necessary infor
to eliminate the most critical vulnerabilities. It consists o
continuous automated scanning of the external perimeter
and assets inside the infrastructure in order to identify new hosts, network ports and vulnerabilities.

The results obtained are verified, whereat they are ranke
according to the degree of criticality and formed into a lis
of identified vulnerabilities and shortcomings.

CYBERSECURITY SOLUTIONS

Implementation, support, audit

Internal and external penetration testing

Checking the security level of infrastructure and applications by simulating the actions of an attacker. It also demonstrates attack vectors that can be implemented using the identified vulnerabilities. The works can be carried out from the Internet or by connecting to a corporate network.
Penetration testing will help to:

- assess the current level of cybersecurity of your infrastructure.;
- check the effectiveness of the cyber defense system.;
- get detailed recommendations on how to fix the vulnerabilities found.

Mobile and Web application Analysis

Assessment of the security status of applications as a separate information system. The work is carried out taking into account generally accepted practices and recommendations OWASP и SANS/CWE. Not only the technical aspects are being checked, but also the business logic of applications and the possibility of attacks on the clients.

Detecting weak passwords

Checking whether passwords used in the corporate network are resistant to hacking or tampering. When performing these tasks, we make a copy of the NTDS (Active Directory) database, depersonalize it, and search for frequently occurring, leaked, or easily guessed passwords. The customer receives a list of those accounts that can be compromised in a short time using online brute force techniques and information about public authentication data leaks.

Social engineering methods testing

Checking the awareness of employees about attacks using social engineering methods. Various scenarios and legends are being developed that exploit human weaknesses
(curiosity, fear, greed, etc.).

Scenario options:

- different types of mail phishing (phishing, spearphishing);
- voice phishing;
- imitation of infected carriers.

Red Team Operations

Verification of the adequacy and correctness of security event monitoring processes (SOC, SIEM, IRP...) by simulating real attacks on the infrastructure using advanced techniques and tools. In the course of operation, the close interaction with the security team is performed to identify possible gaps in the correlation rules, shortcomings in the configurations of information security tools or incident response processes.

Information security risk assessment services

Identification of the main IS risks and priority areas for the development of the information security system. The service offers the collection and analysis of initial data on the company in terms of business processes and IT infrastructure, the development of an IS risk assessment methodology and the conduct of an IS risk assessment itself.

Comprehensive protection of computer systems

Creation of an integrated information security system, providing for the implementation of organizational and technical measures to meet the requirements of legislation and international standards for the creation of information systems protection and security.

Application source code analysis

The service uses both automated tools (scanners) and manual analysis. The subject of the analysis is the unique source code and the third—party components (dependencies) used in it, which may contain known vulnerabilities.

In addition, a deep search for secrets inside git repositories can be conducted in order to identify their potential compromise.

Creating a secure development process

As part of the service, a detailed analysis of the DevSecOps development processes and infrastructure is carried out, including:

- audit of the maturity level of the IS development process;
- audit of the secure configuration of the infrastructure. DevSecOps;
- creation of a roadmap for improving the security and cybersecurity of both the application code and its environment.

Information security audit

Detailed analysis of the IT infrastructure and information security processes for compliance with legislation and international standards (including ISO/IEC 27001)

The service includes an audit of information security processes, technical audit, penetration testing and preparation of the technical papers.

CYBERSECURITY PRODUCTS

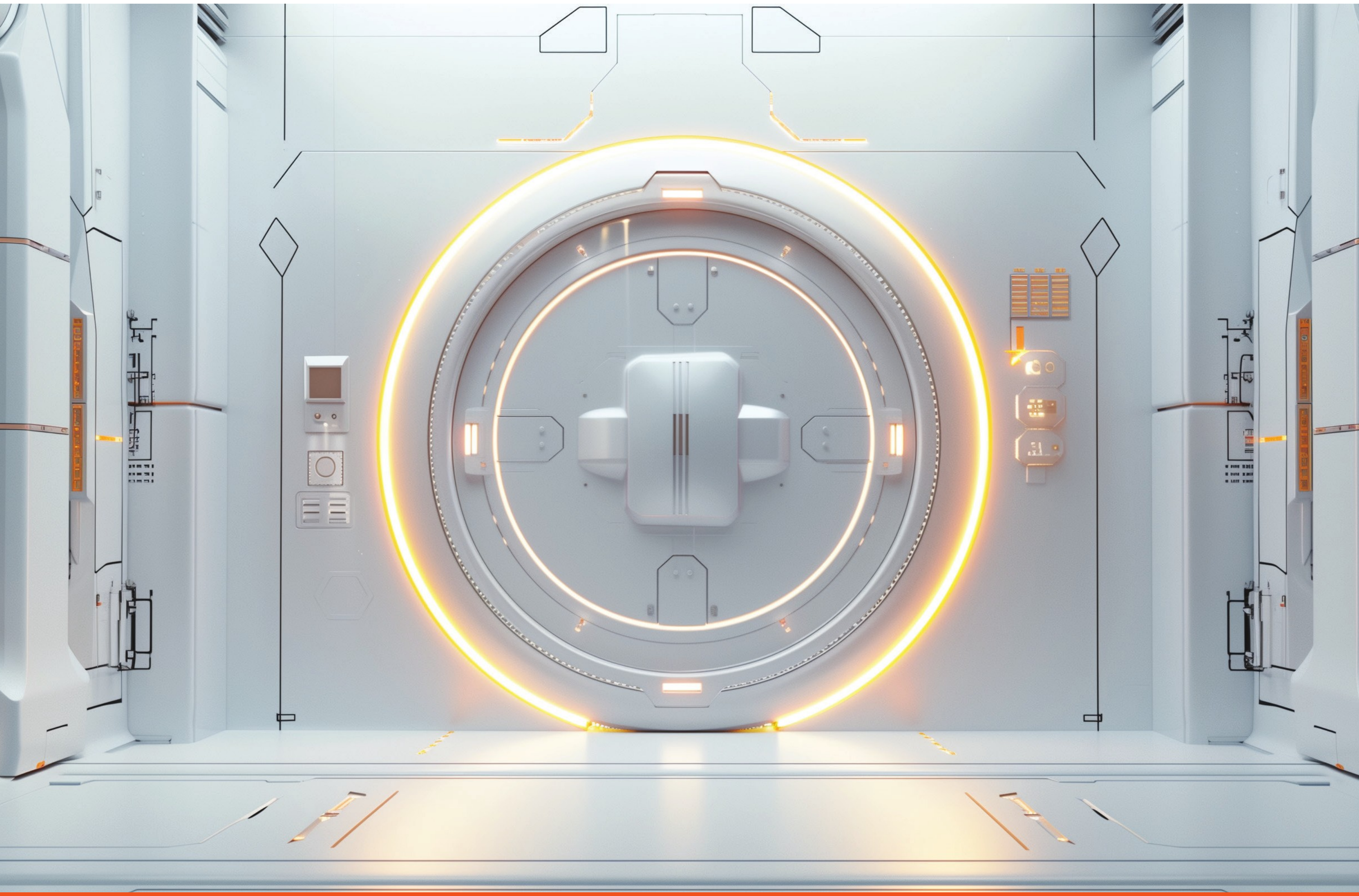
Angara ECHO

A digital footprint management platform. Angara ECHO performs automated monitoring and analysis in indexed and non-indexed sources to detect sensitive information swiftly.

It is much cheaper to take preventive measures than to respond to an IS incident and eliminate its consequences. Angara ECHO will allow you to prepare for the attacks properly or even prevent them at all.

Blazar NAC

Russian Network Access Control class solution. Provides protection of information resources from unauthorized access by configuring and strictly following access policies to the corporate network.



ANGARA SECURITY

ANGARA
SECURITY

SECURITY code

Security Code is a Russian developer of a wide range of software and hardware protection of information systems that meet the requirements of Russian and international standards.

The Security Code protection tools form a single security ecosystem and are designed to protect key elements of IT infrastructure: The company develops several product lines united by a common architectural concept and focused on providing comprehensive security of key components of the IT infrastructure. This approach allows our customers to develop their information security system gradually.

Security Code products are used to protect confidential information, personal data, as well as information constituting state and commercial secrets.

There are more than 3 million jobs under the protection of the Security Code.

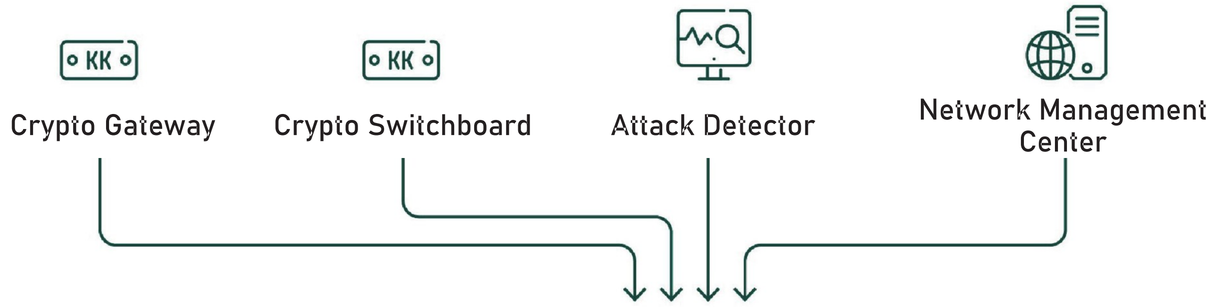
Today, Security Code products are used **more than 50,000 organizations** including government agencies and large commercial companies.

NGFW Континент 4

SCENARIOS:

- External perimeter protection;
- Datacenter network segmentations;
- Distributed networks protections;
- Protection of technological networks.

FEATURES

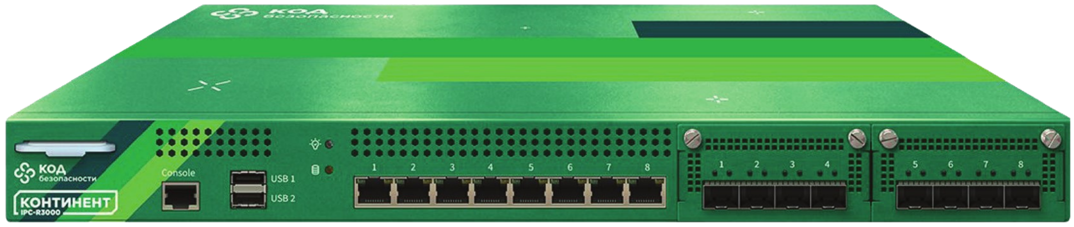


Security Node

FW	IPS	App Control	L2 VPN	L3 VPN	MGMT	Threat Intelligence	Log	URL Filtering

Antivirus	GeoIP

The solution covers all the needs of customers in both small devices and high-performance devices.



High-performance devices

Medium devices

Security Code Orchestrator

SCENARIOS:

- Centralized management of Security Code products
- Unified monitoring system
- Bus integration of heterogeneous products

FEATURES:

Unified Protection Mechanism management Console

Data sources

Creating the organizational structure of the company

Policies

Formation of hierarchical group policies

Applying the resulting policies

Actions

Security Policy Settings

Execution of operational commands

Analytics

Flexible dashboard display settings

Collecting logs

Scalability

Cross-platform

Extensibility

SECURITY code

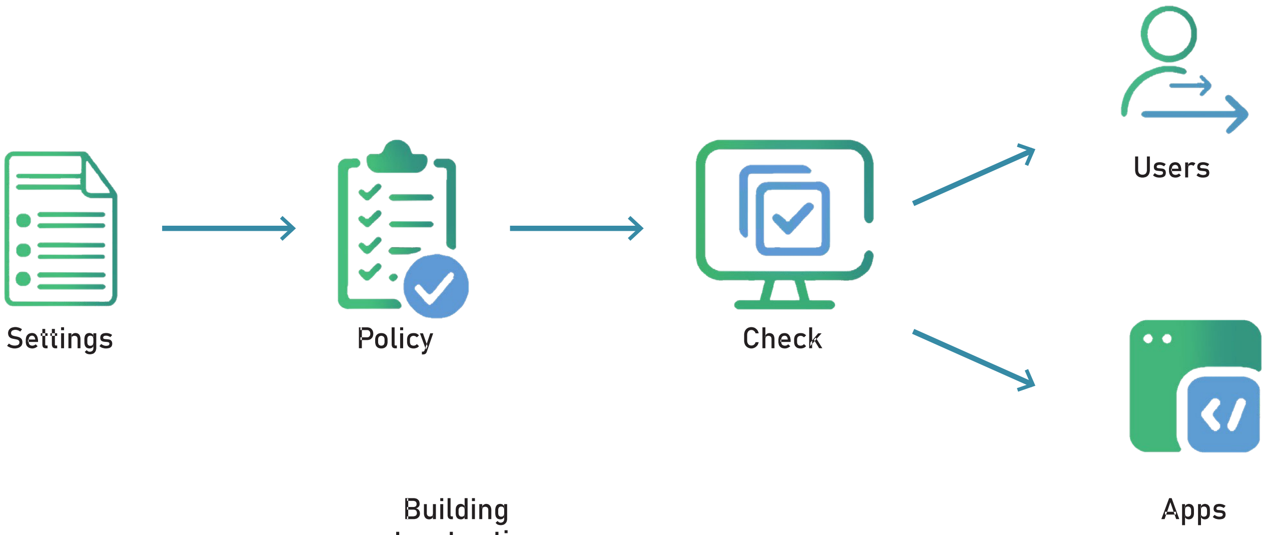
S ecret Net EDR

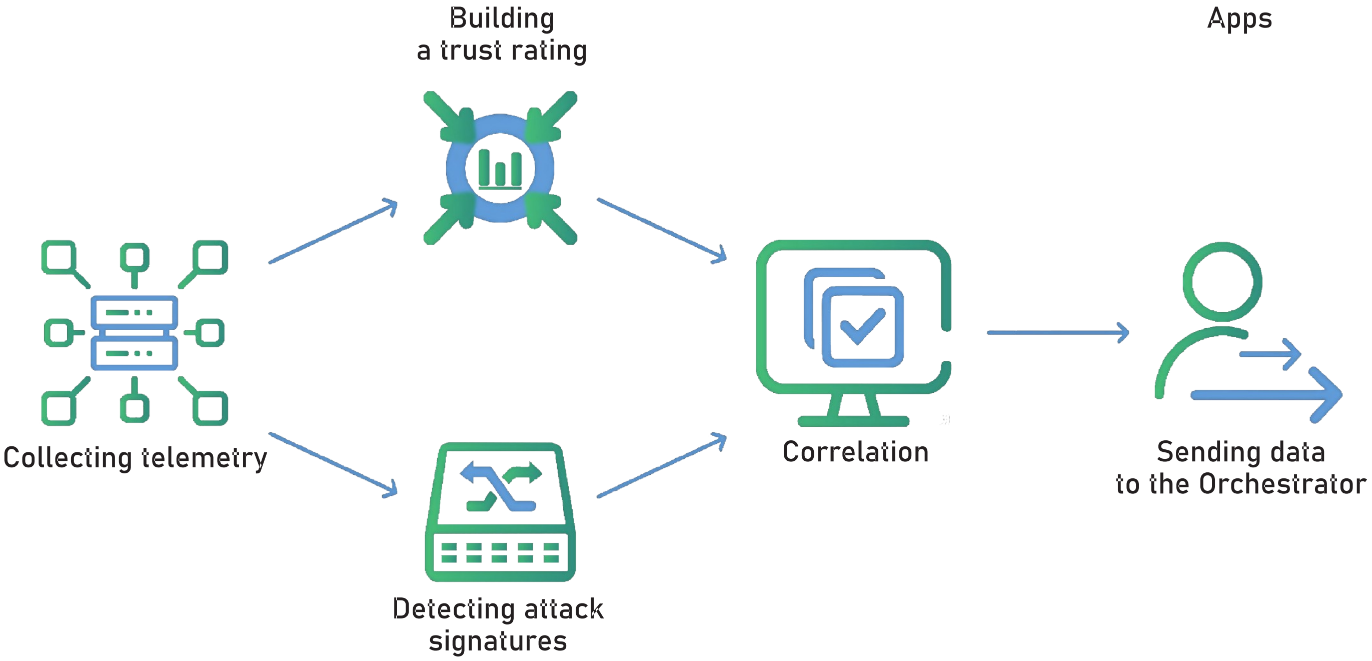
SCENARIOS:

- Collecting and processing telemetry from target devices
- Detecting signs of malicious activity
- Forming a trust rating for the end device for further use by other means of protection
- Checking the endpoint for compliance with security requirements

FEATURES:

Checking for compliance with parameters





CRYPTOGRAPHY MUSEUM

The Cryptography Museum –

the first and only scientific and technological museum in Russia dedicated to cryptography, related disciplines and communication technologies, was opened to the public in December 2021.

The museum is located in Moscow, in a historic building at 25 Botanic Street, built in 1885 as Orphanage by Alexander and Mary for the children of poor priests. For more than 60 years, the building was occupied by schools, orphanages and a special prison - the famous Marfa Sharashka, where prisoners and freelance scientists worked together from 1947 to 1954 to create a secret communication technology.

In the 1950s, Sharashka was transformed into a Scientific Research Institute of Automation. The building remained classified until 2019, when it was transferred to the Cryptography Museum.

The permanent exhibition of the museum tells about the past, present and future of cryptography and communication technologies, about people and inventions that have changed the world. It includes four sections and is built in reverse chronology: from the digital age and computers the route leads to the industrial era, when radio, telephone, television and telegraph were created. Then — to the era of pre-machine cryptography, when letters were the main means of transmitting information.
And finally, to protocriptography — the origin of the very idea of written communication through alphabetic systems and signs. A separate, fifth section of the museum is dedicated to the history of the building and the people whose destinies were intertwined with it.

CRYPTOGRAPHY MUSEUM

The exhibition presents a unique collection of encryption technology and archival documents, most of which are being shown to the general public for the first time, as well as specially created interactive, multimedia and gaming exhibits explaining in simple language to children and adults the essence of complex cryptographic mechanisms and mathematical concepts. They can help you to solve cryptographic riddles, understand the structure of complex encryption systems, learn about the secrets of secure communication in different eras, establish the interrelation between cryptography and important historical events, as well as take a glance to the future.

In the exhibition halls and public spaces of the museum you can also see works of media art that complement the main exhibition and create a special narrative about the impact of science on the life of a human-being and society. The museum's exposition and public spaces are designed to meet the needs of a wide variety of visitors. The museum holds a publishing program, lectures and master classes, film screenings and conferences, temporary exhibitions and other events that meet the main mission of the museum — enlightenment and popularization of science and technology.

Cyberus

We support partner countries in strenghtening their cyber sovereignty

In today's world, cyber sovereignty is becoming a top priority for countries seeking to ensure their security, economic independence, and the well-being of their citizens. Effective national cybersecurity industry not only protects against cyber threats, but also shapes the future of the digital environment, defines a culture of security, and creates the foundation for economic growth.

Cyber sovereignty as the foundation of a nation's prosperity

Cyber sovereignty is an integral component of the independence of the state, its ability to substantively protect national cyberspace, objectively assessing the level of cybersecurity and excluding dependence on other states or foreign corporations. This is a matter of strategic planning and public administration that affects the interests of all sectors of society.

Homeland security

Without control over its own digital resources, a country risks becoming vulnerable to interference from other states or cybercriminals.

Economic independence

The development of proprietary technologies and security systems helps to reduce risks from other countries, ensure economic independence and stimulate internal innovation.

Social welfare

Protecting citizens' data from leaks and fraud is not only a matter of confidentiality, but also a key element of trust in government institutions.

SPIEF, 2024. Signing of an agreement with Oman in the presence of the Minister of Commerce, Industry, and Investment Promotion Qais bin Mohammed Al-Yousef.

Role of the state in digital development

Cyber sovereignty promotes the creation of a sustainable digital environment. The development of a national cybersecurity strategy makes it possible to establish effective cooperation between various levels of government and the private sector, forming a unified cybersecurity policy.

Innovations and talent development

Cyber sovereignty opens up opportunities for the development of the domestic IT market, attracting talents and innovations. Intellectual property protection and support for cybersecurity startups can significantly strengthen the country's position on the global stage.

Global cooperation

Cyber sovereignty stimulates international cooperation. The exchange of experience with other states in the field of cybersecurity makes it possible to create a global network of protection against cyber threats. Achieving the cyber sovereignty of the state is based on three interrelated processes: measuring the effectiveness of the state's cyber defense, developing human capital and national technological competencies.

How Cyberus helps partner countries build cyber sovereignty

Cyberus is a foundation for the development of effective cybersecurity, uniting the forces of cyber defense technology developers, business and the state to build a secure digital future for Russia and the world.

Based on the expertise and experience of Russian companies in the field of cybersecurity and with the state's support, Cyberus is forming a unified country proposal for the development of the cybersecurity industry to achieve the cyber sovereignty of the partner country.

The Foundation offers solutions that transform national industries and create a sustainable foundation for their independent and self-sufficient development.

Three interconnected Cyberus meta-products

1 Human capital development

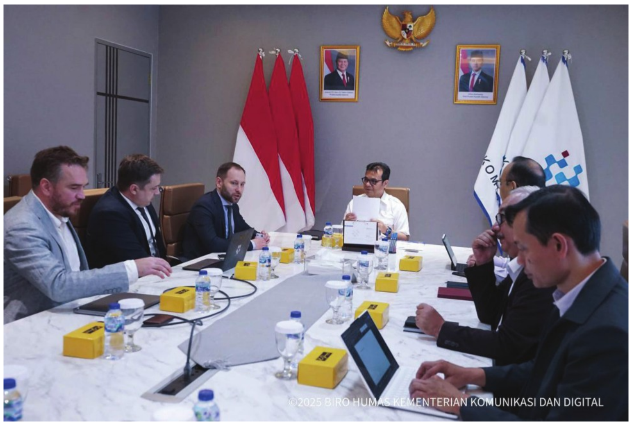
To strengthen cyber sovereignty, it is necessary to create and continuously develop a national community of cybersecurity specialists. Cyberus meta-products include mechanisms aimed at learning, maintaining interest, and creating opportunities for financial and career advancement in this field, which leads to the formation of a self-replicating professional community.

2 Measuring the effectiveness of the state's cyber defense

In order to assess objectively the level of cyber security, it is necessary to identify events unacceptable to the state, as well as the cost of cyber attacks that may lead to them. Cyberus has a methodology for continuous measuring the effectiveness of cyber defense via controlled cyber attacks.

3 Strengthening national technological competencies

Cyberus provides cybersecurity-critical information systems, solutions, and techniques in formats that not only strengthen the cyber sovereignty of partner countries, but also open up opportunities for re-export. Cyberus meta-products are free from modification restrictions.



©2025 BIRO HUMAS KEMENTERIAN KOMUNIKASI DAN DIGITAL

Indonesia, April 2025. Negotiations with the Ministry of Communications and Digital Technologies of Indonesia within the framework of the Russian-Indonesian business forum.

Moscow, March 2025. Signing of an agreement with the CSTO. Signatories: CSTO Secretary General Imangali Tasmagambetov and Cyberus co-founder Yuri Maksimov.

St. Petersburg, April 2024. Cyberus presented the export proposal at a Meeting of High Representatives overseeing security issues.

More than 30 countries are negotiating with Cyberus on the development of a sovereign cybersecurity industry.

The project's partners include Positive Technologies, Innostage, CyberQ, CyberED, Cyberdom, EveryTag, and other representatives of the Russian cybersecurity industry.

CyberED

Create an educational environment for the growth of cybersecurity professionals

The ultra-rapid development of the global cybersecurity industry places increasingly high demands on the level of qualifications of information security specialists, as well as on the number of highly qualified experts to ensure the protection of national interests.

CyberED is an educational platform that is part of the Cyberus Foundation for result-oriented cybersecurity development. The project is aimed at creating and developing educational projects in the field of cybersecurity, through the implementation of which the local expert community is strengthened, business and critical infrastructure security is improved, and innovation is accelerated.

From online learning to assessment and certification

CyberED offers more than 70 programs in various fields of cybersecurity, as well as a set of tools for mastering knowledge and skills, which includes an LMS platform for distance learning, educational content, and platforms for practical exercises and laboratory work.

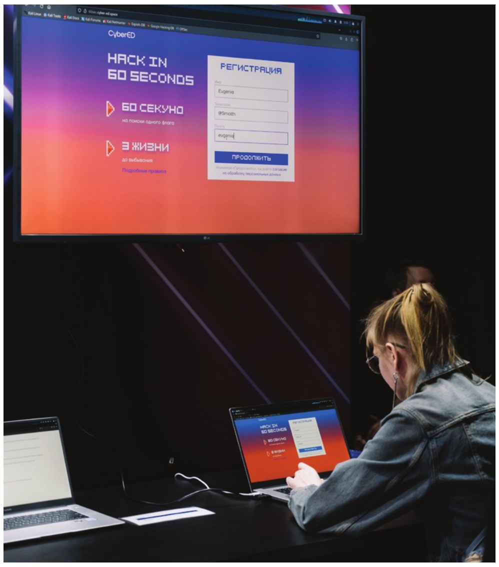
Training from scratch to the level of global experts

CyberED employs practicing educators who effectively help students develop the necessary skills, advance their careers, and gain a deep understanding of the industry's processes.

Integrated approach

CyberED's educational programs cover almost all areas of cybersecurity including offensive and defensive operations.

The goal of CyberED is to create an educational environment where high—quality training meets professional community to share experiences.



We conduct training on the basis of 30+ of our own laboratory stands, simulating the real experience of solving problems.

CyberED graduates are already shaping the future of cybersecurity around the world.

6600+ cybersecurity specialists

have been trained on the CyberED platform for 6 years

300+ Russian companies

entrusted CyberED with employee training

70+ educational programs

with the possibility of modification to meet customer requirements.

When developing programs, the international experience of educational companies in the field of IS is taken into account and adapted.

In 2024, CyberED partnered with Positive Technologies to organize the international hackathon Hack Camps.

Practice in the face of attacks

We cooperate with Standoff 365, one of the world's largest cyber training platforms, providing internships to our students.

International practice

In 2024, CyberED partnered with Positive Technologies to organize the international hackathon Hack Camps. As part of the project, more than 50 foreigners from the Middle East, Africa and Southeast Asia came to Russia for 2 weeks and received relevant skills from the best Russian cybersecurity specialists.

Skills assessment and certification

We evaluate effectively the skills of teams based on the roles of specialists. We provide detailed information about professional development and growth.

Professional competitions

We are organizing CTF (Capture The Flag) competitions with simulation of real threats and incidents to develop teamwork and problem solving skills under stress.

Individual approach

We can adjust existing educational programs or build them from scratch, taking into account the needs of the partner country.

CyberED Programs

1 / Red Team

Ethical Hacker

A course on the basics of ethical hacking for beginners. It includes basic knowledge on hacking systems and information security.

Penetration Testing Specialist

The main course is dedicated to mastering professional skills in penetration testing. It includes practical tasks and work with real attack scenarios.

Web Application Attacks

Additional advanced course specializing in attacks on web applications and the study of their vulnerabilities.

Active Directory Attacks

Additional course on vulnerability analysis and attack methods on Active Directory.

Social Engineering Attacks

Course aimed at studying social engineering methods. It includes practical examples and recommendations on how to protect against such attacks.

2 / Blue Team

Information Security Specialist

Course on learning the basics of information security for beginners. It includes basic methods for protecting systems and detecting attacks.

Security Operations Center Analyst

The main course for training specialists to work in cyberattack counteraction centers. It includes theoretical and practical modules.

Threat Intelligence

Additional course dedicated to the collection, analysis, and use of threat data. It includes practical work with Threat Intelligence platforms.

Defending against Web Application Attacks

Additional course on protecting web applications from attacks. Real cases are considered, as well as their prevention.

Practical Blue Team Course

Additional practice-oriented course in the field of Defensive Security, aimed at improving skills and developing scenarios for detecting complex ART attacks. It is designed to expand the knowledge and improve the skills of SOC specialists.

3 / Secure Software Development

Fundamentals of Secure Software Development

Video course on the basics of secure software development for beginners. The main vulnerabilities and methods of their prevention are considered.

Secure Software Development Specialist

Main course is aimed at professionally mastering the skills of secure application development. Real-world examples and best practices of software security are considered.

4 / Custom Courses

Individual training programs,

developed on the basis of client's requests. Specific needs of the customer and the level of training of employees are taken into account.

cyberdom

Place of power for the cybersecurity industry

To ensure the country's cyber sovereignty, it is necessary to create internal cybersecurity forces - specialists in response and protection, ethical hackers, as well as internal IT and cybersecurity solutions for effective import substitution. But it's not enough just to train specialists. It is important that they do not relocate to other countries that can offer better conditions and interesting projects. The formation of a strong cyber community and the creation of interesting industry projects helps to solve this problem.

Cyberdom is the epicenter of the development of the country's technology industry, as well as its global ambassador on the world stage.

150 thd.

people visited Cyberdom in 2024

1,5 thd.

cybersecurity industry experts

300

projects implemented

An alliance for the country

Cyberdom unites and guides the main actors of the industry to achieve common goals in the field of cybersecurity and cyber sovereignty.
Every audience finds here what is important to them.

Professional community. A comfortable environment for the co-creation and development of industry specialists.

Business. Promotion of advanced products and solutions, support for import substitution.

State. Demonstration of the crucial role of the state in the development of technologies for the safe digitalization of the country.

Human resources and startups. Education and development of the next generation of professionals who will exert the industry and protect the state

Society. Increase the level of digital literacy and popularize professions in the field of information security.

A cyberpolygon where competitions are held on mockups recreating the infrastructure of various industries: oil production, transport, finance, and others.

Cyberpolygon — the heart of Cyberdom

To demonstrate the capabilities of information security technologies, Cyberdom hosts cyberpolygon, a permanent multi—format platform for developing the practical skills of white hackers and immersing viewers dynamically in effective cybersecurity in the show, exposition or cyber battle mode.

Cyberattacks of varying complexity are simulated on the cyber polygon, which can actually occur at facilities in different industries, for example, transport, finance, oil production, etc.
Participants can explore vulnerabilities, practice defensive tactics, and form strategies to counter real-life threats.

Cyberpolygon hosts:

- training sessions of Blue Team and Red Team companies;
- cyber studies for students specializing in information security;
- cyber battles and CTF competitions for both world-class professionals and fresh graduates.

Executive spaces of the Cyberdom – a place for important meetings and negotiations.

From cyber literacy to international cooperation

The universal Cyberdom space can be used for a variety of tasks, including demonstration of national technologies and the level of industry development. Every week, Cyberdom in Moscow hosts delegations from the Middle East, Southeast Asia, Africa and other regions. Among the guests are entrepreneurs, representatives of foreign governments, diplomats and employees of international government organizations such as the United Nations.

The international Cyberdom network allows for a confidential exchange of experience and information between regions and countries through cross-training of specialists, demonstration of internal technologies and products for foreign markets, holding international and regional conferences in offline and online formats, and organizing international cyber battles to train ethical hackers. All this is aimed at the systematic and effective promotion of result-driven cybersecurity and the development of the country's cyber sovereignty.

Examples of projects for localization in your country's Cyberdom

Technology and product development

Independent testing for the development and improvement of information security solutions on the market: WAF-day, NGFW-day, SIEM-day and other events

Startup development and mentoring, M&A

Business club: includes technology development events, CISO clubs, and professional meetings

Conferences for HR and marketing specialists in information security: implementation of best practices for managing IS experts and improving products

CEO-transformation

CEO-club: digital transformation management, digitalization and business security

Gala dinner for CEO: deep insights that change the perception of cyber security

Round tables with the participation of CEOs about the research of business damage from leaks

Foresights and sessions for pumping CEOs in IS with industry experts

Educational track

Cyberdom Academy: Cyber literacy programs for top and middle management

Demo days for universities and school graduates: developing an educational trajectory for young professionals

Student pitch camps: helping businesses funnel effective young staff and interns
Verification and assessment of business security

Verification and assessment of business security

Hacker competitions, Bug Bounty and cyber testing.

Partner events for testing vendors' products and business information systems

Analytical panel of top vendors on the information field in attacks for business

Cyber literacy for business and society

Cyberdom Telegram channel: expert content on the development of personal and corporate digital security

Video podcast on YouTube: interviews with experts on digital fraud, cyberbullying and other relevant topics

Family Day: interactive family events for hands-on anti-cyberbullying training

Cyber Quiz: lecture on cyber literacy and a quiz for reliable consolidation of acquired knowledge

The path from a digital state to a cyber-resilient one

The CyberQ project offers a universal measurement system for any company and organization, a standardized process that is described in the CyberQ methodology and allows the company not only to verify its security, but also to maintain it at a high level.

The main components of CyberQ

CyberQ — a new security assessment tool
that includes the best of existing methods:

1. Focus on results, not formalities. Researchers are not looking for individual vulnerabilities, but full—fledged attack vectors that can lead to critical consequences - unacceptable events. The results of the CyberQ are understandable not only to specialists, but also to top management and the regulator.

2. Inspectability and transparency. The CyberQ mode involves recording all the actions of researchers in the system with the ability on the organization's side to stop them literally «at the touch of a button.»

3. Estimate reliability. The «examiners» of the company are not individual teams or certification centers, but the community of ethical hackers of the country. The results of their work are monitored and evaluated by the independent CyberQ Expert Council, which includes leading representatives of the information security community.

4. Benefits not only for the company, but for the entire industry.
As soon as CyberQ gains critical mass and becomes the industry standard, all its players will join the race to increase the level of security, since no one wants to win the wooden spoon. This practice can be extrapolated first to individual industries, and then to the entire business as a whole.

CyberQ is not the protection of server hardware or information system, it is the protection of people. Employees who are used to constant stress testing by ethical hackers get into digital hygiene habits.

CyberQ in numbers

AO «CyberQ» appeared in 2024. During this time, more than 100 projects have been carried out in various industries.

- The researchers have demonstrated the implementation of unacceptable events in more than 40 companies.
- In 40% of cases, the initiators of CyberQ were not IS specialists, but business owners;
- An individual plan for result-driven cybersecurity development was drawn up for all participants.

Upon successful completion of CyberQ, the organization receives a score that reflects the objective level of security of the company by a certain amount. The higher this amount, the potential reward for the researcher, the more interest ethical hackers have shown in the company.

Resistance to their attacks is a proof of the company's viability in terms of information security.

CyberQ stages (CQ)

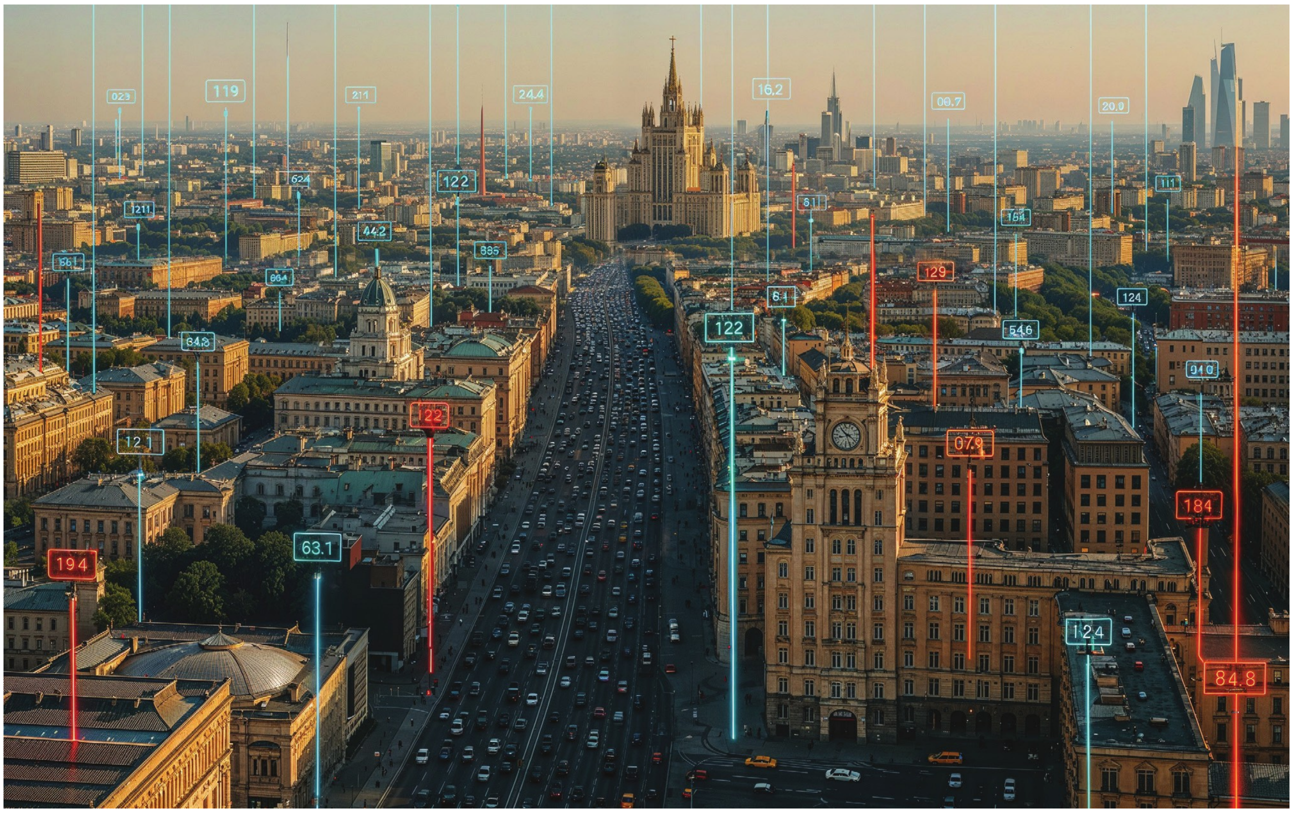
CyberQ allows not only to assess the security of an organization, but also to create a continuous process of increased readiness for everyone — from line employees and cybersecurity specialists to the top management of the company.

Depending on the level of information security and the specifics of the organization, CyberQ can be conducted in different formats, with a general description of all stages as follows:

1. Preparatory stage.
Transmission of recommendations on preparation for CQ, formulation of an unacceptable event. For example, a demonstration of the possibility of stopping production at an enterprise.

2. Principal stage.
Engaging ethical hackers to conduct CyberQ. The recording of the results of their activities and their verification by the expert council. Checking the demonstration of the implementation of unacceptable event and interim reports.

3. Final stage.
Summarizing the CyberQ results and evaluating their viability. Developing recommendations and assigning an assessment (score) of the organization's security level.



CyberQ — is a concept that will inevitably lead to an increase in the level of security, first in a separate industry, then in related industries, and eventually reach the national level, becoming a single measure and «thermometer» of cybersecurity.

In 2024, the CyberQ project launched a grant program in which companies could check whether they could be hacked by white hackers for 1 million rubles.

Security Vision

A SINGLE PLATFORM FOR THE ENTIRE ECOSYSTEM OF PRODUCTS

A set of ready-made modules

No-code / low-code development tools

Built-in analytical engine

Full customization and solution management

IS and IT automation platform

OBJECTS

cards and tables for describing any entities and their interrelationships

INTEGRATIONS

connectors for two-way bond of any third-party solutions

ANALYTICS

widget and dashboard builder for end-to-end interactive analytics

WORK PROCESSES

engine for managing any processes and automating up to 95% of actions related to the tasks of IT and IS specialists

REPORTS

editor for document templates and tables for uploading data as files

ROLES

data access management and personal storefront for users

Solutions for ENTERPRISE and SMB

In addition to the classic enterprise solutions, the Security Vision product line includes «boxed» lightweight versions of solutions suitable for small organizations and including basic functions other than those needed primarily by large structures:

VS Basic

SOAR Basic

CI Basic

SGRC Basic

A choice of OVER 100 CLIENTS from various sectors of the economy.

GOZNAK

FSBI RI "INTEGRAL"

FEDERAL RUSSIAN FEDERATION SECURITY SERVICE

GOVERNMENT OF THE KRASNOYARSK TERRITORY

GOVERNMENT OF THE TYUMEN REGION

GOVERNMENT OF THE YAROSLAVL REGION

FEDERATION COUNCIL OF THE FEDERAL ASSEMBLY OF THE RUSSIAN FEDERATION

DOM.RF

RESEARCH AND PRODUCTION ENTERPRISE "ISTOK"

SEVERSTAL

EVRAZ

ROSENERGOATOM

URALCHEM

NORILSK NICKEL

INTER RAO

RUSHYDRO

SBERBANK

ALFA BANK

ROSBANK

T-BANK

GPB BANK

OTKRITIE FC BANK

SMP BANK

INFOSECURITY

AB RUSSIA

X5 GROUP

MAGNIT

CHERKIZOVO

CHERNOGOLOVKA

RUSAGRO

RUSSIAN POST

CAPITAL GROUP

ROSTEC

CHANNEL ONE

MEGAFON

VIMPELCOM

SOLAR SECURITY

ANGARA SECURITY

TRANSTELECOM

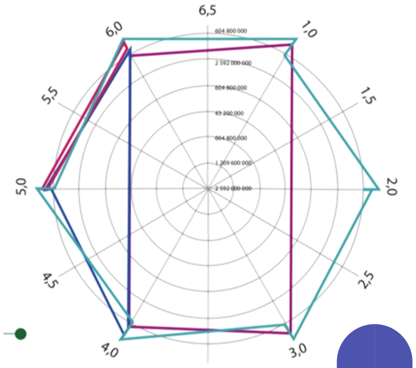
SDM-BANK

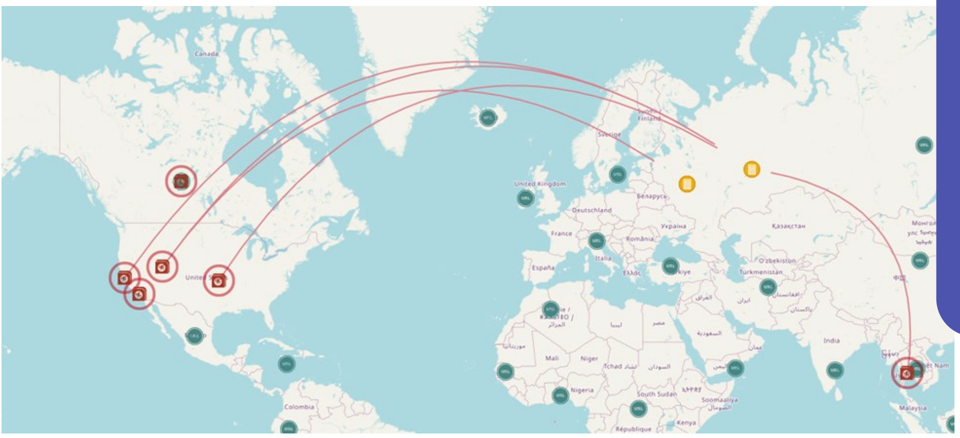
ROSTEC COMMERCIAL SOC

Unified Monitoring and Management Center

Unified data model based on business entities

AI tools and constructors for full manageability





SECURITY VISION

INDIVIDUAL PRODUCTS AND READY-MADE ASSEMBLIES (KITS)

NG SOAR

A set of advanced incident management with AI (built-in assistants and integration with third-party LLM models) for maximum automation of response at all stages of incident and attack processing with dynamically generated scenarios and an object-oriented approach.

The kit includes a SIEM solution, a single resource and service model, an asset and inventory management module (AM/CMDB), as well as two-way integrations with monitoring and response centers (CERT) for automated data acquisition, tasks, and prompt incident notification.

NG VM

A comprehensive solution for finding and eliminating vulnerabilities, including modules for asset management and security settings of technology platforms (configuration compliance and hardening), as well as a security scanner that searches for technical vulnerabilities in infrastructure, programs and operating systems, containers and web applications with automatic task creation and assignment, patching and closing applications upon successful repeated scans.

NG SGRC

The complex of the risk-oriented strategic security management center, which includes audit and compliance of documentation for IT and OT segments of companies of different scales and fields of activity based on standards from the package of expertise and/or implementation of its own methodology.

The kit supports quantitative and qualitative risk assessment with calculation of probabilities and damage of risk scenarios, development and implementation of protection measures to increase the cyber resilience of the organization and processes of ensuring business continuity and self-assessment of the security level.

About us

30+ of the TOP 100 companies in Russia are customers

7 of the TOP 10 banks are customers

10+ MSP information security service providers use the platform to provide the service

30+ competent and trained partner companies

26 professional awards in the field of information security

All the necessary permissive licenses from FSTEC and FSS.

About the platform

The Security Vision automation and robotization platform for information security is a low code /no code IT platform that allows robotization of up to 95% of software and hardware IT/IS functions 24/7.

It is a 100% Russian development, included in the database of the Ministry of Communications of the Russian Federation and in the Unified Register of Russian Computer Software and Databases.

Executed at the level of world analogues,
has received wide recognition from the expert community.

Customers include - Sberbank, Alfa Bank, Evraz, Cherkizovo, the Federal Security Service of Russia, Tinkoff Bank, Gazprombank, Severstal, MKB, Norilsk Nickel, the Federation Council, Goznak, Russian Post, Magnit and many other government agencies and commercial structures.

Winner of 26 professional awards, including:
«For strengthening Russia's security»
"Import substitution"
National Award "Priority"
TAdviser IT Prize in the «Information Security solution of the Year in Russia» nomination
Runet Award in the "Information Security" category

The platform is developing in three directions:

🟩 Technologies

🟦 Processes

🟪 People

SOAR

Responding to information security incidents using dynamic playbooks with information protection tools, building a chain of attacks and an object-oriented approach to incident management and elimination of consequences.

FinCert

Two-way interaction with the Central Bank's centers: managing tasks, transmitting information about incidents and receiving operational notifications/bulletins according to the established regulations of the regulator.

GosSOPKA

Two-way interaction with the NCCCI response centers: task management, transmission of incident information and receipt of operational notifications/bulletins according to the established regulations.

AM

Description of the IT landscape, discovery of new objects in the network, asset categorization, inventory and lifecycle management of equipment and software on the AWP and servers of organizations.

VM

Building a process for detecting and eliminating technical vulnerabilities, collecting information from existing security scanners, an update management platform, expert external services, and other solutions.

VS

Scanning information assets with enrichment from external infrastructure security analysis services, using a set of values to manage vulnerabilities.

SPC

Evaluation of information asset configurations in accordance with the security standards accepted in the organization for building interactions with specialized technology platforms and bringing parameters to reference values.

SOT, Security Orchestration

Security Vision

GRC, Security Orchestration Tools

CI

Audit and compliance with the requirements of FZ-187 «On the Security of the Critical Information Infrastructure of the Russian Federation» and other regulatory documents, including the processes of categorization and task management for compliance.

CM

Audit and compliance with various methodologies and standards as included in the expertise module (orders FSTEC 17, 21, 31, 239, ГОСТ 57580, PCI DSS, NIST, CIS, FZ №152 и №63 etc.), as well as other client documentation.

RM

Formation of a register of risks, threats, protection measures, KRI and other control parameters, qualitative and quantitative assessment methods (FAIR, Monte Carlo, etc.), formation of a list of measures to change the risk level, control of execution.

BCM

Automation of the process of ensuring continuity and recovery of activities after the occurrence of emergency situations, including BIA and BCP to ensure a full cycle.

ORM

Register formation, accounting for operational risk events and other control parameters, assessment for compliance with the requirements of No. 716-P of the Central Bank of Russia to form a list of measures to change the risk level with task performance control.

SA

The organization of the information security assessment process with the choice of assessment methods based on standards from the expertise package or its own processes for the organization as a whole and for its individual elements.

SDA, Security Data Analytics

TIP

Analysis of cybersecurity threats by collecting views from any external sources and detecting matches within the protected perimeter using a combination of technology and AI applications.

UEBA

Behavioral analysis to search for anomalies in user and device activity with the application of various machine learning models, correlation rules, statistical methods, and other guided techniques.