# CERT.LV ACTIVITY REVIEW

# Q1 2024

CERT.LV
Information Technologies Security Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

**Since Russia's full-scale invasion of Ukraine, Latvia continues to experience a high level of cyber threats. In Q1 2024, the number of threats and incidents reduced only by 3% compared to the same period in 2023. In addition, it was 5% higher than in the last three quarters of previous year. Latvia has demonstrated a convincing cyber- resilience, and cyber-attacks recorded so far have not had a significant or lasting impact on society.**

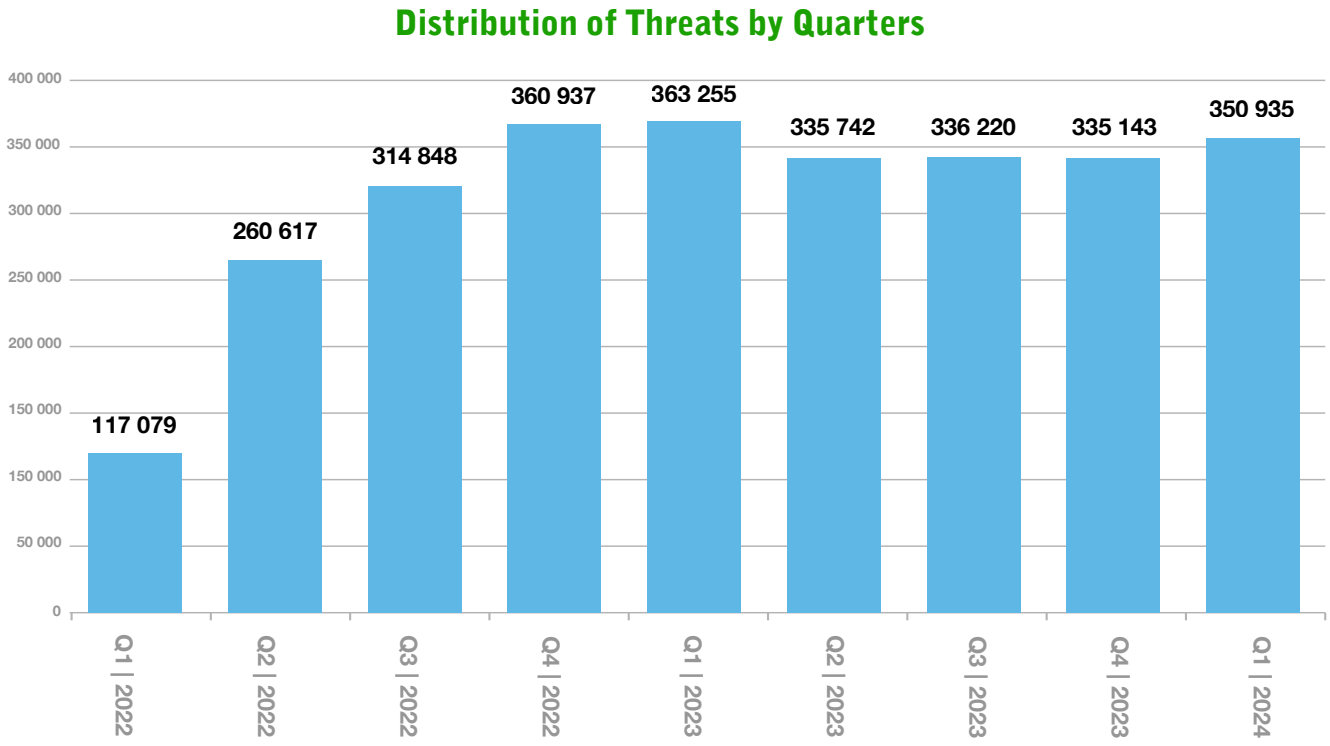


**Figure 1. Unique IP addresses at risk by quarter in 2022-2024**

CERT.LV has actively promoted its role as a leader in threat hunting operations in the European Union, strengthening the cyber resilience of Latvia's critical infrastructure and digital services. As a result of these operations, it has been possible to repeatedly identify and successfully eliminate the presence of cyber operations units of other countries in the Latvian infrastructure. To date, more than 100,000 devices in 25 organisations have been analysed. In partnership with NATO Allies and the Canadian Armed Forces Cyber Command, CERT.LV continues to strengthen international cooperation and collective defence, which is important not only for Latvia, but also for the cybersecurity of the Alliance.

## Cyer Security Threats and Their Trends

No national-level or highly significant threats were recorded during the reporting period. Significant threats with a broad impact on the commercial sector, state and local authorities represent only 0.03% of all categorised threats, yet the number of compromised unique IP addresses registered in this category is 218% higher than in Q1 2023. The upward trend also continues compared to Q4 of last year, with an increase of 26%.

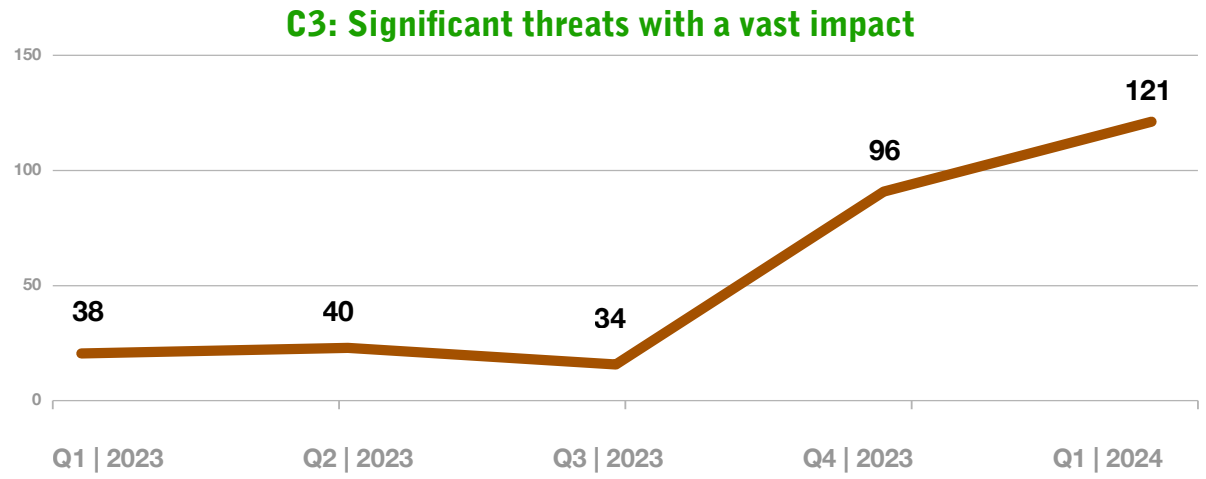


**Figure 2. Number of compromised unique IP addresses in category C3**

Intrusion atempts, malicious code, and harmful content are the main threat types with the highest increase in activity in Q1 2024. In the current geopolitical situation, it can be assumed that this is due to politically motivated Russian hacking attempts, aimed at compromising the critical infrastructure of NATO and EU Member States. These trends highlights to the need to continually strengthen security measures and educate the public about potential threats.

Intrusion attempts are on an upward trend, with an increase of 118% compared to the same period in 2023.

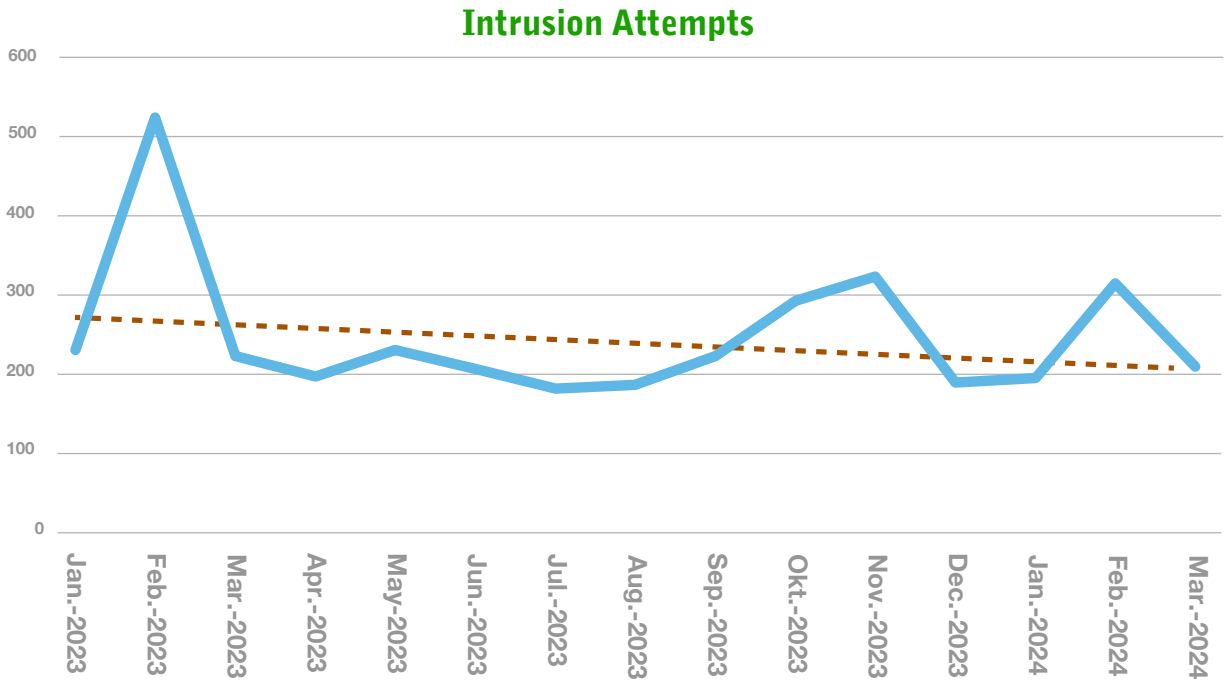


**Figure 3. Number of compromised unique IP addresses**

Information on intrusion attempts was received throughout Q1 at a significant rate. These attacks were carried out in most cases through brute-force attacks against various electronic communications companies, State and local authorities, and the private sector. Attackers also exploited long-known configuration flaws in widely used products. The recorded cyber-attacks, however, did not have a significant or lasting impact on resources and services.

Most often, unauthorised access to a web server and unauthorised modification of its files occurs through vulnerabilities in versions of content management systems (CMS) or the plug-ins used by these CMS that have not been updated . Thus, the delayed update of CMS and their plug-ins is the predominant cause of compromised web servers. WordPress-based websites are more frequently compromised than others. This is due to the fact that WordPress is the most commonly used CMS.

Cyber attackers' interest in technologies used for remote working, such as Remote Desktop Protocol (RDP), Virtual Private Network (VPN), and online meeting and chat platforms, has not diminished. Attackers do research before attacking, they look for weaknesses in the resources an organisation is using, before attempting intrusions. The 'weakest' link in the chain is the one used to carry an attack through.

**Vulnerabilities and vulnerable systems are an ongoing risk,** affected by newly discovered critical vulnerabilities, misconfiguration of IT systems, and outdated IT solutions. Supply chain attacks have been observed against organisations with a high level of security - attackers gain access to a target by attacking software developers and other outsourced service providers.

**In Q1 2024, the number of unique IP addresses compromised with malicious code registered by CERT.LV increased by 22%** compared to the same period last year. In addition, 6,272 unique IP addresses were registered with this threat type in January this year. This is the second highest number in the last three years. The main types of malware in the reporting period were: user data hijackers, botnets, ransomware, and remote access Trojans – all aimed at data retrieval or further infrastructure compromise.

The most common user data-jacking malware targeted insecure, locally stored authentication data and passwords, i.e., extracting passwords from a web browser or unencrypted files. Compromised emails or app accounts were used to further spread malware. For example, several cases of Agent Tesla malware being spread from compromised emails by sending fake invoices were identified. The number of cases where users deceived by fake advertising have installed fake AI plug-ins in their web browser themselves has not decreased. Encryption ransomware was also distributed for profit, attacking the victim's device, decrypting the data and demanding a ransom to recover it.

**Politically Motivated Denial of Service Attacks (DDoS)** by Russian hacktivist groups continue in waves, targeting public administrations and companies in specific sectors. The proportion of successful attacks is decreasing, which shows the readiness of Latvia's infrastructure, the effectiveness of the centralised DDoS protection service funded by the Ministry of Defence, and the ability of communication operators to provide services continuously in the event of an external attack.

**Financially motivated attacks most commonly use e-mails and text messages from an apparently trustworthy source.** During the reporting period, scammers most often posed as representatives of the State Revenue Service, the State Police, the court, or banks. Phishing on behalf of various courier services continues, and scammers with fake job offers have become more active. Phone scammers have started to actively use artificial intelligence tools, creating simulated versions of real people's voices. 21% of victims fall into the trap set by scammers due to haste and inattention.

## Effectiveness of DNS firewall active protection

In the reporting period, DNS firewall users were protected from malicious websites more than half a million times. Every detected threat indicator is placed in a centralised active protection infrastructure - the DNS firewall - to effectively protect all Latvian citizens, businesses, and organisations that use the protection provided by CERT.LV. In two years, the use of the DNS firewall service has increased by around five times, with around 1.5 million DNS requests processed per month.

CERT.LV offers companies and institutions that maintain their own DNS recursive servers the possibility to use the DNS RPZ (Response Policy Zone) maintained by CERT.LV, which contains lists of dangerous resources identified by CERT.LV. In addition, CERT.LV also maintains lists created by competent authorities that include resources that, according to the laws and regulations in Latvia, shall be restricted from accessing electronic communications networks. CERT.LV has also created a separate DNS RPZ for each competent authority list and cooperates with the creators of these lists.

## Early Warning System (EWS), or a Network of Sensors to Identify Threats

During the reporting period, CERT.LV continued to maintain and expand the EWS system. The operation of the sensor software was also improved. On average, the EWS detects 6,000 high-priority (high potential threat) incidents per month in national, local, and critical infrastructure  institutions. During the reporting period, the total number of alerts generated by EWS is almost 718 million.

## Coordinated Vulnerability Disclosure (CVD)

During the reporting period, efforts to develop and promote the CVD platform continued with the introduction of a security researcher rating to motivate security experts to be more proactive in reporting vulnerabilities discovered, and efforts to engage new members to ensure a diverse perspective and approach to vulnerability management. By the end of the reporting period, there were 42 Security Researchers, seven active institutional programmes, and 24 vulnerability reports registered on the cvd.cert.lv platform.

**CVD** enables researchers to log a report of an observed vulnerability, as well as all the parties involved (the institution, the researcher, and CERT.LV) to review the submitted information, communicate with each other and track the progress of the vulnerability remediation.

## Cooperation with Critical Infrastructure (CI) Holders

Cooperation with CI holders continues, both in monitoring the situation in cyberspace and in providing advice and support to strengthen the cyber resilience of CIs and to improve cross-sectoral cooperation. CERT.LV actively coordinates the installation of sensors and DNS RPZs in institutions and enterprises to facilitate the faster identification of CI threats and more effective prevention.

## Support to Latvian National Law Enforcement Authorities

During the reporting period, CERT.LV provided support to Latvian law enforcement authorities in the investigation of cybercrime incidents, carrying out in-depth research and preparing responses to the State Police on several security incidents.

CERT.LV emphasises the need to continue raising awareness among the Latvian public about cyberspace and the risks of cybercrime in order to strengthen the resilience of society to cyber-attacks, mitigate their impact and contribute to their prevention. Particular attention should be paid to preventive methods and initiatives to block websites created for criminal purposes or used for criminal activities, to the recognition and implementation of these initiatives, and to improving the cooperation between the institutions involved and the speed of response by the responsible authorities.

## Security Tests and Assessments

During the reporting period, the CERT.LV team carried out a full security test of the systems used for the European Parliament elections. There were a total of three systems tested. For the resources that were subjected to intrusion tests, no critical vulnerabilities were identified, however, four medium- and three low-risk vulnerabilities were identified.

Reports on the results of the tests were provided to the resource holders and developers and recommendations were made to remedy the deficiencies. CERT.LV insisted on the need to carry out load tests based on the experience of previous elections and adapted to real load conditions. Several iterations of testing took place to make sure they are ready for the elections.

## Threat hunting operations

CERT.LV has been carrying out proactive cyber threat hunting operations in cooperation with partner countries in infrastructure systems critical to Latvia since 2022.

The role of cyberspace as a strategic environment has been discussed for several years already. In times of war, it is given the same strategic importance as land, sea, air, and space. This has become particularly important in the wake of Russia's full-scale invasion of Ukraine, as the Russian armed forces are also openly referring to cyberspace as the 5th domain for warfare.

CERT.LV team is a leader in organising and conducting threat hunting operations in the European Union. Threat hunting operations have significantly strengthened the cyber resilience of Latvia's critical infrastructure and digital services. CERT.LV threat hunting operations are carried out with the aim of identifying the presence of cyber threats in infrastructure systems important for Latvia.

According to CERT.LV, Latvia's 'new cyber-doctrine' is a significant increase in cyber defence capabilities, including with allied countries, developing capabilities and counter-attack capacity to prevent any possibility of an attack. Contributing to NATO's collective defence, CERT.LV continues its threat hunting operations in close cooperation with the Canadian Armed Forces Cyber Command.

During the reporting period, CERT.LV specialists, together with representatives of the Canadian Cyber Command, finalised the first edition of the Threat Hunt Playbook. The Playbook is to be continuously updated and refined. Information on what has been achieved, which is a major breakthrough in threat hunting worldwide, will also be shared with other partners.


In March, the first edition of the Playbook was solemnly presented to the NATO CCDCoE in Tallinn. The practical application of the CERT.LV Threat Hunting Playbook will be promoted through a series of hands-on workshops to be organised in Riga and open to Latvian and foreign partners.

## CERT.LV Support to the Digital Security Monitoring Committee Secretariat

CERT.LV actively participates in the work of the Digital Security Monitoring Committee (DDUK), providing support in the monitoring of qualified electronic identification service providers and trusted certification service providers and also maintains the LV trust list (LV TSL). In addition, CERT.LV experts have been involved in reviewing the draft eIDAS 2.0 Regulation and assessing its impact on the work planned by the DDUK..

## CERT.LV Support to the Digital Security Monitoring Committee Secretariat

Active involvement in the Latvian Central Election Commission's (CEC) Election Working Group continues, providing recommendations for the development and maintenance of secure electoral systems. CERT.LV experts regularly participated in the meetings of the Election IT Working Group, providing recommendations on security aspects of systems and testing. CERT.LV also provided its perspective on IT risks to the CEC in the context of securing the 2024 European Parliament elections.

CERT.LV is also actively involved in the Inter-institutional Working Group led by the National Coordination Centre (NCC-LV), which aims to facilitate the exchange of information between public administrations and organisations on activities and measures in different areas of cybersecurity to promote efficiency and cooperation.


On 2 February, CERT.LV hosted the Minister of Defence of the Republic of Latvia, Andris Sprūds, to discuss the activities being implemented to strengthen Latvia's cyber capabilities and cyber governance.


On 4 March, CERT.LV hosted the State President, Edgars Rinkēvičs to present the work of the CERT.LV team and the progress made so far in strengthening the security of Latvian cyberspace. During the visit, the President of Latvia visited the Operations Centre and the Industrial Control Equipment Laboratory of CERT.LV, met the CERT.LV Incident Response Team, and gained a deeper insight into the daily work of CERT.LV. E. Rinkēvičs especially praised the successful cyber threat search operations carried out by CERT.LV together with allies.

## Education and Improvement of Youth Cyber Skills

CERT.LV participates in the working group organised by the Saldus Technical School administration for the development of the standard for the qualification "Cybersecurity Technician", sharing its experience and providing its vision on the knowledge, skills, and competences required by specialists to ensure that the holders of the qualification acquire the necessary knowledge and become highly valued specialists already during their training.

During the reporting period, the European Union Cyber Security Division of the Ministry of Defence organises the Latvian national selection of the European Cyber Security Challenge 2024 (ECSC), a pan-European cybersecurity competition for young people. Latvia is participating in the European Cyber Security Challenge for the first time. The activity is part of the NCC-LV project coordinated by the Ministry of Defence.

CERT.LV contributes to the development of the ECSC national selection website, as well as in the preparation of the infrastructure and task set required for the national selection.

The Latvian Cyber Security Challenge 2024 will take place in three rounds. The results will be collated and the winners announced after Round 3 in May.

## International Cooperation and Projects

CERT.LV continues representing Latvia's interests and strengthening cooperation with other countries' cybersecurity incident response teams and international organisations, including the CSIRTs network, ENISA, European Union institutions, and NATO.

During the reporting period, CERT.LV employees also provided their vision and input to various working groups, sharing experience and best practices, providing advice and support, as well as making presentations at international conferences and seminars. Employees also continue to learn new skills and improve their qualifications through international training.

CSIRTs Network

CERT.LV regularly participates in the network meetings of the NIS (Network and Information Security) directive CSIRTs Network. The work of the CSIRTs Network is coordinated by ENISA, the European Union Agency for Cybersecurity, which contributes to EU policy on cybersecurity.

During the reporting period, CERT.LV participated in the CSIRTs Network Maturity Working Group, which is dedicated to improving the maturity level of EU Member States' CSIRTs Network teams.

**CSIRTs Network** - the network of Computer Security Incident Response Teams of the Member States of the European Union ensures cooperation between cybersecurity incident response teams in the EU. The meetings take place three times a year and are currently organised by the country holding the Presidency of the Council of the EU in cooperation with ENISA. Joint sessions with the NIS Directive Cooperation Group and CyCLONe also take place.

CERT.LV experts also continued to actively participate in working groups organised by ENISA:

- **Coordinated Vulnerability Disclosure (CVD) Task Force** – work is underway on the development of EU-level guidelines for a coordinated vulnerability disclosure policy;
- **EU Cybersecurity Index** – a methodology for calculating the value of the cybersecurity index is being developed to assess the cybersecurity of Member States; work is continued on developing the EU Cybersecurity Index platform;
- **CSIRT Services Framework** – work was continued on developing a common framework for roles, competencies and skills of CERT team members. During the reporting period, the development of a methodology for defining the types of CERT teams was carried out, which would facilitate the identification of roles and competences required for the tasks to be performed.

**CSIRT Network Situation Update Meetings:** Regular participation in meetings aimed at exchanging information on current developments in cyberspace between CSIRT Network members continued during the reporting period.

**European Commission EHDS (European Health Data Space) Regulation Working Group:** CERT.LV experts contributed to a working group aimed at promoting the availability of electronic patient data and cooperation between stakeholders at the European level. During the reporting period, the working group assessed the Regulation's relationship with the Artificial Intelligence Act, the Data Governance Act, and the General Data Protection Regulation.

**Regular participation of CERT.LV experts in European Cybersecurity Certification Group (ECCG) meetings, including** two online meetings in March, representing Latvia's interests and providing their vision on problematic issues affecting the further progress of the EU Cloud Certification Scheme (EUCS) in EU countries.

**ENISA-organised training CYBER EUROPE 2024:** The training will take place on 19-20 June, online. Latvia will be represented by the Ministry of Defence and CERT.LV, as well as participants from the energy sector and data centres.

**Cooperation within FIRST:** Regular participation in the FIRST Membership Committee meetings continues to discuss future rules for membership and recruitment, as well as the application of the SIM3 model in the team certification process.

CERT.LV Manager Baiba Kaškina, who continues to serve as Chair of the FIRST Membership Committee, participated in the review of new member applications and contributed to the improvement of the membership application process.

**FIRST** is a cybersecurity organisation bringing together CERTs, CSIRTs, PSIRTs, SOC teams and other cybersecurity professionals from around the world. As of April 2024, FIRST has members from 107 countries.

**Cooperation within TF-CSIRT:** During the reporting period, CERT.LV is one of 47 TF-CSIRT/Trusted Introducer certified teams in Europe (there are 515 teams in the community). This attests the high level of maturity and preparedness of the CERT.LV team.

To maintain the certification, a re-certification process is required every three years. On 28 October 2022, at the TF-CSIRT meeting in Vilnius, Lithuania, it was announced that CERT.LV has been successfully re-certified for the next three years (accordingly, the next re-certification process is planned for 2025).

**TF-CSIRT/Trusted Introducer** is the organisation for CERTs in the European region, bringing together incident response teams from all sectors. The Trusted Introducer service maintains a trusted register of CERTs and accredits and certifies teams according to their demonstrated level of maturity.

CERT.LV has been a certified Trusted Introducer team since 1 September 2016.

The certification is based on SIM3: Security Incident Management Maturity Model approach. SIM3 assesses the maturity of an organisation by looking at organisational, human resources, technical tools and processes used and their application to ensure the quality of the organisation's operations, primarily assessing the maturity of the incident handling process.

During the reporting period, CERT.LV continued its work in several TF-CSIRT working groups.

According to the contract with the European Commission No. INEA/CEF/ICT/A2020/2373165, which was approved and launched on 1 July 2021 under the 2020 CEF Telecom Call – Cybersecurity, the implementation of the JTAN project will continue until 30 June 2024.

**Open Cyber Security Conference:** From 26 February to 1 March, CERT.LV cyber security specialists participated in the Open Cyber Security Conference in Spain: Rūdolfs Ķelle with a presentation 'Prototyping a Network Intrusion Detection System: A Deep Dive into CERT.LV's IACS Lab for Safeguarding Critical Infrastructures' and Kārlis Svilans with a presentation 'Defending From the Beast in the East - Multinational Threat Hunting Operations'.

***Prague* Cyber Security Conference 2024:** From 19 to 20 March in Prague, Czech Republic at the Prague Cyber Security Conference 2024 CERT.LV cyber security expert Kristiāns Teters participated in the panel discussion 'Cloud Sovereignty or Cloud Solidarity? Finding Common Approach to Cloud Security' and shared his experience on the current situation in the field of cloud security and Latvia's experience with cybersecurity requirements for cloud service providers, as well as the position in the field of cloud certification.


**Implementation of the Joint Threat Analysis Network project:** The CERT.LV team continues its work on the implementation of the Joint Threat Analysis Network project (hereinafter – JTAN project). The overall objective of the JTAN project is to create a Joint Threat Analysis Network. The network would be open to a European CSIRT cooperation group focusing on the exchange and analysis of technical, operational, and strategic threat intelligence.

The leading partner of the project is CERT.PL, the Polish Information Technology Security Incident Response Team, which operates within the Naukowa i Akademicka Sieć Komputerowa (NASK) institute. Partners from Austria, France, Estonia, Luxembourg, Romania, and Slovakia are also participating in the JTAN project.

CERT.LV continues the development of the Graphoscope solution as planned. During the reporting period, CERT.LV allocated additional resources to the implementation of the project, and participated in monthly remote JTAN project meetings, where project partners are briefed on individual project tasks and results.

Regular participation of CERT.LV experts in monthly meetings of the EU CyberNet project continues. The project aims to strengthen and develop cybersecurity expertise not only within the EU, but also beyond its borders (www.eucybernet.eu). Participation in the project provides an opportunity for CERT.LV experts to engage in various projects, strengthening their knowledge and capacity.

## Communication with the Public and Raising Awareness of Cyber Security Issues

During the reporting period, CERT.LV via 31 educational events (seminars, conferences, table-top exercises) reached 4737 participants on IT security. Events aimed at promoting cyber literacy for both individual users and organisations so that everyone is able to ensure the security of their data and systems.

**Cybersecurity Breach Investigation table-top exercise** - an addition to the usual training seminars.

CERT.LV continues to inform the public about cyber security risks, cyber hygiene promotion and best practices, as well as other current events in Latvian cyberspace, including by compiling and publishing on the website www.cert.lv a monthly report 'Cyber Weather Report' on the highlights in cyberspace **i**n the TOP five categories - scams, malware and vulnerabilities, denial-of-service attacks, intrusions and data leaks, and the Internet of Things.

In Q1, CERT.LV with 324 media publications had a potential to reach audience of 13.42 million.

**CERT.LV continues to promote cybersecurity and be a trusted opinion leader in Latvian cyberspace.**

**CERT.LV mission is to promote information technology (IT) securityin Latvia.**

Main objectives of CERT.LV are: to update information about IT security threats; to provide support to state institutions regarding national IT security; to provide support regarding IT security incidents to every private end user or legal entity, if the incident involves a Latvian IP address or .LV domain; to conduct research, orgnaize educational events and trainings in the field of information technologies security.

**Contact CERT.LV:**

Telephone: +371 67085888

E-mail: cert@cert.lv

Web: www.cert.lv

**Follow CERT.LV:**

www.twitter.com/certlv

www.facebook.com/certlv



CERT.LV
Information Technologies
Security Incident
Response Institution