CERT.LV
Information Technologies
Security Incident
Response Institution

CERT.LV activities, role in Latvia and globally

Baiba Kaskina, CERT.LV

30.11.2016., Sofia, Bulgaria

CERT.LV Overview

CERT.LV

CERT.LV
Information Technologies
Security Incident
Response Institution

- Information Technology Security Incident Response Institution of the Republic of Latvia
- Operates on basis of IT Security Law
- Overseen by Ministry of Defense
- State funded
- All services are free of charge
- Mission – to improve IT Security in Latvia

IT Security Law

CERT.LV
Information Technologies Security Incident Response Institution

- In force since 1 February 2011
- Established CERT.LV with rights and duties
- Sets duties for:
  - State institutions and local authorities
  - IT Critical Infrastructure
  - Internet Service Providers

IT Security Law – more on that

CERT.LV
Information Technologies Security Incident Response Institution

- **CERT.LV can request disconnect of an end user (up to 24h)**
- **Additional legislation on**
  - **Minimal security requirements for IT systems**
  - **Requirements for ISPs**
  - **Requirements for Critical Infrastructure**

CERT.LV history

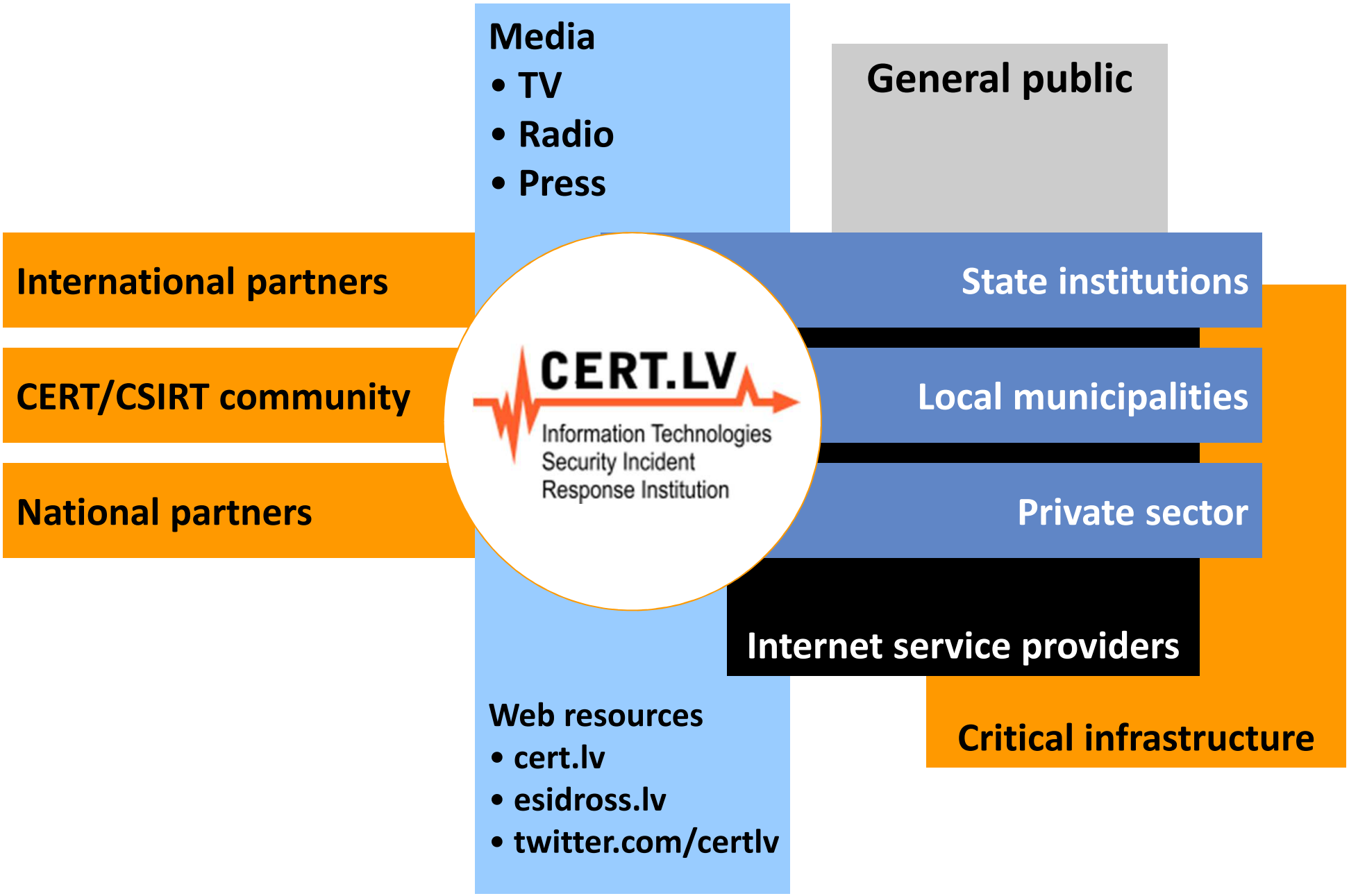
CERT.LV
Information Technologies
Security Incident
Response Institution

- LATNET CERT – established on 1 August 2006
- Since 2008 – CERT NIC.LV
- Since 2008 Accredited @ Trusted Introducer
- Since 2009 FIRST full member
- 2011 – merger of CERT NIC.LV & DDIRV = CERT.LV
- Since 2016 Certified @ Trusted Introducer

CERT.LV organization

CERT.LV
Information Technologies Security Incident Response Institution

Flat structure	• Manager • Deputy manager • One team
Low administrative overhead	• Part of Institute of Mathematics and Computer Science • Centralized procurement, accounting, HR • Short «chain of command» • Easy escalation/ de-escalation process
Technical part	• Incident handling • Monitoring • Testing • Technical exercises
Partner engagement part	• National cooperation • International cooperation • Public relations • Awareness raising


Media
• TV
• Radio
• Press
General public
International partners
CERT/CSIRT community
National partners
CERT.LV
Information Technologies
Security Incident
Response Institution
State institutions
Local municipalities
Private sector
Internet service providers
Critical infrastructure
Web resources
• cert.lv
• esidross.lv
• twitter.com/certlv

CERT.LV timeline

CERT.LV
Information Technologies Security Incident Response Institution

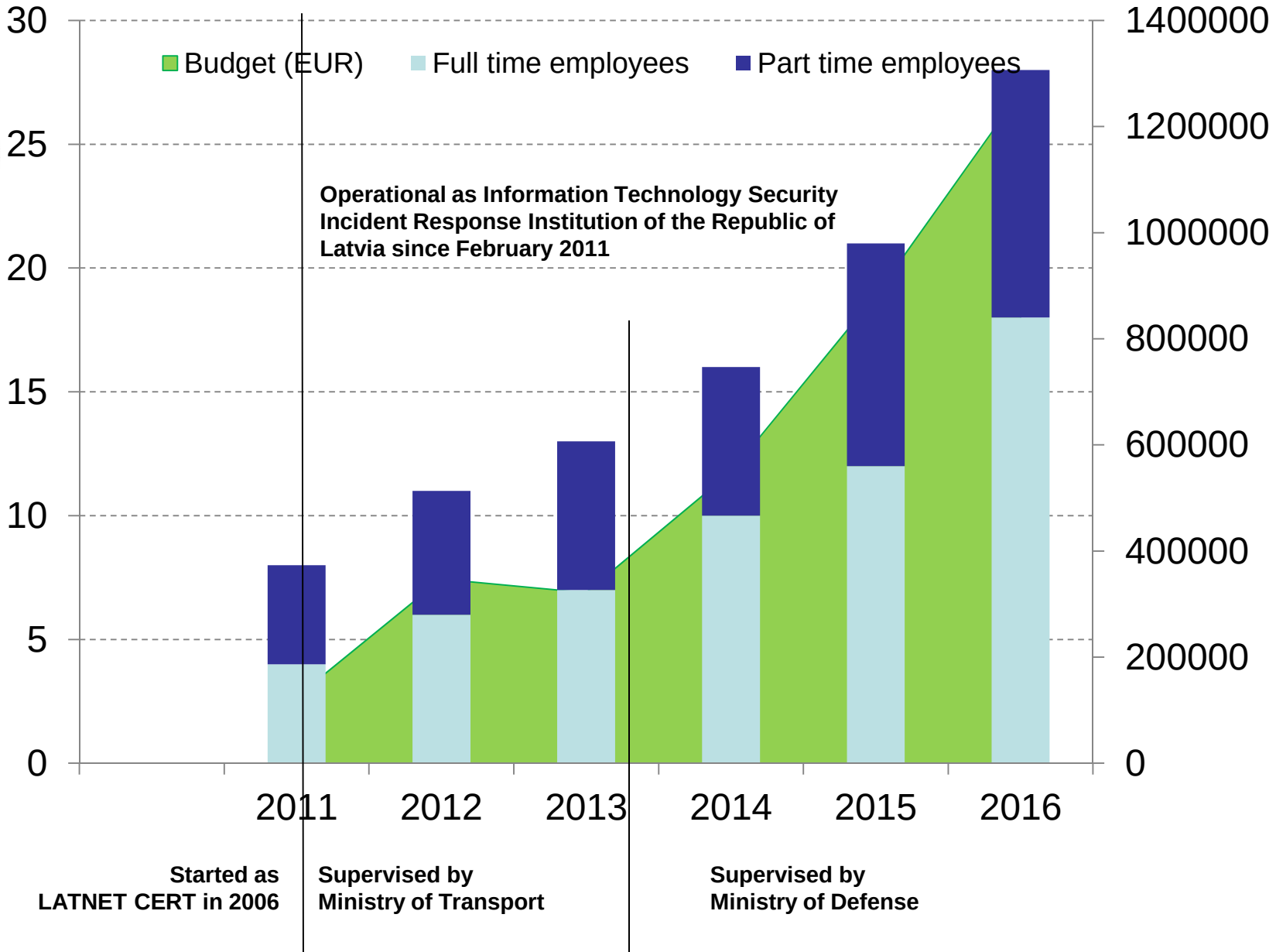
Memberships:

TF-CSIRT Trusted Introducer

Certified team since 1 September 2016

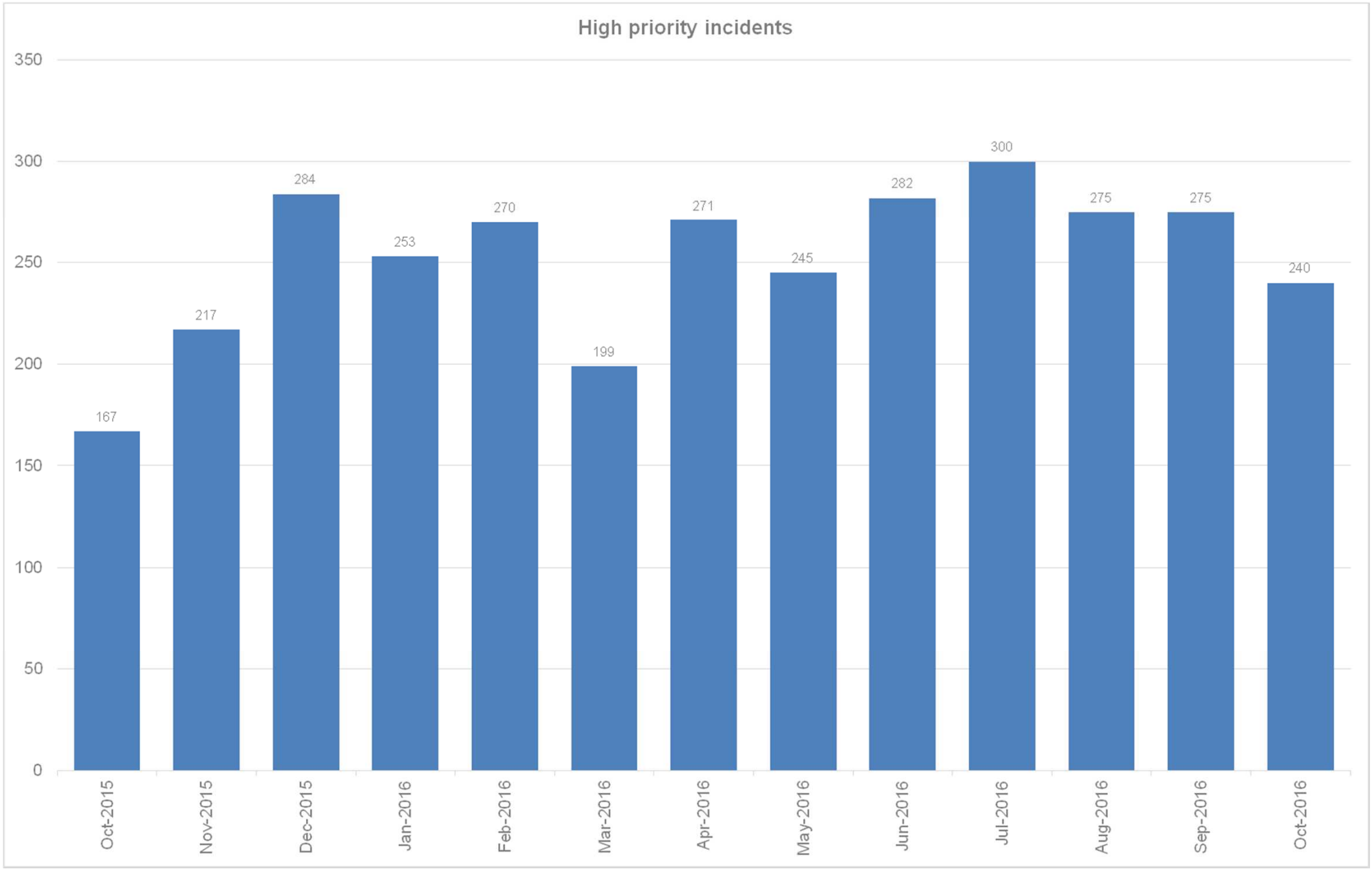
FIRST Improving Security Together

Member since 08 April 2009



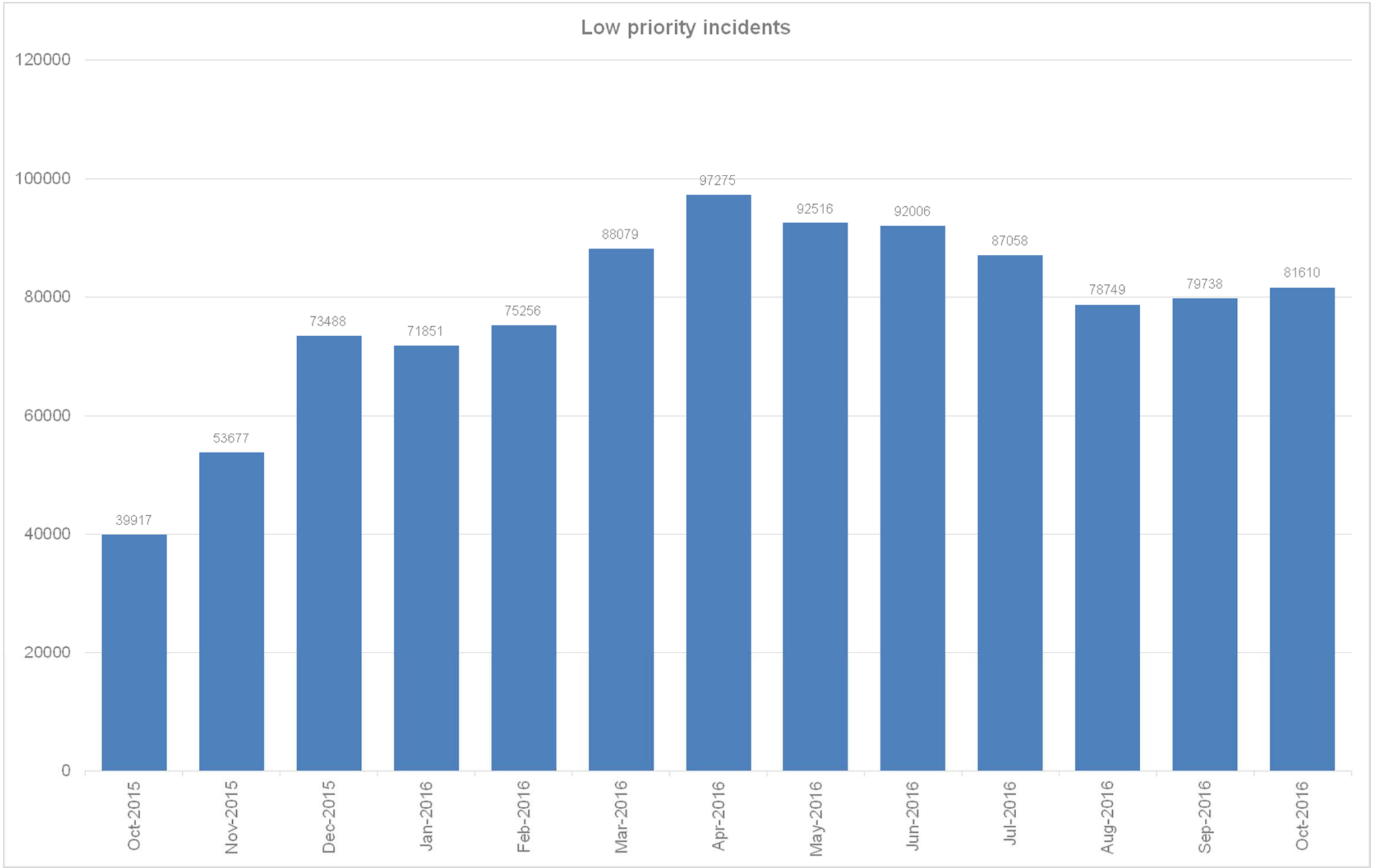
High priority incidents

CERT.LV
Information Technologies Security Incident Response Institution



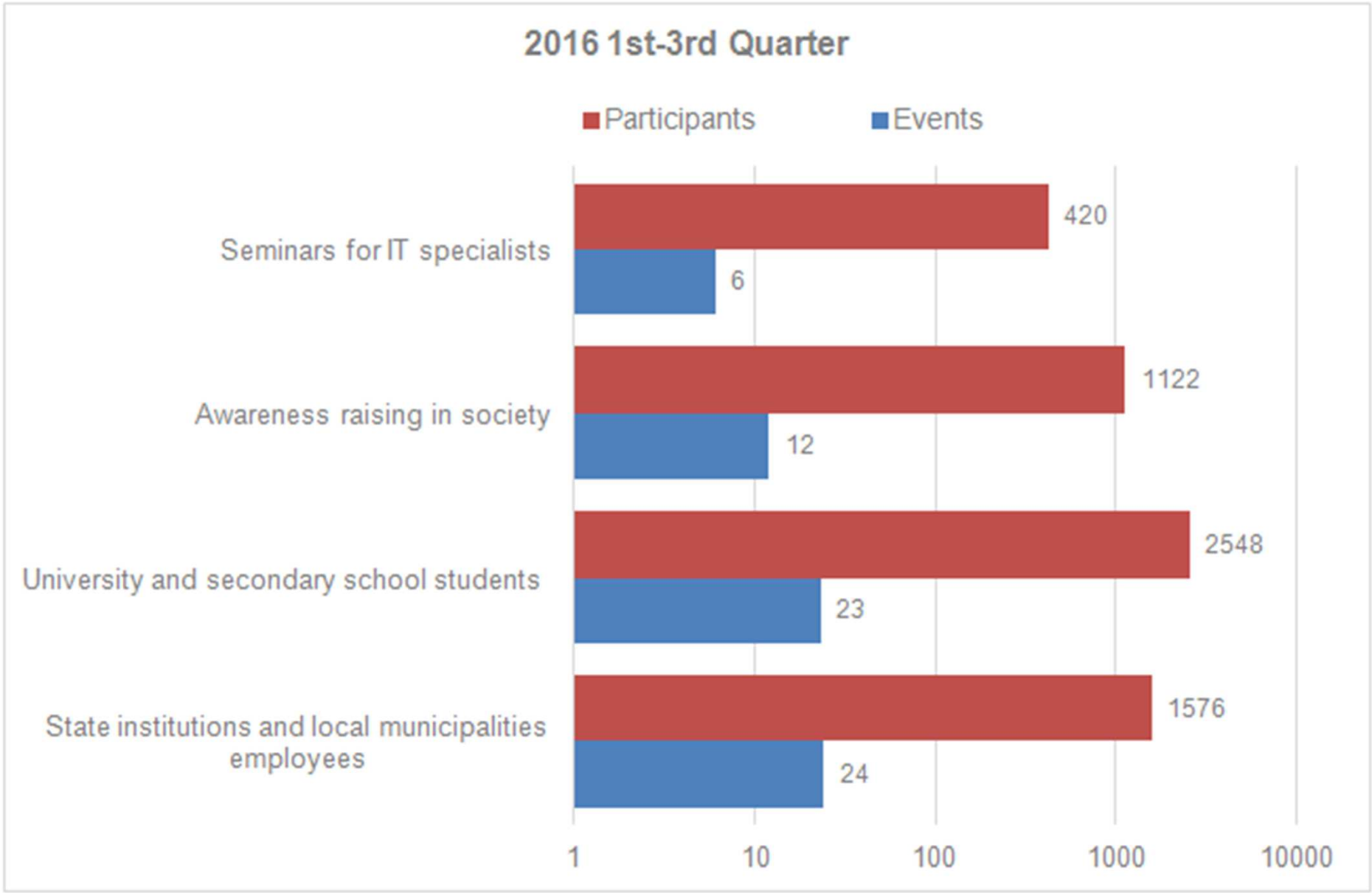
Low priority incidents

CERT.LV
Information Technologies Security Incident Response Institution



Awareness raising

CERT.LV
Information Technologies Security Incident Response Institution



Awareness raising programs

CERT.LV
Information Technologies Security Incident Response Institution

- **5 different presentations (regularly updated)**
  - **Tailored to different audiences**
  - **Available for free**
- **Seminar «ESI DROŠS» – twice a year**
- **Annual conference in cooperation with ISACA Latvia**

Exercises

CERT.LV
Information Technologies Security Incident Response Institution

- CERT.LV regularly participates:
  - Cyber Europe
  - Locked Shields
  - NATO exercises
  - Self organised - "March mist", "Cyber mill"
- International and local
- From table top to Full Live
- Different training audiences
- CERT.LV role – organizer, participant, monitoring

Educational web site esidross.lv

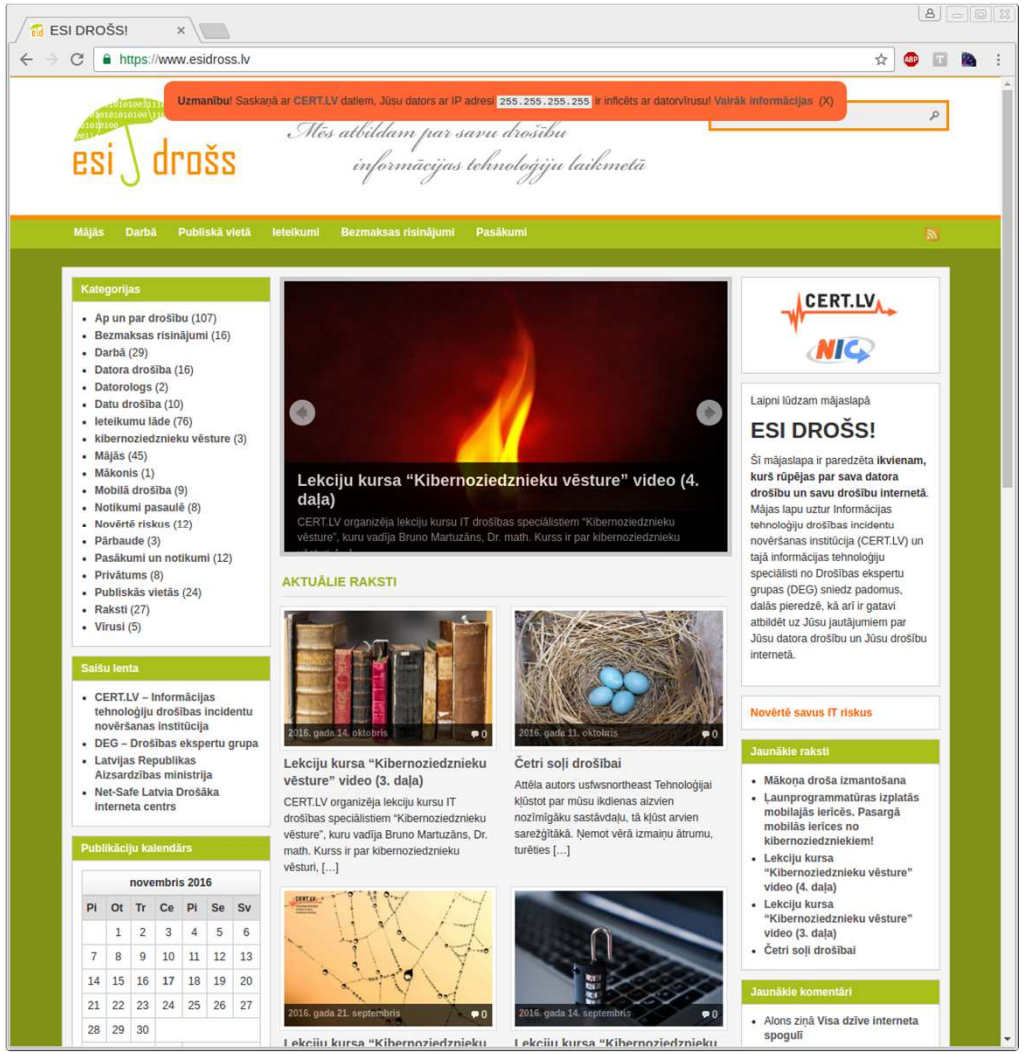
CERT.LV
Information Technologies Security Incident Response Institution

- Information for general public
- Best practices, suggestions
- Information if IP is reported malicious
- Contributors – CERT.LV, security experts
- SANS OUCH!

Educational web site esidross.lv

CERT.LV
Information Technologies Security Incident Response Institution

- Information for general public
- Best practices, suggestions
- Information if IP is reported malicious
- Contributors – CERT.LV, security experts
- SANS OUCH!

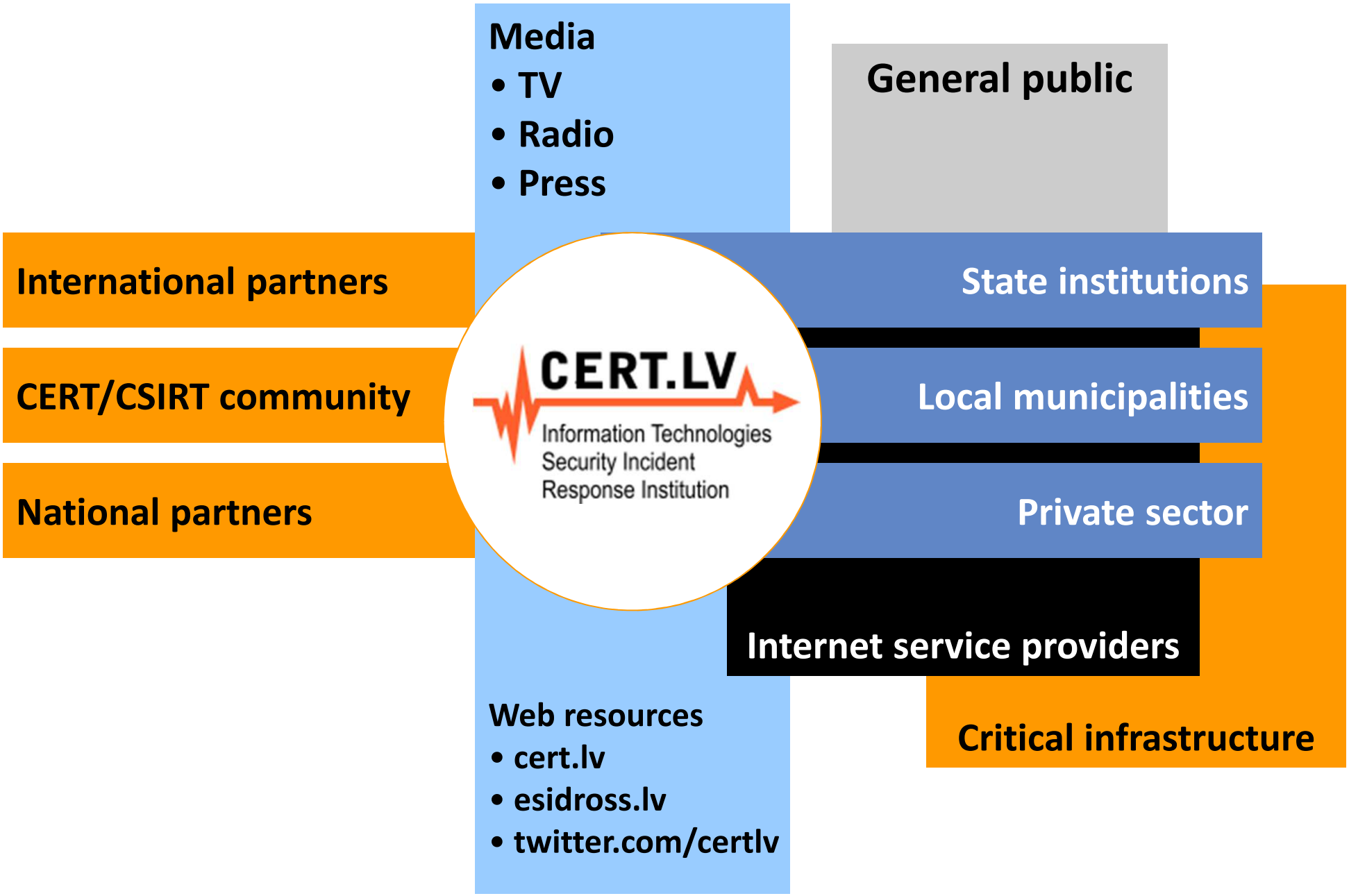


CERT.LV role in Latvia

CERT.LV role in Latvia

CERT.LV
Information Technologies
Security Incident
Response Institution

- **The only state institution with expertise in cyber security**
  - **Involved in many non-CSIRT activities**
  - **Additional tasks**
- **Central role in bringing together all stakeholders**
- **Strong cooperation with Ministry of Defence**


Media
• TV
• Radio
• Press
General public
International partners
CERT/CSIRT community
National partners
CERT.LV
Information Technologies
Security Incident
Response Institution
State institutions
Local municipalities
Private sector
Internet service providers
Critical infrastructure
Web resources
• cert.lv
• esidross.lv
• twitter.com/certlv

Cooperation with public sector & CI

CERT.LV
Information Technologies Security Incident Response Institution

- Defined in the law
- Direct constituency of persons responsible for IT security in their institutions (~ 1200 people)
- Collaboration on incident response, sensor network
- Education & awareness raising
  - Seminars at the institutions
- Support with documentation
- General consultancy

Responsible ISP

CERT.LV
Information Technologies Security Incident Response Institution

- Symbol of quality, received by ISP that:
  - Cooperates with CERT.LV and provides incident information to end users
  - Cooperates with Net-Safe Latvia for illegal material takedown off the Internet
  - Provides free Internet content filter customers request
- Memorandum of Understanding

Security expert group

CERT.LV
Information Technologies
Security Incident
Response Institution

- Group of IT security professionals
- Meetings once a month
- Statutes and code of conduct
- Discussions on current topics
- Presentations/Events

Cyber defence unit

CERT.LV
Information Technologies Security Incident Response Institution

- Established in 2013
- Cyber security centre in 2015
- Unit operational within National Guard
- Main task - to provide support for CERT.LV and National Armed Forces in responding to the IT security incidents and mitigation of the consequences
- Cooperation with CERT.LV – trainings and exercises

Cooperation globally

International cooperation

CERT.LV
Information Technologies Security Incident Response Institution

- CSIRTs community (FIRST, TF-CSIRT)
- ENISA, EU
- NATO
- FI-ISAC (Financial Institutes - Information Sharing and Analysis Centre)
- Bilateral cooperation, MoUs

European CSIRT community

CERT.LV
Information Technologies Security Incident Response Institution

- **TF-CSIRT community – all inclusive**
- **Trusted Introducer community – listed (278), accredited (142) and certified teams (19)**
- **European Government CERT group – limited**
- **NIS directive CSIRT cooperation group**

Certification

CERT.LV
Information Technologies
Security Incident
Response Institution

- **TF-CSIRT Trusted Introducer service**
- **Evaluation of CSIRT based on SIM3 model**
- **Looks at**
  - Organisation parameters
  - Human parameters
  - Tools parameters
  - Processes parameters

Reasons

CERT.LV
Information Technologies
Security Incident
Response Institution

- International recognition
- Outside look
- Team inventory
- Process update and improvement
- Way to increase teams' maturity

Thank you!

https://www.cert.lv/

baiba.kaskina@cert.lv