CERT.LV ACTIVITY REPORT

Q4 2024

CERT.LV
Cyber Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

The Activity Report for Q4 2024 contains publicly available information and does not include information about CERT.LV activities that contain classified information. The report is for informational purposes only.

Contents

Q4 2024 in Latvian cyberspace

Latvia maintains a high level of cyber resilience despite a significant increase in the number, complexity and intensity of cyber threats. Financially and geopolitically motivated cyber attacks continue to occur in cyberspace. Cyber attackers exploit human carelessness and technological vulnerabilities through clever use of phishing, scanning, weak authentication and targeted delivery of malware.

In Q4 2024, the number of unique IP addresses compromised in Latvia reached an all-time high, indicating a significant increase in the number and intensity of cyber threats.

The number of reports logged by CERT.LV has increased by 3% compared to Q3 and by 25% compared to Q4 2023.

The cyber security landscape continues to be shaped by geopolitical tensions and ideological conflicts around the world. Cyber threats in Latvia are mainly linked to

Cyber threat dynamics by quarter

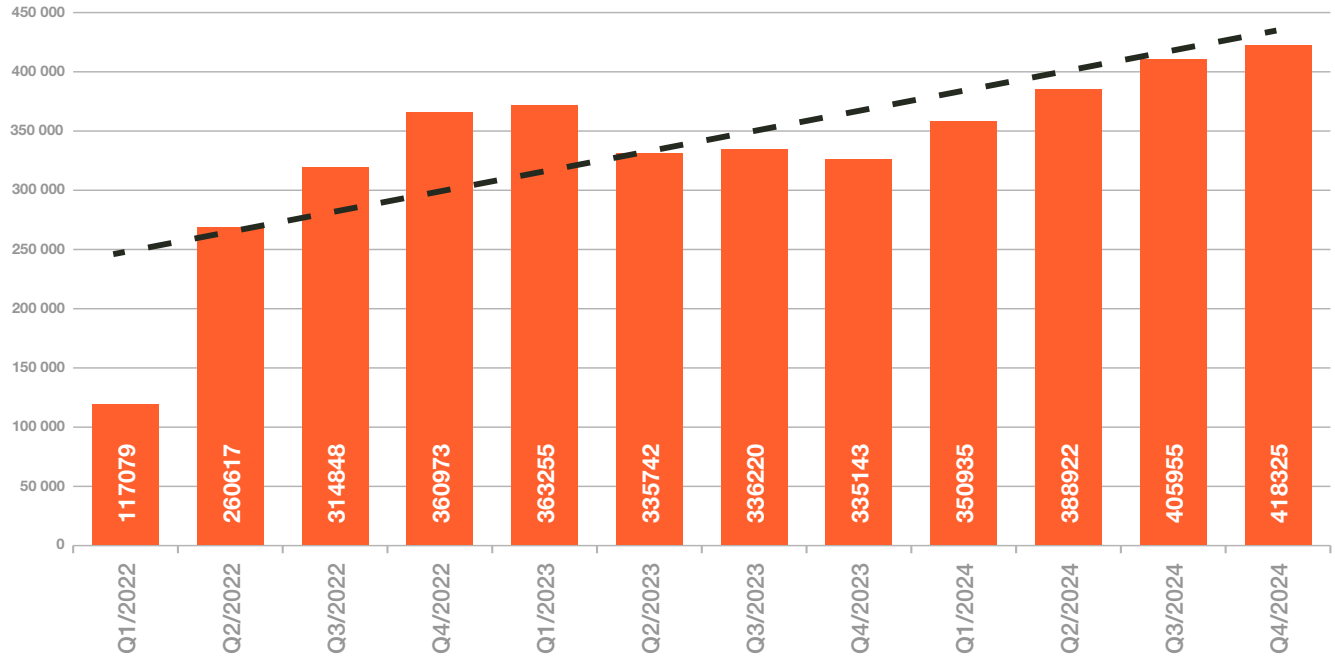


Figure 1. Unique IP addresses at risk by quarter in 2022–2024

pro-Russian cyber attackers. There is also an increased interest in Latvia's ICT infrastructure from cyber attackers, possibly linked to China, indicating a new development in cyber operations by Chinese-backed cyber attackers. There is also a marginal presence of cyber attackers possibly linked to Belarus and North Korea.

Cyber attackers mostly use DDoS attacks, various vulnerabilities, insecurely exposed equipment on the Internet and sophisticated social engineering tactics to disrupt services, infect unpatched equipment, conduct cyber espionage and steal data.

Fixed cyber attacks have generally not had a significant impact on public safety and essential and critical services, indicating an effective set of protection measures. However, the types, intensity and complexity of cyber attacks are evolving rapidly. It is important to continue to work and invest in cyber resilience and defence solutions to fully protect networks and information systems. There is a need to continue to raise end-user awareness, both by providing information on the current situation, cyber threats and vulnerabilities, and by promoting good cyber hygiene practices.

The CERT.LV DNS firewall, the international hunt for cyber security threats and the growing awareness of cyber hygiene among public administration personnel provide a solid basis for stronger defences.

The strengthening of Latvia's cyberspace continues to be facilitated by the National Cybersecurity Law (NCSL), which entered into force on 1 September 2024, expanding the range of organisations subject to the requirements of the substantially updated Directive 2022/2555 of the European Parliament and of the Council on Network and Information Systems (NIS2).

1. Key cyber threats: statistics and trends

Latvia continues to successfully demonstrate high cyber resilience, despite the highest ever level of cyber threats, serious challenges and intensity of cyber attacks.

No C1 or national-level threats were recorded in the reporting period. In category C2, which includes high-profile threats, 5 compromised unique IP addresses were recorded out of all categorised threats. C3, or significant threats with a broad impact on the commercial sector, State and local government authorities, accounted for 52 compromised unique IP addresses out of all categorised threats. The highest proportion of cyber threats was recorded in the minor threat cluster C6, which is related to widespread, everyday, automated attack attempts.

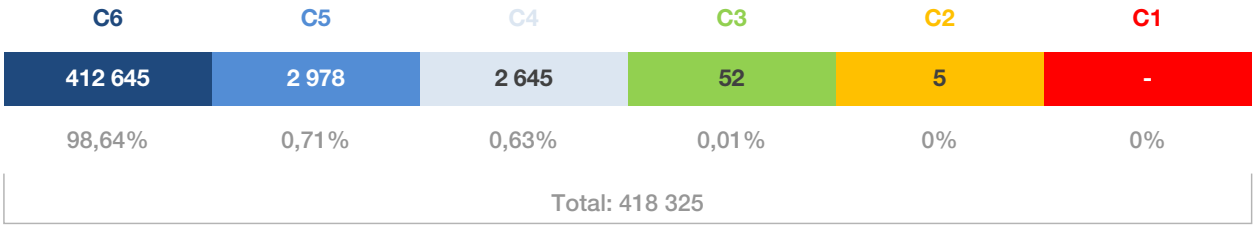


Figure 2. Categorisation of unique IP addresses compromised in Q4 by threat impact

Cyber attacks targeted public authorities as well as service providers in the financial, transport, energy and telecommunications sectors. Service attacks were observed in the financial sector, which temporarily disrupted the availability of the services affected by the cyber attack to bank customers. However, in most cases reported to CERT.LV, the impact of cyber incidents was minor or non-existent. This indicates the existence of cyber resilience and effective protection measures.

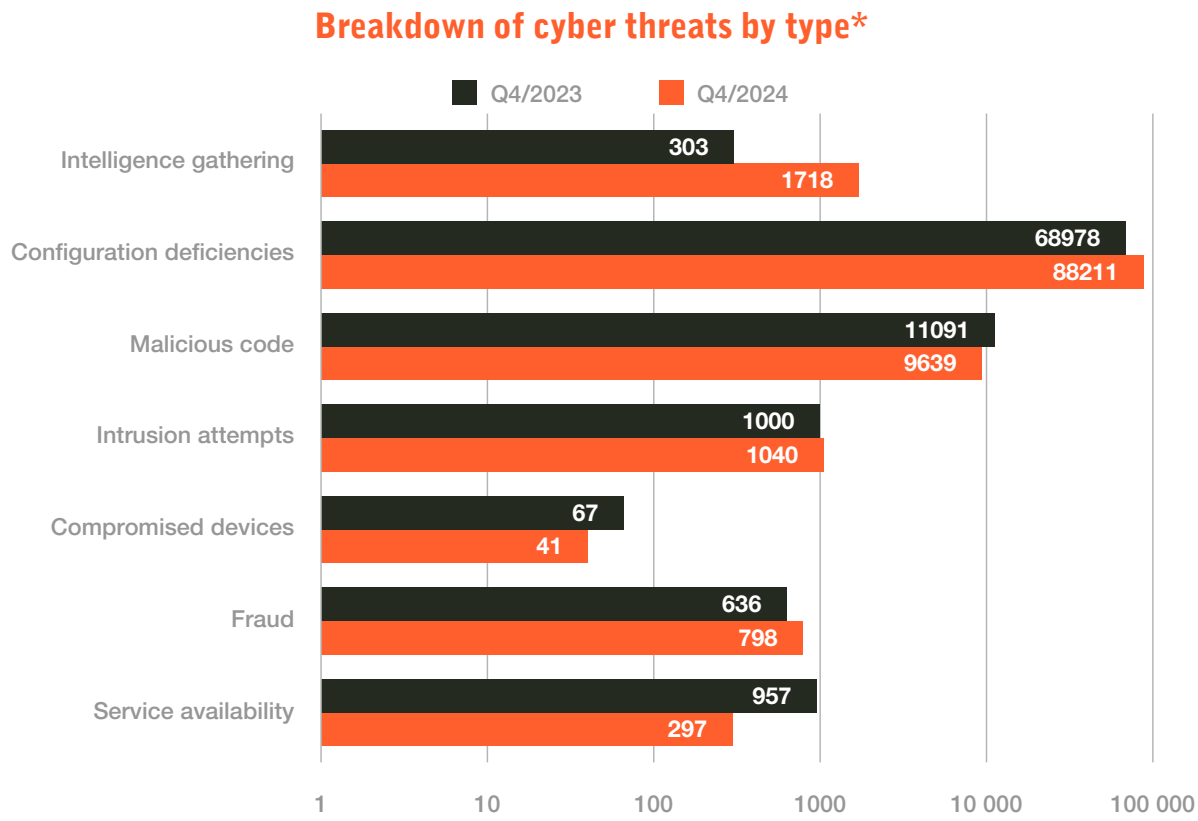


Figure 3. Comparison of the number of unique IP addresses compromised by type.

*Other, Information Security, Harmful Content are not included in the graph.

In terms of quantitative indicators, the top 5 cyber threats are configuration deficiencies, malicious code, information gathering, intrusion attempts and fraud. Compared to the same period a year ago, the following types of threats show the largest increase:

- Intelligence gathering +98%
- Configuration deficiencies +28%
- Fraud +25%
- Intrusion attempts +4%

Exploiting already discovered and known vulnerabilities remains one of the main access points for cyber attacks to penetrate systems and steal valuable data. In parallel, long-known configuration deficiencies in widely used products and newly discovered vulnerabilities are exploited to penetrate organisations' internal networks and gain unauthorised access to sensitive information. The human factor and the use of weak passwords also pose serious risks, allowing cyber attackers to compromise even seemingly well-protected systems.

As a result of configuration deficiencies, the proportion of devices exposed insecurely on the Internet, allowing access to systems and data, is increasing. This reflects the increasing complexity of technologies and systems, making them more difficult to manage and configure, a contributing factor is also the continuous shortage of skilled cyber security professionals in organisations.

DDoS attacks have declined in quantitative terms, while becoming more complex, concentrated and powerful, making them potentially more 'painful'. Despite the increasing intensity of cyber attacks, their impact was minimal.

Cyber threats related to data leaks to organisations that store personal data are on the rise. The most significant data breach incident in Latvia occurred during the reporting period, when cyber attackers managed to access a database on a server hosted by ZZ Dats. This incident directly affected 42 Latvian local municipalities. As a result, the security of personal data has been compromised and may be used in future in targeted phishing against citizens.

The amount of money defrauded in fraud cases continues to grow as fraudsters use increasingly effective social engineering techniques and artificial intelligence tools. Active fraud campaigns that had the greatest impact on the public related to parcel delivery services. Fraudsters also continued to impersonate banks, government and law enforcement officials. Telephone scams and fake investment platforms had a big impact.

Quantitatively, the number of cyber incidents caused by malicious code has decreased, indicating effective protection mechanisms, but the number of unique IP addresses compromised remains high. Malware and phishing, such as malicious attachments in emails used to gain control over sensitive data from companies and personal electronic devices, are becoming increasingly sophisticated, posing serious security risks to data integrity. Phishing is the preferred method for spreading malware through social media and popular email marketing platforms.

The types, intensity and complexity of cyber attacks are evolving rapidly. It is important to continue to work and invest in resilience and defence solutions to fully protect networks and information systems.

Key trends

Latvia continues to experience politically motivated cyber attacks against resources in the public and private sectors. Latvian cyberspace has seen mainly cyber attackers potentially linked to Russia, including financially motivated attacks, but there has also been increasing interest in Latvian infrastructure from attackers potentially linked to China. There is also a minor presence in Latvian cyberspace from attackers potentially linked to Belarus and North Korea. The activities of attackers potentially linked to Belarus overlap with Russian interests, while the operations of those potentially linked to North Korea are aimed at obtaining financial means to achieve their objectives.

The exploitation of vulnerabilities remains a key access point for both state sponsored cyber-operative groups and financially motivated cyber criminals to infiltrate systems and steal valuable data.

The use of configuration vulnerabilities to gain access to systems and data is on the rise. The complexity of technologies and systems continues to increase, making them more difficult to manage and configure. Organisations lack the resources to effectively manage and configure complex systems and perform regular checks.

Cyber threats related to data breaches are on the rise, mainly targeting organisations that store personal data. This underlines the need for continuous, thorough systems management and regular security testing. It is essential to take care of all digital resources under an organisation's control, and to update them regularly.

The amount of money defrauded in fraud cases continues to grow as fraudsters use increasingly effective social engineering techniques and artificial intelligence tools. Data on fraud cases collected by the Finance Latvia Association show that Latvian citizens are defrauded of a total of EUR 1-1.5 million every month by self-certifying payments.

Weak passwords are still used and multi-factor authentication is not used. This problem exists on both the service users' and the service providers' side, although technical solutions have existed for quite a long time.

Reports received by CERT.LV show that citizens do not always have a clear understanding of official communications from authorities, which leads to the disclosure of personal information and the transfer of payment card and bank account details to fraudsters.

2. Cyber Threat Prevention

DNS firewall: In Q4 2024, DNS firewall users were prevented from visiting malicious sites **459 213** times by redirecting the end-user to the CERT.LV alert site. This is **344%** more than in Q3. On average, 1 million requests are handled every month, blocking around **8000** attempts to open fraudulent links per day.

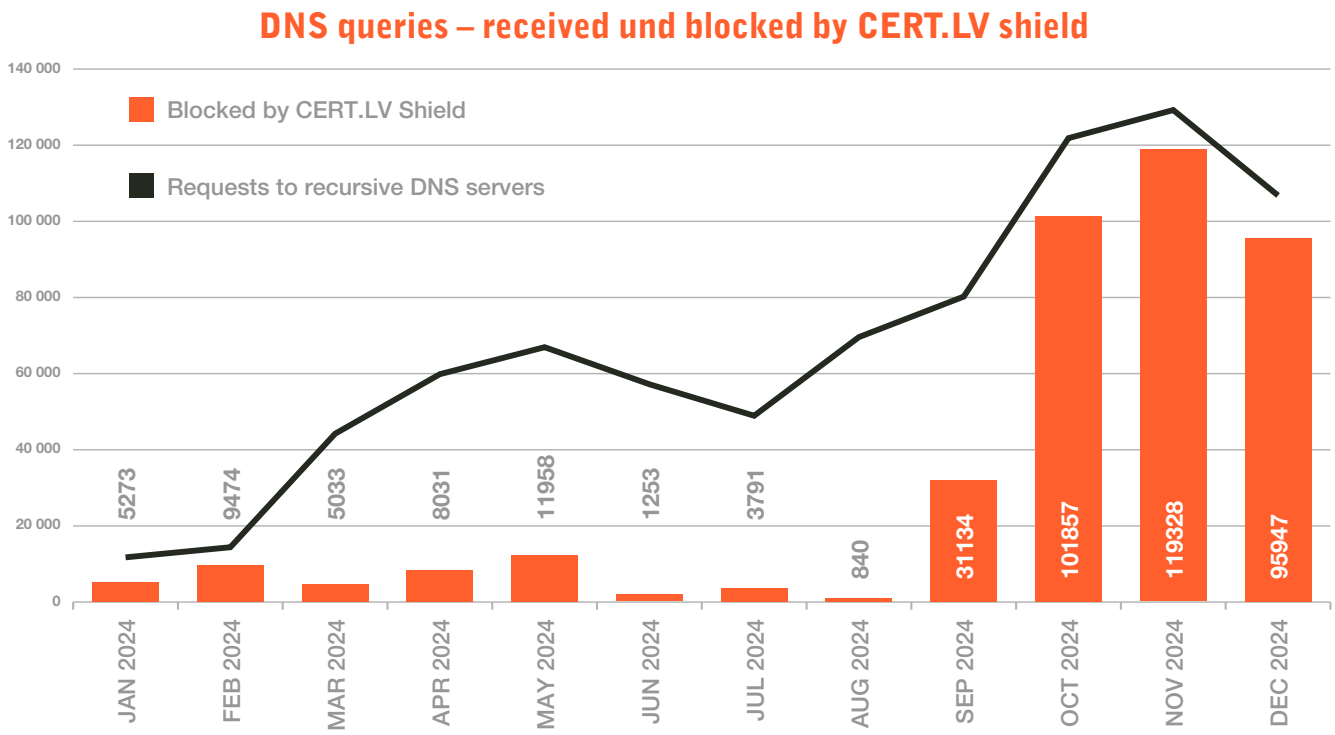


Figure 4. DNS queries – received and blocked by CERT.LV shield

A mobile app for the DNS Firewall is available from autumn 2024, which is easy to download and activate on mobile devices for Android and iOS users. The app not only protects against visiting malicious links used in fraudulent campaigns that are currently in use in Latvia, but also blocks phone calls from numbers that CERT.LV has identified as fraudulent. The app provides feedback on the threats that have been prevented.

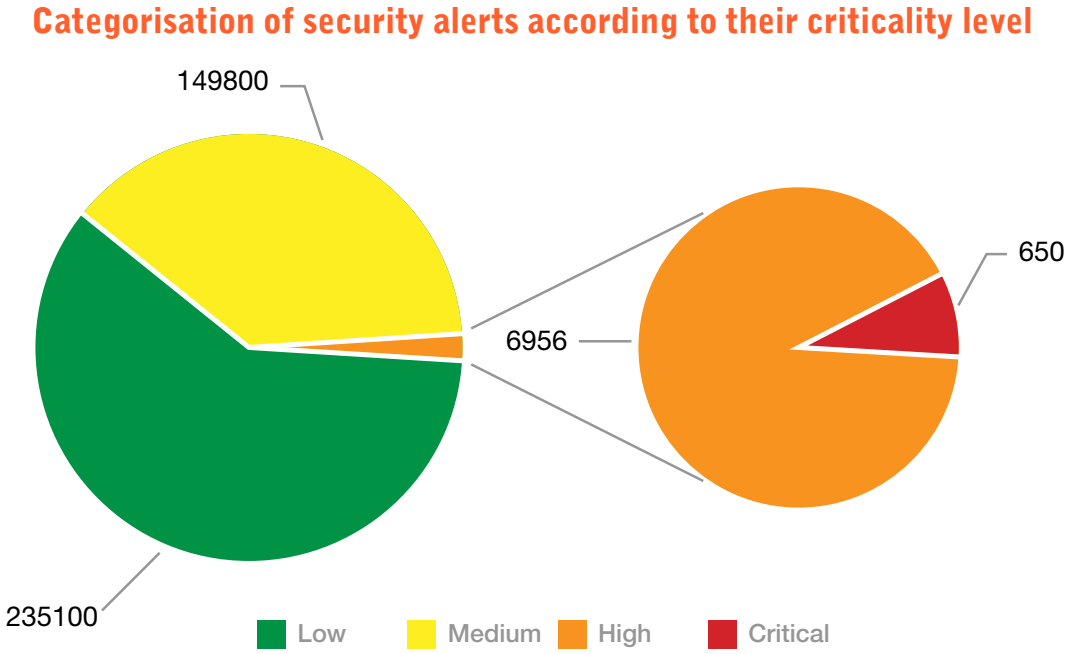


Figure 5. Number of security alerts as of the end of 2024

Security Operations Centre (SOC): By the end of the reporting period, the number of SOC-monitored devices in the customer infrastructure reached **5290**, ensuring the identification of cyber threats and compromised systems. A total of more than **392 000** security telemetry alerts were recorded, of which **650** were critical.

SOC centrally collects security telemetry from the customer's infrastructure and correlates events in the customer's infrastructure with the entire set of threat indicators and knowledge available to CERT.LV in order to identify, warn, stop and prevent a cyber threat or cyber incident in a timely manner.

Early Warning System (EWS): The total number of alerts generated by EWS during the reporting period was **2,4 billion**, half a million more than in Q3 2024. This is due to an increase in the number of large-scale phishing and computer virus-related alerts. The EWS detects, on average, **6000** high priority cyber threats (incidents with a high hazard potential) in governmental, local municipality and ICT critical infrastructure institutions every month.

Coordinated Vulnerability Disclosure (CVD): CERT.LV continues its work on the development and promotion of the CVD platform, acting as the coordinator and facilitator of the coordinated vulnerability disclosure process, as well as the developer, maintainer and manager of the platform.

During the reporting period, the number of security researchers on the CVD platform increased by **13%**, active institutional programmes increased by **20%** and the number of vulnerability reports increased by **23%**. The reporting practices of the CVD help to learn about vulnerabilities in a more timely manner and to coordinate vulnerability research and remediation, thus organising measures to protect cyberspace more effectively.

3. Strategic partnerships in Latvia

Cyber security threat hunting operations

In the period from 2022 to December 2024, more than **150 000 devices in 35 organisations** were tested by cyber security threat hunting operations with the aim of identifying the presence of cyber threats in critical ICT infrastructure systems important for Latvia.

In about **20% of the cases, the presence of attackers, who could potentially be supported by other countries was detected**. These attackers carry out a wide range of cyber operations, also in cooperation with financially motivated attackers from whom they tend to buy or otherwise gain initial access. Both Russian and potentially Chinese-linked groups have been observed.

CERT.LV is a European leader in large-scale cyber security threat hunting

Strengthening Latvia's cyberspace, CERT.LV, together with strategic partners, continues to conduct threat hunting operations to identify the presence of cyber threats in ICT infrastructure systems important to Latvia.

In several cases, overlapping cyber operations potentially involving Russia and China have been identified, leading to speculation of cooperation between groups. Both sides have been found to use behaviours, tools, language and tactics typical of attackers from the other country to potentially mislead analysts on attribution issues.

CERT.LV, both individually and with a joint team of partners, operates in a pre-selected network of information systems (the choice of target institution is assessed in cooperation with national security authorities) to identify the presence of an attacker, to detect, monitor and analyse malicious activities, and to analyse attack tactics, techniques and procedures. The threat hunting report, which is provided to the management of the target institution after each operation, includes information on all findings and provides recommendations for mitigating the effects of attacks and strengthening cyber resilience.

Despite the high intensity of cyber threats, Latvia is not only rising to these challenges, but has become an example for other countries. CERT.LV, in cooperation with the Canadian Armed Forces, has developed a Threat Hunting Handbook, which includes recommendations for conducting threat hunts, and held its first workshop for international partners, sharing its experience to date. The workshops are planned to continue in 2025.

IT system security tests

In Q4 2024, CERT.LV experts conducted **4** security tests and **7** phishing attack simulations in ICT critical infrastructure and service delivery organisations. During these tests, several vulnerabilities were identified and addressed, including a total of **2** critical, **5** high risk, **9** medium risk and **8** low risk vulnerabilities, and the cyber hygiene skills of the personnel of these organisations were trained.

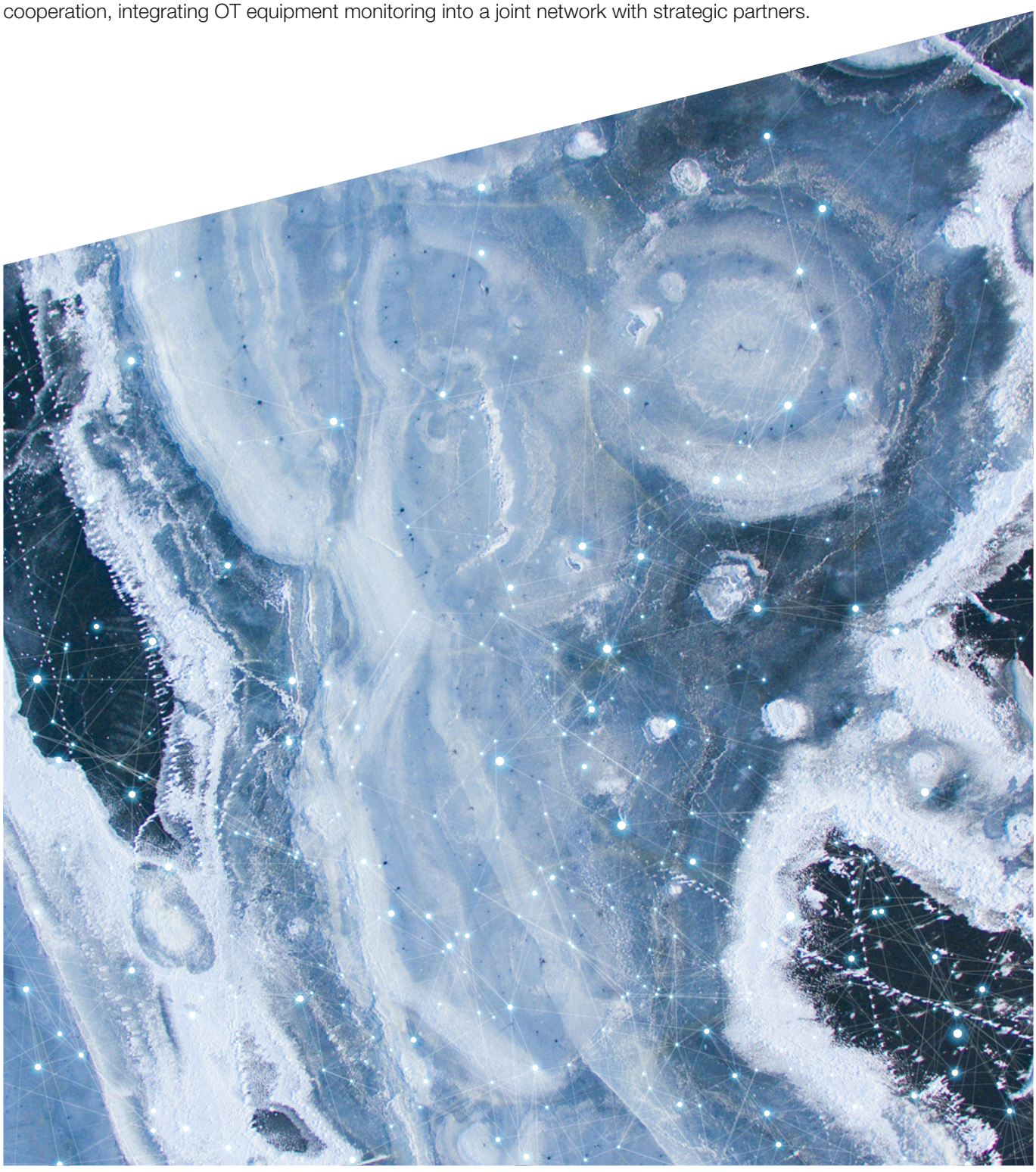
Cooperation with ICT critical infrastructure holders

Cooperation with ICT critical infrastructure holders continued, both in terms of operational support and centralised protection against cyber attacks, as well as support to strengthen cyber resilience and enhance cross-sectoral cooperation.

CERT.LV provides a wide range of professional services, including promoting the security of industrial automation and control systems, providing laboratory services for testing the security of operational technology (OT) equipment, software and communication protocols.

CERT.LV offers security testing of industrial automation and control components to infrastructure holders in various sectors (energy, transport, water, etc.). During the reporting period, active cooperation with heating and water supply service providers was initiated, and cooperation with Latvian energy sector companies continued.

In February 2025, Latvia will take a significant step towards energy independence – the Baltic States will completely disconnect from the Russian-controlled BRELL (Belarus, Russia, Estonia, Latvia, Lithuania) power grid and join the continental European power system. In order to be prepared for this event from the cyber security point of view, CERT.LV will be involved from early 2025, with focus on the security of the BRELL disconnection process and strengthening cyber resilience. CERT.LV cooperates with Augstsprieguma tīkls AS and is actively consulting the company's cyber security and OT specialists. In parallel, CERT.LV experts are also involved in international cooperation, integrating OT equipment monitoring into a joint network with strategic partners.



4. Communication with the Public

The CERT.LV team continues to be active in educating the public by organising and participating in various thematic seminars, providing information about current cyber security developments and promoting cyber hygiene best practices.

In the reporting period, **74 (+57)** events were implemented with a total of **15 593 (+7806)** participants, promoting a culture of cyber security among citizens and organisations and strengthening cyber resilience across Latvia.

CyberChess 2024 Conference

From 1 to 3 October, Riga hosted the 11th International Cybersecurity Conference CyberChess 2024, bringing together experts from countries such as Ukraine, USA, Switzerland, UK, Canada, etc. to discuss the most pressing cyber security challenges and their potential future scenarios.

Bringing together more than 500 cyber security professionals in person and more than 5000 online from more than 25 countries,

63 speakers, including speakers from CERT.LV, shared their research and experiences on cyber security related topics, with a particular focus on combating existing cyber threats.

October is traditionally celebrated as Cybersecurity Month in Europe, and the conference at the very beginning of the month marked a symbolic start of a broader discussion on the importance of cyber security in today's society in Latvia.

This year's conference focused on various topics: the role of artificial intelligence (AI) in enterprise cyber security; the protection of critical infrastructure through threat hunting; and cooperation between Europe and NATO in improving alliance cyber security. The speakers at the conference agreed that cyber attacks will only increase in the future and will become more sophisticated and increasingly difficult to combat.

At the opening of the conference, the participants were addressed by CERT.LV Manager Baiba Kaškina, along with the Minister of Defence Andris Sprūds and the Director-General of the National Cybersecurity Centre Rolands Heniņš.

"CyberChess 2024 is an important conference that draws attention to the growing cyber security challenges we face today, when the number of attacks has reached a high level and they are becoming more and more complex."

Baiba Kaškina, CERT.LV Manager

The main stage of the conference hosted the #CyberChess strategic and policy session, while parallel sessions included #CyberStory, which brought together topics related to the future and innovation, and #CyberShock, which was dedicated to deep technical research and practical demonstrations.

For the fifth year, CERT.LV organised and followed up the CyberChess 2024 conference with Capture The Flag (CTF), an online cyber security competition that allowed competitors (70 teams with 186 players from 9 countries) to face various cyber security challenges in categories such as cryptography, network analysis, forensics, binary code. A summary of the CTF results and team performances was presented at the end of the conference.

The conference is organised by CERT.LV, the Ministry of Defence of the Republic of Latvia and the National Cybersecurity Centre in cooperation with the ISACA Latvian Chapter and the Institute of Mathematics and Computer Science, University of Latvia. The conference is co-funded by the European Union and supported by the Latvian National Coordination Centre of the European Cybersecurity Competence Centre (NCC-LV). A short summary video of the conference is available at: cyberchess.lv.

NCC-LV
LATVIJAS KIBERDROŠĪBAS KOORDINĀCIJAS CENTRS

Līdzfinansē Eiropas Savienība

5. International cooperation

CERT.LV continues representing Latvia and building partnerships with cyber incident response teams from other countries and international organisations, including the CSIRTs network, ENISA, FIRST, EU institutions, NATO, and other security partners in the Euro-Atlantic region and in international security overall, providing advice and support through various working groups, and consistently working with the public at international conferences.

Cooperation with the CSIRTs Network, ENISA, European Union institutions and NATO

NIS Directive CSIRTs Network meetings: The CSIRTs Network is coordinated by ENISA, the EU's Cybersecurity Agency, which contributes to EU policy on cyber security. During the reporting period, CERT.LV continued its participation in the CSIRTs Network working group Maturity, which is dedicated to increasing the maturity level of EU Member States' CSIRT teams. In September 2024, CERT.LV participated remotely in the 24th CSIRTs Network Meeting held in Bucharest, Hungary.

CSIRT Network Maturity Peer-review: CERT.LV Manager Baiba Kaškina participated in the peer review of CSIRT.SK processes, which demonstrates high professional competence and confidence in international cooperation in the field of cyber security.

Participation in working groups organised by ENISA: Coordinated Vulnerability Disclosure Task Force – work is underway to gather EU-level coordinated vulnerability disclosure experience and practices. EU Cybersecurity Index – work continues on developing the EU Cybersecurity Index platform.

European Health Data Space Group: CERT.LV experts contribute to promoting the availability of electronic patient records and stakeholder cooperation at 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.

> "The cooperation provides valuable exchange of experience and international contacts, which in general contributes to cyber security both in Latvia and internationally."
>
> Baiba Kaškina, CERT.LV Manager

European Cybersecurity Certification Group: CERT.LV experts participated in the meetings, representing Latvia's interests and providing their perspective on issues of concern regarding the further progress of the EU Cloud Certification Scheme (EUCS) in EU countries and on other issues related to the implementation of cyber security certification for ICT products in EU countries.

ENISA organised exercises: Cyber Europe 2024 and Cyber Europe 2026: From 25 to 26 November, CERT.LV experts participated in the final meeting of the Cyber Europe 2024 exercise, where Member States agreed on the content and publication modalities of the final reports, shared their experience on the organisation of the previous exercise cycle, and participated in the initial planning meeting for Cyber Europe 2026.

The Cyber Europe 2026 exercise is planned for May 2026. Potential scenarios for the exercise include the public administration and electoral authorities, or the transport sector, such as railways and ports. This decision will be taken by Member States voting on the scenarios accordingly. As in previous years, the exercise will include technical as well as crisis management and communication tasks.

NATO CCDCOE organised exercise Crossed Swords 2024: During the reporting period, CERT.LV participated in the Crossed Swords 24 test exercise (12–14 October) and the main exercise (11–14 December), providing support to the organisers (White Team) in the preparation and play-out of information operations scenario incidents, preparation of strategic communication documents and information flow, simulating the communication of the Joint Staff Strategic Communications Department with the Cyber Command.

This was the first time that a strategic communication exercise took place during Crossed Swords exercise. It was found useful by the Cyber Command representatives for situational awareness, audience analysis and communication planning. The CCDCOE plans to continue developing this area in the future.

Cyber Coalition exercise organised by NATO: From 2 to 6 December, the CERT.LV team participated in the Cyber Coaltion exercise as a training audience, dealing with incidents related to civilian critical infrastructure – the health sector – providing incident analysis, reporting on the MISP platform and communication with international counterparts. Incident responders also provided support in the analysis of cyber attacks on military critical infrastructure – military hospitals.

Cooperation within FIRST

Regular participation in the FIRST Membership Committee meetings continues to discuss future rules for membership and recruitment, membership categories, and the application of the SIM3 model to the team certification process. CERT.LV Manager Baiba Kaškina, as the Chair of the FIRST Membership Committee, participated in the review of new member applications and contributed to the improvement of the membership process.

Cooperation within TF-CSIRT

CERT.LV is one of 42 TF-CSIRT/TI certified teams in Europe. At the end of the reporting period, there were 526 teams in the community. CERT.LV continued its work in several TF-CSIRT working groups.

CERT.LV is the highest-level Trusted Introducer certified cyber security incident response team, which reflects the high level of maturity and preparedness of CERT.LV.

Latvia and Canada develop a unique training course to strengthen cyber capabilities

A unique training course combining international experience and expertise in effective threat hunting has been developed in cooperation between CERT.LV, the Latvian Ministry of Defence and the Cyber Command of the Canadian Armed Forces.

During the reporting period, two consecutive workshops on developing and strengthening cyber capabilities were held in Riga:

- From 21 to 23 October, the first international Threat Hunt Workshop organised by CERT.LV and the Cyber Command of the Canadian Armed Forces took place: Threat Hunt Workshop.
- From 24 to 25 October, the US European Cyber Command (EUCOM) organised a workshop on Cyber Threat Intelligence: Cyber Threat Intelligence.

"This unique training course is the result of many hours of cooperation between Latvian and Canadian cyber security teams. Together we have created something unique that will not only strengthen our own capabilities, but also serve as a model for others to work with."

Varis Teivāns, CERT.LV Deputy Manager

Highlighting the importance of the cyber threat hunting training course, the training was opened by Canadian Ambassador to Latvia Brian Szwarc, Director of the Cybersecurity Policy Department of the Ministry of Defence Edgars Kiukucāns, CERT.LV Deputy Manager Varis Teivāns and Deputy Director of the State Police College Anita Fišere. The training was attended by 20 experts from various cyber security authorities of NATO member states. Training was delivered by experts from Latvia and Canada.

CERT.LV shares its experience and knowledge

On 12 December, CERT.LV hosted colleagues from the Moldovan Cybersecurity Agency and other institutions in Latvia. The purpose of the visit was to discuss cooperation opportunities, as well as to share information on the implementation of the NIS2 Directive in Latvia, the current situation and trends in cyberspace and to talk about CERT.LV services.

Latvian team competes for the first time in the European Cybersecurity Competition for youth

In October 2024, for the first time the Latvian team participated in the European Cybersecurity Challenge 2024 (ECSC 2024) a competition for youth with 37 teams participating. This took place from 8 to 11 October in Turin, Italy. It was an unforgettable experience for the young people, who proved to be persistent, energetic and highly motivated competitors throughout the competition.

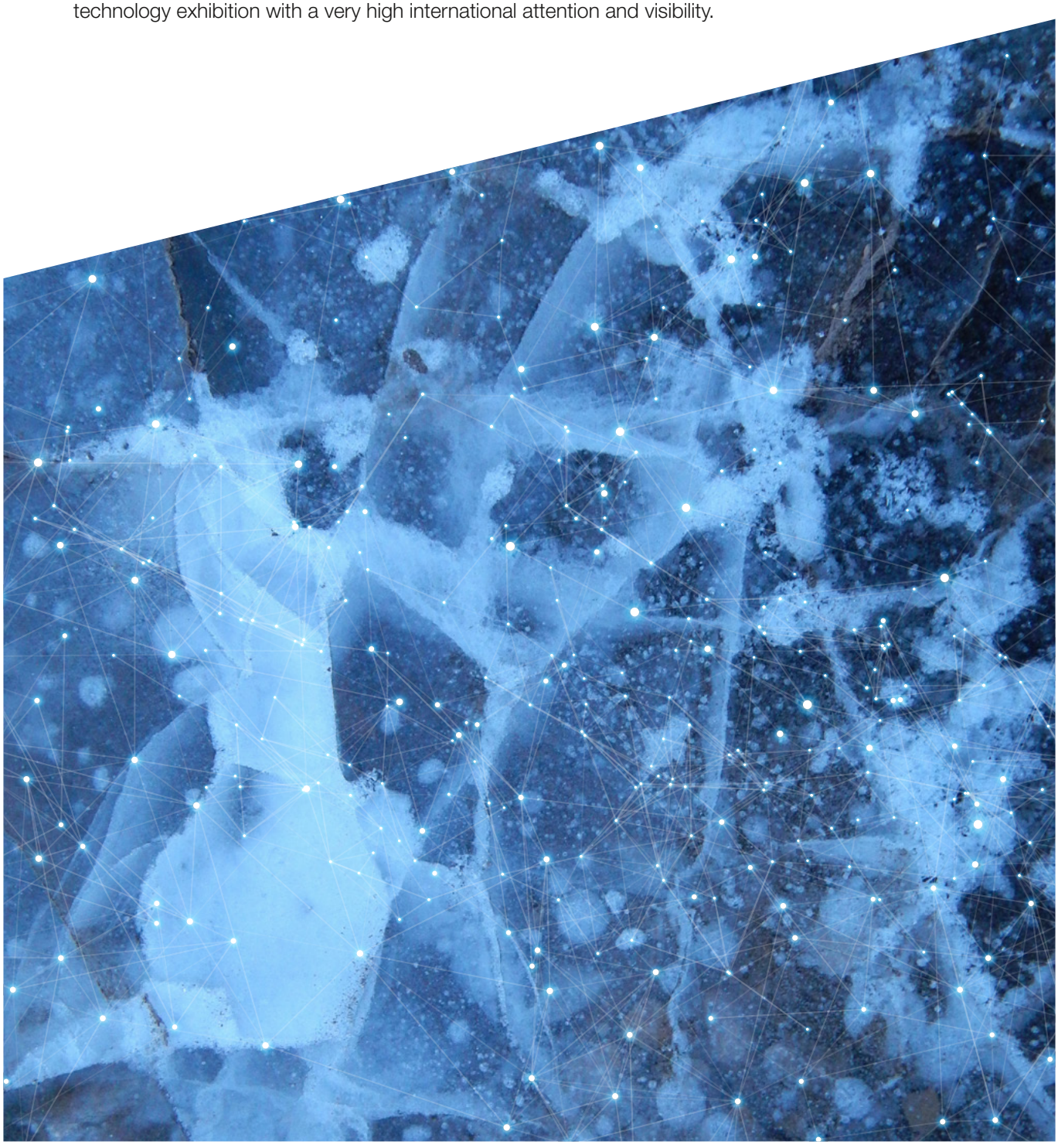
CERT.LV is actively involved in promoting cyber security skills among young people, both by supporting the preparation of the National Cybersecurity Challenge and by participating in the preparation of the Latvian team for the ECSC competition. CERT.LV expert Rihards Kauliņš participated in the Latvian team as a member, and CERT.LV expert Mārtiņš Vecstaudžs supported the team both in preparation and during the competition by participating in the work of the competition committees.

The national selection was organised by the Ministry of Defence in cooperation with CERT.LV, the University of Latvia and the Cyber Defence Unit of the National Guard (from January 2025 the Cyber Defence and Electromagnetic Warfare Battalion of the National Guard).

The ECSC 2024 is organised by the EU Cybersecurity Agency (ENISA) in cooperation with the Italian Cybersecurity Agency and the Cybersecurity National Laboratory (CINI). More information: https://ecsc2024.it/.

Speaking at other major international events

- **On 10 October in Brussels, Belgium, at the CERT.EU conference Tales From the Real World**, CERT.LV expert Kārlis Svilans gave a presentation "Defending From the Beast in the East – CERT.LVs Approach to Multinational Threat Hunting".
- **On 15–16 October in Tirana, Albania, and on 24–25 October in Belgrade, Serbia, two-day seminars for cyber security professionals were held within the EU-supported Cyber Balkans project**. During these seminars, CERT.LV cyber security expert and Head of Incident Response Armīns Palms shared his experience with CERT.LV's practice in dealing with cyber security incidents.
- **On 15–18 October in Tokyo, Japan, during the CEATEC 2024 – Toward Society 5.0 conference**, Dr. Bernhards Blumbergs, CERT.LV Cyber security Professional, spoke on the thematic panel "AI for All" with a focus on the interplay of cyber security with AI/ML. CEATEC is the world's largest electronics and technology exhibition with a very high international attention and visibility.



CERT.LV's mission is to foster IT security in Latvia.

The main tasks of CERT.LV are to maintain and update information on IT security threats, provide IT security support to government institutions, assist in the clean-up of IT security incidents affecting any natural individual or legal entity if the incident involved a Latvian IP address or was in the .LV domain, and organise information and education events for the employees of government agencies, IT security professionals, and other interested parties.

Contact CERT.LV:

Phone: +371 67085888

E-mail: cert@cert.lv

Website: www.cert.lv

Follow CERT.LV news on:

@cert.lv

CERT.LV
Cyber Incident
Response Institution