LUXEMBOURG'S CYBERSECURITY ECOSYSTEM

THREAT LANDSCAPE

Statistics 2014

80 000

events

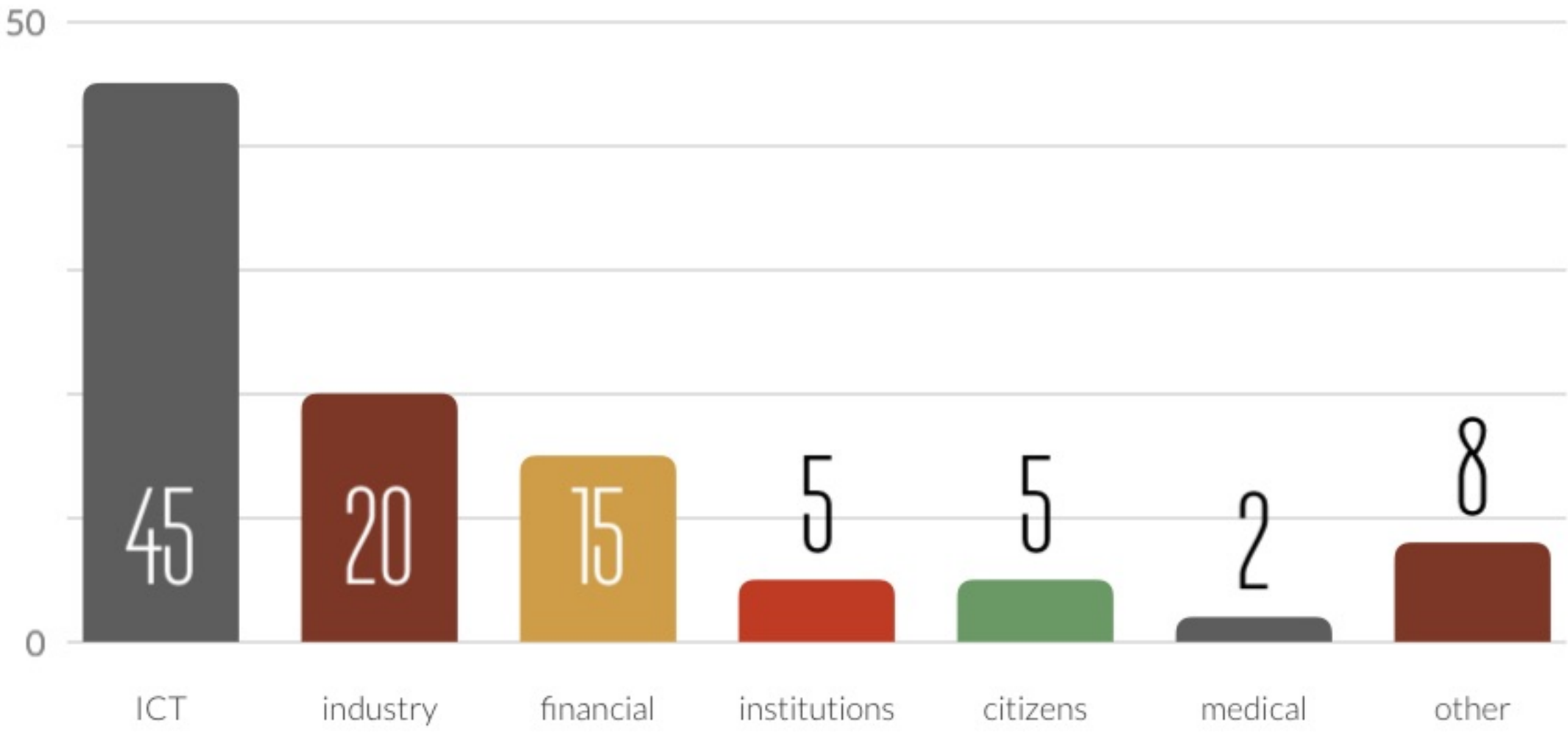
3 000

technical investigations

3

times more then in 2013

BY SECTOR (%)


50
0
45
20
15
5
5
2
8
ICT
industry
financial
institutions
citizens
medical
other

MOTIVATIONS

1	CYBER CRIME	50%
2	CYBER ESPIONNAGE	40%
3	CYBER ACTIVISM	10%

CASES EXAMPLES

BASED ON REAL INCIDENTS IN LUXEMBOURG

BANKING FRAUD

- using malware or phishing to access mailboxes
- banking details are replaced
- also combined with social engineering (via a phone)
- extreme cases: dedicated malware targeting corporate banking systems
- targets: mainly huge invoice processing organisations

RANSOMWARE

- recent ransomware (like CTB-Locker) also encrypts removal drives and shares
- BYOD increased cases
- 50% of LU victims had a non-functionnal/incomplete backup

VOIP/PBX ATTACKS

- scan for vulnerable PBX interfaces or VoIP servers
- such systems are often outsourced or outside security scope
- direct financial benefit by toll fraud

TARGETED ATTACKS (APT)

- avoid attribution
- stay stealthy, hide in the crowd (abuse browsers, byod, set-top boxes)
- exfiltrate data/information (via legite cloud provider)

CYBERSECURITY ECOSYSTEM

ECOSYSTEM

- multidisciplinarity
- collaboration
- competition
- self-organising networks
- scalability
- sustainability
- common public private effort

NATIONAL STRATEGY

- Cyber security goes beyond ICT
- Cyber security represents an economic opportunity
- Democratisation, creating synergies & governance
- Reduction/harmonisation of compliance costs
- Risk governance based approach
- Cyber Security as Infrastructure

ACTORS

- Cyber Security Board
- Authorities/Regulators (sectoral)
- Public prosecutor & Police forcesOperational Entities (CERTs)
- (Critical) Infrastructure Providers
- Operational Entities (CERTs)
- Awareness & Informations sources
- YOU !

DON'T BE THE WEAKEST LINK

NOR SUFFER IN SILENCE

JOIN THE EFFORT

cases.lu

Secure. Innovate. Lead.

START-UP
SECURITY KIT

PROTECT YOUR DATA
SECURE YOUR HARDWARE
ADJUST YOUR BEHAVIOUR

START

Get a head start in terms of security. Avoid the most common traps and

FIT

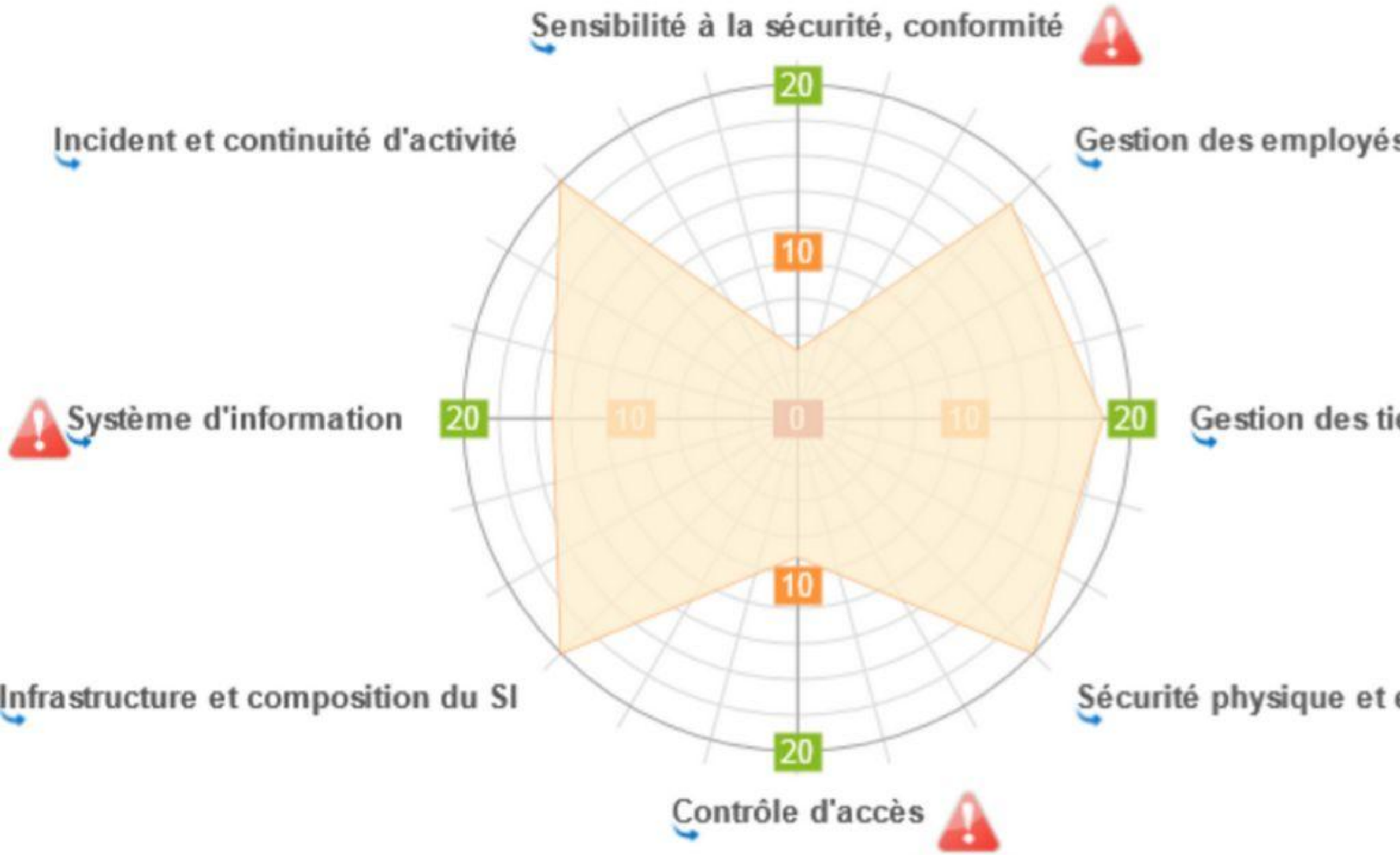
Reinforce your defences. Organise your security. Develop your resilience.

TOP

Adopt the best protection techniques. Monitor your information systems.

customised
check-up:
CASES
DIAGNOSTIC

Ma situation



cert.lu

Cyber Emergency Response Community Luxembourg

Home About Members

Stronger Together!

An initiative to enhance the collaboration between public and private CERTs in Luxembourg.

4 public CERTs

5 private CERTs

1 more to join soon

circl.lu

Detect. React. Innovate.

MAP.CIRCL.LU

```
New event targeting IP addresses in Luxembourg from Jiaxing,China (source: blackhole)
New event targeting IP addresses in Luxembourg from Cambridge,United Kingdom (source: blackhole)
New event targeting IP addresses in Luxembourg from Beijing,China (source: blackhole)
New event targeting IP addresses in Luxembourg from Shanghai,China (source: blackhole)
New event targeting IP addresses in Luxembourg from Englewood,USA (source: blackhole)
New event targeting IP addresses in Luxembourg from Fremont,USA (source: blackhole)
New event targeting IP addresses in Luxembourg from Hefei,China (source: blackhole)
New event targeting IP addresses in Luxembourg from USA (source: blackhole)
New event targeting IP addresses in Luxembourg from Bursa,Turkey (source: blackhole)
New event targeting IP addresses in Luxembourg from Switzerland (source: blackhole)
New event targeting IP addresses in Luxembourg from Chuncheon,South Korea (source: blackhole)
New event targeting IP addresses in Luxembourg from Sun City,USA (source: blackhole)
New event targeting IP addresses in Luxembourg from Silver Spring,USA (source: blackhole)
New event targeting IP addresses in Luxembourg from Beijing,China (source: blackhole)
New event targeting IP addresses in Luxembourg from San Jose,USA (source: blackhole)
```

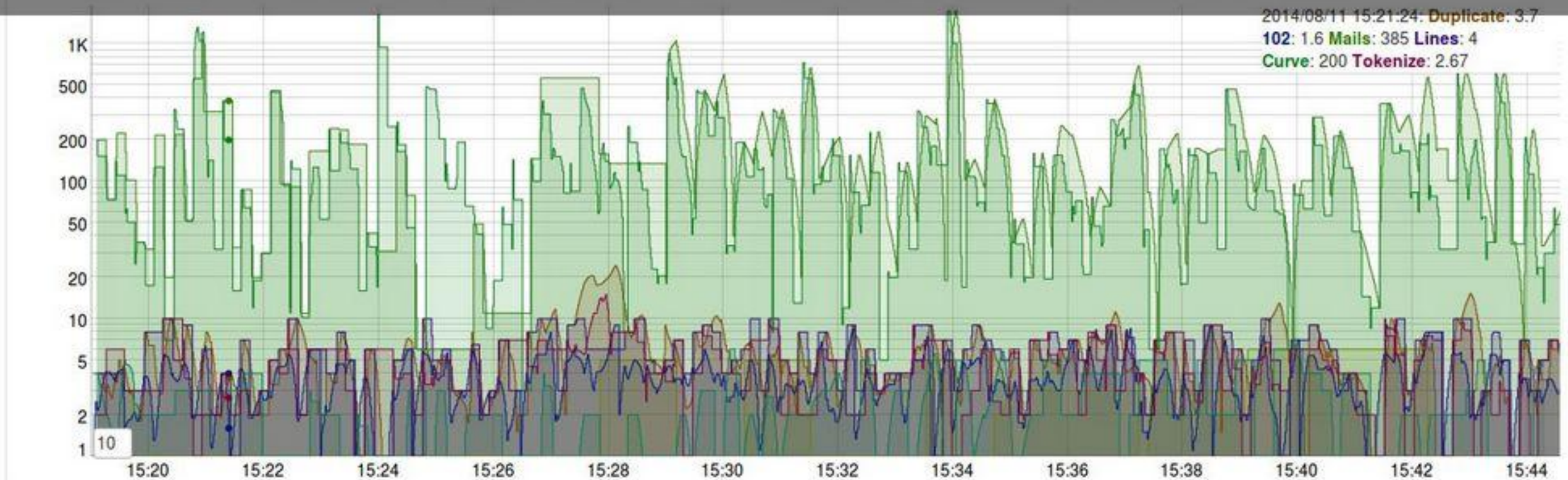
CIRCL
Computer Incident
Response Center
Luxembourg

Partners hosting a CIRCL sensor

verizon

P&T LUXEMBOURG

AIL - ANALYSIS OF INFORMATION LEAKS



Logs

10 INFO WARNING CRITICAL

Channel	Level	Script Name	Source	Date	Paste name	Message
Script	INFO	Categ	pastebin.com	20140811	T5qu3ub1.gz	Detected 1 http
Script	INFO	Categ	pastebin.com	20140811	qmjgEhWm.gz	Detected 9 http
Script	INFO	Url	pastebin.com	20140811	T5qu3ub1.gz	3 Valid url detected
Script	INFO	Categ	pastebin.com	20140811	vULV0yjM.gz	Detected 2 https
Script	INFO	Categ	pastebin.com	20140811	vULV0yjM.gz	Detected 1 http
Script	INFO	Categ	pastebin.com	20140811	8qEgyXvH.gz	Detected 1 http
Script	INFO	Categ	pastebin.com	20140811	8qEgyXvH.gz	Detected 1 password
Script	INFO	Url	pastebin.com	20140811	qmjgEhWm.gz	9 Valid url detected
Script	INFO	Url	pastebin.com	20140811	vULV0yjM.gz	3 Valid url detected
Script	INFO	Url	pastebin.com	20140811	8qEgyXvH.gz	1 Valid url detected

SnT - Interdisciplinary Institute for Security and Trust : Partnership Programm 6 public, 15 private, 2M turnover

CONCLUSION

PREVENTION IS NOT ENOUGH

- be proactive, be organised, have a CISO
- you are already compromised
- detect and handle it right (set-up/work with CERTs)
- prepare for a crisis
- get an insurance

THERE ARE NO SMALL INCIDENTS

- Minor incidents escalate fast
- Exploitation is still too easy
- Multi-compromises are used and abused
- IoT makes it even worse
- Attacks & attackers don't stop at the borders

Pascal Steichen
SECURITY
MADEIN.LU

SECURITY MADE IN LU

aware.lu

circl.lu

cases.lu