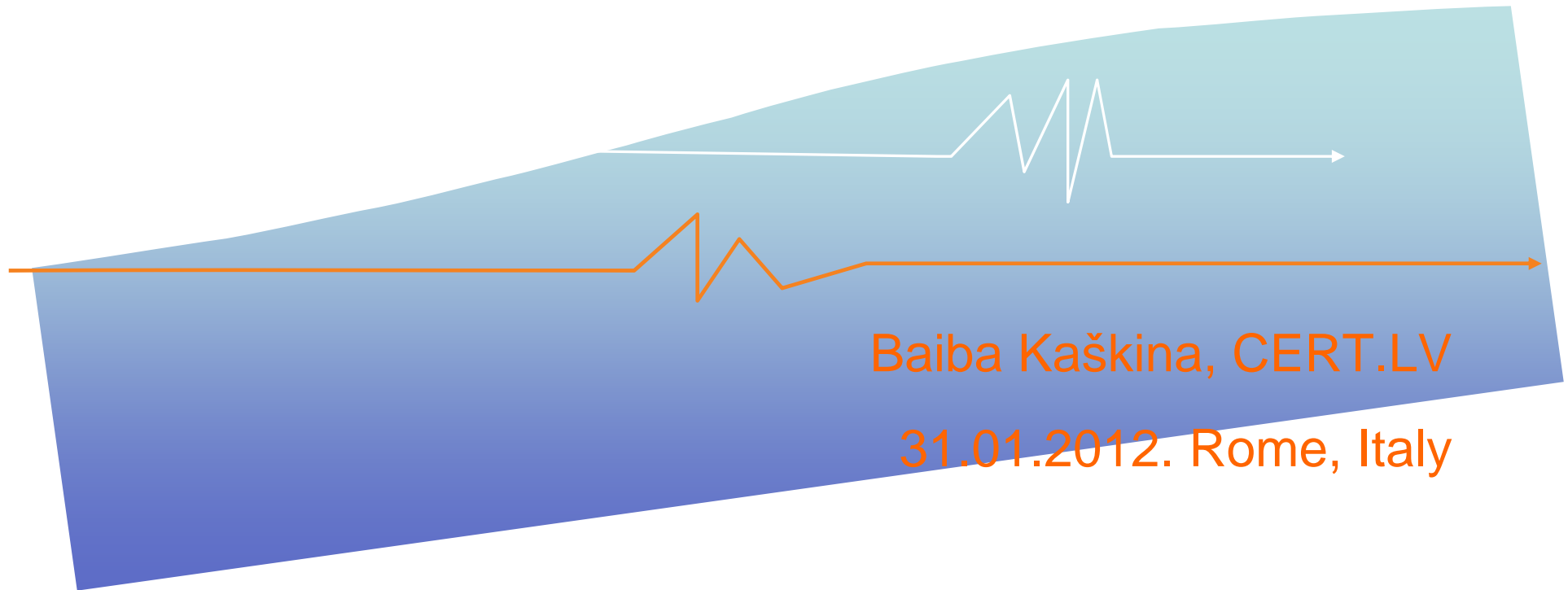


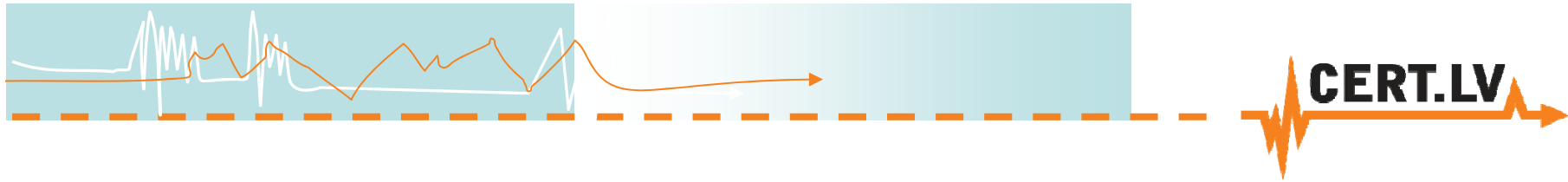


***Dealing with the whole country:
creating a National CSIRT***



Baiba Kaškina, CERT.LV

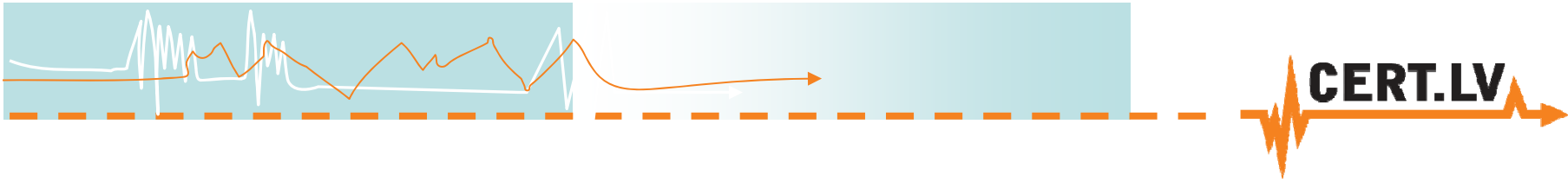
31.01.2012. Rome, Italy



Outline

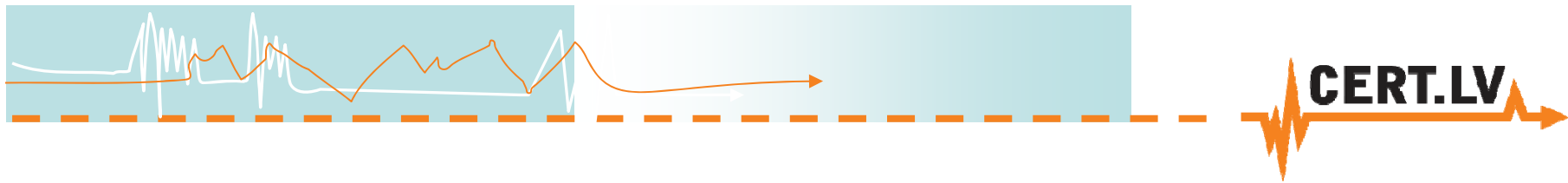
- Short history & IT Security law
- First year results
- How to deal with the whole country
- Future plans





Short history & IT Security law

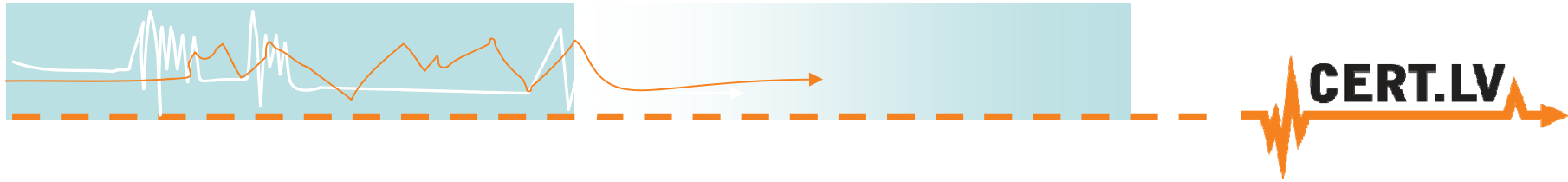




CERT.LV

- Operational since 1 February 2011
- Operates on the basis of IT Security Law
- Tasks delegated to Institute of Mathematics and Computer Science, University of Latvia
- Merged CERT NIC.LV + DDIRV
- State funded
- Year 2011 - 10 people, 5 FTE

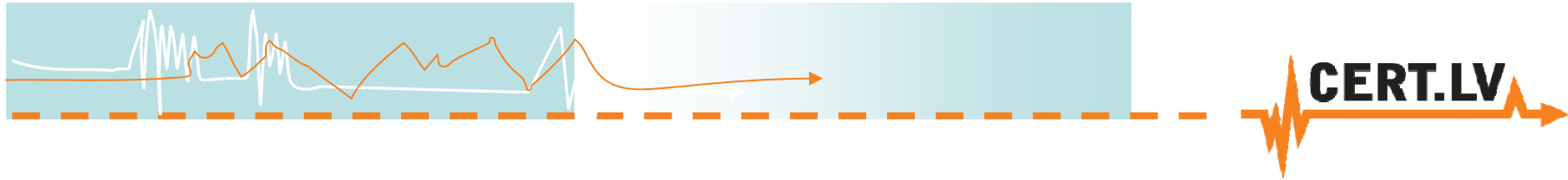




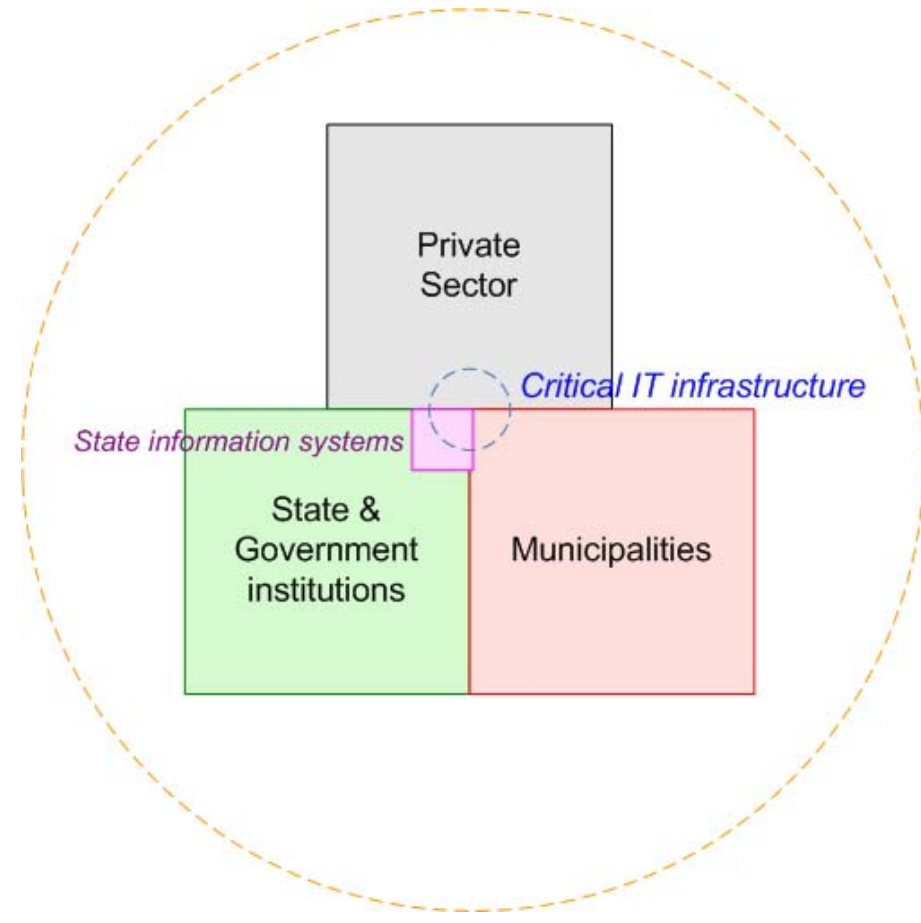
CERT.LV

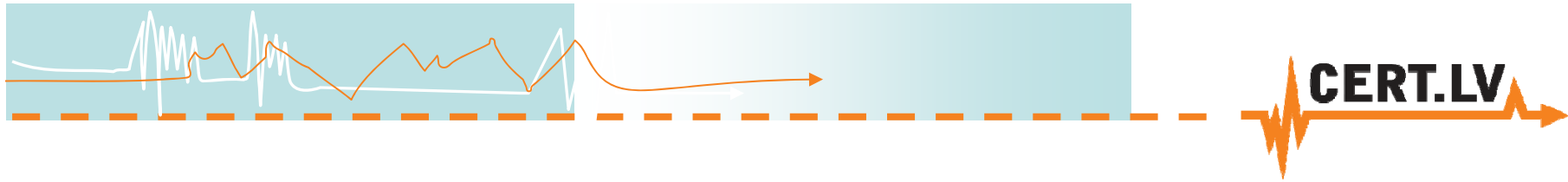
- Experience in security incident handling since 2006 (LATNET CERT, CERT NIC.LV)
- Full member of FIRST since 2009
- Accredited by Trusted Introducer since 2007





CERT.LV Constituency

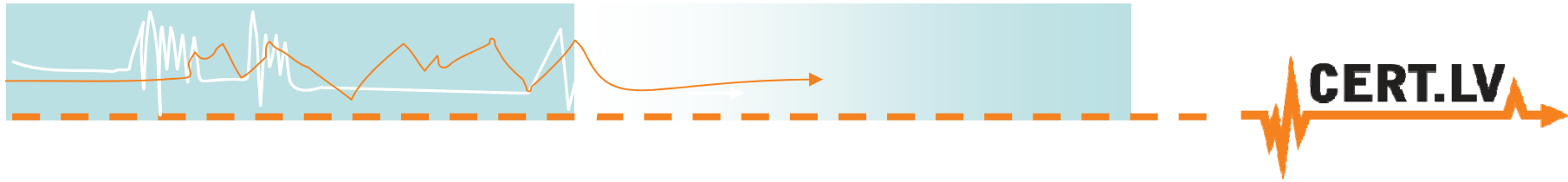




IT Security law

- In force since 1 February 2011
- Implemented in 2011
- Sets CERT.LV tasks and responsibilities
- Sets responsibilities for:
 - Public sector
 - ISPs
 - Critical IT infrastructure owners

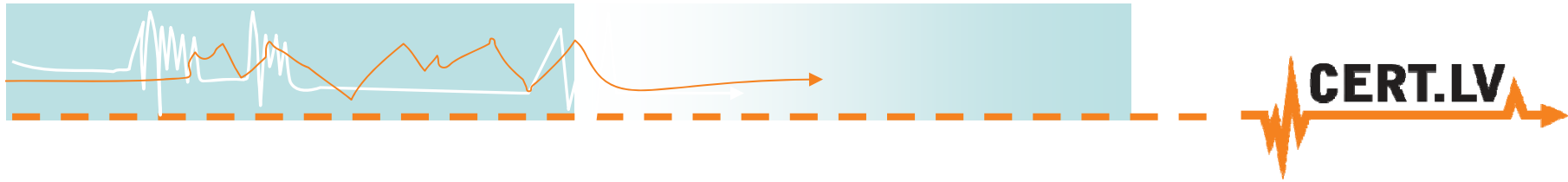




IT Security law – Public sector

- In every institution – responsible person for IT security, his/her tasks:
 - To establish IT security documents for institution
 - To organise IT security audits
 - To educate at least once per year all employees
 - To report CERT.LV security incidents
 - To participate in CERT.LV seminars

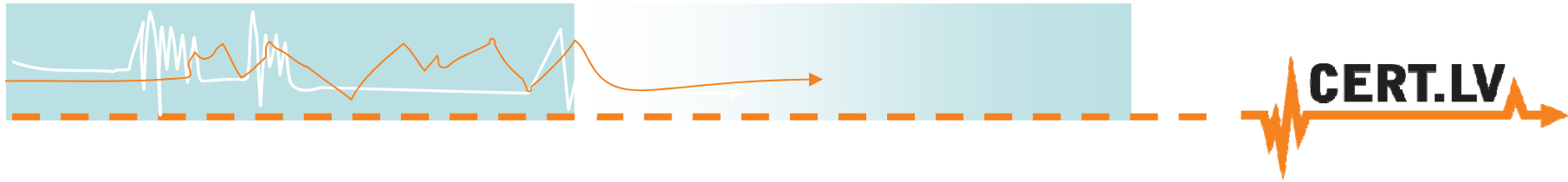




IT Security law - ISPs

- All ISPs have to submit to CERT.LV
“Action plan for continuous operations”
- Report to CERT.LV major incidents
- CERT.LV can request
 - IT Security documentation
 - IT Security audits
 - Disconnect of an end user

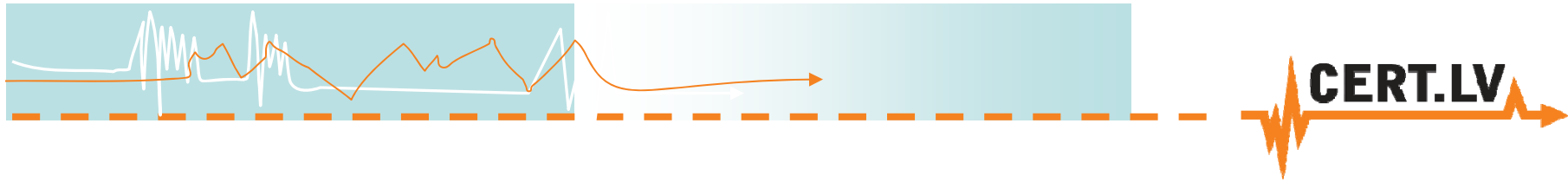




IT Security law - disconnect

- CERT.LV can request disconnect of an end user
- To up to 24 hours
- If threatens rights of other users, their IS or security of networks
- Reasoning needs to be provided
- Documentation in place, never implemented

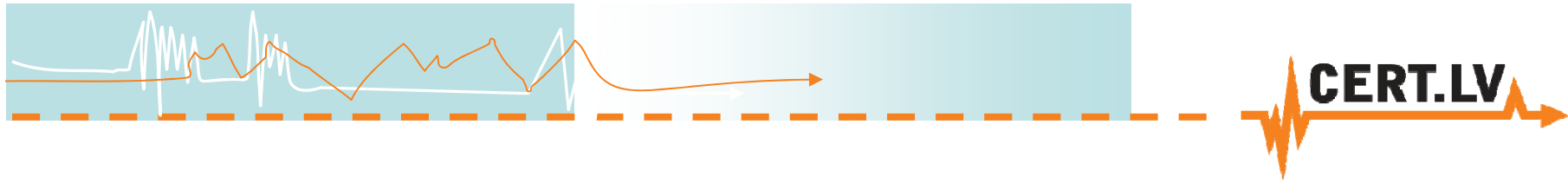




IT Security law – Critical infrastructure

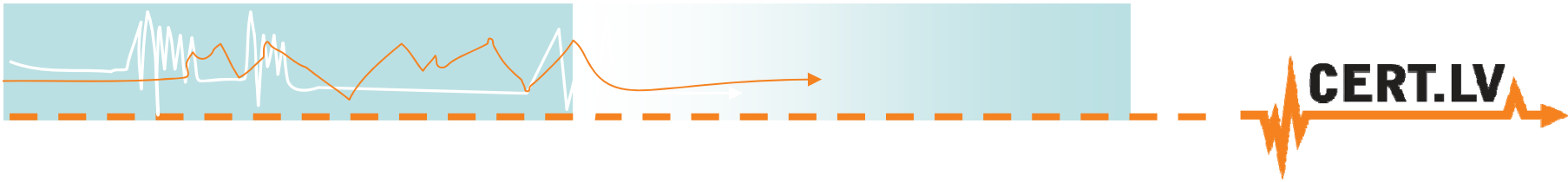
- List – State secret
- Report incidents to CERT.LV
- Establishes IT Security documentation
- CERT.LV can do pentesting





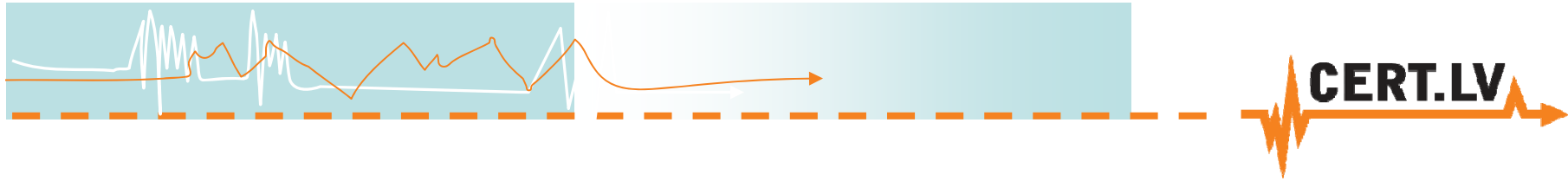
First year results





Monitoring of Latvian IT space and incident response

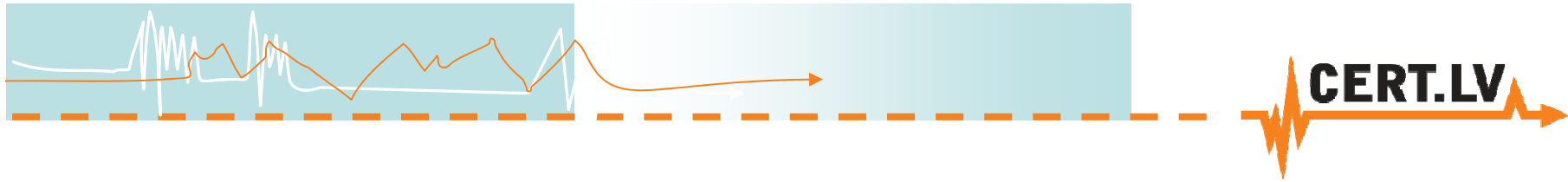




Situation in Latvia

- Overview of infected IPs in Latvia – on 31.12.2011. 3300 infections (bots)
- Different information sources
- Only part of infections become incidents in tracking system
- Cooperation with ISPs

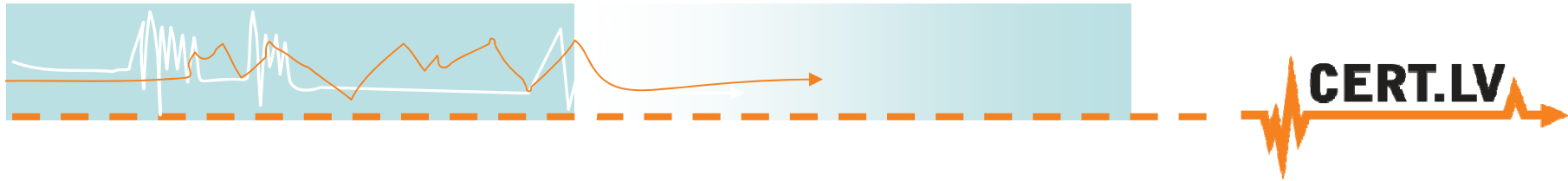




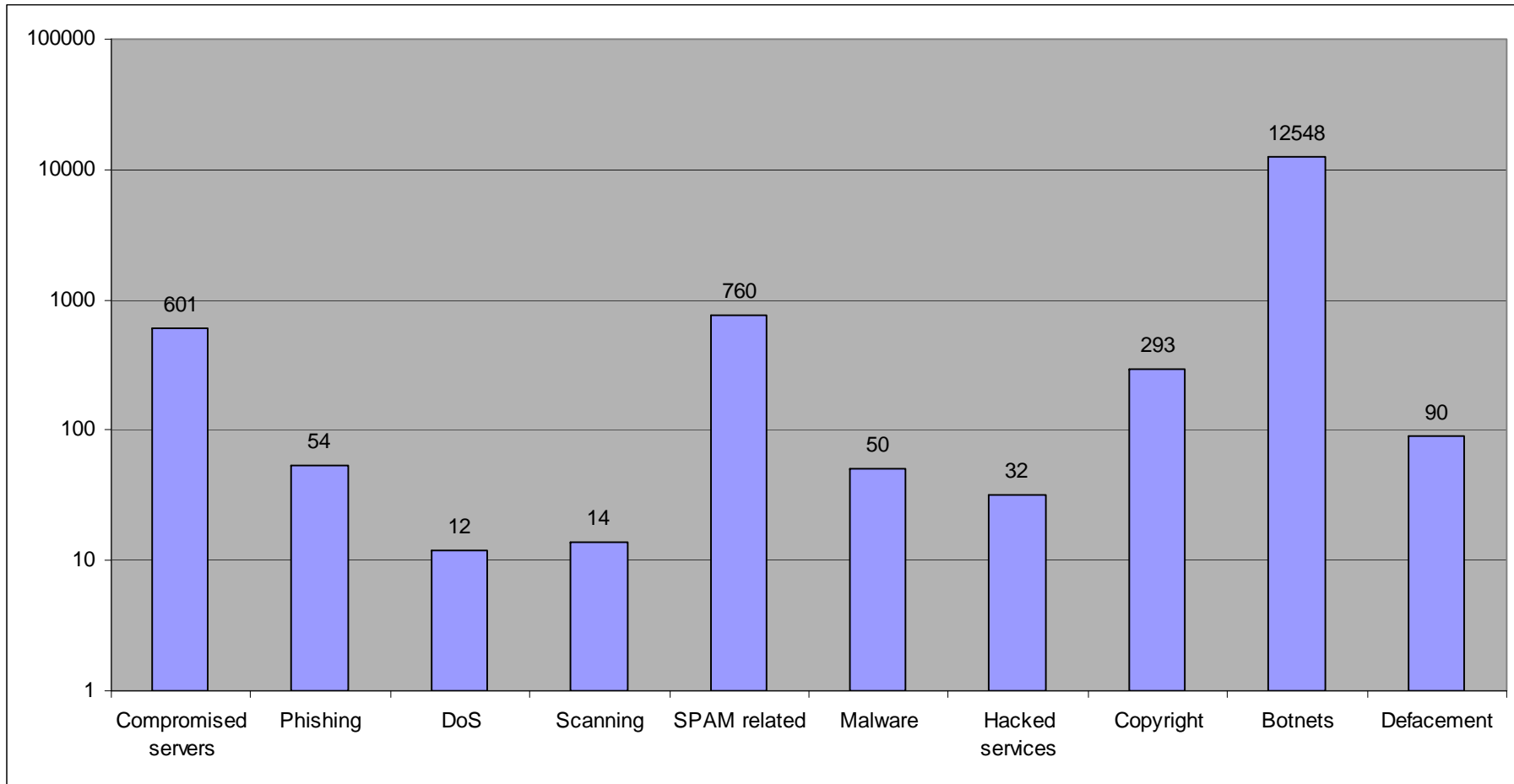
Incident response

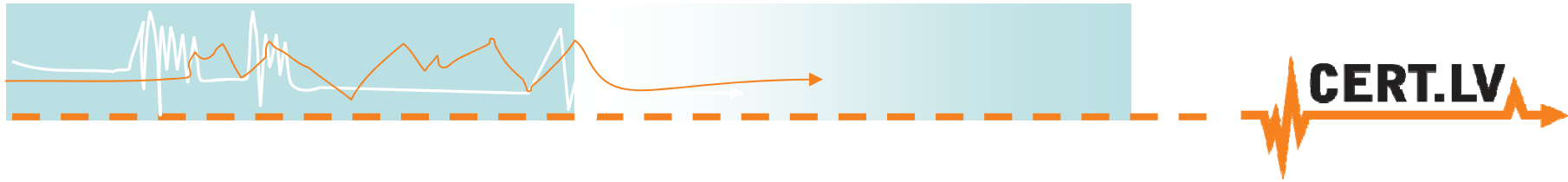
- Dealt with almost 15000 incidents
- More incidents reported by individuals
- More frequently report those who already have had a good collaboration experience with CERT.LV





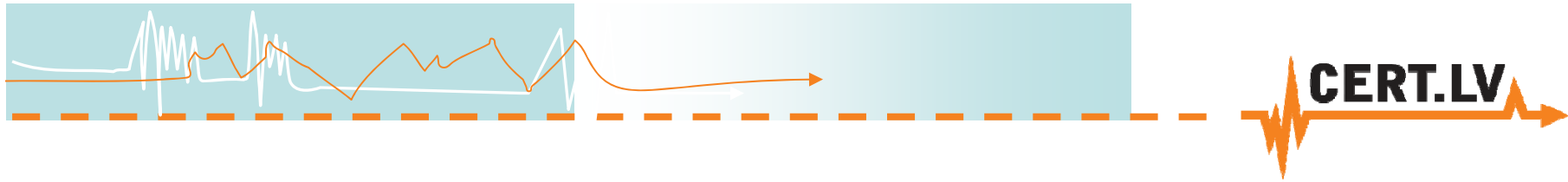
CERT.LV incident statistics





Awareness raising, education,
exercise organization,
recommendations





Information, recommendations

- Website, information on newest viruses and threats
- Articles, suggestions
- Examples for IT security principles and rules
- Portal www.esidross.lv (“be safe”)
- Twitter account “certlv”



Tēmas

- Ap un par drošību (10)
- Darbā (10)
- Ietīstori tīkla (12)
- Mājās (10)
- Notikumi pasākumi (1)
- Pasākumi un notikumi (1)
- Publiskā vietā (11)

Saistīta tēma

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Satiksmes ministrija
- LV CSIRT iniciatīva
- Net-Safe Latvia Drošība Internetā centrs

Publiskā vietā kalendārs

novembris 2011						
P	D	T	C	P	S	Sv
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				
» Okt						

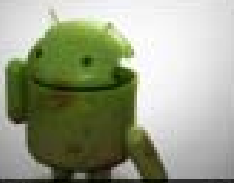
Aktuāli



Android – augošās popularitātes tumšās puses

Moderne dzīve atstāj tik strauj, ka ne visi ir spējīgi un ierastuši tai izkopt. Bet tā tā kā ir tādas, kas...

AKTUĀLIE RAKSTI



2011. gada 8. novembris

Android – augošās popularitātes tumšās puses

Moderne dzīve atstāj tik strauj, ka ne visi ir spējīgi un ierastuši tai izkopt. Bet tā tā kā ir tādas, kas...



2011. gada 24. oktobris

Paroju pārvaldnieki

Mūsu šķērsā arvien pasugrā loma ir dažādām parolēm un kodiem, kuri ir jāatceras, lai piekļūtu dažādām sistēmām – e-pastam, internetā...



Lapri Ķīzān mājlapā

ESI DROŠI!

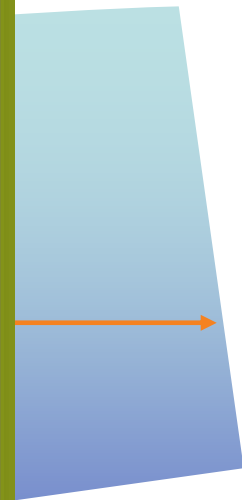
Šī mājlapa ir paredzēta lietotājam, kuri rūpējas par savu darbu drošību un savu drošību internetā.

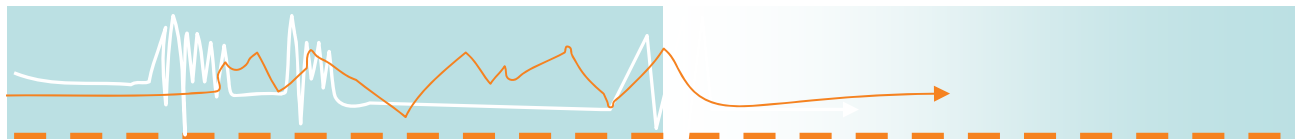
Mīļie lasi uzta informācija tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) un tāsi informācijas tehnoloģiju speciālisti no LV-CSIRT iniciatīvas grupas sniegt padomus, dalās pieredzi, kā arī ir gatavi atbildēt uz Jūsu jautājumiem par Jūsu darbu drošību un Jūsu drošību internetā.

Jautājuma raksti

- Android – augošās popularitātes tumšās puses
- Paroju pārvaldnieki
- Kas ir SQL injekcijas?
- Kas ir XSS uzbrukumi?
- Tīmekļa vietnes drošība un tās izpildītāja tās drošības apdraudējumi

Jautājuma kalendārs





*Mēs atbildam par savu drošību
informācijas tehnoloģiju laikmetā*



Mājās Darbā Publiskās vietās Ieteikumi Pasākumi Notikumi pasaulē Par drošību Raksti



Tēmas

- Ap un par drošību (5)
- Darbā (7)
- Ieteikumu lāde (9)
- Mājās (15)
- Notikumi pasaulē (1)
- Pasākumi un notikumi (1)
- Publiskās vietās (7)

Saišu lenta

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Satiksmes ministrija



VIDEO: Kā justies droši elektroniskā vidē?

Jūties droši elektroniskā vidē from EsiDrossLV on Vimeo. CERT.LV piedāvā jums noskatīties Latvijas Universitātes Informācijas sistēmu drošības pasniedzējas Ilzes Murānes...

Uzmanību! Saskaņā ar CERT.LV datiem, Jūsu dators ar IP adresi [redacted] ir inficēts ar datorvīrusu! [Vairāk informācijas.](#)

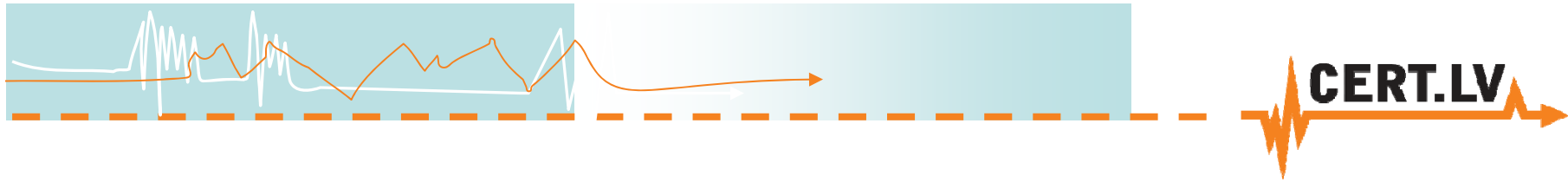


Laipni lūdzam mājaslapā

ESI DROŠS!

Šī mājaslapa ir paredzēta ikvienam, kurš rūpējas par sava datora drošību un savu drošību internetā.

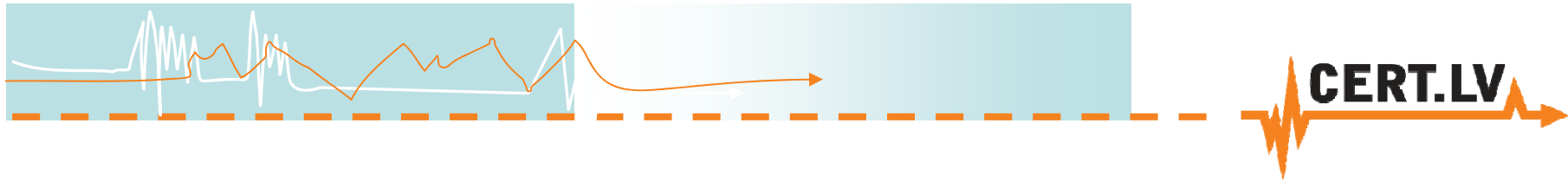




Events, presentations

- “Be safe -1” and “Be safe-2” seminars for state institutions
- IT Security exercises
 - Theoretical
 - Technical
- Seminar for Internet Service providers
- Targeted events
 - Legal issues
 - How to organize exercises
- Participation in World Wide Safer Internet day

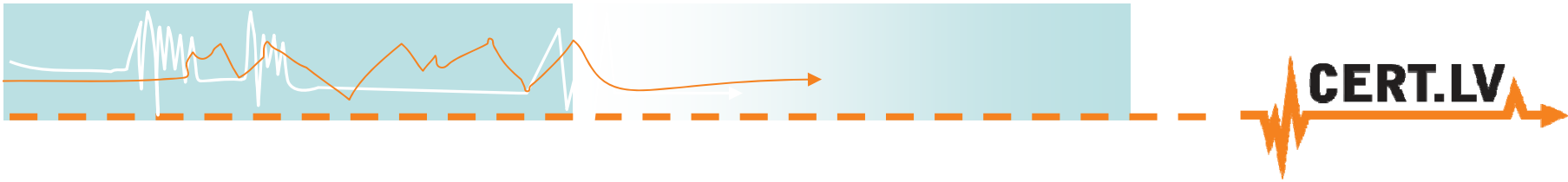




Contacts

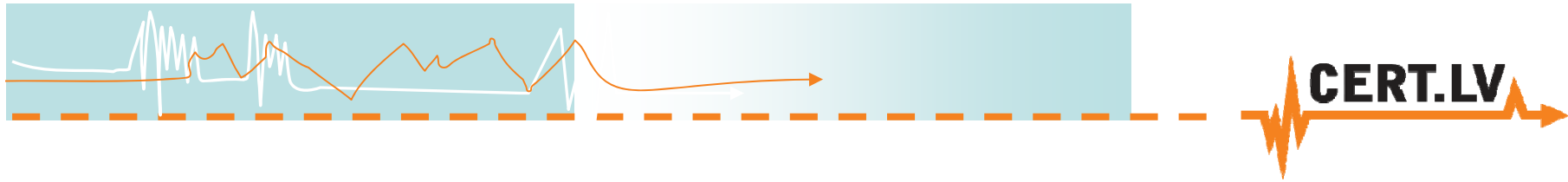
- Responsible persons for ~400 institutions
- Actions plans for ~30 ISP (out of ~400)
- > 500 people participated in CERT.LV events





How to deal with the whole country

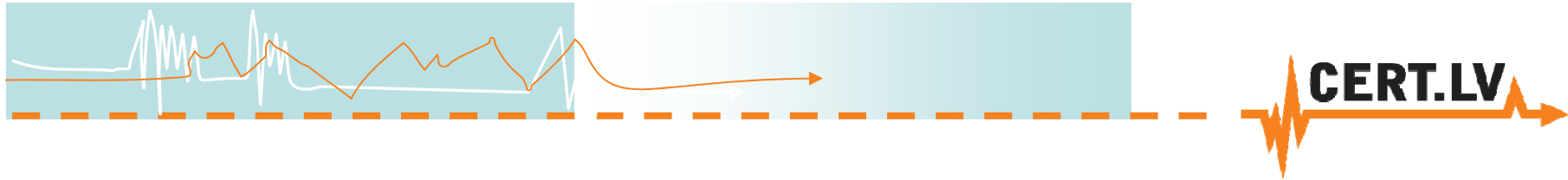




We need automation

- Collaboration with ISPs
- Abuse Helper
- To separate incidents in two groups
 - Serious ones – processed by hand
 - Mass infections - processed automatically

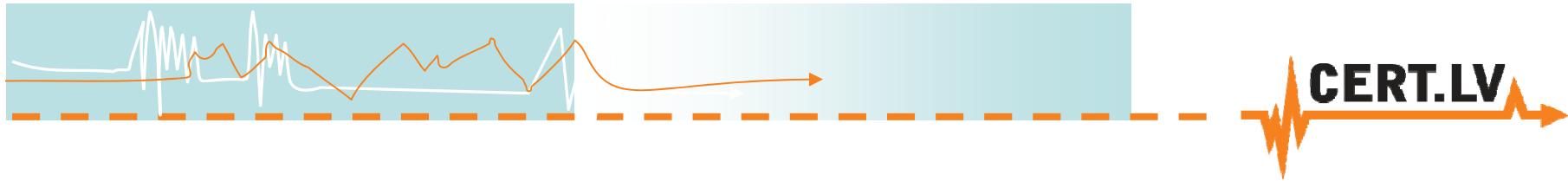




Not all are equal 😊

- Which customers are more important?
- What should be processed by hand?

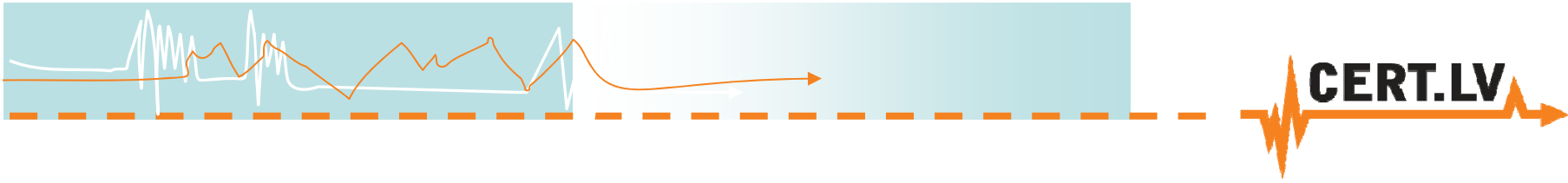




Incident processing – the goal

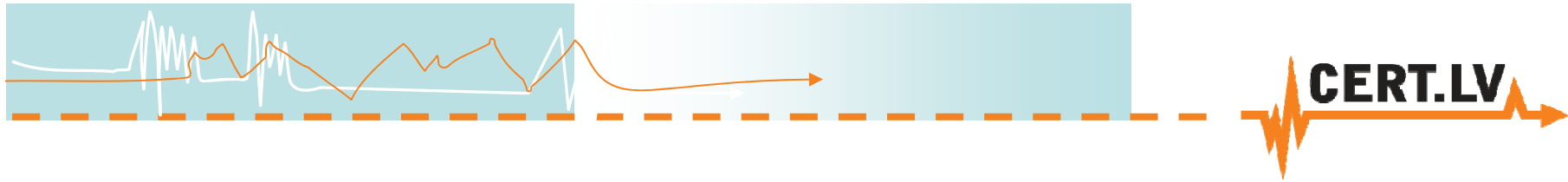
- Manual processing
 - All high priority institutions
 - All human submitted incident reports
 - Legacy – SigmaNet and Latnet incidents
- Automatic processing
 - All automated reports (via Abuse Helper)
 - Daily reports to ISPs





Future plans

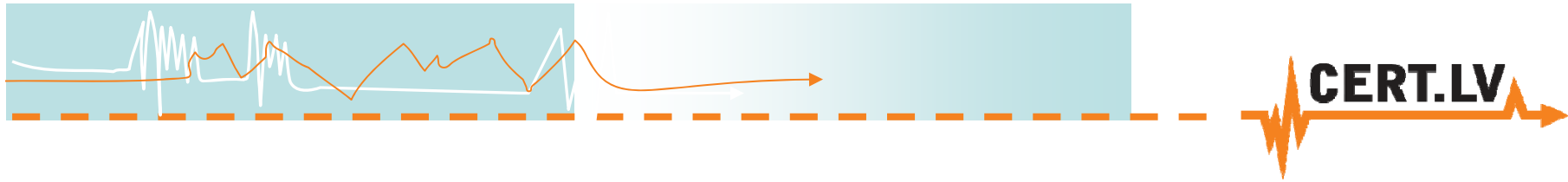




Great changes

- 2,5 times more money from 1 March 2012
- Increase staff to 10 FTE
- New incident classification, more automation
- Ability to participate in more exercises, events, etc.
- Establishment of IT Security Guards
- More PR and awareness raising activities

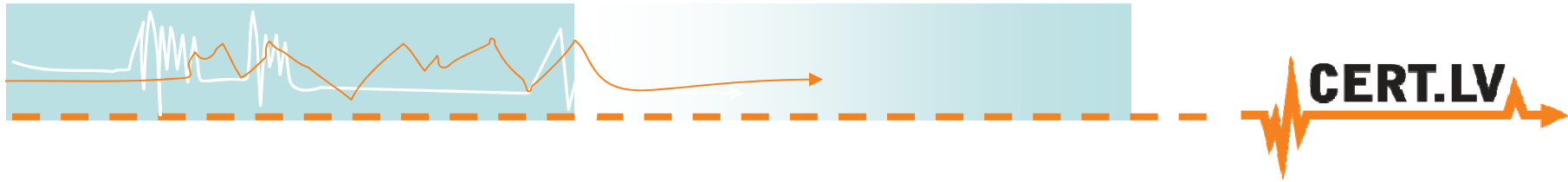




Summary

- All parts of IT Security law are in place
- Established contacts with all parts of constituency
- People report more incidents
- Gaining political attention
- Need for incident response automation
- Growing responsibility





Thank you!!!

<http://www.cert.lv/>
cert@cert.lv
baiba.kaskina@cert.lv

