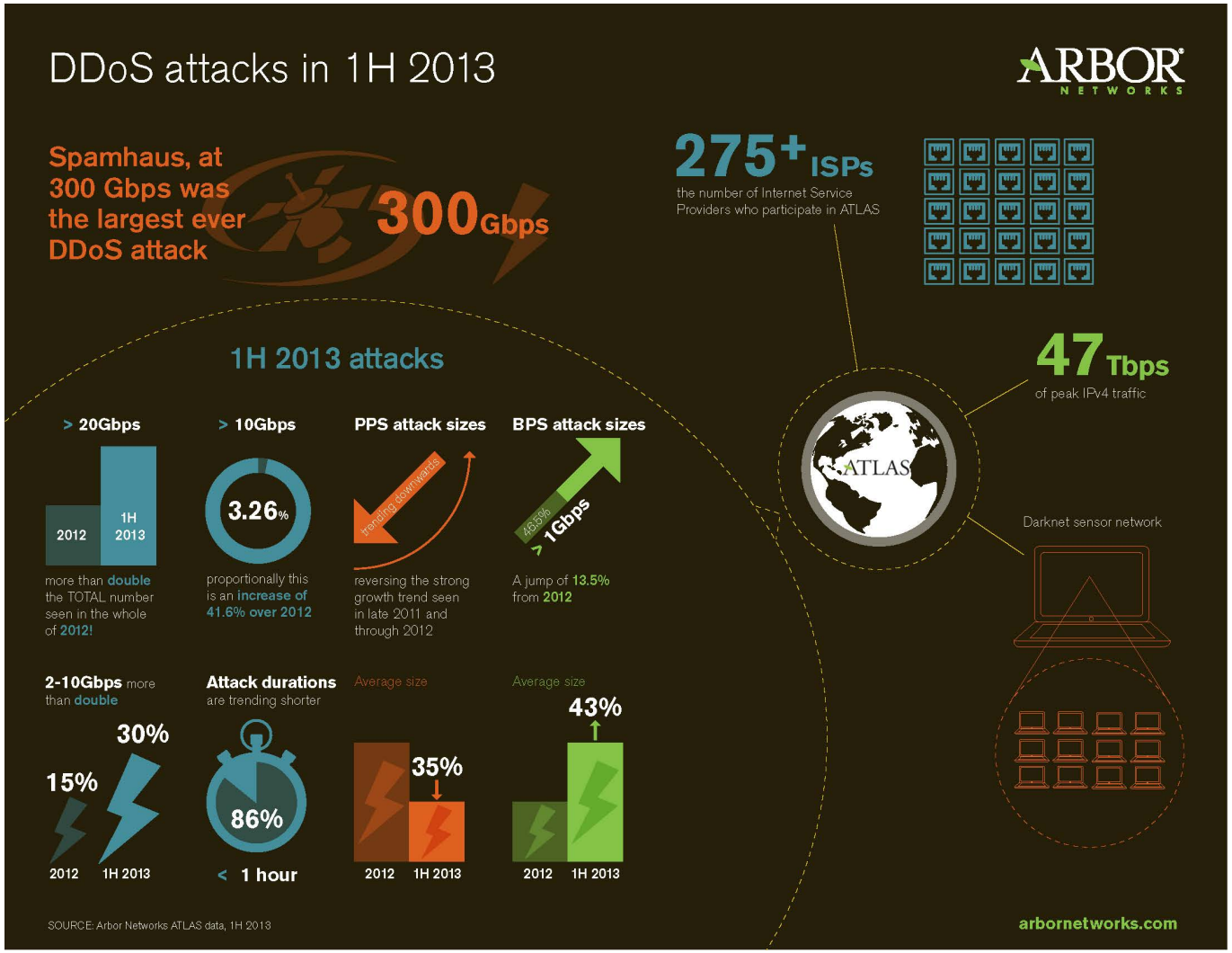
Welcome to

Early warning for security attacks

2013

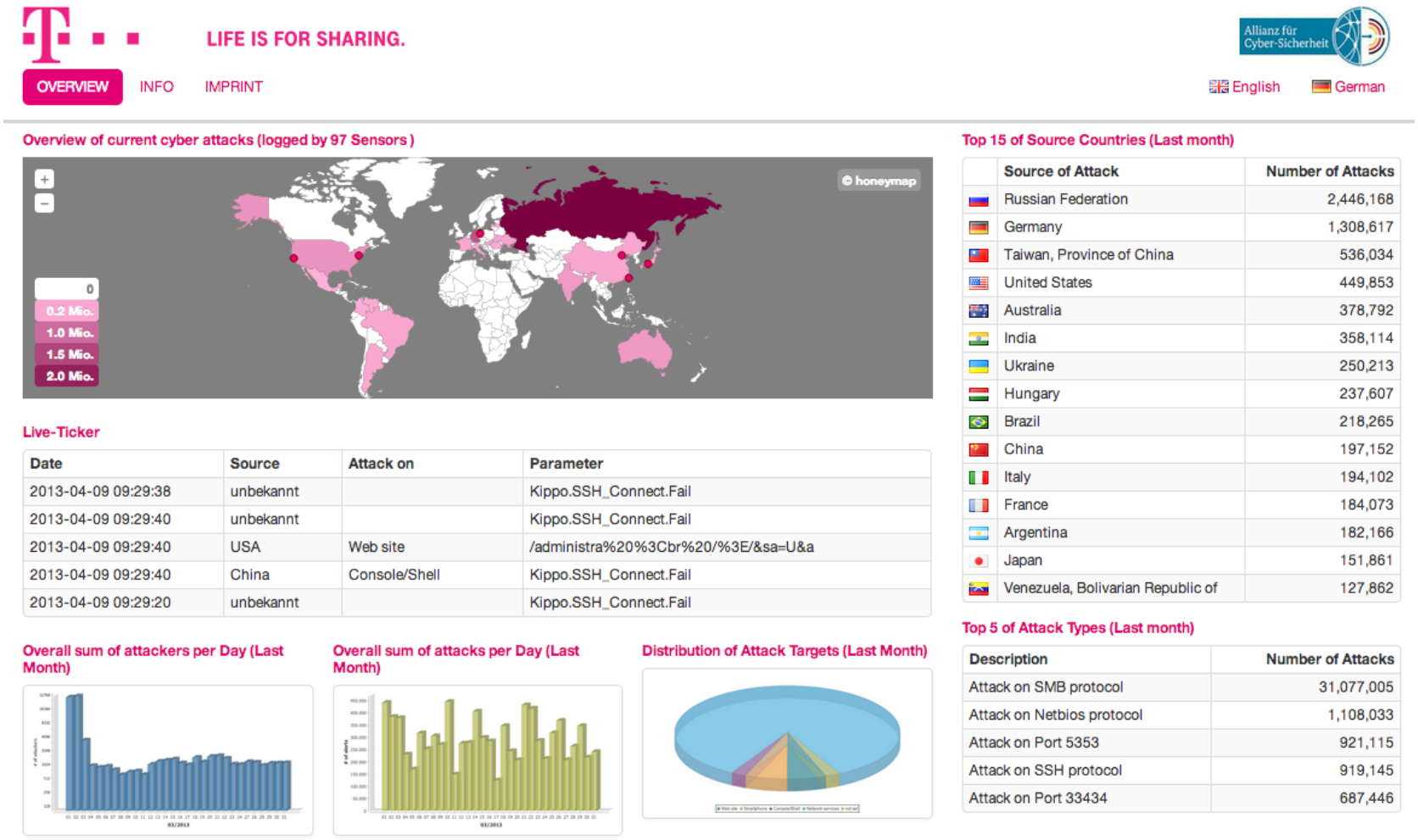
Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com



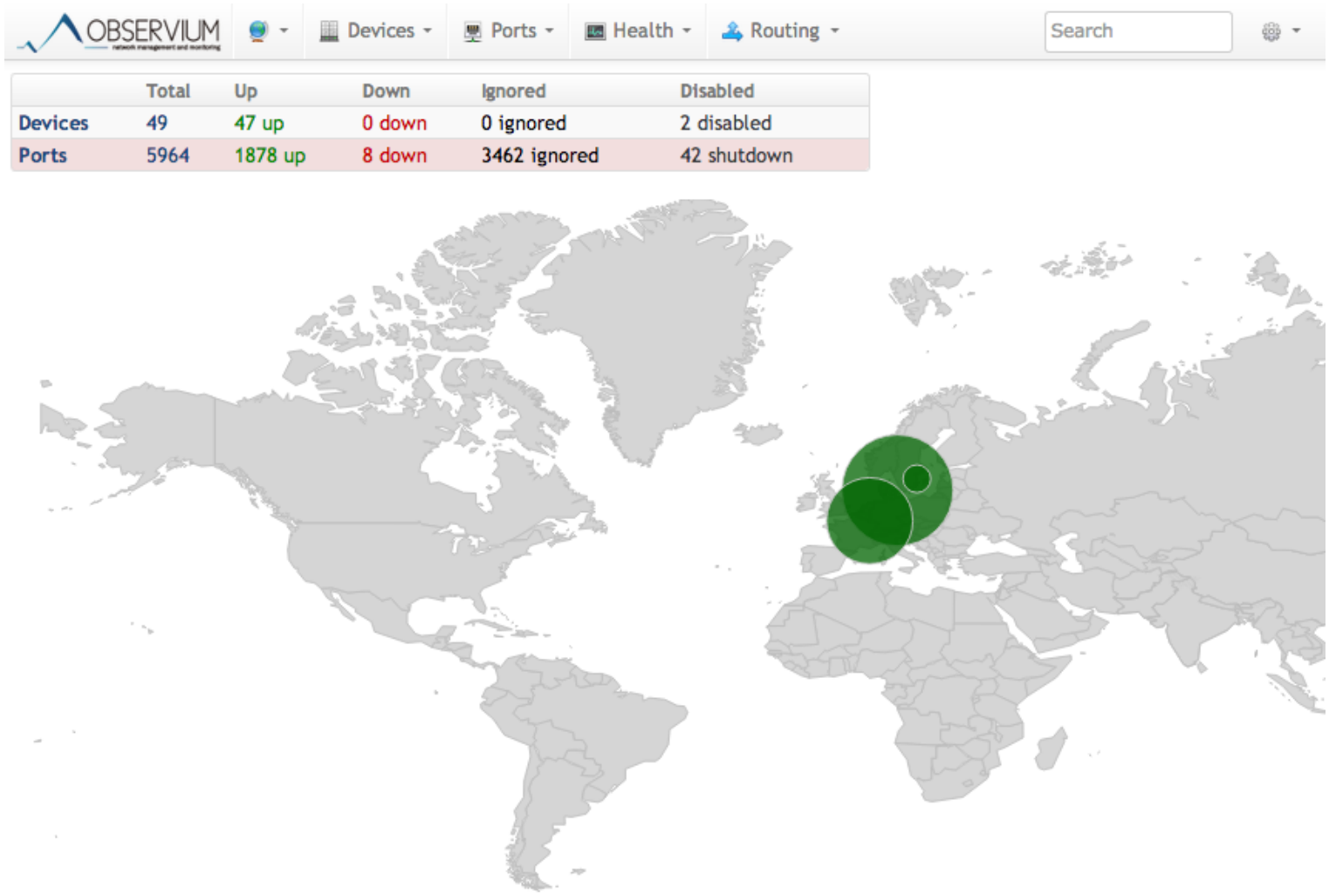
Security attacks and DDoS is very much in the media

Attack overview



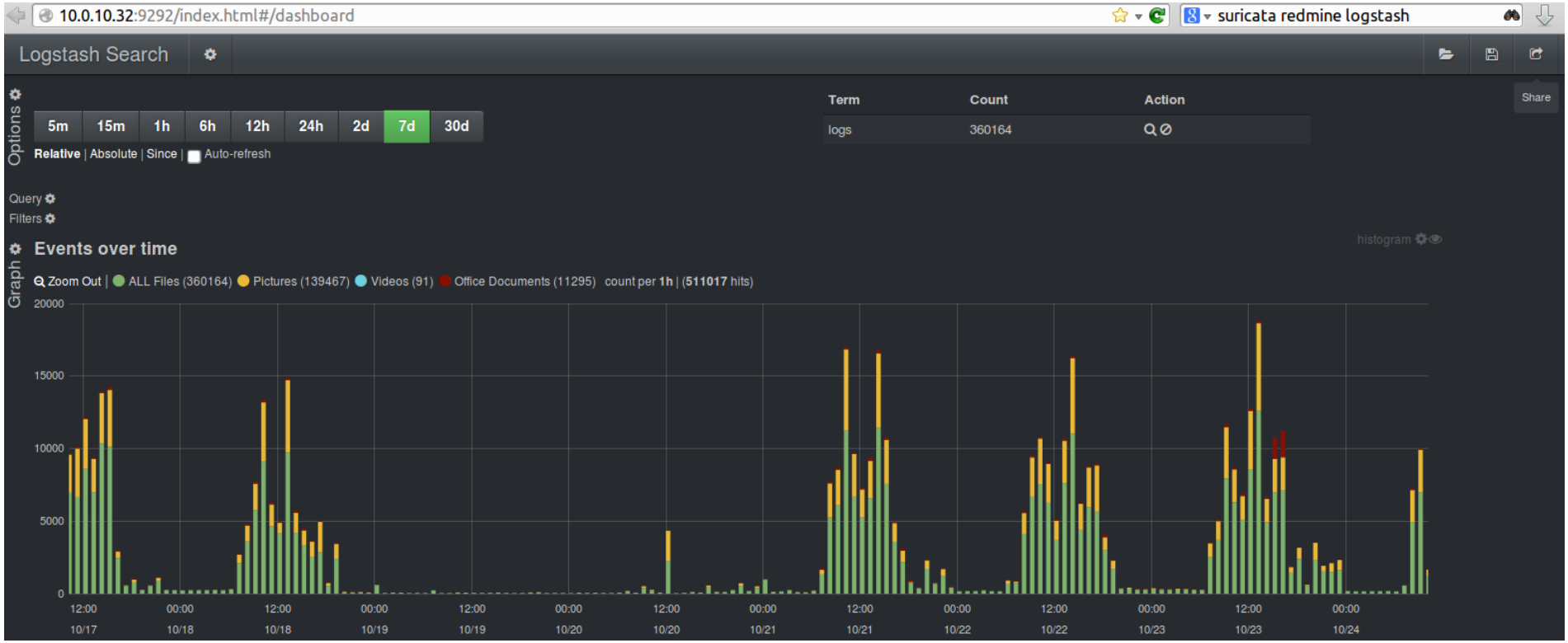
http://www.sicherheitstacho.eu/?lang=en

Graphs and Dashboards!



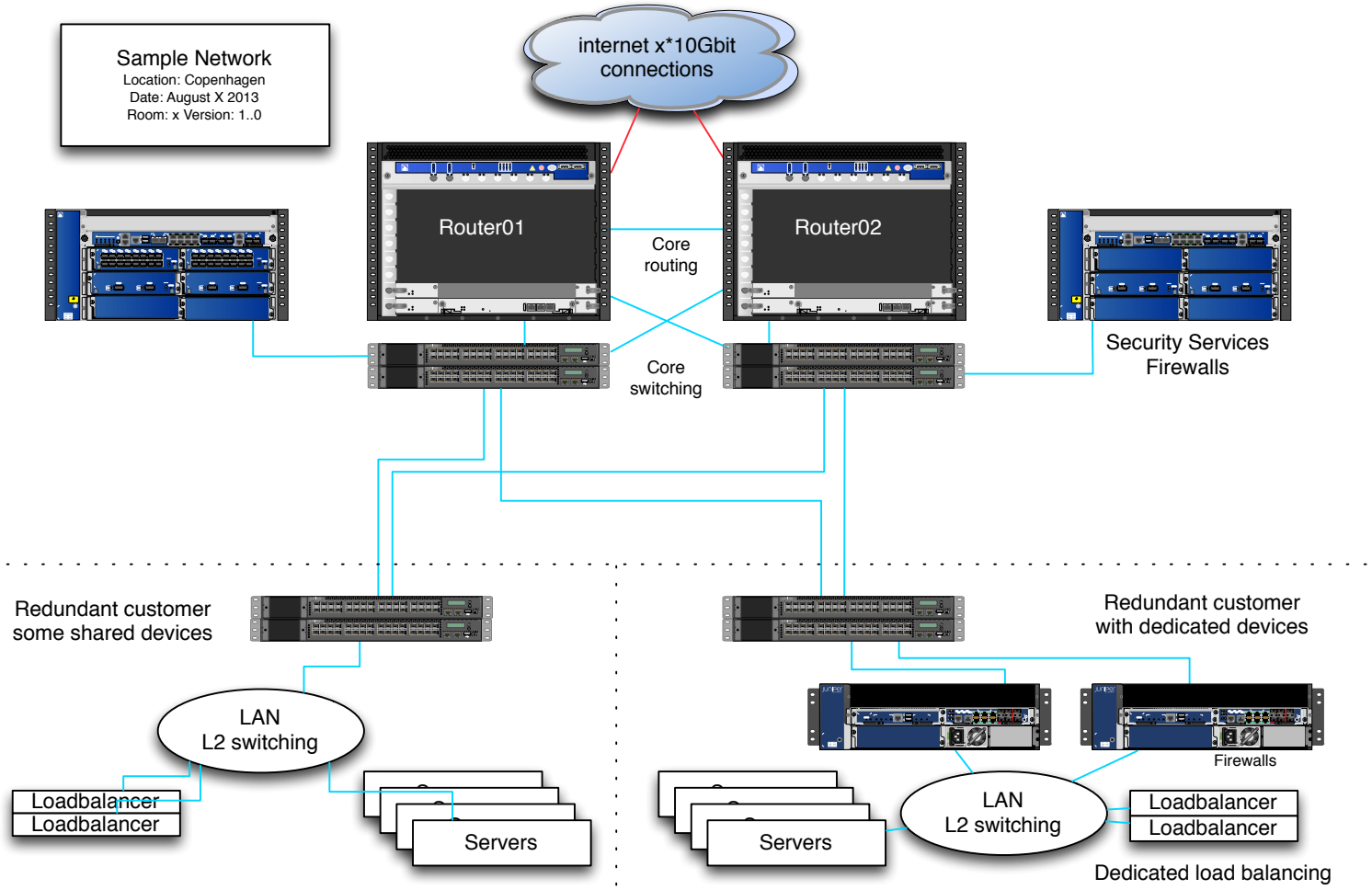
https://observium.solido.net/

Graphs and Dashboards!

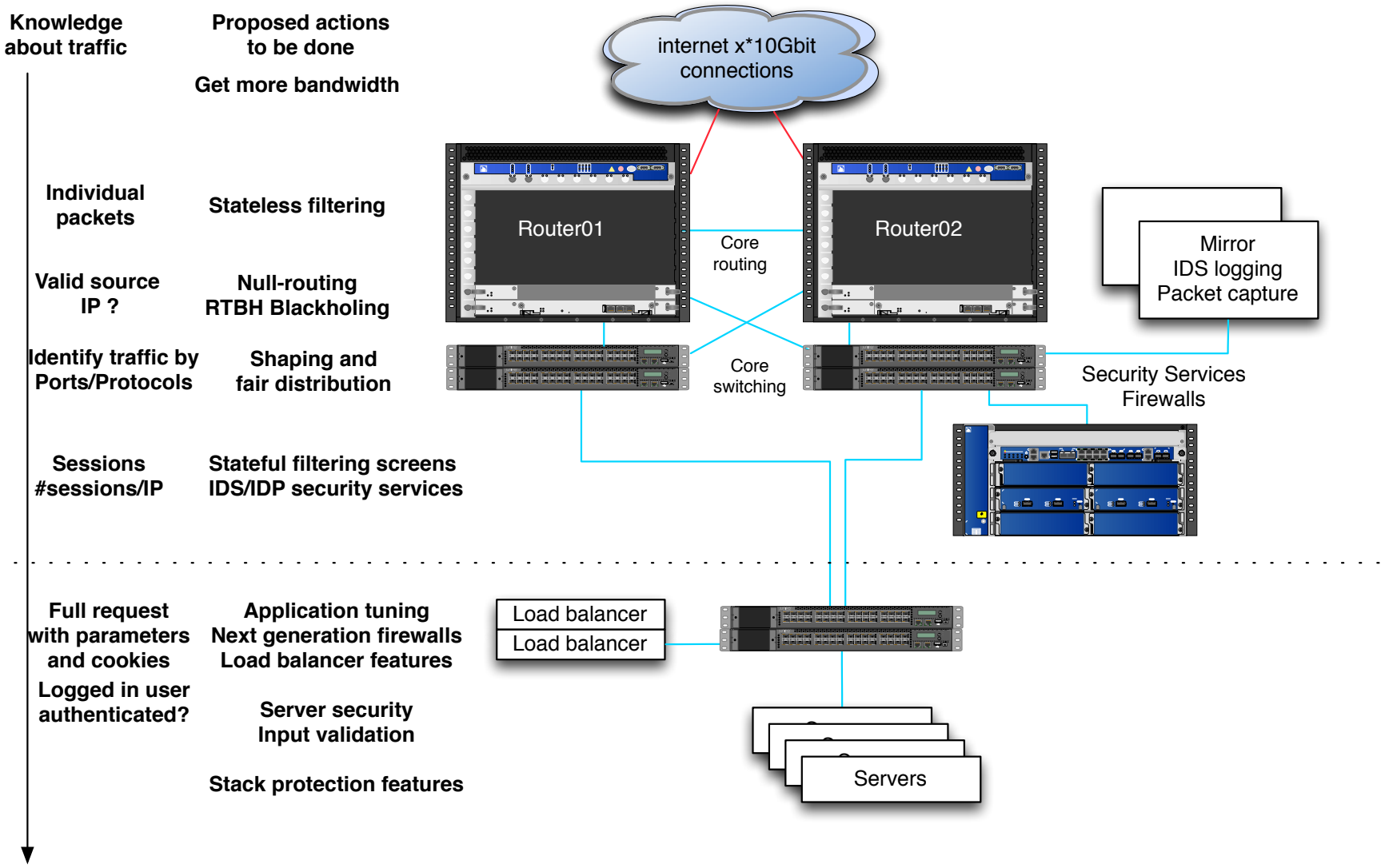


- Screenshot from Peter Manev, OISF
- Shown are Suricata IDS alerts processed by Logstash and Kibana

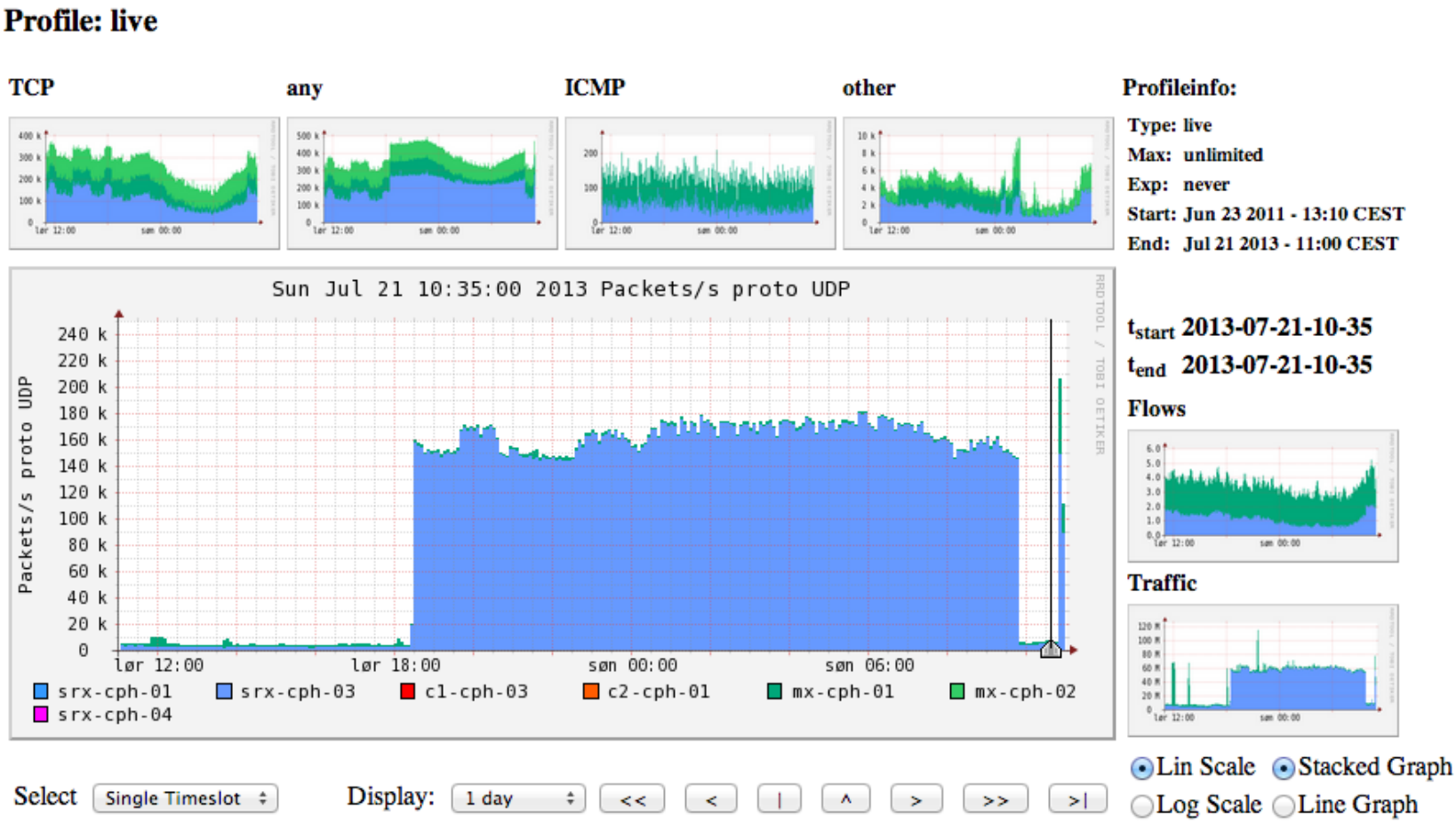
Networks today



Defense in depth - multiple layers of security

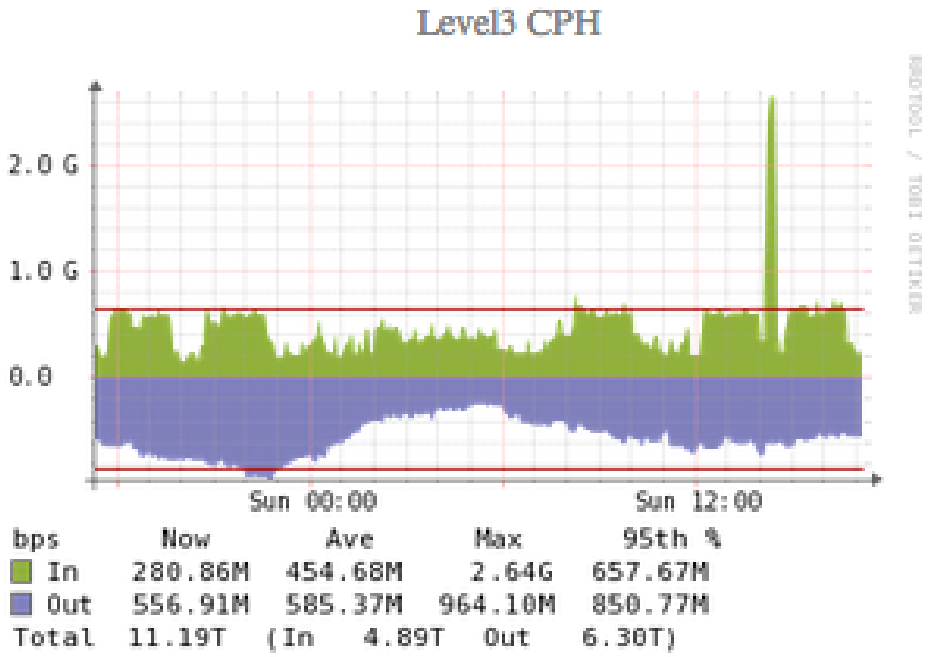


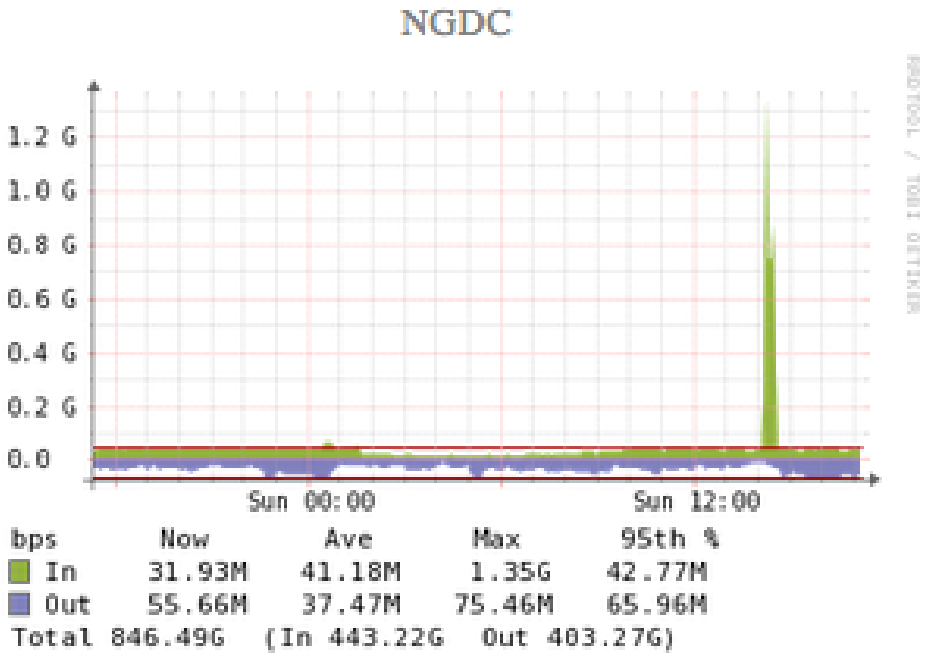
Netflow NFSen



An extra 100k packets per second from this netflow source (source is a router)

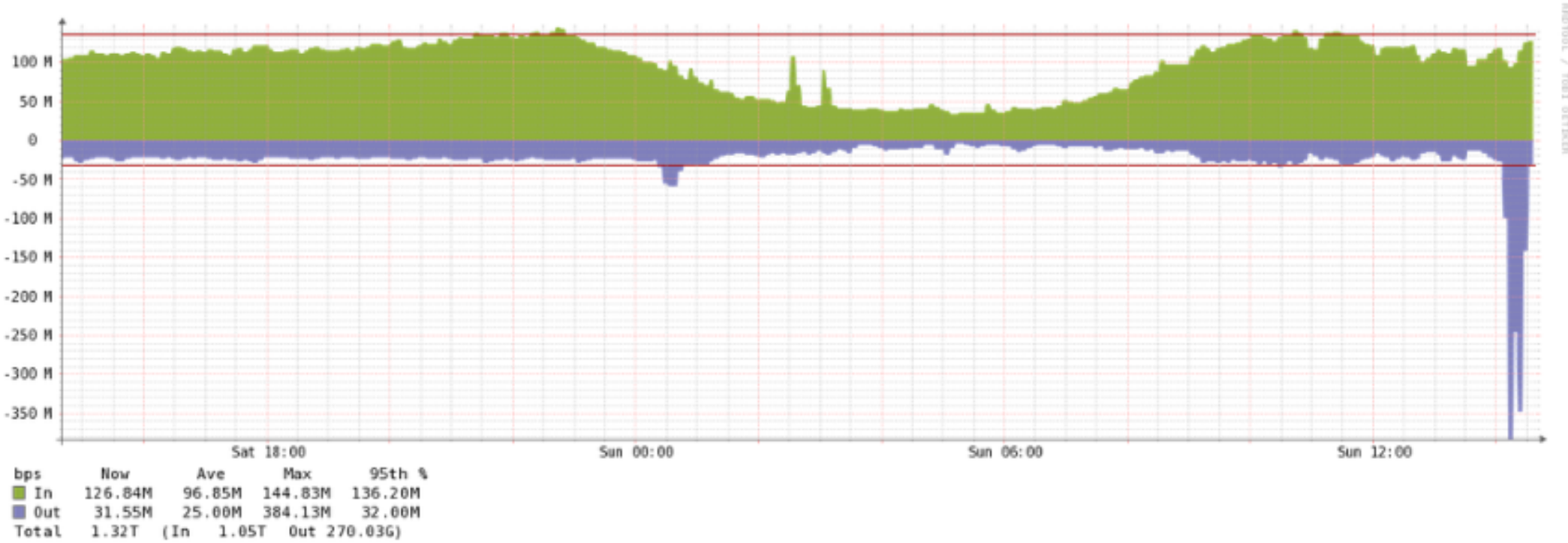
DDoS traffic before filtering





Only two links shown, at least 3Gbit incoming for this single IP

DDoS traffic after filtering



Link toward server (next level firewall actually) about 350Mbit outgoing

How to get started

How to get started searching for security events?

Collect basic data from your devices and networks

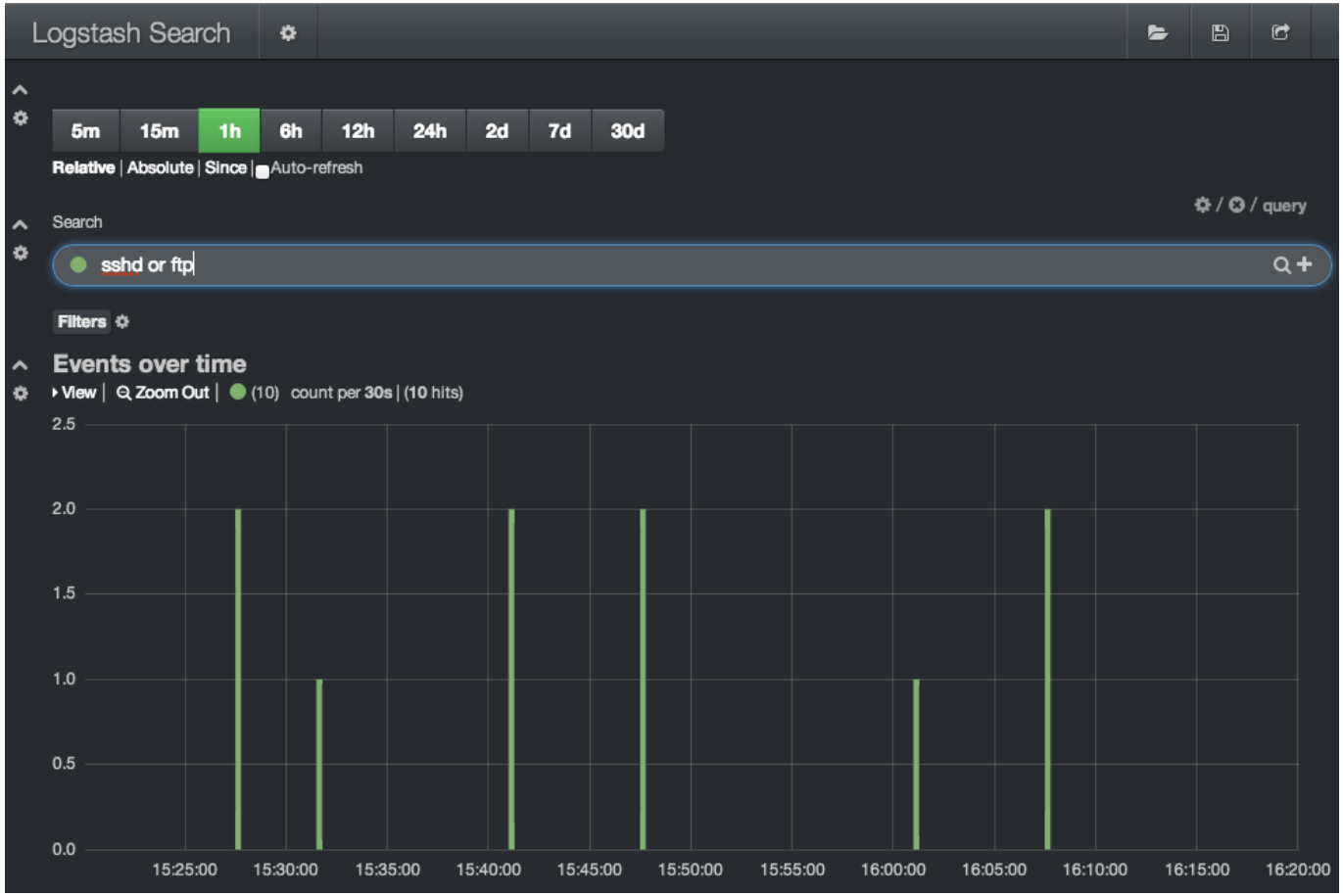
- Netflow data from routers
- Session data from firewalls
- Logging from applications: email, web, proxy systems

Centralize!

Process data

- Top 10: interesting due to high frequency, occurs often, brute-force attacks
- *ignore*
- Bottom 10: least-frequent messages are interesting

View data efficiently



View data by digging into it easily - must be fast

Logstash and Kibana are just examples, but use indexing to make it fast!

Security Onion

Security Onion is a Linux distro for IDS (Intrusion Detection) and NSM (Network Security Monitoring). `http://securityonion.net`

Next steps

In our network we are always improving things:

Suricata IDS `http://www.openinfosecfoundation.org/`

More graphs, with **automatic identification** of IPs under attack

Identification of **short sessions without data** - spoofed addresses

Alerting from **existing** devices

Dashboards with key measurements

Conclusion: Combine tools!

Questions?

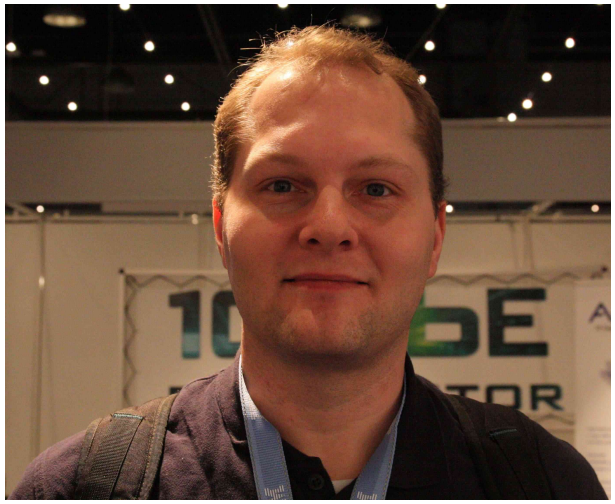
SOLIDO NETWORKS

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

You are always welcome to send me questions later via email

Contact information



- Henrik Lund Kramshøj, IT-security and internet samurai
- Email: hlk@solido.net Mobile: +45 2026 6000
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- CISSP certified
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks ApS