2026 Q3

LATVIAN CYBERSPACE SITUATION

PERIOD: 01.07.2026–30.09.2026



CERT.LV
Cyber Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

Summary

In Q3 2026, the intensity of cyber threats and the impact of incidents in Latvian cyberspace increased. Attackers increasingly exploited system vulnerabilities, compromised digital identities, and caused data leaks. The threat landscape was also characterised by automated attacks and social engineering methods. Artificial intelligence (AI) enabled attackers to carry out attacks more quickly and create more convincing fraud schemes. At the same time, the threat of geopolitically motivated cyber attacks persisted.

The volume of cyber threats continued to increase. During the reporting period, the number of identified compromised devices reached 1.4 million – 250% more than in Q2 2026 and 123% more than in the same period last year. The increase was driven by both actual threats and changes in data sources. At the same time, the number of alerts registered by the CERT.LV Security Operations Centre (hereinafter – SOC) increased, with high-level and critical alerts growing significantly faster than the total number of alerts. This dynamic indicates an increased risk to the confidentiality, integrity and availability of information systems, and the need for enhanced monitoring of potential threats.

CERT.LV manually processed 785 cyber incidents – significantly more than in the previous quarter and the same period last year. The large share of fraud cases in the total number of incidents confirms that user cyber hygiene and the ability to recognise fraud attempts remain essential prerequisites for cybersecurity.

The most significant threats were credential compromise, phishing and the exploitation of vulnerabilities in internet-accessible systems. Cyber attacks by financially motivated groups continued. Fraud dominated in terms of volume, affecting the broadest segment of the population. In terms of potential impact, state-backed cyber attacker groups (APT) continue to pose significant threats. Russia remains the main source of cyber threats to Latvia. DDoS attacks and hacktivist activity related to the geopolitical situation and Latvia's support for Ukraine continue to test the resilience of the country's digital services. The combination of these factors poses a particular threat to state institutions, local governments, critical infrastructure, and operational technology (hereinafter – OT) control systems.

The largest and most significant incident during the reporting period was a cyber attack against the State Joint Stock Company "Road Traffic Safety Directorate" (CSDD), in which data relating to approximately 1.2 million natural persons and 200 thousand legal persons were affected, resulting in a large-scale breach of data confidentiality. This and other events in recent months highlighted significant shortcomings in cybersecurity management at institutions and companies, emphasising the need to identify and remediate system vulnerabilities in a timely manner.

Groups linked to Russia continued to probe the OT environment, including energy and industrial control systems. Latvia is strengthening proactive capabilities to prevent threats. CERT.LV has already remediated several dozen vulnerabilities in this area, the exploitation of which could have caused incidents.

In preparation for the 15th Saeima elections, CERT.LV tested the information systems involved in the election process, conducted threat hunting, strengthened the resilience of the institutions involved, and implemented additional protection measures.

CERT.LV strengthened preventive protection and expanded cyber threat detection capabilities. The DNS firewall blocked 4.7 million requests to access fraudulent websites – 12 times more than in the same period last year. At the same time, the CERT.LV SOC expanded centralised cybersecurity monitoring and real-time threat detection. The number of monitored National Cybersecurity Law subjects increased by 20%, while the number of their endpoints increased by 25%. A broader monitoring scope improves the ability to identify potential threats in a timely manner. Meanwhile, 927 reports were registered on the Coordinated Vulnerability Disclosure Platform (CVD) – the highest number of reports since its launch. Alongside the development of technical capabilities, CERT.LV expanded its educational activities, reaching more than 5 600 participants through cybersecurity training.

Summary

As cyber threats become more intense and complex, timely risk identification, preventive protection and regular user education are essential to Latvia's cyber resilience. Organisations must understand their IT systems, remediate vulnerabilities in a timely manner, strengthen access control, and monitor the security of outsourced services. The effectiveness of these measures depends on coordinated cooperation and the ability to respond to threats in a timely manner.

By combining testing, day-to-day protection, threat analysis, and the expertise of the cybersecurity community, CERT.LV continues to strengthen Latvia's cyber resilience. Every vulnerability remediated in time and every threat stopped makes Latvia a more difficult target for cyber attackers.

CERT.LV key indicators for Q3 2026

785 | +17%

Number of manually processed cyber incidents
(Q3 2026 vs Q3 2025)

1,4 milj. | +123%

Number of identified compromised devices
(Q3 2026 vs Q3 2025)

2 953 | +153%

Fraud campaigns automatically identified and stopped
(Q3 2026 vs Q2 2026)

4,7milj. | +1086%

Requests to malicious websites blocked by the CERT.LV DNS firewall
(Q3 2026 vs Q3 2025)

126 | +20%

Number of CERT.LV SOC clients
(total as of 30.09.2026)

71 243 | +25%

Number of endpoints covered by CERT.LV SOC visibility
(total as of 30.09.2026)

909 | +47%

Manual processing of alerts and creation of cases by CERT.LV SOC, including 19 incidents detected
(total as of 30.09.2026)

Completed 6 threat hunting operations, with 16 in progress

(data for Q3 2026)

2 657

emails sent in phishing attack simulations: 55% were opened; of these, 38% of users entered data.
(data for Q3 2026)

927 | +36%

Vulnerability reports registered on the CVD platform
(total as of 30.09.2026)

41 | +58%

Cybersecurity educational activities/ events conducted by CERT.LV experts within the cybersecurity community
(Q3 2026 vs Q3 2025)

5 652 | +32%

Total number of participants trained in various cybersecurity community activities/events
(Q3 2026 vs Q3 2025).

Contents

Summary 1

CERT.LV key indicators for Q3 2026 3

1. Latvian cyberspace in figures 5

2. Threat trends in cyber attack types 8

2.1. Attack vectors, threat dynamics 8

2.2. Sector-specific risks 10

2.3. Conclusions and recommendations 10

3. CERT.LV services: day-to-day protection, testing and education 12

3.1. DNS firewall 12

3.2. Cybersecurity Early Warning System (EWS) 13

3.3. Security Operations Centre (SOC) 13

3.4. IT system security tests and phishing attack simulation campaigns 17

3.5. Cybersecurity threat hunting operations 17

3.6. Coordinated Vulnerability Disclosure Platform (CVD) 18

3.7. Operational technology (OT) security 19

3.8. Education – lectures and participation in cybersecurity events 20

4. Overview of the activities of the LIA Safer Internet Centre Reporting Line 21



1. Latvian cyberspace in figures

Threat intensity in Latvian cyberspace

In Q3 2026, the number of compromised devices identified by CERT.LV in Latvian cyberspace reached 1 387 431 – 250% more than in Q2 and 123% more than a year ago.

During the reporting period, the increase in the statistics was driven both by an increase in the number of potentially compromised devices and by the use of new data sources (feeds), which expand the range of devices that can be identified. The increase was partly influenced by the resumption of the Microsoft DCU CTIP *Infected feed* after a brief interruption in Q2. Consequently, the increase in the number of compromised devices reflects both actual threats and changes in data sources.

The threat level is increased by widespread vulnerabilities in popular network devices, publicly accessible management services, outdated software versions and delayed installation of security updates, as well as more active automated scanning by cyber attackers for vulnerable systems.

Artificial intelligence (AI) tools significantly accelerate attack automation. Vulnerability exploitation tools often become available soon after information about a vulnerability or software patch is published, so organisations must be able to remediate vulnerabilities within increasingly shorter timeframes.

During the reporting period, the number of high-level and critical security alerts registered by the CERT.LV SOC increased significantly faster than the overall volume of alerts. This dynamic indicates an increased risk to the confidentiality, integrity and availability of information systems, as well as the need to pay increased attention to potential threats.

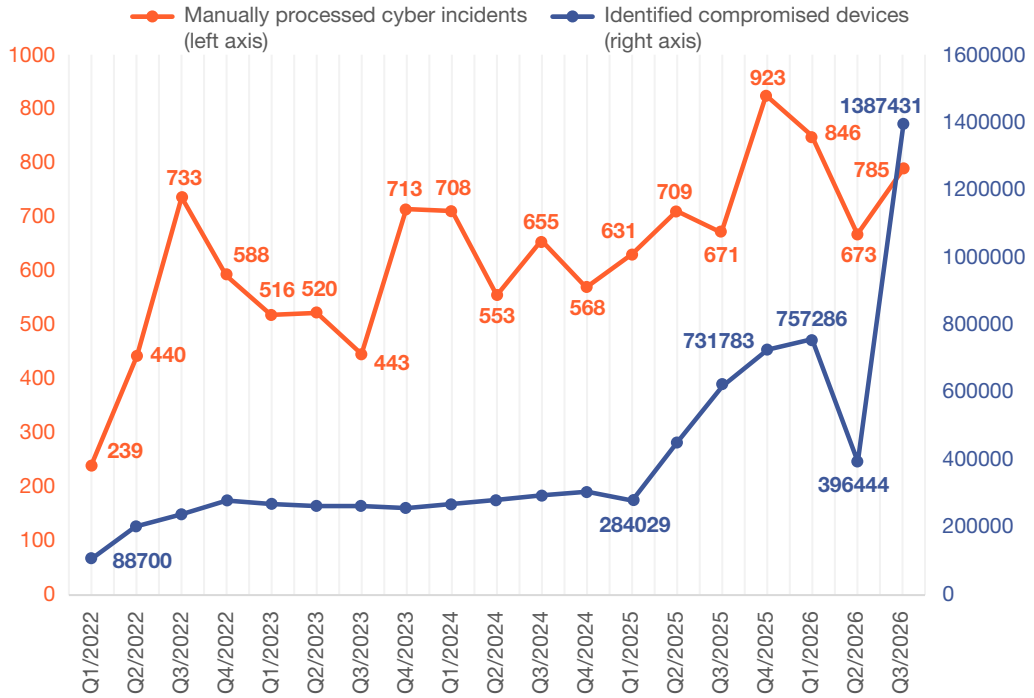


Figure 1. Dynamics of cyber incidents and identified compromised devices (number)

In Q3 2026, a total of 785 manually processed cyber incidents were registered in Latvian cyberspace – 16.6% more than in Q2 and 17% more than in the same period last year.

The number of registered cyber incidents is the third-highest figure recorded to date. This dynamic indicates that user cyber hygiene and the ability to recognise fraud attempts remain essential prerequisites for cybersecurity.

In the first nine months of this year, the CERT.LV DNS firewall blocked an average of 1.08 million user requests to malicious websites per month. In September, the number of blocked requests reached a record – approximately 1.7 million. These data demonstrate the importance of the DNS firewall in protecting users by proactively identifying and blocking access to malicious websites.

At the same time, CERT.LV proactively identified and stopped 2 953 active fraud campaigns – 153% more than in the previous quarter – before they reached users at scale and caused financial losses, demonstrating the growing importance of automated protection.

For followers of "Cyber Weather", a monthly overview of the most significant cyber incidents and threats in Latvian cyberspace, organised into TOP 5 categories, is available in the News section of the CERT.LV website – https://cert.lv/lv/zinas/kiberlaikapstakli.

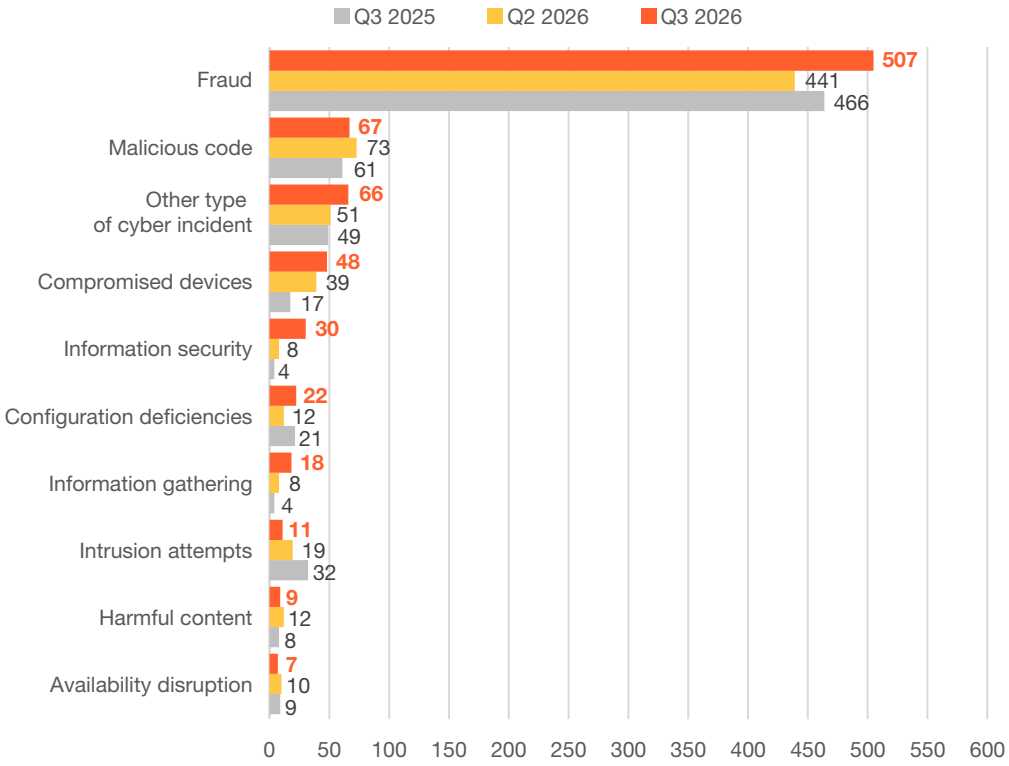


Figure 3. Dynamics of cyber incident types

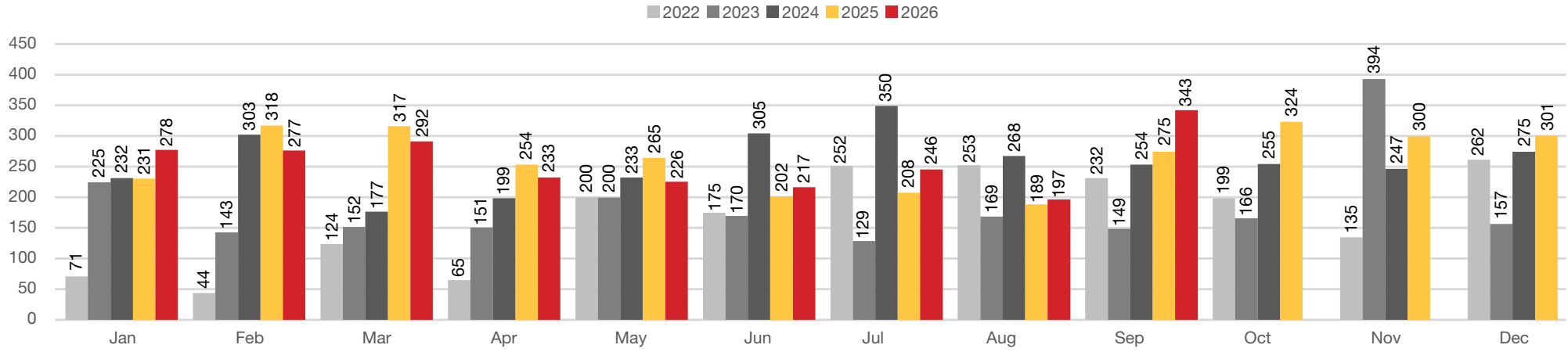


Figure 2. Cyber incident trends by month

Most common types of cyber incidents

Fraud dominates, accounting for nearly two-thirds of incidents registered by CERT.LV. The number of fraud cases increased by 15% compared with the previous quarter and by 9% compared with the same period last year.

Information security incidents showed the fastest relative increase – 275% compared with the previous quarter and 650% compared with the same period last year.

The number of compromised devices increased by 23% compared with the previous quarter and by 182% compared with the same period last year.

The number of intrusion attempts decreased by 42% compared with the previous quarter and by 66% compared with the same period last year.

Availability disruptions account for 0.9% of the total number of incidents. Their small share may indicate the effectiveness of DDoS protection measures.

Most common malware types

- **Data-stealing malware**
- **Botnet malware**
- **Remote access trojans for data extraction and infrastructure compromise**

Data-stealing malware (infostealers) obtains credentials from web browsers or unencrypted files. It is distributed via malicious browser extensions or executable files attached to phishing emails.

TOP 10 malware

The prevalence of the malware most frequently detected in Q3 2026 indicates large-scale, automated and persistent threats. “Android.badbox2” has dominated for several quarters, although its prevalence decreased by 4% during the reporting period compared with the previous quarter.

“Android.badbox2” threatens Android devices by incorporating them into a botnet. The main risks are credential theft, remote control of infected devices, and their use in subsequent cyber attacks. Users and organisations may be unaware that their devices are involved in botnet activity.

The other malware families included in the top ten account for a smaller share, but reflect the diversity of attack types and create additional risks to device security.

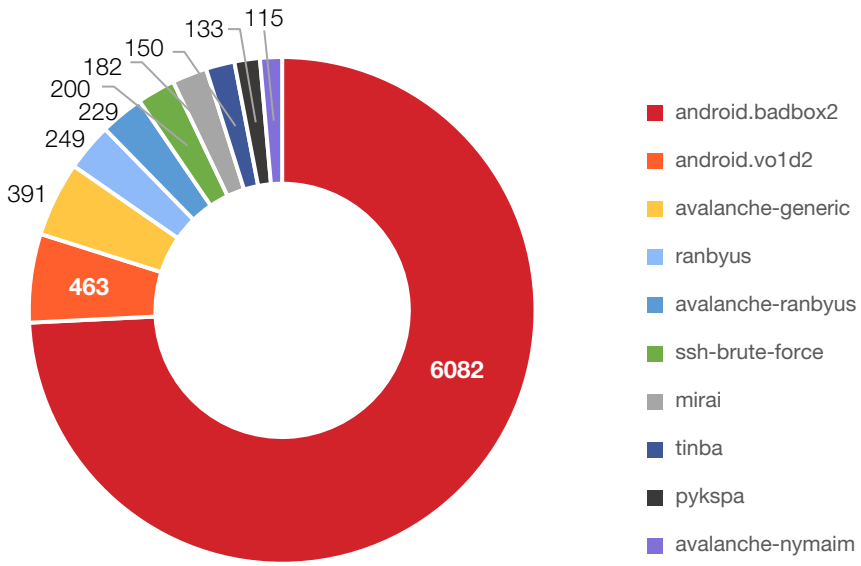


Figure 4. TOP 10 malware (number; Q3 2026)

2. Threat trends in cyber attack types

2.1. Attack vectors, threat dynamics

During the reporting period, five interrelated trends emerged, characterising both the attack methods used and the growing impact of incidents on organisations and residents.

1. The impact of data leaks is increasing



During the reporting period, the State Joint Stock Company "Road Traffic Safety Directorate" (CSDD) experienced a large-scale cyber incident in which data relating to approximately 1.2 million natural persons and 200 thousand legal persons were affected. The incident demonstrates that, alongside disruptions to service availability, threats to data confidentiality are also a significant cybersecurity risk in Latvia.

The CSDD data leak was facilitated by shortcomings in cybersecurity management, including incomplete coverage of security testing, insufficient network protection, deficiencies in software development, and the lack of multi-factor authentication (hereinafter – MFA). CERT.LV helped stop the cyber attack, conducted a technical investigation, analysed the leaked data, and identified the access channels used in the attack.

CERT.LV warns that the consequences of the incident may be long-lasting even after the incident itself has been resolved. Attackers may use the leaked data for personalised fraud, identity misuse and social engineering campaigns. Large-scale data leaks can also undermine public trust in digital services.

Residents should be particularly cautious when receiving personalised calls, text messages and emails. For additional protection, MFA should be used, and the CERT.LV DNS firewall and its mobile app are also recommended, as they block identified fraudulent websites and calls. Organisations should strengthen access control, implement MFA, monitor logs, and systematically manage software versions and vulnerabilities.

2. Vulnerabilities in publicly accessible systems – a significant initial access risk



Attackers are increasingly searching for internet-accessible, insufficiently protected systems. This trend was particularly pronounced during the reporting period. VPN gateways, firewalls, routers, web and management services, email systems, and remote access solutions (RDP) are particularly at risk. Compromising them enables attackers to penetrate deeper into an organisation's infrastructure, access data, and disrupt service availability.

The cyber incident registered during the reporting period in an information system managed by the Consumer Rights Protection Centre (PTAC) **clearly demonstrated the risks posed by outdated content management systems and vulnerabilities that are not remediated in a timely manner**. By exploiting a vulnerability in this internet-accessible system, the attacker obtained the contact details of 697 representatives of businesses and 34 PTAC officials.

Automated vulnerability discovery and mass exploitation are also increasing. This risk is illustrated by an incident at the LMT Group company "TSC", which became a target not as a result of deliberate selection, but because the attacker used automated tools to search for vulnerable systems. This means that **any insufficiently protected, internet-accessible system can become a target** regardless of the size or sector of the organisation.

3. Digital identity is becoming a key security perimeter



Attacks on user accounts and their credentials are increasing – passwords, access and API keys, session tokens, service accounts, and other authentication data.

Attackers use stolen credentials, MFA bypass techniques and insufficiently protected service and API accounts to operate in

systems as legitimate users. The risk is compounded by inadequate access rights management, insecure storage of sensitive data in code repositories, insufficient protection of software and code version control systems, and the use of unverified AI-generated code. Alongside network and endpoint protection, systematic management of digital identities and access rights is becoming increasingly important.

4. Fraud remains dominant, while social engineering increases the phishing risk

Fraud remains the most common type of cyber incident in Latvia. Fraud campaigns operate continuously and on a large scale, combining various methods and communication channels. This approach makes it possible to reach a broad audience and adapt fraud scenarios to different situations.

During the reporting period, fraudsters attempted to deceive residents by impersonating representatives of trusted institutions, companies and digital service providers. By exploiting users' trust and creating a sense of urgency, they sought to obtain authentication codes, internet banking credentials, personal data, and payment card information. Emails, text messages, phone calls, fake websites, and advertising platforms were actively used in fraud campaigns. CSDD-themed scams and email credential phishing dominated.

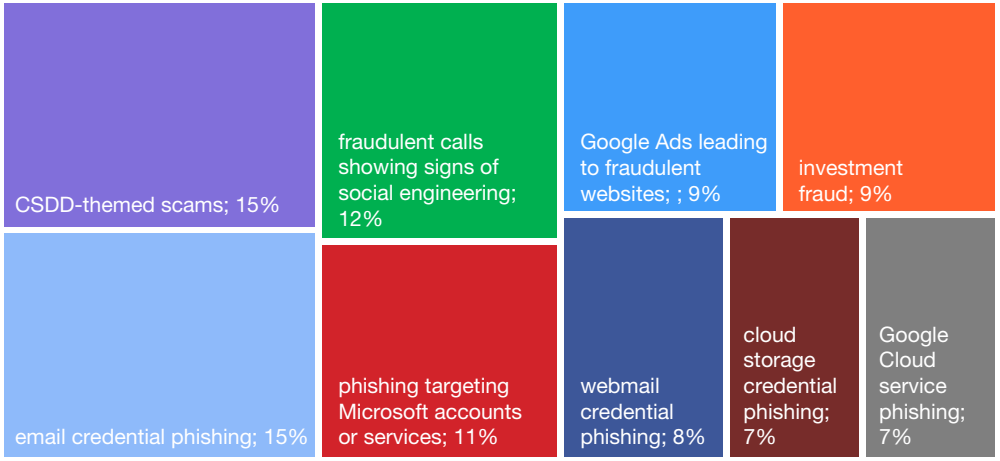


Figure 5. Most common social engineering and phishing campaigns (percentage of total; Q3 2026)

Data-stealing malware, fake software updates and malicious browser extensions also posed a significant threat. Social engineering was widely used in attacks, prompting users to perform the actions needed by the fraudsters on their own. More than half of the incidents registered by the CERT.LV SOC were related to "ClickFix" attacks, in which users were deceived by fake "CAPTCHA" checks on compromised websites.

Data from the Finance Latvia Association show that in the first nine months of 2026, financial institutions prevented attempts to defraud customers of EUR 16.6 million – 73% more than in the same period last year. Meanwhile, bank customers who authorised payments themselves were defrauded of EUR 10 million – 11% more than in the same period last year. The scale of the prevented fraud attempts demonstrates the importance of timely detection of attempts to defraud customers. Alongside the protection solutions implemented by companies in the financial and other sectors, residents' ability to recognise fraud is also essential. However, the increase in the amount defrauded indicates that the risk remains high. Fraudsters are expected to continue adapting their methods and seeking new ways to defraud people of money. Therefore, everyone must remain vigilant.

5. Geopolitically motivated threats persist

The impact of the geopolitical situation on Latvian cyberspace persists. The most significant threats are linked to the activities of state-backed groups, hacktivism and the reconnaissance of ICT critical infrastructure.

Groups linked to countries hostile to Latvia (APT) continue reconnaissance and phishing activities targeting state administration, local governments and companies of national importance. Russia continues to be identified as the primary source of cyber threats to Latvia and is the dominant state-backed threat with high escalation potential. At the same time, cyber threats must be assessed in the broader context of hybrid threats, including the risks of sabotage, information influence and threats to ICT critical infrastructure.

DDoS attacks and hacktivist activity continue to be used as an instrument of geopolitical pressure. Their intensity may increase following political events or public statements in the context of Latvia's support for Ukraine.

Protection measures to date have largely made it possible to avoid prolonged or significant impacts on service availability, but the risk of attacks remains. Latvia must continue to strengthen its defence and preparedness against various types of cyber threats.

2.2. Sector-specific risks

State administration, local governments and election infrastructure: heightened attention was expected in connection with the 15th Saeima elections scheduled for 3 October 2026 in Latvia. During the reporting period, attacker groups backed by countries hostile to Latvia (APT) and organised crime groups continued reconnaissance and phishing activities targeting ministries, local governments and companies of national importance.

While monitoring cyberspace in September as part of the CERT.LV SOC service, a cyber incident was detected on a local government email server. A more in-depth analysis of the incident showed attacker interest in the keywords "velesanas" and "namejs". Such activity indicates the possibility that the attack may have been politically motivated. As the attack was stopped at the stage when the attackers were conducting reconnaissance on the compromised server, no large-scale email data leak occurred.

In September, cyber attacks against municipal surveillance cameras and smart building management components were detected in several regions of Latvia. Links to Russia were observed in these incidents. The number of incidents was small, but their significance is substantial. Attackers attempted to access cameras, alter images, carry out digital vandalism or display their messages. CERT.LV does not link these cases to the election process. However, they show that municipal smart infrastructure can become a target for reputational impact and undermining public trust. Therefore, not only election infrastructure but also state and local government websites, communications systems and other related digital services require continuous monitoring.

Energy and OT control systems: Russia-linked APT groups continued to survey the OT environment, particularly energy and industrial control systems. Publicly accessible or insecurely configured OT management interfaces pose a significant risk. Their compromise can create risks not only to information security but also to physical processes. Latvia is strengthening proactive capabilities. CERT.LV has already remediated several dozen vulnerabilities in this area, the exploitation of which could have caused incidents. Organisations are encouraged to implement technologies more responsibly and monitor outsourced services more closely.

Financial sector: cyber attacks by financially motivated groups and fraud campaigns continue. The number of fraud attempts using AI to develop more sophisticated schemes and more convincing content is increasing.

2.3. Conclusions and recommendations

In Q3 2026, both the intensity of cyber threats and the impact of incidents increased in Latvian cyberspace. Cybersecurity risks are increasingly shaped by a combination of interrelated factors: exploitation of vulnerabilities in publicly accessible systems, threats to data confidentiality, compromise of digital identities, attack automation, social engineering, and geopolitically motivated threats. The use of AI tools accelerates the preparation and execution of attacks.

The interaction of these factors increases the risk of threats, particularly for state institutions, local governments and critical infrastructure organisations, including the OT systems they use.

The large share of fraud cases in the total number of incidents confirms that user cyber hygiene and the ability to recognise fraud attempts remain essential prerequisites for cybersecurity. The substantial increase in the number of identified compromised devices indicates an increased risk to the confidentiality, integrity and availability of information systems.

These trends highlight the need to strengthen user vigilance and technical protection measures, with particular attention paid to timely system updates, vulnerability remediation, threat detection, and incident response.

Key recommendations

State institutions, local governments, critical infrastructure organisations, as well as providers of essential and important services, are advised to prioritise the following:



Protection of organisations

1. **Implement multi-factor authentication (MFA)**
   For users of high-security systems, administrators of basic security systems and users who access them remotely from an external network, as well as for all publicly exposed and essential systems.

2. **Take a complete inventory of IT assets**
   Pay particular attention to internet-accessible systems.

3. **Remediate vulnerabilities promptly**
   Minimise the time required to deploy updates.

4. **Centrally collect and analyse logs**

5. **Separate administrator accounts from everyday user accounts**

6. **Rapidly identify and isolate compromised systems**
   Ensure the capabilities required for this purpose.

7. **Regularly test preparedness plans**
   for incident response and business continuity.



Critical infrastructure and OT

Segment industrial control systems from the corporate IT network and closely monitor access by outsourced service providers.

It is advisable to block public internet access to management tools for surveillance cameras and smart control devices. Remote management and monitoring functions on these devices should be performed through an institution-managed VPN connection.



International cooperation

Continue exchanging information and cyber threat intelligence data (IOC/CTI) with allies. Actively participate in NATO and EU coordinated initiatives.



Public awareness

Regularly inform the public about current fraud campaigns, phishing and social engineering techniques, as these threats affect the broadest segment of the population.

3. CERT.LV services: day-to-day protection, testing and education

3.1. DNS firewall

Campaign-based fraudulent activity regularly occurs in Latvia – both redirection to fake websites to steal user account credentials and the distribution of malware. CERT.LV proactively monitors and stops identified fraud campaigns, promptly adding campaign indicators to the DNS firewall.

In Q3 2026, the CERT.LV DNS firewall blocked 4.7 million user requests to malicious websites – 89% more than in Q2 and 12 times more than in the same period last year*.

*Statistics do not include data from lists maintained by other competent national authorities for restricting illegal online content.

Since 2024, the DNS firewall mobile app has been downloaded a total of 91 854 times on Android and iOS devices – the increase accounts for 4% of the total. The DNS firewall mobile app protects users not only from fraud campaigns in cyberspace but also from identified fraudulent calls.

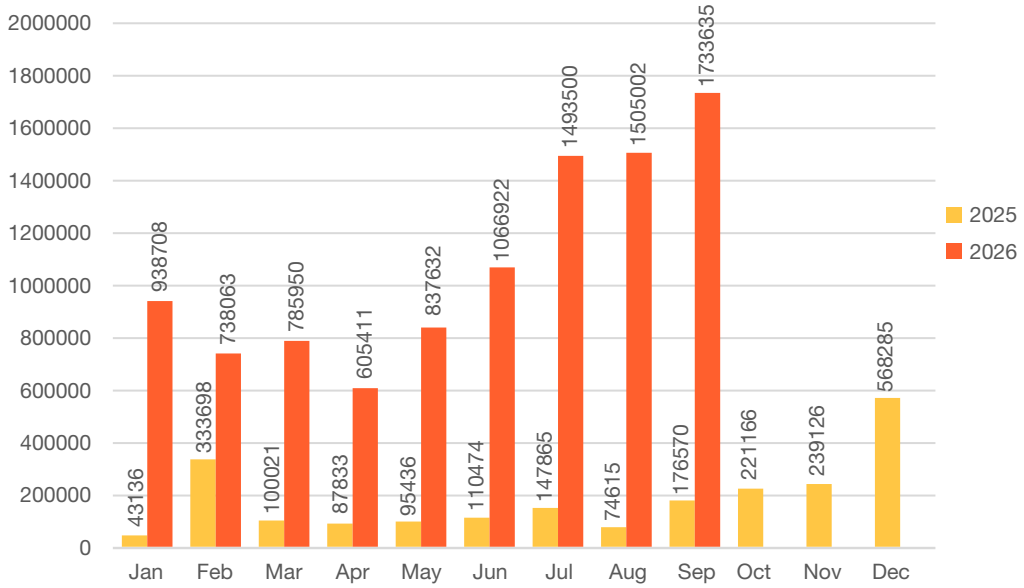


Figure 6. Requests to malicious websites blocked by CERT.LV DNS firewall lists

Major active defence episodes:

- requests to websites distributing “ClickFix” and “ClearFake” malware were blocked;
- requests to websites involved in malicious botnet activity and malware distribution were blocked;
- access to fraudulent cryptocurrency investment platforms advertised using the “LSM” and “Jauns.lv” names and visual identities was blocked.

Cyber threats are persistent and mostly financially motivated. The CERT.LV DNS firewall effectively protects users from phishing pages, malware download sites and fraudulent platforms. When attempting to access a malicious website included in the CERT.LV DNS firewall block list (cert-shield, malware, phishing, high-risk), the user is redirected to a secure warning page.

Residents also help strengthen protection by forwarding fraudulent emails to cert@cert.lv and reporting text messages and suspicious links via “WhatsApp” to 23230444. CERT.LV compiles the reports received and adds malicious domain names to the DNS firewall block list. More information: dnsmuris.lv

3.2. Cybersecurity Early Warning System (EWS)

Implementation of the EWS service

The EWS is a service provided by CERT.LV for analysing data traffic anomalies and identifying signs of cyber attacks in the service recipient's infrastructure. The EWS service is primarily intended for National Cybersecurity Law (NCL) subjects and critical infrastructure organisations.

The EWS service includes the continuous analysis of data traffic anomalies and detection of malware activity, the sending of alerts about identified high-priority cyber threats, regular updates of the cyber threat indicators used by CERT.LV, as well as consultations and support for clients.

CERT.LV continues to implement and maintain the EWS, expanding the range of service recipients in line with the NCL and strengthening their protection and resilience against cyber threats.

Detection and prevention of cyber threats and incidents

In Q3 2026, the number of alerts registered by the EWS was 1.2 billion – 18% more than in Q2.

During the reporting period, as the number of service recipients and sensors increased, the volume of data traffic analysed also increased, along with the workload involved in identifying anomalies and malware activity, sending alerts and providing support.

The most significant threats during the reporting period:

- requests to domains distributing "ClickFix"/"ClearFake" malware;
- requests to domains distributing malicious remote administration tools (RAT);
- requests to domains associated with identified phishing and fraud campaigns;
- after vulnerabilities are publicly disclosed, attackers often scan systems at scale to find and exploit existing vulnerabilities.

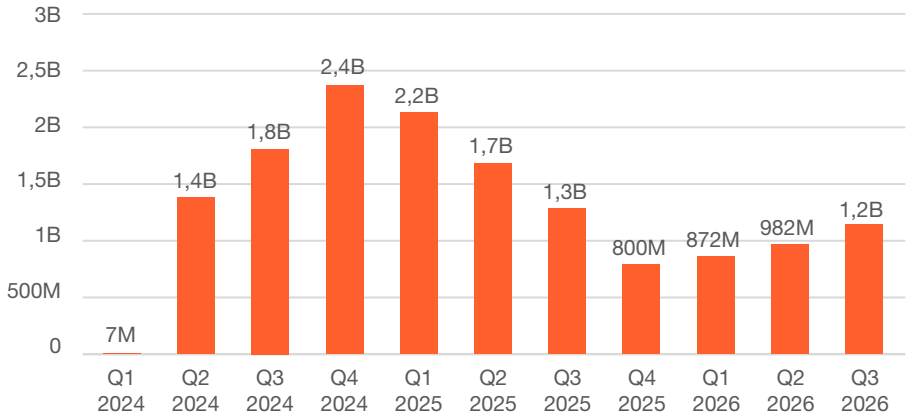


Figure 7. Quarterly dynamics of alerts registered by the CERT.LV EWS (number in millions/billions)

3.3. Security Operations Centre (SOC)

Implementation of the SOC service

CERT.LV continues to develop SOC services and attract new clients, expanding the client base in line with the NCL and promoting more effective protection and resilience against cyber threats. The SOC centrally collects security telemetry from client infrastructure, correlates events, and links them with the complete set of threat indicators and knowledge available to CERT.LV.

The contribution of SOC analysts is particularly significant; using specialised software and available data, they prevent harm in a timely manner – identifying, warning about, and stopping a threat or cyber incident.

By the end of the reporting period, the number of SOC clients had reached 126 – an increase of 20%.

CERT.LV SOC solutions are used by organisations across various sectors, including NCL subjects – providers of essential and important services. The most widely represented are ministries (54%), local governments (19%) and healthcare institutions (9%).

SOC visibility dynamics

- ➔ **Overall, visibility was provided across 71 243 endpoints, including servers and workstations. The increase in Q3 2026 accounted for 25% of the total.**
- ➔ **As the monitoring scope expands, the number of events analysed and alerts generated increases, as does the ability to identify threats in a timely manner.**

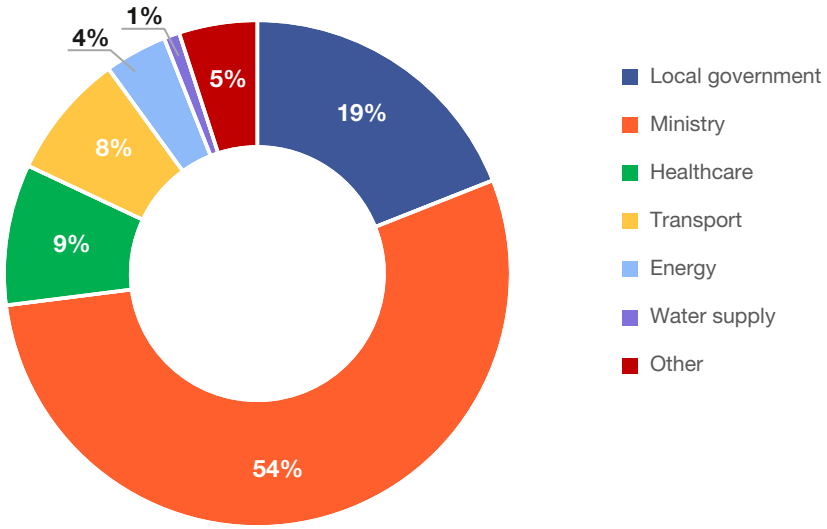


Figure 8. Breakdown by organisation type/sector using CERT.LV SOC (percentage of total: 126)

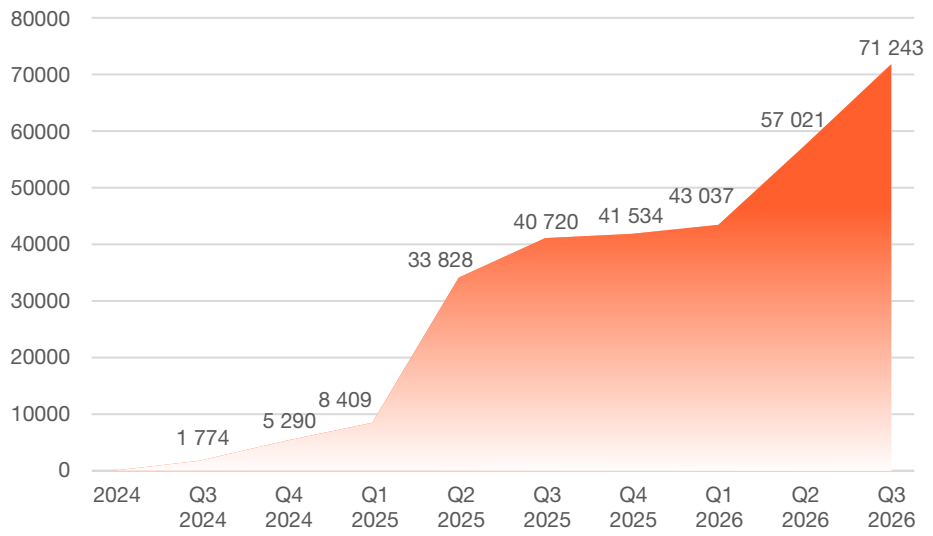


Figure 9. CERT.LV SOC visibility dynamics: number of endpoints (2024-2026)

During the reporting period, 29 million security alerts were registered – 16% more than in Q2 2026.

The increase in the number of security alerts primarily reflects the expansion in the number of endpoints monitored by the SOC and an improved ability to identify potential threats. At the same time, this indicates an increase in attack intensity in cyberspace.

Low- and medium-level alerts still account for the majority, creating a very “noisy” environment and making it more difficult to identify the most significant alerts in a timely manner.

High-level and critical alerts together account for 0.3% of the total. At the same time, the sharp **increase in high-level and critical alerts, by 67% and 37% respectively, is a significant risk indicator**. This means that during the reporting period, the proportion of events with a potentially greater impact on confidentiality, integrity or availability increased. This volume also represents a significant operational workload for the CERT.LV SOC team.

Incidents and security alerts: threat detection and prevention

Indicators	Number	Change compared with Q2 2026 (%).
Total number of registered security alert reports in Q3 2026:	~29M	+16%
Low-level alerts	~10M	+66%
Medium-level alerts	~19M	+6%
High-level alerts	~27K	+67%
Critical alerts	~47K	+37%
Number of manually created cases	909	+47%
Number of false positive cases*	890	+49%
Number of cyber incidents	19	0

* A false positive in cybersecurity is a situation where a security system incorrectly identifies normal activity as an incident or threat.

Cases created within the SOC service and recorded cyber incidents

- ➔ **In Q3 2026, 909 cases were manually created within the CERT.LV SOC, which is 47% more than in the previous quarter.**
- ➔ **A total of 19 cyber incidents were registered, with the number remaining unchanged.**

A large number of "false positive" alerts is still observed (a 49% increase in Q3) – this means a greater volume of low-value work for SOC analysts when reviewing events, creating a risk that a genuine attack may be overlooked among the "false positives".

The most common reasons for false alerts in client infrastructure:

- ► incomplete or outdated inventories of ICT resources and a lack of centralised management at the institutional or municipal level;
- ► endpoint configurations are not standardised;

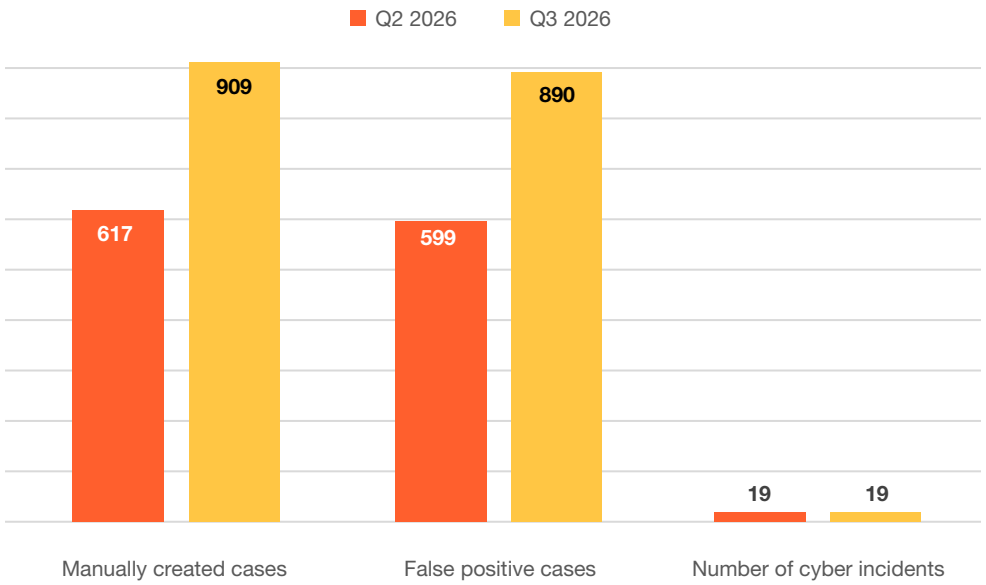


Figure 10. CERT.LV SOC: Structure and comparison of security events

- ► no list of approved software has been established, and compliance with it is not enforced;
- ► web browser plugins and extensions are not managed or controlled;
- ► multiple remote access tools are used unnecessarily for user support;
- ► logging is not enabled, and documentation and procedures are lacking;
- ► the use of USB flash drives is not monitored, and the execution of files stored on them is not controlled.

The workload of SOC analysts is increased both by the growing volume of endpoints and events and by increasingly complex and higher-risk incidents. At the same time, there is a growing need to assess alerts rapidly, set priorities, and coordinate action effectively with clients. Strengthening SOC capacity is an essential prerequisite for continuing to ensure service quality and timely response under increasing workloads.

Overview of cyber incidents recorded within the SOC service during the reporting period

The largest number of alerts is caused by uncontrolled, unwanted software – **executable files downloaded from the web and run by users**. For example, game installation files downloaded from the web often also contain malware. In several cases, unwanted software was found to have affected endpoint operation, and the alerts were therefore registered as cyber incidents.

During the reporting period, more than half of the registered incidents (10) were related to "ClickFix" attacks, in which users on compromised websites are deceived by **fake "CAPTCHA"** checks. This is a common initial access method that prompts the user to copy and execute a malicious command. The execution of the copied commands varies depending on the configuration of the institution's IT systems. After the command is executed, malware is downloaded to the device and may steal user credentials, install additional malicious software or perform other malicious actions.

Recommendations for users on mitigating the threat of "ClickFix" attacks are available on the CERT.LV website: **https://cert.lv/lv/2025/04/viltus-captcha-var-inficet-jusu-datoru**.

During the reporting period, several incidents were registered in which initial access was obtained through **phishing emails, infected email attachments or browser plugins**. The threat posed by these access methods remains relevant going forward.

In three incidents, **client servers were compromised:** in two cases, initial access was gained through a **vulnerable website content management system**, and in the third through **vulnerable email server software**.

The most common situation in a compromised environment:

- **the principle of least privilege has not been implemented**, allowing an attacker to rapidly expand access rights and move through the infrastructure;
- **a lack of network segmentation** allows a compromise in one part of the network to spread unhindered to other systems;
- **software execution restrictions have not been implemented**, allowing malicious code and unauthorised applications to be executed without significant obstacles;
- **unified IT environment management and centralised security telemetry are not provided**, making timely threat detection, correlation and effective incident response more difficult;
- **remote administration tools are used without control, with various** administration solutions operated without centralised management, monitoring or security policies, significantly expanding the attack surface and making unauthorised access more difficult to identify.

Dominējošie sākotnējās piekļuves vektori



Fake CAPTCHA checks



Phishing and malicious email attachments



Browser plugins



Unwanted software
executable files downloaded from the web and run



Website content management systems



Vulnerable email server software

3.4. IT system security tests and phishing attack simulation campaigns

Phishing attack simulation campaigns

In 2026, CERT.LV conducted 12 phishing attack simulation campaigns in total, including 4 phishing attack simulation campaigns in four institutions in Q3. A total of 2 657 emails were sent as part of these campaigns. More than half, or 55%, of users opened the link in the email, and 38% of those who opened it entered user data.

The purpose of phishing attack simulation campaigns is to train users and enhance employees' ability to identify potentially risky behaviour patterns, as well as recognise and prevent cyber threats and information leakage.

IT system security tests

A total of 24 IT system security tests were conducted in 2026.

In Q3, CERT.LV monitored the remediation of deficiencies identified in the security audit of election systems. Several repeat tests were also carried out to ensure that all previously identified deficiencies had been remediated and that no new ones had arisen during development.

CERT.LV also tested selected IT systems and websites, conducted security tests of election systems, and provided recommendations for improving security.

In IT system security testing, CERT.LV analyses network security, assesses software and IT infrastructure vulnerabilities, evaluates web application security, and provides consultations and recommendations for improving security.

3.5. Cybersecurity threat hunting operations

Cybersecurity threat hunting is a proactive process in which CERT.LV cybersecurity experts search Latvian ICT systems for signs of potential threats or unauthorised activity in order to identify risks and mitigate potential threats in a timely manner. Since CERT.LV launched cybersecurity threat hunting in 2022, threat analysis has been conducted in the infrastructure of more than 50 NCL subjects and ICT critical infrastructure organisations.

During the reporting period, 6 threat hunting operations were completed, while 16 operations remain in progress.

Analysis of endpoints identified several cybersecurity shortcomings, including insecure software and device configurations and the use of outdated components exposed to security vulnerabilities, which increases the risk of potential cyber incidents.

Latvia and Canada continue to strengthen NATO cybersecurity capabilities through the Threat Hunting Training Course

The fifth consecutive Threat Hunting Training Course on cyber threat hunting will take place in Riga on 19-23 October 2026 and will be jointly led by CERT.LV and Canadian cybersecurity experts. The training is organised by CERT.LV in cooperation with the Latvian Ministry of Defence and the Canadian Armed Forces Cyber Command.

The aim of the Threat Hunting Training Course is to support and strengthen NATO allies' capabilities to identify potential threats before they become actual cyber incidents.

3.6. Coordinated Vulnerability Disclosure Platform (CVD)

The Vulnerability Reporting Platform **cvd.cert.lv** (hereinafter – CVD platform) is operated by CERT.LV, which acts as the coordinator of the coordinated vulnerability disclosure process and performs the tasks laid down in the NCL regulating the coordinated vulnerability disclosure and remediation process at the national level.

The CVD platform has been available to users for three years. To promote cooperation that is acceptable, open and fair to all parties involved, and to align the procedure for using the platform and its terminology with changes in the regulatory framework, the platform's terms of use and the procedure for processing personal data have been reviewed. The changes took effect on 1 August 2026.

The platform processes reports concerning resources under the control of a natural or legal person registered in the Republic of Latvia. Such a person may be an NCL subject, a state or local government institution that is the owner, holder, possessor or controller of an ICT resource or a .lv domain name.

CVD platform indicators

At the end of Q3 2026, the following had been registered in total*:



245

security researchers

an increase of 60



28

active institutional programmes

10 added



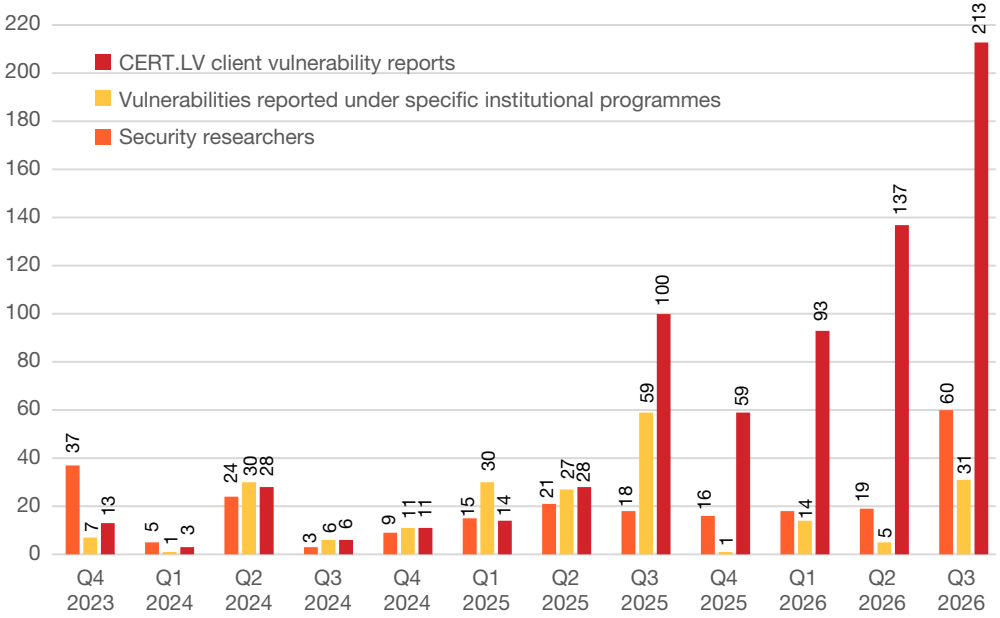
927

vulnerability reports

an increase of 244

*The increase is shown since the end of the previous quarter.

During the reporting period, the highest number of reports since the platform was launched was registered – **927** reports, including **705** vulnerability reports submitted to CERT.LV (an increase of 213) and **222** vulnerabilities reported under institutional programmes (an increase of 31).



11. attēls. CVD platformas attīstības dinamika (skaits)

View active institutional programmes on the CVD platform:
https://cvd.cert.lv/programs/all

CERT.LV invites organisations to create and manage their programmes on the CVD platform so that security researchers can test resources exposed to the external network for vulnerabilities. Security researchers are invited to report vulnerabilities discovered in the resources of public administration institutions and companies registered in Latvia through the platform, contributing to faster remediation.

The contribution of security researchers to vulnerability discovery helps strengthen the security of Latvian cyberspace. At the same time, CERT.LV reminds researchers that vulnerability research must be conducted responsibly, proportionately and in accordance with the rules of the specific programme.

Cyber Resilience Act reporting requirements for manufacturers start to apply

From 11 September 2026, under the European Union (EU) Cyber Resilience Act (CRA; **https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=OJ:L_202402847**), manufacturers are required to report actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements available on the EU market. Reports must be submitted through the Single Reporting Platform (SRP) developed by the European Union Agency for Cybersecurity (ENISA): **https://portal.cra-srp.enisa.europa.eu/**. In Latvia, these reports are processed and will continue to be processed by CERT.LV.

Information on the legal reporting requirements, guidance for report submitters, and answers to frequently asked questions are published on the ENISA website: **https://www.enisa.europa.eu/news/the-cra-single-reporting-platform-is-launched**.

3.7. Operational technology (OT) security

Activities

CERT.LV has established cooperation with operators in Latvia's energy, water supply, district heating, and transport sectors, and has concluded operational technology (OT) security service agreements. OT system security is strengthened in three main areas: system monitoring and anomaly identification; security testing; and incident response.



System monitoring and anomaly identification
CERT.LV continues to expand the sensor network for monitoring OT system data traffic. To detect anomalies in data collected by OT sensors more effectively, machine-learning-based detectors are being developed and deployed. Their operation is continuously improved by analysing the data obtained. Alongside monitoring data traffic within internal OT networks, Latvia's IP address space is continuously monitored to identify publicly exposed systems and their potential vulnerabilities. Based on the information obtained, access restrictions to these systems and the remediation of identified deficiencies are coordinated.



OT system security tests
Security checks of OT system components test various smart and industrial control devices. The aim is to identify potential vulnerabilities and supply chain weaknesses that could allow manufacturers or external attackers to control these devices or entire systems without authorisation. During the reporting period, system tests were carried out, identifying a range of improvements and discussing them with the developers of these systems.



International cooperation
Broader cooperation with Nordic and Baltic (NB8) cybersecurity authorities continues. The cooperation includes the regular exchange of information on current cyber threats.

Threats, incidents, impact

CERT.LV continues to proactively identify potential risks and vulnerabilities in order to reduce their possible impact. **The resilience of Latvia's OT systems against cyber attacks is generally at an appropriate level and continues to improve**. Regular checks identify private or small OT systems that are accessible from the internet. CERT.LV informs the operators of these systems about the identified risks and works with them to reduce or prevent the potential impact of cyber threats.

Persistent cyber threats from countries hostile to Latvia are also expected to continue, with the aim of gaining control over the systems of critical infrastructure operators and carrying out destructive actions within them. In Europe, such activities are carried out by cyber attackers linked to Russia, China and Iran.

As the capabilities of large language models increase, they are increasingly used for automated vulnerability discovery and exploitation at various stages of an attack, including the execution of a full attack chain.

To reduce the potential impact of threats and strengthen Latvia's resilience, CERT.LV will continue to improve OT system security by expanding visibility into these systems and threat identification capabilities, conducting security tests and ensuring a coordinated incident response.

3.8. Education – lectures and participation in cybersecurity events

CERT.LV continues to strengthen the cybersecurity knowledge and skills of individual users and organisations.

In Q3 2026, CERT.LV experts reached an audience of 5 652 people across 41 events. Compared with the same period in 2025, the number of events increased by 58%, while the number of participants increased by 32%.

The training formats most widely used by CERT.LV experts were lectures and seminars – both in terms of the number of events and the size of the audience reached. Practical methods are more difficult to implement for large groups of participants, but they help reinforce the knowledge and skills acquired. Training games, challenges and escape rooms are particularly suitable for specific target groups, such as IT, security, management or business continuity teams.

CERT.LV offers everyone the opportunity to improve their cybersecurity knowledge using **Kibertests.lv**. It is a free platform where users can test their knowledge of the most common cybersecurity risks in a few minutes and receive practical recommendations on how to act more safely in everyday life. **Kibertests.lv** is suitable for both individuals and organisations. Individuals can complete the tests anonymously and receive results immediately, while companies can assess employees' knowledge levels and obtain aggregated results that help plan targeted cybersecurity training.

To register for cybersecurity training and other educational events, CERT.LV invites users to write to **events@cert.lv**. More information on the lectures, training games and events offered is available in the **"Services"** section of the CERT.LV website.

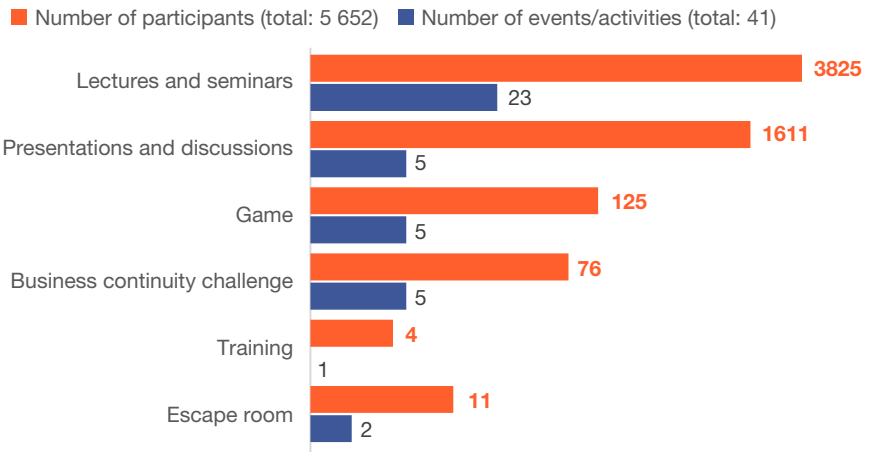


Figure 12. Education formats and audience reached (number; Q3 2026)

At the heart of Cybersecurity Month – the "CyberChess 2026" conference

In October, during European Cybersecurity Month, Riga will bring together the Latvian and international cybersecurity community. The international cybersecurity conference "CyberChess 2026" will take place on 14 and 15 October. Before the conference, the CTF cybersecurity competition will take place on 10-11 October, followed by practical workshops on 13 October. During the reporting period, CERT.LV continued organisational work for these events.

Following an eventful summer, the threat level in Latvian cyberspace remains high. The conference will therefore focus on current cyber threats, practical preparedness and strengthening organisational resilience, while promoting the exchange of experience between the public and private sectors and closer cooperation with international partners.

More information: **cyberchess.lv**. The conference is co-financed by the European Union within the project of the Latvian National Coordination Centre of the European Cybersecurity Competence Centre (C-STRONG-NCC-LV).

4. Overview of the activities of the LIA Safer Internet Centre Reporting Line

From 01.07.2026 to 30.09.2026, the Latvian Internet Association Safer Internet Centre Reporting Line (RL) received and assessed 926 reports. Of these, 332 reports concerned child sexual abuse material; 61 cases involved pornography displayed without an age restriction warning; 27 reports concerned defamation; 3 reports concerned hate speech; and 3 reports concerned violent material. The Reporting Line received 21 reports of attempted financial fraud online; the content of 460 reports was not illegal; and in 19 cases, reporters were advised on how to resolve the issue.

Twenty-eight reports concerning child sexual abuse material hosted on servers in Latvia were forwarded to the State Police. A total of 285 reports concerning child sexual abuse material located outside Latvia were entered into the INHOPE Association database and submitted to the reporting line in the relevant INHOPE country for further action to remove the illegal content from public access.

During the reporting period, of the 28 reports concerning child sexual abuse material hosted in Latvia, the content of 26 reports was removed from public access online, while the content of 2 reports was still in the process of being removed.

Overview of reports received from 01.07.2026 to 30.09.2026

Reports	Jul-26	Aug-26	Sep-26	Q3
Erotic/pornographic content without displayed warnings	24	27	10	61
Paedophilia/prostitution of minors/ child sexual abuse material	103	68	161	332
Violent material	0	1	2	3
Defamation/insult	11	4	12	27
Incitement to hatred/racism	2	0	1	3
Financial fraud	11	6	4	21
Consultations/advice	5	5	9	19
Other	16	57	387	460
TOTAL:	172	168	586	926

Reports sent to the State Police	4	15	9	28
Reports sent to the INHOPE Association	94	43	148	285
TOTAL SENT FOR REVIEW:	98	58	157	313

CERT.LV's mission is to promote cybersecurity in Latvia.

The main tasks of CERT.LV are to maintain and update information on cybersecurity threats, support state institutions in the field of cybersecurity, and provide support to natural and legal persons in resolving cyber incidents involving a Latvian IP address or a .lv domain. CERT.LV also organises informational and educational events for employees of state institutions, IT security professionals and other interested parties.

The report includes publicly available information and does not contain any restricted information. This report is for information only.



Contact CERT.LV:

Phone: +371 67085888

E-mail: cert@cert.lv

Website: www.cert.lv

Follow CERT.LV news on:

@cert.lv

© CERT.LV, 2026
Indicate the source when republishing is required.