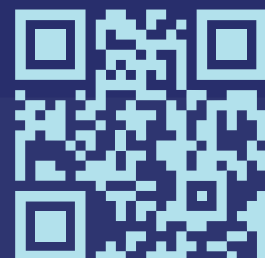


XII 2024

International Meeting of High Representatives for Security Issues



Russian Cybersecurity:
Sovereignty Approved by Time

Информационная безопасность России:
суверенитет, проверенный временем.

Ciberseguridad de Rusia:
Soberanía Confirmada por el Tiempo

Cybersécurité Russe:
une Souveraineté Confirmée par le Temps

April 23-25

EXPOFORUM
Convention and Exhibition Centre
Saint Petersburg

KOMIB..... 3

Angara..... 4

VEB.RF..... 8

Kaspersky 10

Security Code 14

Cryptography Museum 18

Cyberus..... 20

Solar..... 24

Positive Technologies 28

Security vision 34



KOMIB — a new tool for creating a fair, reliable and sustainable International Cybersecurity System (ICS)

“Partnership for International Information Security Coordination Centre” (KOMIB) was established 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.

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;
- realizes properly the current situation in the Russian cyber security industry;
- has established working relationships with commercial companies for involving concerned organizations in execution projects in the context of the G2G agreements.

See also:





★ ANGARA SECURITY

A leading Russian integrator and provider of more than 80 information security services. We specialize in protecting data and business systems, preventing and investigating cyber attacks.

- Accredited by the Ministry of Finance of the Russian Federation
- Licenses of the FSTEC and the FSB of Russia
- GosSOPKA Class A Corporate Center

MONITORING AND MANAGEMENT OF CYBER SECURITY INCIDENTS (SOC)

Round-the-clock detection and verification of CS incidents in the infrastructure, investigation and response.

The service is provided using a consistent stack of software products from solutions of the IRP, SIEM and EDR class, which allow you to build flexible CS-incident management processes, automatize routine tasks for analysts, collect and analyze an exhaustive amount of telemetry from end hosts that go beyond the regular audit capabilities of operating systems, and also from cyber security tools used by the customer, as well as respond to cyber security incidents.

CYBER SECURITY INCIDENT RESPONSE AND DIGITAL FORENSICS (DFIRMA)

The service includes:

- **incident response** (localization and containment of an ongoing computer attack);
- **malware analysis** (identification of tools used by attackers, identification of IOC, creation of yara rules for infrastructure scanning);
- **incident investigation and digital forensics** (establishing the circumstances of the incident, collecting digital evidence, developing recommendations);
- **internal investigations' support.**

As a part of the service, it is possible to conduct the **infrastructure analysis for compromise** (Compromise assessment). Establishing the presence or absence of the facts of compromising the infrastructure by retrospectively searching for relevant indicators, as well as other traces.

BRAND PROTECTION AND OSINT

Tracking the dissemination of confidential information, detecting cybersquatting and phishing resources that use the corporate identity and trademarks of the organization for fraudulent purposes (impersonation), etc.

This is also relevant when working with external IT and CS contractors: when there is a risk that keys, passwords, tokens and other secrets will end up in the contractors' open repositories or fragments of the implemented solutions' source code will be published.

The OSINT and brand protection service includes the search and analysis of information posted in both indexed and non-indexed segments of the Internet.

INTERNAL AND EXTERNAL PENETRATION TESTING

It is possible to check whether the cyber security infrastructure and processes are ready for possible hacks by controlled modeling of the actions of potential intruders. In the process, we identify weaknesses and potential attack vectors.

In addition to expert analytical actions, commercial solutions that have proven themselves in the market and Angara Group's own tools are also used. The level of expertise of specialists is confirmed by the first place in the National Cyberpolygon.

MOBILE AND WEB APPLICATION ANALYSIS

Evaluating the security of an application as a separate information system allows to gain a full understanding of the quality of the code and component settings. The work is carried out with generally accepted practices and recommendations of OWASP and SANS/CWE taken into account. Not only the technical aspects are checked, but also the business logic of applications, as well as the possibility of attacks on application clients. The result of the work is a list of actual bottlenecks and detailed instructions on how to fix them.

DETECTING UNSTABLE PASSWORDS

The use of weak or simple passwords by users is one of the main factors in hacking and account selection. We offer a set of actions aimed at verifying the durability of passwords to corporate information systems. As a result, 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 leaks of authentication data.

TESTING USING SOCIAL ENGINEERING METHODS

User awareness of social engineering attacks can play a key role in the cyber security processes of the entire company. As a part of the service, a set of actions is performed with the purpose of checking the awareness of employees about attacks using social engineering methods. Various scenarios and legends are being developed exploiting human weaknesses: curiosity, fear, greed, etc.

ANGARA ASM

SERVICE FOR MANAGING THE AREA OF EXTERNAL ATTACKS

The service will show the existing vulnerabilities of the external perimeter with a description of their elimination. This provides the opportunity to reduce the number of applicable attack vectors in relation to the studied infrastructure.

Using Angara ASM allows to discover forgotten VPN services of IT specialists, open test environments or developer's environments, and most importantly, to see the vulnerabilities that this or that unaccounted asset entails.

RED TEAM OPERATIONS

One of the ways to check the level of cyber security processes in a company with the ability to track and prevent a possible attack is to involve a team of pentesters. During the work, the close interaction with the security team is performed to track possible gaps in the correlation rules, incident response processes and deficiencies in cyber security configurations.

CYBER SECURITY RISK ASSESSMENT SERVICES

The modern information system of an organization is a distributed and heterogeneous formation. Thus the task of proper, efficient and safe management of this formation becomes much more complicated. As a result, the number of deficiencies, violations and vulnerabilities in the system increases, which pose certain CS risks for the organization. Our experts will help to create a methodological basis for assessing the CS risks and conduct such an assessment.

COMPREHENSIVE PROTECTION OF INFORMATIZATION SYSTEMS

The creation of an integrated information security system calls for the implementation of a set of organizational and technical measures to meet the requirements of local legislation on the creation of systems for the protection and security of information in "turnkey" information systems with the examination, development of a threat model, development of technical specifications, design, supply and implementation of information security systems.

APPLICATION SOURCE CODE ANALYSIS

Analyzing the source code of your software manually and using statistical analyzers. Our experts will verify the identified suspected vulnerabilities on the test bench, rank the confirmed vulnerabilities and offer recommendations for their correction. The service can be performed on an ongoing basis.

DevSecOps

CREATING A SECURE DEVELOPMENT PIPELINE

Any application development requires the inclusion of a security process to protect sensitive user data, prevent information leaks and reduce the risks associated with cybersecurity. Compliance with the requirements of safe development has a positive effect on the company's reputation and increases the trust of customers and partners.

Based on the results of the analysis of your business tasks and infrastructure, we will offer solutions to ensure cybersecurity and code quality control, as well as environment protection (container environments, repositories).

VEB.RF: HELPING HIGH-TECH COMPANIES ACCESS INTERNATIONAL MARKETS

We contribute to Russia’s economic growth and foster stronger international ties. We facilitate connections between Russian enterprises and potential clients across 30 countries spanning the CIS, Europe, Africa, South America, and Southeast Asia.

WHO WE ASSIST:

- **Developers and exporters.** If you have innovative cybersecurity technology, we can help you connect with potential partners.
- **Foreign buyers.** If you are seeking top-tier practices and reliable technologies from Russia, we can assist in linking you with reputable suppliers and facilitating transactions.
- **Foreign financial institutions.** If you are looking to support the exchange of advanced technologies, we can help you prepare and organize transactions smoothly.

COMPREHENSIVE SUPPORT

Financing. We provide investment for projects before export and help partners acquire assets in other countries.	Administration. We assist in opening letters of credit and securing guarantees for various purposes, including post-financing and tender participation (e.g., standby letters of credit).
Representation. We participate in exhibitions, seminars, business councils, and government commissions. We also initiate the development of the regulatory framework and work closely with businesses.	Arrangement. We scout for business partners for Russian enterprises and help them draft promising joint venture proposals. We also offer support with paperwork and transaction preparation.

CONTRIBUTION TO TECHNOLOGICAL INDEPENDENCE

over \$530M allocated for portfolio investment in high-risk technological projects, including cybersecurity, telecommunications hardware, oilfield service technologies, and unmanned aerial vehicles.

Our goal is to strengthen the position of Russian companies in the market in areas that were previously dominated by imports.

Project partner SK Capital will serve as a key platform for establishing technology holdings in strategically important industries. It will merge the financial resources, investment expertise, and technological expertise of VEB.RF and the Skolkovo Foundation.

WORLDWIDE CYBERSECURITY LEADERSHIP

In collaboration with Cyberus, we are developing a national product focused on safeguarding against cyber threats. This initiative requires engagement from various industry stakeholders.

The product offers a holistic system suitable for private, public, and intergovernmental use. It encompasses efforts in legislative development, personnel training, hardware and software development, ongoing security testing, and insurance coverage for residual cyber risks.

Join us in building proactive defense strategies: retaining control over cyberspace, preventing unacceptable events, and staying ahead of cybercriminals.

CAPABILITIES AND INFRASTRUCTURE

VEB.RF is a trustworthy and promising partner:

Sovereign rating. Our international credit ratings align with those of Russia.	Operating across various markets. This includes high-risk ones.	Handling complex projects. We specialize in organizing large, long-term transactions with intricate structures.
Extensive partner network. We collaborate with numerous global financial institutions.	Accompanying you at all stages. We offer assistance with partner identification, transaction preparation, and financing.	

SUPPORTING RUSSIAN EXPORTS

VEB.RF is a leading provider of export financing, which is essential for supporting various sectors of the economy. We offer favorable conditions to enhance the competitiveness of local products in global markets.

300 investment projects	over \$36.6B in investments
-------------------------	-----------------------------

“Our mission is simple and clear — we are building a safe world. Using our experience and achievements, we want to make the digital space secure — so that everyone can enjoy the limitless possibilities offered by technologies”.


Evgeny Kaspersky,
CEO of Kaspersky Lab




BUILDING A SAFE WORLD FOR MORE THAN 25 YEARS

“Kaspersky Lab” is an international company working in the field of cybersecurity and digital privacy for more than 25 years. During this time, we have evolved from a manufacturer of antiviruses for private and corporate users to a provider of comprehensive cyber protection for businesses of various sizes and fields of activity.


We protect organizations of all industries




Oil-and-gas
and fuel-
and-energy
companies




Finance




Transport




Telecom




Manufacturing



ICT



Retail



Government
agencies

Today, organizations need the support of a reliable cybersecurity partner with many years of experience, global expertise and understanding of modern cyber challenges in both corporate and industrial spaces, as well as at their intersection.

>220 000
users worldwide are protected
by our technologies

>400 million
corporate customers
worldwide

~5000
top specialists

>400 000
unique malicious objects
detected daily

>200
large APT groups closely
monitored

50%
of our employees are R&D
specialists and researchers

EXPERT PROTECTION FOR YOUR BUSINESS

To counter complex cyber threats successfully and adapt effectively to new challenges in an ever-changing threat landscape, you need modern technologies backed up by threat analytics, experienced specialists with the necessary skills, and the support of world-class experts. In this case, you will have at your disposal the entire range of measures to counter the most complex APT threats and targeted attacks. Kaspersky Lab offers a full arsenal of advanced security technologies, analytics and services that will increase the efficiency of your CS department and SOC team.

Kaspersky Lab’s extensive portfolio includes advanced technologies for protecting IT and OT segments, a number of specialized products and a wide range of expert services, as well as cyberimmune solutions to combat complex and constantly evolving cyber threats.

ECOSYSTEM OF CUSTOMIZED SECURITY TOOLS

Today, more than ever, an ecosystem approach to business cybersecurity is important, which would include mutually complementary classes of EPP, EDR and XDR technologies and at the same time meet the requirements of regulatory authorities. Kaspersky Lab follows this approach, embodying it in the Kaspersky Symphony line of solutions.

The Kaspersky Symphony solution line is a complex of closely integrated technologies and solutions based on expertise and many years of practical experience. With its help, companies increase the effectiveness of the security system and the transparency of the infrastructure and are ready to repel attacks of any scale and complexity successfully. In addition, it helps to ensure compliance with regulatory requirements. The ecosystem approach is most fully embodied in the Kaspersky Symphony XDR level. This is an XDR class solution that protects numerous entry points into the organization, including the network, mail and end devices, from potential threats. The Solution is enriched with knowledge of the global threat information system, it protects the company from mistakes by ordinary employees (for example, as a result of a phishing attack) and is ready to integrate easily into the existing security system.

UNIQUE ANALYTICAL DATA

Countering modern cyber threats is closely linked to deep understanding of tactics, techniques and procedures used by attackers. With petabytes of detailed threat data, Kaspersky Lab provides Kaspersky Threat Intelligence organizations with reliable analytical threat data from around the world in various formats, which helps to ensure protection even from unprecedented cyber attacks.

ADVANCED AUTOMATED CONTROL SYSTEM PROTECTION TECHNOLOGIES

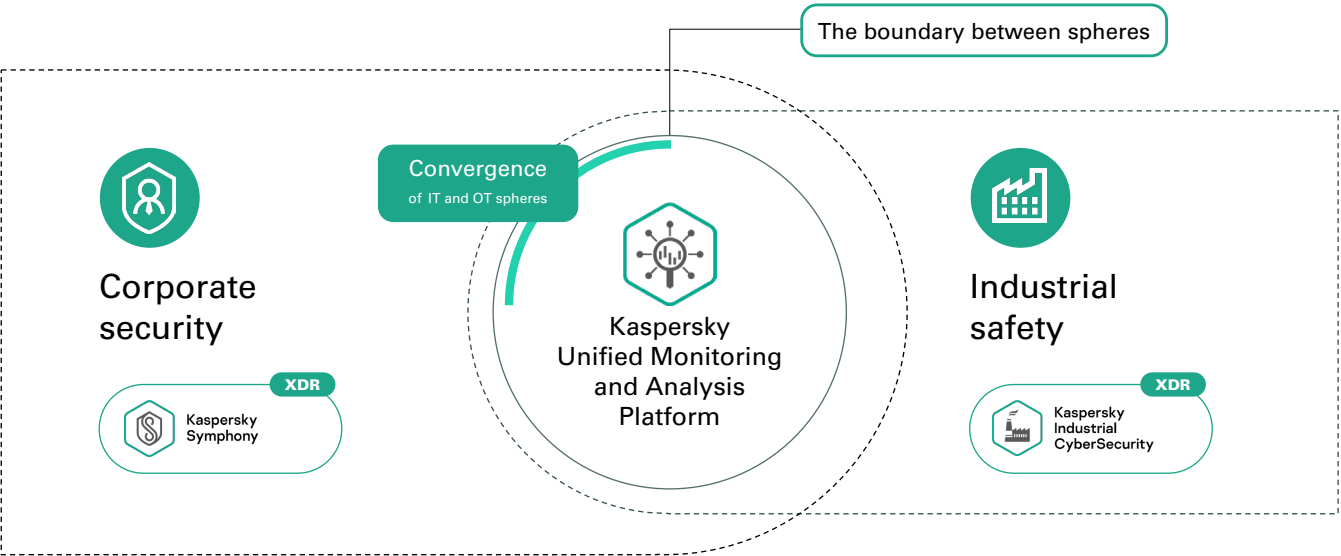
Kaspersky Industrial CyberSecurity (KICS) is a specialized industrial XDR platform designed for comprehensive protection of the main components of automation and production management systems at all levels. Thanks to the excellent integration of the platform components with each other, you will be able to control centrally all disparate industrial networks, workplaces and automation systems. This helps to raise awareness of the situation and counter complex threats more effectively.

A COMPREHENSIVE APPROACH FROM A GLOBAL SUPPLIER ON THE ISSUE OF IT/OT SECURITY

One of the key components of the cybersecurity ecosystem of both the industrial and corporate segment is Kaspersky Unified Monitoring and Analysis Platform, a SIEM class solution designed for centralized collection, analysis and correlation of CS events from various data sources to identify potential cyber incidents and neutralize them on time. Kaspersky Unified Monitoring and Analysis Platform combines Kaspersky Lab products and third-party vendors into a single CS system. It is a key component in the implementation of an integrated security approach that helps to comprehensively approach the issue of compliance with the requirements of legislation in the field of CS.

Due to its close integration with the SIEM system, the Kaspersky Industrial CyberSecurity platform allows you to implement more scenarios of interaction with third-party solutions and expand investigation and response activities. It also allows you to protect your business not only in an industrial environment, but also in the part where the industrial environment intersects with the corporate one, cooperating closely with the Kaspersky Symphony XDR corporate XDR platform.

A complete offer to protect the OT and IT segments



STRATEGIC PARTNER

Choosing a cybersecurity partner is an important step for companies that want to maintain stability and resilience in any environment. Kaspersky Lab is ready to become your strategic partner and provide protection against threats of any complexity aimed at your business.

Global reach and international recognition

Proven technologies

Transparency and compliance

World-class experience and knowhow

High status in the InfoSec industry

25 years of excellence

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.

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

The Security Code protection tools form a single security ecosystem and are designed to protect key elements of the 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.

There are more than 3 million jobs under the protection of the Security Code. Today, Security Code products are **used by more than 50,000 organizations**, including government agencies and large commercial companies..

UNIFIED SECURITY ARCHITECTURE:

PROTECTION OF WORKSTATIONS AND SERVERS

- Secret Net Studio is a comprehensive solution for protecting workstations and servers at the level of data, applications, network, operating system and peripheral equipment.
- Secret Net LSP — information security tool for Linux OS
- “Sobol” is a certified hardware and software module for trusted boot (APMDZ).

PROTECTION OF NETWORK INTERACTION

- NGFW Continent 4 is a multifunctional firewall for protecting network infrastructure and creating VPN networks using GOST algorithms.

PROTECTION OF VIRTUAL INFRASTRUCTURES

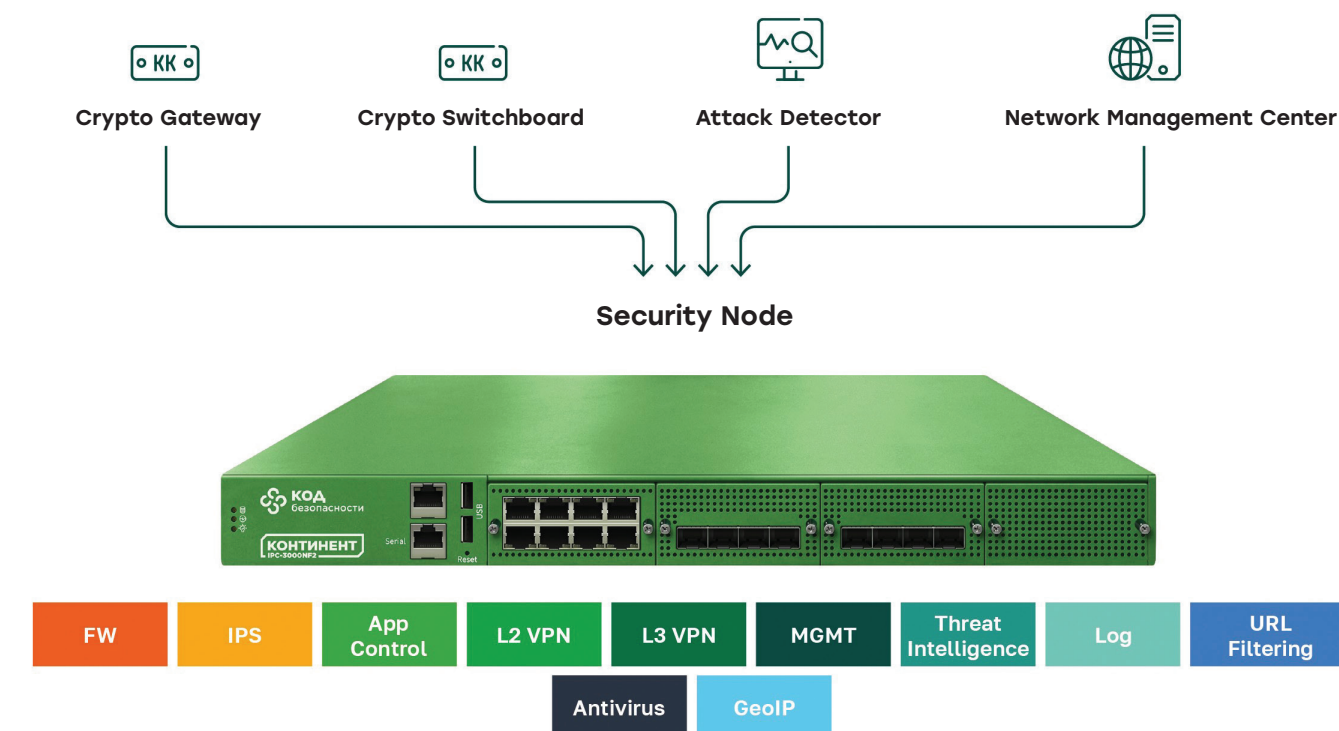
- vGate is a means of micro-segmentation and protection of the life cycle of virtual machines.

NGFW CONTINENT 4

SCENARIOS:

- External perimeter protection;
- Datacenter network segmentations;
- Distributed networks protections;
- Small and medium networks security;
- OT networks security.

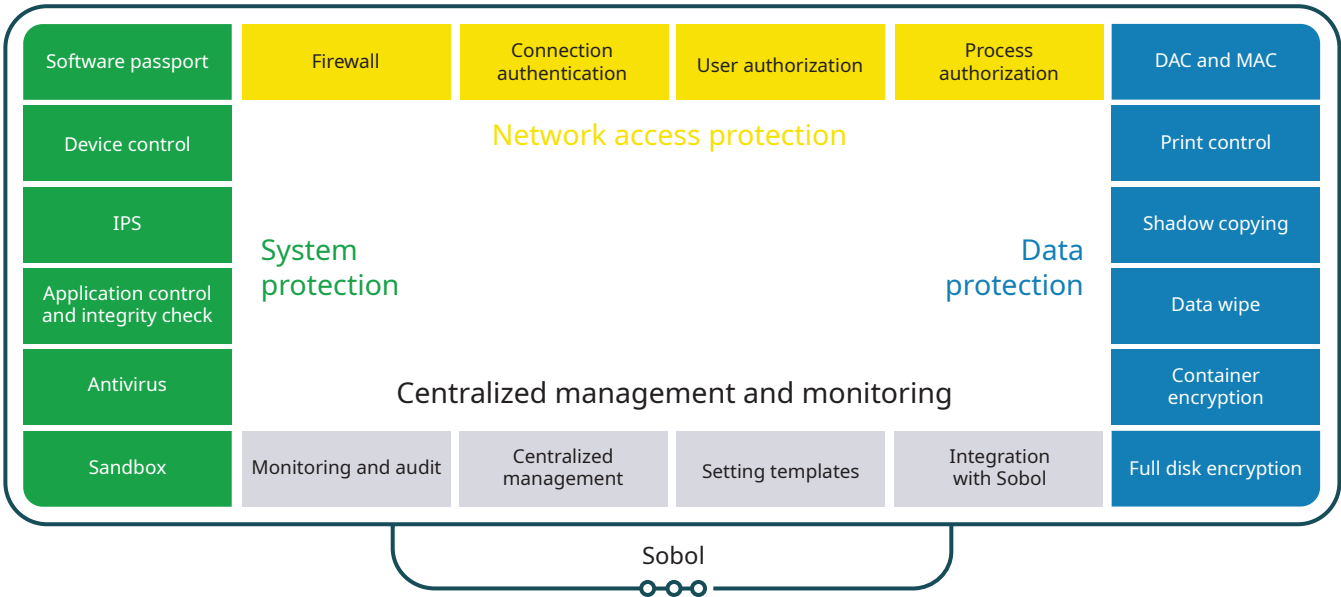
FEATURES:



SCENARIOS:

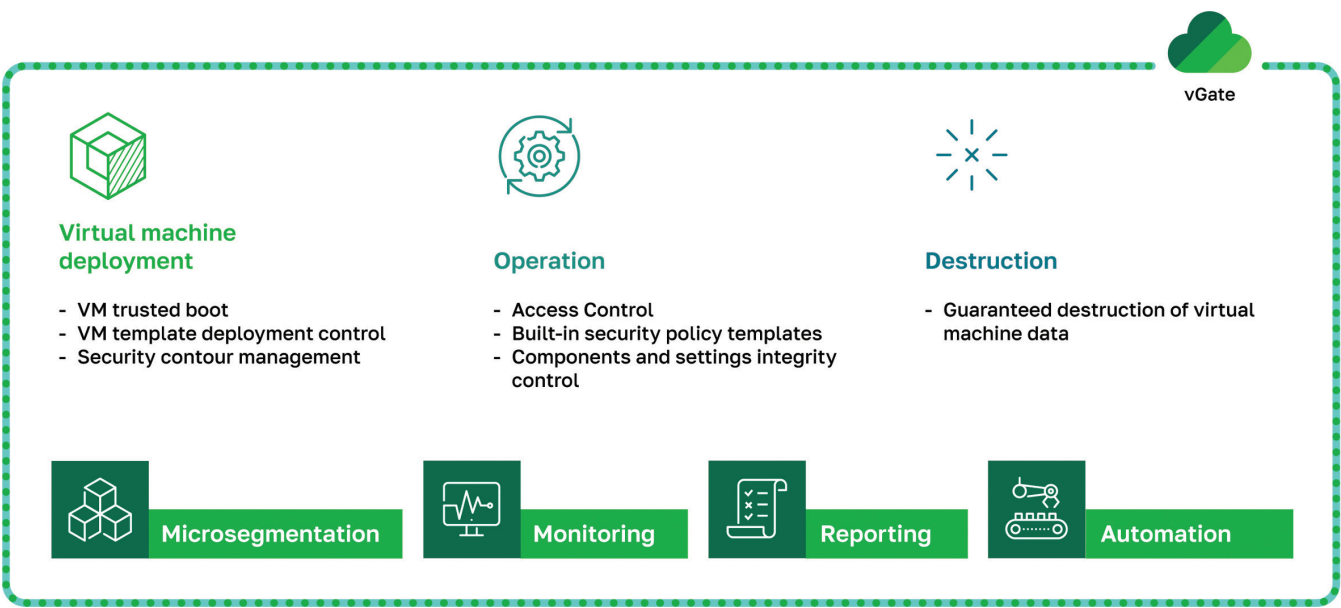
- Protection of workstations and servers from viruses and malware;
- Protection against network attacks;
- Protection against counterfeiting and interception of network traffic within a local network;
- Protecting information from unauthorized access;
- Protection from insider actions;
- Protection against information theft in case of media loss;
- Control of leaks and information distribution channels.

FEATURES:



SCENARIOS:

- Critical VM access control;
- Administrator access segregation;
- Microsegmentation.





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 protocryptography – 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.

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: ESTABLISHING A SELF-RELIANT CYBERSECURITY INDUSTRY IN PARTNER NATIONS

In the past two years, the world has seen the onset of cyber warfare. Major corporations, government agencies, and industries have faced unprecedented cyber-attacks. Russia, in particular, has experienced a record rise in cyber crimes during this period. These attacks target critical sectors of the national economy, such as the industrial sector, military, energy, finance, healthcare, construction, and services.

Russian businesses, entire industries, and government agencies have faced cyber threats. This has helped them become highly skilled at pushing back advanced attacks. This knowledge and these protection methods are valuable beyond Russia's borders. Therefore, the industry is working on a model to build and improve cybersecurity at the state level. Cyberus is ready to mimic this model in Russia's partner countries with local players.

NEW INTERNATIONAL CYBERSECURITY ARCHITECTURE

Changes in the world's geopolitical landscape naturally lead to changes in other domains. To sustainably develop the entire system, it is vital to ensure that all states respect each other's digital sovereignty. No country should rely only on major players. Each should have its own resources; this is particularly true for skilled individuals who can create new technologies and independently secure critical areas within the country.

New global projects in finance, transportation, energy, and the industrial sector require a unified approach to infrastructure cybersecurity. This approach must consider the sovereign interests of all parties involved. Therefore, countries must have their own solutions and technologies based on shared principles.

CYBERSECURITY TODAY:

The technological framework is the foundation for cybersecurity. Cybersecurity requirements are determined by the technology employed. The effectiveness of protection can only be measured during an actual attack.



CYBERSECURITY TOMORROW:

The technological infrastructure prioritizes modern cybersecurity needs. Information architecture requirements are based on a list of unacceptable events. Protection reliability is continually verified through cyber tests in a unified measurement system.

BLUEPRINT FOR DEVELOPING A ROBUST CYBERSECURITY SECTOR AT THE STATE LEVEL

The model, created by leading experts from Russian cybersecurity companies, offers a methodology for choosing effective technologies to build a local cybersecurity industry.

ASSESSING YOUR CURRENT LEVEL OF CYBERSECURITY

We will test the protection mechanisms to see if they can endure simulated hacker attacks that could cause critical damage.

With representatives of partner countries, we decide what needs protection and how to assess security effectively. The verification tool is an objective **cybersecurity testing**. This approach is used to evaluate the security of critical state systems.

Cybersecurity testing

Independent researchers continuously check vital infrastructure for cyber threats. They will be guided by recognized

BUILDING RESULTATIVE PROTECTION IF WE FIND VULNERABILITIES

Cyberus experts help identify key events for the country and create a strategy to achieve the desired cybersecurity level.

This strategy sets unified goals for cybersecurity. They also establish regulations for new tasks to oversee the final outcome. Additionally, Cyberus assists in implementing protection using Russian technologies, open-source solutions, and products from local cybersecurity companies.

CREATING A LOCAL CYBERSECURITY INDUSTRY

The Cyberus approach helps build the country's defense with existing solutions and fosters a local cybersecurity industry by training new personnel. This boosts the number and quality of specialists and encourages innovation in defense technologies to repel cyber-attacks.

To develop a new wave of hackers, **CyberED** offers an online platform for training cybersecurity specialists and ethical hackers. These experts conduct realistic cyber tests on systems. With over 70 training programs led by 80 experts, CyberED has trained 5,000+ specialists in Russia in five years. It aims to extend this expertise to other countries and help them establish national cyber armies, which are fundamental for sovereignty.

CyberDome was established to unify and advance the cybersecurity industry. It promotes a professional community and a dialog among cybersecurity, IT, government, and business sectors. Tested and proven, this concept is now export-ready to other countries.

CyberDome

A phygital (physical + digital) space to attract, develop, and retain cybersecurity specialists. It provides infrastructure for skill training and expertise enhancement.

The goal of this effort is to achieve fully sovereign protection, where the partner country can independently address 100% of its cybersecurity needs.

EXPORTING SOLUTIONS TOGETHER

Nations will seek proven and tested cyber defense systems from their partner countries for export.

The cybersecurity market in countries less reliant on other states will reach \$40 billion by 2026. United industries in Russia and partner countries could capture 20% of this market.

\$8 billion a year

potential revenue from exporting cybersecurity products and services

THE CYBERSECURITY INDUSTRY OPERATES ON A GOVERNMENT-TO-GOVERNMENT MODEL

Cyberus is communicating with government agencies to develop a local cybersecurity industry in partner countries. This cooperation follows the government-to-government (G2G) model and involves leading state corporations in transaction agreements.





ABOUT

Solar Group is an architect of complex cybersecurity. The key areas of activity are CS outsourcing, development of proprietary products, training of CS specialists, analytics and research of cyber incidents.

Since 2015, Solar has been providing CS solutions to organizations from small businesses to the largest enterprises in key industries. There are more than 850 significant Russian companies under the protection of Solar. It offers the services of Russia's largest commercial SOC — Solar JSOC, an ecosystem of managed CS services — Solar MSS. The line of proprietary products includes the Solar Dozor DLP solution, the Solar WebProxy web security gateway, the new generation Solar NGFW firewall, the Solar inRights IdM system, the Solar SafeInspect PAM system, the Solar appScreener code analyzer and others. Develops a platform for practical fine-tuning of cyber threat protection skills “Solar Cyberworld” and Solar 4RAYS Cyber Threat Research Center.

The Group invests in the development of the cybersecurity industry and helps solve the problem of personnel shortages.

PROTECTING THE DIGITAL FUTURE

№1
in the cybersecurity
services market

24/7
ensuring cybersecurity

2000+
employees

600+
ongoing projects a year

850+
organizations
under protection


200+ billion
analyzed events per day

SOLAR GROUP'S OFFER FOR GOVERNMENT CUSTOMERS

Solar Group, as part of the expansion of economic cooperation between the Russian Federation and foreign countries, is ready to present a comprehensive solution — a “National-level cybersecurity Platform”.

«PLATFORM» IS DESIGNED FOR:

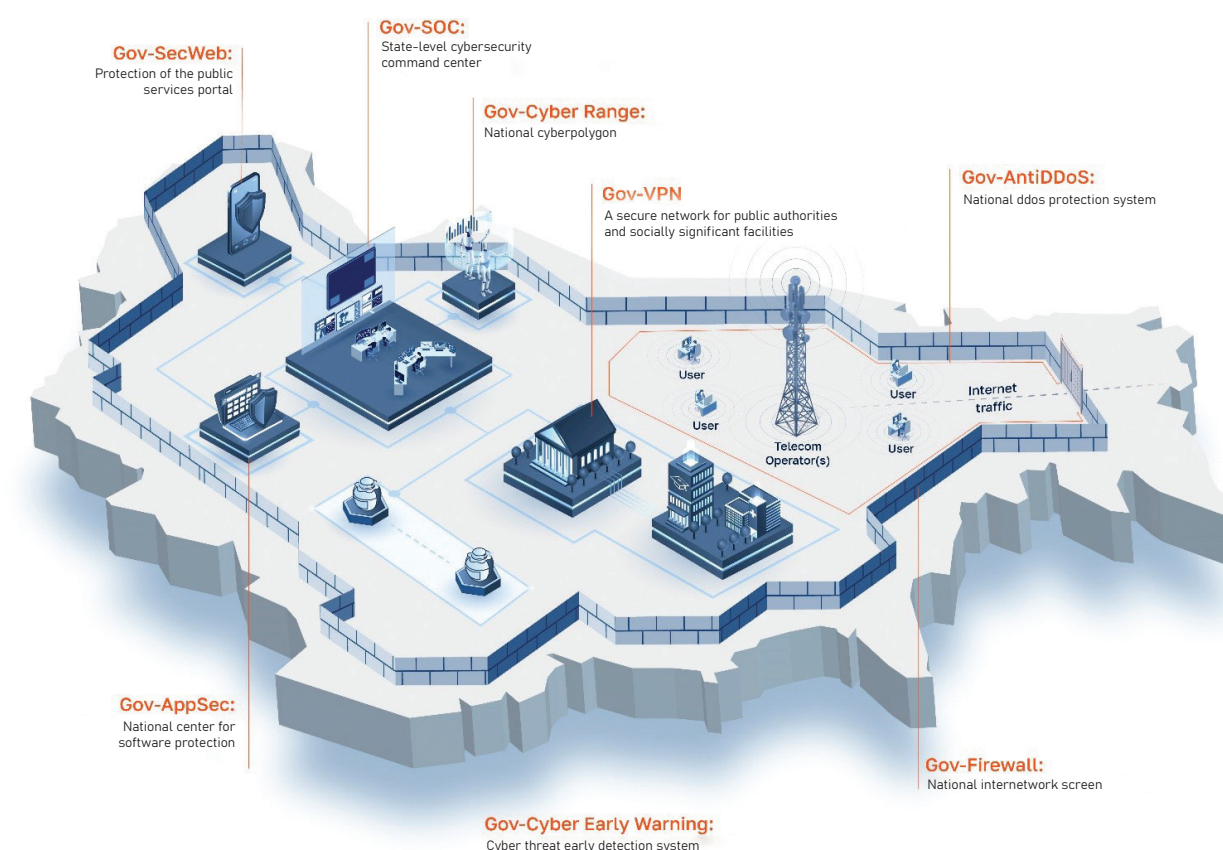

Government agencies,
ministries and
departments


Organizations with critical
information infrastructure
(financial sector, fuel and energy
sector, military-industrial complex)


Socially significant facilities
(education, healthcare, etc.)

As part of the implementation of the “Platform”, Solar Group carries out the transfer of advanced technologies in the field of cybersecurity, creates a high-tech infrastructure to ensure it, trains highly qualified specialists, including through the development and launch of specialized training programs in local educational institutions, as well as provides further technical and expert support for the entire range of solutions.

“PLATFORM” CONSISTS OF:





GOV-SOC: STATE-LEVEL CYBERSECURITY COMMAND CENTER

It is an operational center that counteracts cyber threats of any level of complexity (coming from both single hackers and hacker groups supported by state intelligence services), which can potentially lead to attacks of a political, terrorist, industrial and criminal nature.



GOV-APPSEC: NATIONAL CENTER FOR SOFTWARE PROTECTION

Ensures the implementation of interrelated organizational and technical measures aimed at the development and use of secure software of any type. Organizational measures include the development of a regulatory framework, the definition of approaches, methodology and classification of the software, the compilation of a unified register of secure software, as well as the creation of accredited laboratories that monitor software security nationwide. Technical measures involve the use of special tools for automatic verification of binary and source code for vulnerabilities, caches and undeclared features.



GOV-FIREWALL: NATIONAL INTERNETWORK SCREEN

An information system for monitoring and managing national internet traffic, organized in order to combat terrorism, child pornography, drug trafficking, providing a response to mass attacks on the internet, abuse of its resources, illegal activities, and allowing blocking and reducing (degradation) the speed of access to dedicated internet resources and mobile applications to prevent illegal actions.



GOV-VPN: A SECURE NETWORK FOR PUBLIC AUTHORITIES AND SOCIALLY SIGNIFICANT FACILITIES

A virtual secure network(s) that provides safe and sheltered communications for public authorities and socially significant facilities (for example, between educational and medical institutions). It is also designed to provide secure access to information systems and the Internet. In addition, individual nodes of a Secure Network can be provided with a content filtering service that allows you to block automatically resources and information that are legally prohibited (for example, extremist materials, pornographic materials, information about drugs and their distribution, calls for suicide, etc.).



GOV-SECWEB: A COMPREHENSIVE PROTECTION SYSTEM FOR INTERNET PORTALS PROVIDING PUBLIC SERVICES TO PEOPLE

This system is a set of organizational measures and technical means aimed at ensuring safe communication of citizens with government agencies on the Internet. The system is protected from any attempts to hack the portal and unauthorized receipt of personal data of legitimate users who have access to the System.



GOV-CYBER EARLY WARNING: CYBER THREAT EARLY DETECTION SYSTEM

It is designed to identify previously unknown types and types of attacks on cybersecurity systems of organizations. The System consists of separate servers, a group of servers, or virtual automated user workstations located

in various parts of the country and interconnected, to which relatively easy access is intentionally provided to potential attackers via pre-prepared "false" vulnerabilities. During the penetration attempt, the System identifies intruders and allows you to study the methodology and technique of their actions to carry out attacks on information systems, as well as identify the malicious software and equipment used in order to work out and apply methods of countering such attacks to «combat» systems.



GOV-CYBER RANGE: NATIONAL CYBERPOLYGON

A software and hardware complex designed to increase the state's readiness to repel cyber attacks and strengthen national security, including standard infrastructures of facilities with critical it infrastructure, as well as a platform for conducting cyber studies of any scale to practice interaction skills during cyber attacks, training specialists in actual practical cyber attacks' protection skills.



GOV-ANTI-DDOS: NATIONAL DDOS PROTECTION SYSTEM

A comprehensive system of protection against attacks of the distributed denial of services type (hereinafter ddos) provides reliable protection against massive distributed attacks on the critical infrastructure of the state at the l3/l4 levels of the osi model. The deployed system neutralizes even the most complex and massive attacks up to 7.6 Tbps and ensures round-the-clock availability of internet resources to users.

Positive Technologies is an industry leader in result-driven cybersecurity and a major global provider of information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage. Over 4,000 organizations worldwide use technologies and services developed by our company. Positive Technologies is the first and only cybersecurity company in Russia publicly available on the Moscow Exchange (MOEX: POSI), with 205,000 shareholders and counting.

For over 20 years, we've been developing our own visionary approach to creating solutions. Our technology and strategies are transforming the industry and significantly increasing the security of companies to a level that makes entire industries and nations safer. With our help, any company in the world can adopt result-driven cybersecurity.

Positive Technologies has handled a range of security projects for major federal and global events, including the Olympic Games in Sochi, the Universiade in Kazan and Krasnoyarsk, the FIFA World Cup, and the Russian presidential elections.

We develop our solutions based on longstanding experience and the unique know-how of our research center, one of the largest in the world. Here white hats analyze the security of systems in collaboration with cybersecurity experts focused on investigating real incidents and studying the techniques hackers use to attack. Our products come together to power a series of unique solutions that leverage Positive Technologies experience in protecting businesses of all types and implement national and international security standards.

Today, our range of protection technologies is the biggest on the domestic market, over the past two years and beyond proving their effectiveness in practice and consolidating their position as the de facto standard in a number of areas. Positive Technologies solutions are in demand and competitive on international markets and poised to catapult the Russian cybersecurity sector to become a significant export of the domestic economy.

METAPRODUCTS

Our new class of solutions-metaproducts-focuses on result-driven cybersecurity. **MaxPatrol 02** automatically detects and prevents attacks before the company is exposed to non-tolerable damage. This first metaproduct can replace a company's entire security monitoring center team, and it only takes one person to manage. The MaxPatrol 02 protection system requires minimal knowledge and effort from a specialist. To demonstrate that our result-driven approach to information security truly works, we conduct cyberexercises (on our own and on the infrastructure of other companies) and test our products publicly.

PRODUCT PORTFOLIO

<div><div></div><div>Perimeter protection</div></div> <div><div></div><div>Centralized management</div></div>	<div>PT NGFW</div> <div>The first next-gen domestic Russian firewall with high performance, reliability, and stability. In building PT NGFW, our specialists with experience in leading global network equipment manufacturing companies kept an open ear to the feedback of direct users among Positive Technologies' clients and partners.</div>
<div><div></div><div>Shows what is happening on the network</div></div> <div><div></div><div>Detects complex targeted attacks</div></div>	<div>PT Network Attack Discovery</div> <div>A deep network traffic analysis (NTA) system for detecting attacks on the perimeter and inside the network. It shows what's going on in the network, detects malicious activity even in encrypted traffic, and helps investigate incidents.</div>
<div><div></div><div>Protection against targeted and mass attacks</div></div>	<div>PT Sandbox</div> <div>A sandbox that helps protect company infrastructure against targeted and mass malware attacks and zero-day threats. It checks incoming files and links in an isolated virtual environment, gives a verdict on if they're malicious or legitimate, and blocks threats.</div>
<div><div></div><div>More than 400 built-in rules for detecting CS violations</div></div> <div><div></div><div>Ease of implementation and scaling</div></div>	<div>PT ISIM</div> <div>An ICS network traffic analysis system. It helps locate traces of information security breaches on ICS networks and detects cyberattacks, malware activity, and unauthorized employee actions (malicious or unintentional) at an early stage and in compliance with all regulatory requirements.</div>
<div><div></div><div>Blocking zero-day attacks</div></div> <div><div></div><div>Protection against DDoS attacks at the application level</div></div>	<div>PT Application Firewall</div> <div>A web application firewall. It protects company web resources against cyberattacks (L7 DDoS and zero-day attacks) and threats from the OWASP Top 10 and WASC lists. Gartner's Magic Quadrant visionary.</div>
<div><div></div><div>Convenient collaboration</div></div> <div><div></div><div>Automatic confirmation of vulnerabilities</div></div>	<div>PT Application Inspector</div> <div>A tool for detecting vulnerabilities in applications. It combines static (SAST), dynamic (DAST), interactive (IAST), and software composition analyses (SCA). Infosec specialists use the tool to identify and confirm vulnerabilities in source code, and it also helps developers fix code faster in the early stages of development.</div>



Configured individually according to the customer's requirements

PT BlackBox

A security scanner for web applications. It makes security researchers' jobs easier and provides useful information to help fix vulnerabilities.



Cloud Security

PT Container Security

A high-tech, innovative solution for comprehensive protection of hybrid cloud infrastructure. It ensures the secure development of software systems that use containerized virtualization.



Allows to prioritize vulnerabilities according to the level of their danger to business processes

MaxPatrol VM

A system that helps build vulnerability management processes and control corporate IT infrastructure security. The system collects, updates, and stores all information about assets to detect new vulnerabilities on hosts and notify users about them, including trending and highly dangerous vulnerabilities that need to be eliminated first.



For small IT infrastructures



Affordable start to the world of SIAM

MaxPatrol SIEM

An information security event monitoring system. It's regularly updated with expert knowledge on how to detect current threats and adapts to changes in the protected network. In 2020, MaxPatrol SIEM sales grew by 85%. Positive Technologies is among the top three global vendors with the highest annual sales growth of SIEM solutions. According to a study by IDC Global, Positive Technologies is the only Russian vendor in the top 20 SIEM systems globally (2021).



Collects important data for conducting investigations

MaxPatrol EDR

A system that protects company employees and devices from complex and targeted attacks. It helps identify complex threats and targeted attacks fast, responding confidently and automating routine operations based on the company's specific cybersecurity infrastructure and processes.



Ability to scan the network in test mode

MaxPatrol 8

A system used to assess IT infrastructure security. It helps determine the effectiveness of security processes and ensures compliance with standards.



Checks for vulnerabilities

XSpider

A vulnerability scanner built to show the real state of a company's network security. It scans workstations, servers, network devices, and web applications, and analyzes hosts without using preinstalled agents.

SERVICE PORTFOLIO

- **Detection of complex incidents, response and investigation, and monitoring the security of corporate systems** with the PT Expert Security Center (PT ESC). ESC monitoring powered by Positive Technologies products proved its effectiveness at the 2014 Winter Olympics in Sochi and 2018 FIFA World Cup by helping repel approximately 38,000 cyberattacks on transportation services.
- **Continuous business security assessment** helps evaluate company protection from attacker actions in a continuous manner, prevent attacks in time, and mitigate the consequences of security incidents. Assessment types include Pentest 360, APT Emulation, and Red Team vs Blue Team.
- **Hardware vulnerability analysis** by our experts provides the information needed to eliminate risks associated with hardware vulnerabilities.

Positive Technologies is proud to be the creator of the **Standoff 365** platform, designed to improve business security through hands-on cyberexercises and security system research. The platform helps:

- Businesses test the resistance of their real systems to cyberthreats and bolster the skills of their infosec specialists to improve company security
- Security researchers explore different types of infrastructure, improve their vulnerability detection methods, and earn prizes

Today, the platform has more than 8,000 active users and includes the following:

- **The Standoff cyberbattle**—an international offline event that has been bringing together infosec specialists and security researchers to test and hone their skills on the most realistic infrastructure possible since 2016. At the cyberbattle, companies test the maturity of their infosec services in an onslaught of live attacks from pentesters, and security researchers compete to identify vulnerabilities in different security systems and bring their experience back to their companies. More than 1,500 security researchers and 100 infosec teams have shown what they're made of over 12 battles in eight years. The Standoff cyberbattle is the largest and most recognizable event in the segment.
- **The Standoff online cyberrange** —a virtual copy of companies' IT systems to test the skills of security researchers and infosec specialists. The cyberrange is open 24/7 all year round so that companies' infosec specialists can practice identifying, investigating, and repelling attacks to use this experience later on the job, and security researchers can test hypotheses about the realization of non-tolerable events using different attack vectors and hone their vulnerability identification skills. The cyberrange includes more than 400 virtual machines forming a single infrastructure.
- **Bug Bounty Standoff** — a platform for searching for vulnerabilities in company systems. The rules are simple: companies make their apps or infrastructure

available publicly or privately to test their reliability. Companies can also list specific vulnerabilities or events that security researchers need to trigger to earn a reward. Then if researchers manage to identify vulnerabilities or realize a non-tolerable event, they prepare and submit a step-by-step report. The company only pays if a specific event is triggered and a report is submitted that describes the entire course of the attack in full. An additional triage service is offered to help companies verify the accuracy of the report and provide recommendations on how to eliminate the identified vulnerability. Since the program was launched two years ago, more than 4,500 vulnerability reports have been submitted. Today, the platform hosts 55 programs.

The Positive Technologies team readily shares what we know about information security:

- For 12 years, we've been holding Positive Hack Days, our own research and practical forum. As one of the largest information security events in Russia and the CIS, it's attended by thousands of people who care about cybersecurity, including IT and infosec experts, business and government representatives, and white hats. Positive Hack Days hosts hundreds of talks, workshops, and competitions on the analysis of protection of industrial control systems, banking and mobile services, and web apps. In 2023, the forum was held for the first time as an open cybersecurity festival to bring together infosec experts, technology developers, and everyone else interested from the general public;
- Check out the latest information security news on our SecurityLab.ru portal;
- We develop educational programs for leading universities and help students get a head start in their careers: Positive Education materials created by our company experts are used at over 65 universities.

Security Vision is a Russian company developing a platform for robotization of up to 95% of the software and hardware functions of an information security operator. A single platform for all products (including partner developments) ensures continuous analysis, response to threats and cyber incidents, and reliable protection of information assets of the largest state and commercial structures, including Sberbank, Alfa-Bank, Evraz, Cherkizovo, FSO of Russia, Tinkoff Bank, Gazprombank, Severstal, MKB, Nor Nickel, Federation Council, Goznak, Russian Post, Magnit and many other government agencies and commercial structures.

Security Vision is the winner of 26 professional awards, including "For Strengthening Russia's Security", "Import Substitution", the National Priority Award, the TAdviser IT Prize in the nomination "CS Solution of the Year in Russia", the Runet 2023 Award in the nomination "Cyber Security".

SECURITY VISION IN FIGURES:

120+

professionals in the team

30+%

of the Russian TOP 100 companies as Customers

7/10

of the TOP 10 Banks as Customers

14/20

of the TOP 20 Banks as Customers

1

proprietary data center

30+

competent and trained partner companies

2010

the year of the first research in automation

5+

MSSP information security service providers use the platform to provide services

Security Vision solutions are developing in three directions according to the classic triangle of connections:

1 TECHNOLOGY +

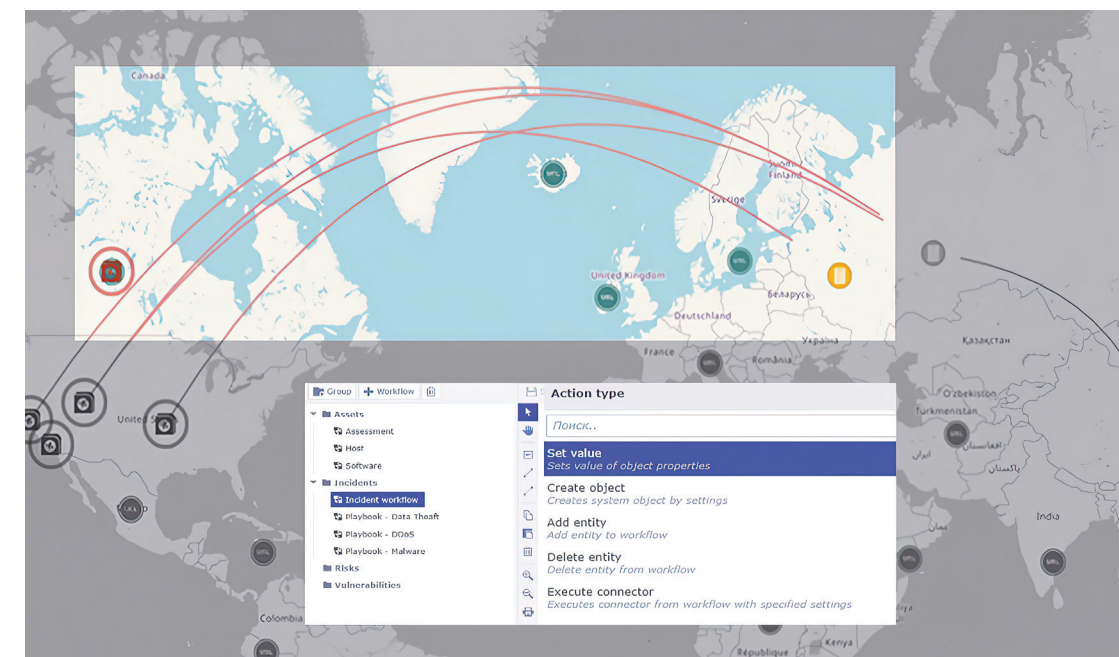
2 PROCESSES +

3 PEOPLE

All solutions can be used as independent products or as modules within a single installation to solve complex problems. The main tasks and solutions are listed in the catalog below.

1. SOT – SECURITY ORCHESTRATION TOOLS

This direction combines products for managing practical security and creating an ecosystem of disparate products with their subsequent orchestration.



1.1 NG SOAR (NEXT GENERATION SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE)

Complex product consisting of 5 modules: **SOAR** (1.2) + **SIEM** (Security Information and Event Management with built-in baseline rules correlations) + **VM** (1.3) + **VS** (Vulnerability Scanner for search technical vulnerabilities) + **AM** (1.4)

1.2 SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE)

Management of information security incidents when collecting data from connected information security tools (SIEM, UEBA, AV/EDR, NGFW, WAF, Proxy, etc.) and IT systems, as well as collecting the surroundings of incidents using built-in mechanisms. The response is built according to the NIST methodology with the construction of a kill chain, a built-in classifier (200+ types of incidents) and the MITER ATT&K database (100+ techniques and tactics). Dynamic playbooks with support for object-oriented response are built automatically depending on the type of incident and environment (internal/external host, account, email address, URL, malware, process, vulnerability). At various stages of incident processing, response recommendations from experts and automatic SLA configuration are built in.

1.3 VM (VULNERABILITY MANAGEMENT)

Vulnerability management with the ability to connect external scanners (for example, via API for collecting data and launching scans), using reports (for example, XML) and a built-in CVE database (BDU FSTEC, NVD by NIST, Microsoft bulletins and other sources). Support for external analytical services (VulDB, Vulners, AttackersKB, OpenCVE, etc.) that complement the quality of source reports. The solution automatically determines SLA in

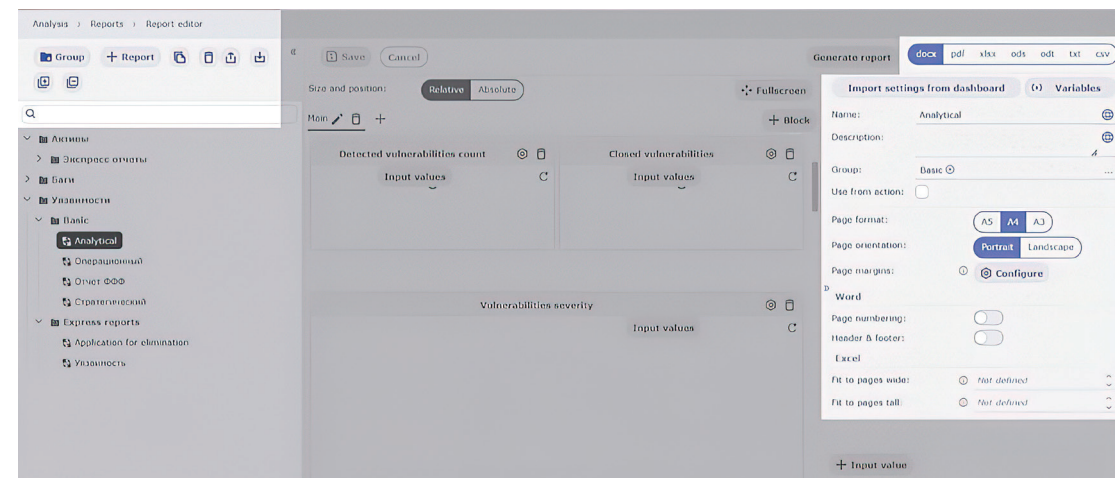
requests for elimination based on a set of various parameters (for example, CVSS and IT asset data) with the creation of tickets both within the solution and in third-party ITSM/SD systems (Jira, Naumen, etc.).

1.4 AM (ASSET MANAGEMENT)

Asset and inventory management with support of regular agentless search for new objects, customizable distribution into categories without restrictions on the number of objects, their types, network segments, users and roles for companies of any size. Inventory can be performed autonomously (execution of PS, SSH scripts) or using third-party solutions, for example: AV/EDR, DLP, VM, LDAP, SIEM, etc. The solution provides control over the composition and condition of assets (hardware, software, accounts etc.) from a single web interface with the ability to run automation scripts as part of collecting information and conducting investigations, incl. proactive steps to respond.

2 GRC – GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

This direction combines products designed to solve problems of “paper” security and business process management in a company.



2.1 CM (COMPLIANCE MANAGEMENT)

Management of compliance with selected regulatory and methodological recommendations (measures and requirements of ISO, Personal data, etc.) with the creation of work processes, cards and questionnaires sent to all audit participants (with or without the involvement of an expert group) for subsequent assessment of compliance. Supports the ability to set and track tasks to eliminate comments for connecting performers, as well as flexible editors of reports and dashboards for generating reporting and analytics in real time.

2.2 CERT (COMPUTER EMERGENCY RESPONSE TEAM)

Interaction with regulators (for example FinCERT) with the sending of information about incidents by the operator. Can be carried out in both automatic and semi-automatic modes via the main (API) or backup (corporate mail) channels for fault tolerance. Generation based on the information received (new tasks, requests or incidents – depending on the customer’s built-in internal processes).

2.3 RM (RISKS MANAGEMENT)

Risk management (cybersecurity or operational) with maintaining a directory of threat modeling results (objects of impact, information security threats, potential of an intruder, protective measures, methods of implementation, etc.) according to its own or built-in methodology. Support is provided for the formation of an expert group, filling out questionnaires, assessing the likelihood of threats occurring and the effectiveness of protection measures with the involvement of experts and owners of information systems using qualitative/quantitative or combined methods.

2.4 BCP (BUSINESS CONTINUITY PLANNING)

Business continuity management with BIA (Business Impact Analysis) algorithms for assessing the criticality of business processes and objects, BCP (Business Continuity Plan) for planning requirements and priorities in case of emergency situations, regular testing of plans with assessment of key performance indicators according to various standards (ISO 22301, GOST 22301 and others). Supports the ability to set and track tasks to eliminate comments for connecting performers, as well as flexible editors of reports and dashboards for generating reporting and analytics in real time.

3 SDA – SECURITY DATA ANALYSIS

This direction combines solutions that solve analytical problems to help employees solve technical problems. For processing big data machine learning technologies are used.



3.1 TIP (THREAT INTELLIGENCE PLATFORM)

Analysis of cybersecurity threats and conducting cyber intelligence with the formation of a base at all levels of threat analysis: technical (hash, IP address, URL, domain, email), tactical (process, JARM, registry key), operational (vulnerabilities, malware) and strategic (attribution of data about attackers and threats). The solution includes 50+ integrations (with the ability to develop new ones) for receiving events from solutions of various classes (SIEM, NGFW, Proxy/Email server, etc.), using universal formats (Syslog, CEF, LEEF, EMBLEM, Event log), and optimizing data for long-term storage. For detection and response, advanced mechanics are built in combination: DGA mechanisms using machine learning, match and retro search based on the collected data detect a match based on any object parameters.

3.2 UEBA (USER AND ENTITY BEHAVIOR ANALYSIS)

Behavioral analysis with the collection of “raw” events from various sources through integration with information security and other sources of information security events (when collected, events are converted into incidents when their number accumulates, for example, when volume indicators and total weight are exceeded. White lists are supported (for exceptions) and lists of critical systems (for automatically creating incidents without taking into account events and their weight), as well as various analysis technologies: correlation rules (~30 pieces) in combination with methods of mathematical statistics (~50 rules) and machine learning based on open-source datasets (DDoS, bots, lateral, malware, suspicious etc.), emulation of attack scenarios at the Security Vision cyber testing site, as well as “training” of the system on client traffic (“supervised” models).

The Security Vision Platform is a base for boxed and project modules (see above), as well as a low-code/no-code environment for conducting in-house development. To create content, special constructors, available to users of any product are sewn into the platform:

- **Constructor of objects** — cards and tables for displaying different types of data, buttons, chats, logs, etc. For example, assets, users, vulnerabilities, incidents, or remediation requests.
- **Workflow Constructor** — for organizing and/or automating various actions. For example, the life cycle of an asset, the process of proceeding an application, or automation of SLA assignment
- **Connector Constructor** — integrations available out of the box and configurable using low-code through the interface for different types of transport. For example, interaction via API, proprietary protocol, working with the database directly or parsing a file
- **Role model and menu Constructor** — to delineate areas of responsibility and customize menu items. For example, a manager, an OT specialist, L1/L2 CS specialists or a risk analyst
- **Widget and Analytics Constructor** — BI for displaying the necessary data in graphs and interactive dashboards. For example, a pie chart by asset type, a chart by the number of incidents, or the location of objects on a world map, city, or office
- **Report Constructor** — an editor for creating document templates. For example, weekly uploading of an express report on an asset/incident to doc or a weekly report on the necessary objects to xls

XII

**International Meeting
of High Representatives
for Security Issues**

April 23-25

EXPOFORUM
Convention and
Exhibition Centre
Saint Petersburg



expo.komib.ru

2024