SOLAR | Rostelecom

United Nations Convention against Cybercrime
SIGNING CEREMONY
& HIGH-LEVEL CONFERENCE

Cybersecurity and national digital sovereignty

Solar – National cybersecurity services provider

SOLAR | Rostelecom

[01] ARCHITECT OF COMPLEX CYBERSECURITY PROJECTS

Solar has vast experience in developing and implementing complex cybersecurity systems on a national level

[02] PROVIDER OF CYBERSECURITY SERVICES

Being one of the top providers in the world Solar's cybersecurity service portfolio covers all existing areas

[03] MANUFACTURER OF CYBERSECURITY PRODUCTS

Solar produces the widest variety of cybersecurity products and constantly develops new advanced technologies

SOLAR Protecting the most critical and attacked organizations, web-resources, processes and events in Russia

№1
On Russian cybersecurity services market

Top-5
Managed Security Service Provider (MSSP) in Europe

2500+
Cybersecurity experts

1500+
Organizations protected

600+
Projects completed per year

200 bln
Events analyzed per year

1,5 bln
Cyberattacks repelled per year

100 mln
Users protected every day

Solar – part of Rostelecom Group

SOLAR | Rostelecom

13,4 mln
Users of high-speed Internet services

49 mln
Users of mobile network services

11,8 mln
Households with subscription TV services

125+ thous
Experts in the group of companies

Rostelecom

Russia's national telecommunications operator and largest state provider of digital services

- High-speed Internet
- Mobile Network
- Data Centers
- OTT Media
- Streaming Services
- Cloud Services
- E-Government
- Cybersecurity

Develops and operates critical public information systems and a wide range of solutions for the digital services ecosystem

Key technological partner of the State in the most significant digitalization processes and National projects

- Digital Economy of the Russian Federation 2019-2024
- Data Economics and Digital Transformation of the State 2025-2030

Main reasons for the increasing importance of National Cybersecurity

SOLAR | Rostelecom

TECHNOLOGICAL BREAKTHROUGH

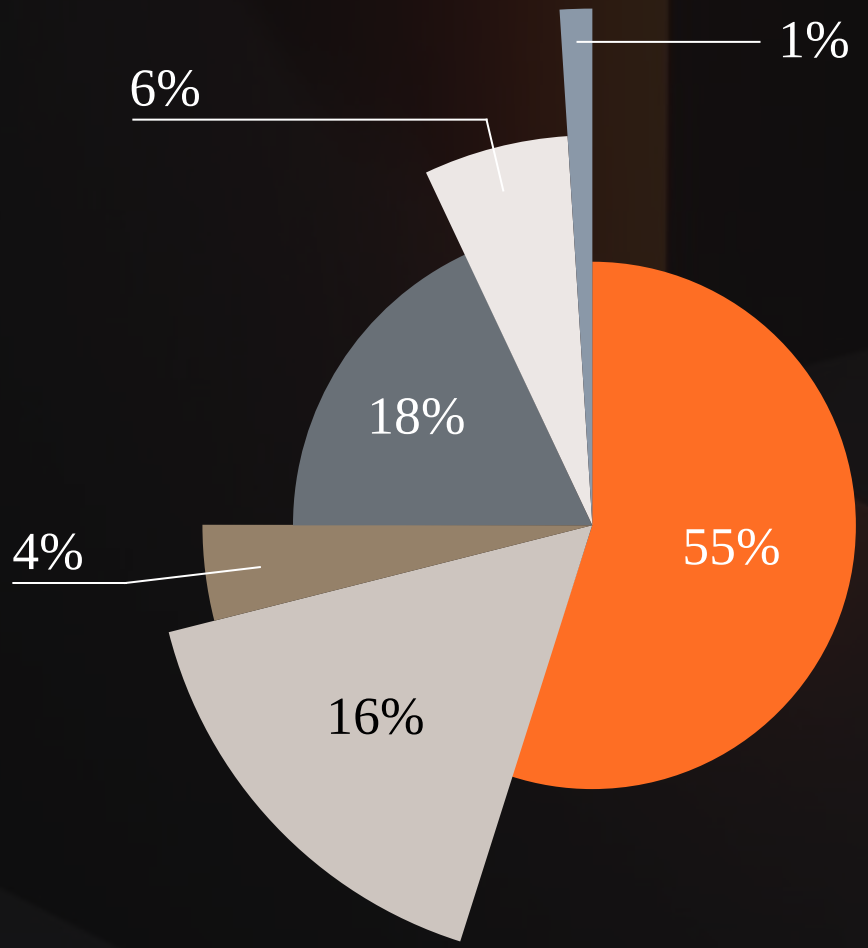
- Rapid technological progress
- Digitalization of governments and military
- Emerging Artificial Intelligence
- Rising number of web-resources

CYBER RISKS

- Interstate geopolitical conflicts
- Terrorism and extremism
- Rising cybercriminal activity
- Existing vulnerabilities and exploits

Critical public infrastructure – main target of cybercriminals

SOLAR | Rostelecom



- Public sector
- Food industry
- IT sector
- Transport
- Financial sector
- Healthcare

MALWARE INFECTION

NETWORK ATTACKS

ATTEMPTS TO EXPLOIT VULNERABILITIES

Cybersecurity – a worldwide necessity

SOLAR | Rostelecom

Investment in cybersecurity is not dependent on geography. Absolutely all countries regularly face new digital attacks

The average number of cyber attacks on organizations in Africa increased by 39% — more than the global average

Latin America is one of the least protected regions, with an average cybersecurity score of 10.2 out of 20

Public sector, transport and healthcare are the least protected sectors in the CIS

Ransomware, data loss and cyberespionage are among the main cyberthreats in MENA region

Southeast Asia countries are among the most frequently attacked and their mentions on the darknet have increased unprecedentedly

Solar's experience

SOLAR | Rostelecom

SOLAR JSOC | MSS: THE VAST MSSP EXPERIENCE, A SERVICE-BASED ECOSYSTEM MODEL

Center for countering cyberattacks

- Russia's leader in commercial MSSP
- 1500+ organizations under protection
- Top-5 European MSSP
- Top-15 Global MSSP

Ensures the security of the country's key infrastructures, including: State services, direct lines of the President, electoral processes

CYBERTHREAT RESEARCH CENTER

4RAYS by SOLAR

Unique and largest database of threats relevant to the Russian Federation

- Data from the sensors of telecom network of Rostelecom - largest in the Russia
- Telemetry of services of the largest commercial SOC in the Russia, as well as Solar products
- Results of own cyber-landscape research

SOLAR CYBERRANGE AND «CYBERMIR» PLATFORM

Proprietary platform for conducting cyberdrills and trainings on twins of actual digital infrastructures

- Created within the National Digital Economy Project
- 500+ conducted cyberdrills
- Adaptability of infrastructures
- Most up to date scenarios

Vast experience in conducting international championships, drills and other events

MANAGEMENT CONSULTING ON CYBERSECURITY

Practical experience of implemented cybersecurity management consulting projects in key industries

- Development of cybersecurity strategy: from assessment of maturity and diagnosis, to analysis of personnel expertise
- Quantification of cybersecurity risks: trend analysis, construction of a risk management system, diagnosis of the cybersecurity service model

Solar’s solutions lineup

SOLAR | Rostelecom

Application Security

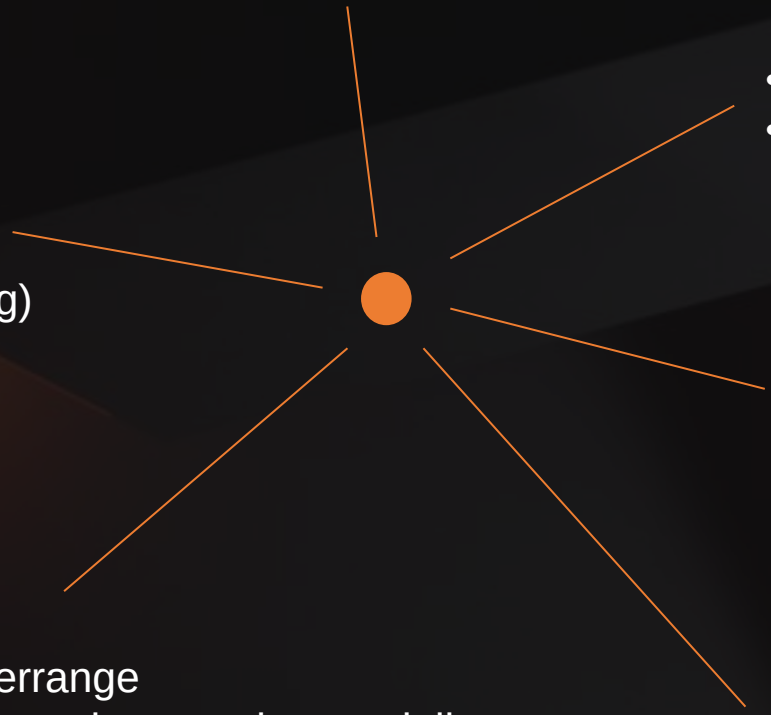
- DevSecOps processes development
- SAST, DAST, SCA, SCS Technologies
- Application Security Center

Access control

- Identity management / Identity Governance & Administration (IdM / IGA)
- Privileged Access Management (PAM)
- Data Access Governance (DAG)

Data and network protection

- Data Loss Prevention (DLP)
- Secure Web Gateway (SWG)
- Next Generation Firewall (NGFW)
- ERP Scan (Enterprise Resource Planning)



SOC & MSS

- Security Operation Center consulting
- Managed Security Services
- Offensive security, penetration testing
- Threat Intelligence feeds (TI)
- Digital Risk Protection (DRP)

Education and training

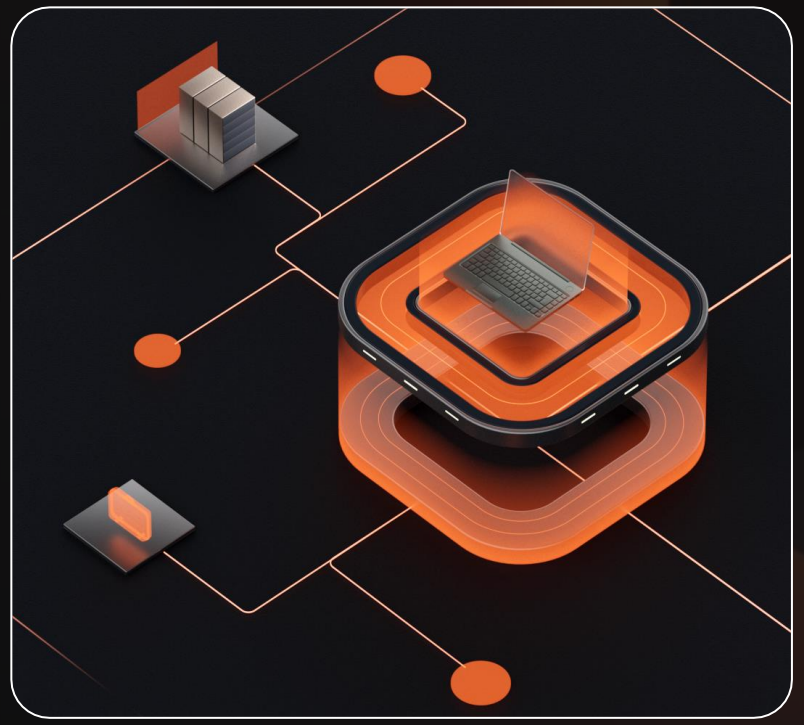
- Practice-based education on Solar Cyberrange
- Development of educational programs for cybersecurity specialists
- Evaluating the skill level of cybersecurity personnel
- Cyber exercises for various cybersecurity specialists
- Security Awareness
- Cyberdrills and cyberchampionships

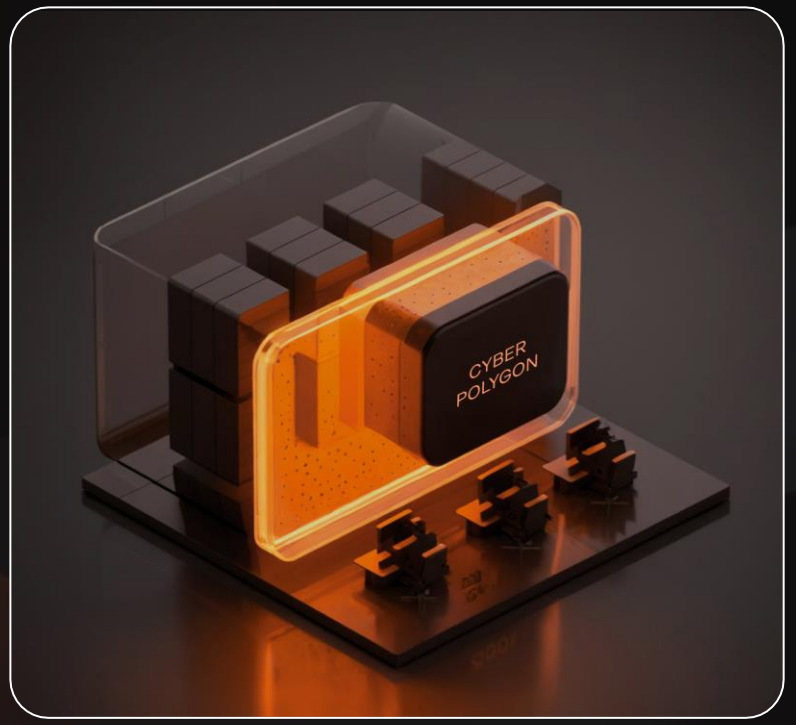
Sovereign Cyber Defense

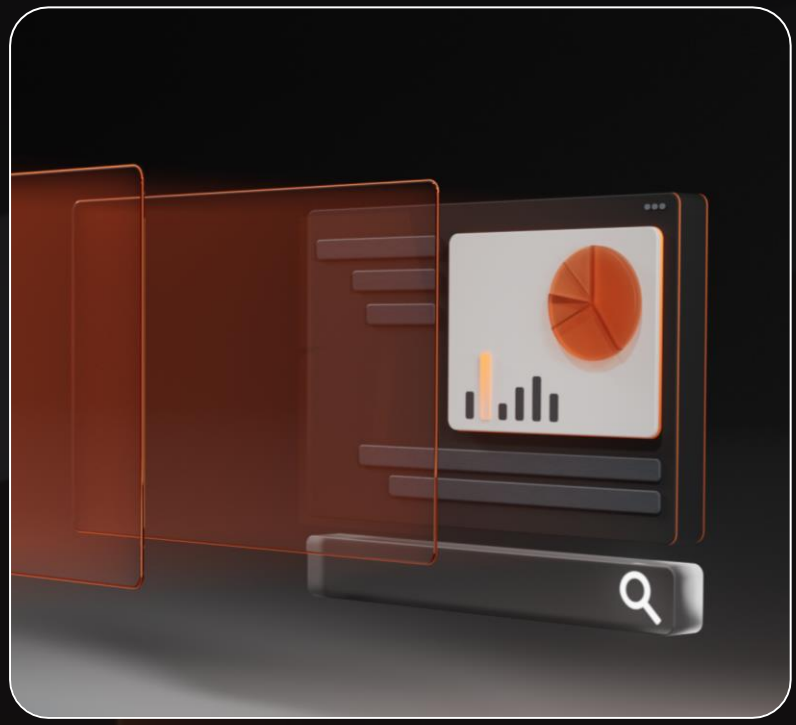
- DNS Radar – Cisco Umbrella alternative
- Own Cyber Fortress – Shodan alternative
- Solar Space – CloudFlare alternative

Solar’s expertise in helping build Digital Sovereignty

SOLAR | Rostelecom







INFRASTRUCTURAL SOLUTIONS

Creating computer incident response centers and security operations centers; building cyber ranges; implementing a web resource protection system and network security; building a software protection center; etc.

EDUCATIONAL SOLUTIONS

Conduct of cyber-drills at the Solar Cyberrange; exercising the most relevant scenarios and techniques for countering cyberattacks in conditions close to real ones, on digital infrastructure doubles; training courses for cybersecurity specialists

ARCHITECTURAL SOLUTIONS AND SERVICES

Assessment of the maturity of infrastructure; building a cybersecurity system at all levels; assessment of the competences of teams of cybersecurity specialists; testing and analysis of security; streamlining of processes

National cybersecurity system

SOLAR | Rostelecom

Education and training:
National system for constant training and enhancing skills of cybersecurity experts

Combatting cyberattacks:
National Center for monitoring and responding to computer incidents

Network protection:
Perimeter protection of national telecom networks through traffic analysis

Data protection and access control:
Up to date solutions for protection of information in critical infrastructure

Application security:
National system for protection of applications and software

Security awareness:
Continuous work on raising digital literacy of personnel and users

National regulation:
Competent cybersecurity Public Authority and robust legal framework

Proactive security:
Continuous work on threat analysis, digital risk protection, security analysis, testing, etc.

CYBERSECURITY ROADMAP: EFFECTIVE WAY TO IMPROVE INFRASTRUCTURE & SKILLS

Cybersecurity Management Session: Tabletop Exercise

SOLAR | Rostelecom

Side Event format: Management simulation

Time: 13:00 to 15:00, 26 October 2025

Place: Room R309A

Participants: Delegates of the Ceremony regardless of background and expertise

Scenario: 10 questions dedicated to 10 stages of a cyberattack. Each stage includes multiple-choice questions with response options. Participants receive expert explanations and practical insights throughout the simulation

Reviewing the results of online Cybersecurity Training & Exercise

25 teams from 10 countries participated in online cyber-exercise on 25 October 2025

Participants: 20 Blue teams and 5 CERT teams consisting of cybersecurity experts representing various regions

Infrastructure: Digital infrastructure twin created on Solar Cyberrange modeling real-life critical information infrastructure

Scenario: Participating teams were tasked with combatting waves of cyberattacks in the most up to date scenarios, as well as coordinating with CERT teams in responding to computer incidents

SOLAR | Rostelecom

Контакты:

Дамир Зарипов
Менеджер продаж UZTELECOM
+998 95 008 01 75