

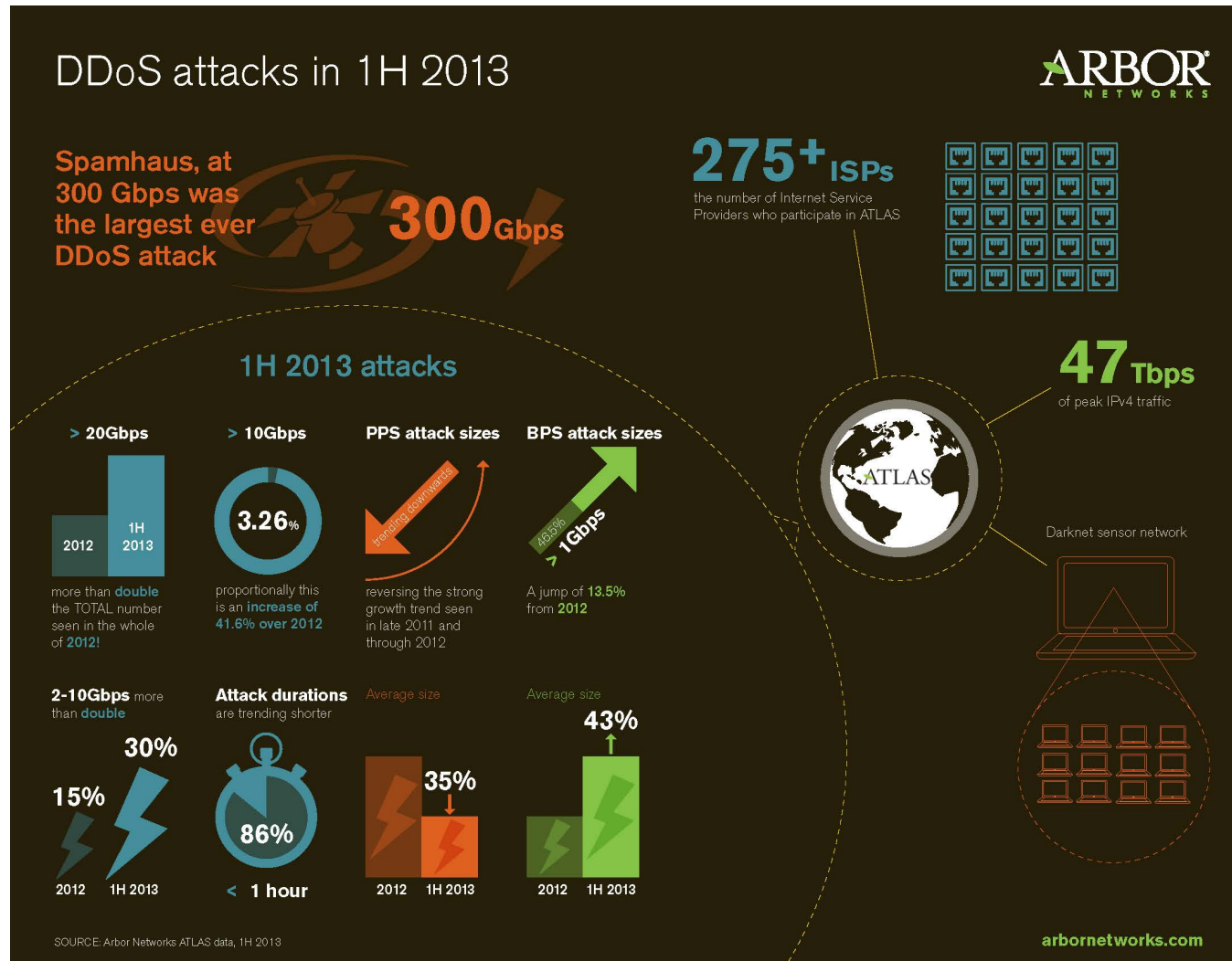
Welcome to

# 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



OVERVIEW

INFO

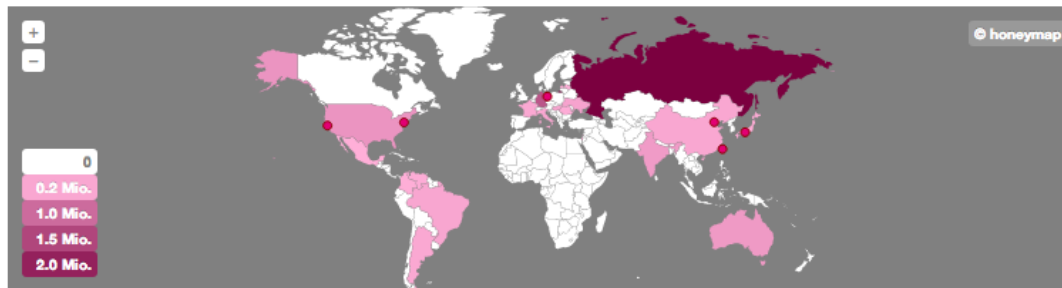
IMPRINT



English

German

## Overview of current cyber attacks (logged by 97 Sensors)



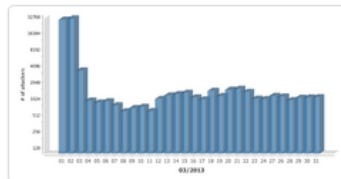
## Live-Ticker

Date	Source	Attack on	Parameter
2013-04-09 09:29:38	unbekannt		Kippo.SSH_Connect.Fail
2013-04-09 09:29:40	unbekannt		Kippo.SSH_Connect.Fail
2013-04-09 09:29:40	USA	Web site	/administra%20%3Cbr%20/%3E/&sa=U&a
2013-04-09 09:29:40	China	Console/Shell	Kippo.SSH_Connect.Fail
2013-04-09 09:29:20	unbekannt		Kippo.SSH_Connect.Fail

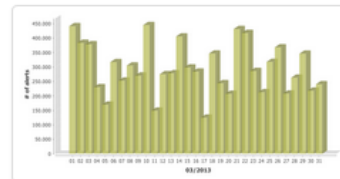
## Top 15 of Source Countries (Last month)

Source of Attack	Number of Attacks
Russian Federation	2,446,168
Germany	1,308,617
Taiwan, Province of China	536,034
United States	449,853
Australia	378,792
India	358,114
Ukraine	250,213
Hungary	237,607
Brazil	218,265
China	197,152
Italy	194,102
France	184,073
Argentina	182,166
Japan	151,861
Venezuela, Bolivarian Republic of	127,862

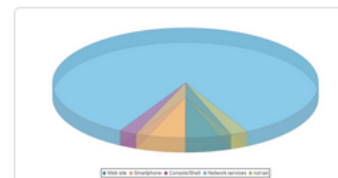
## Overall sum of attackers per Day (Last Month)



## Overall sum of attacks per Day (Last Month)



## Distribution of Attack Targets (Last Month)

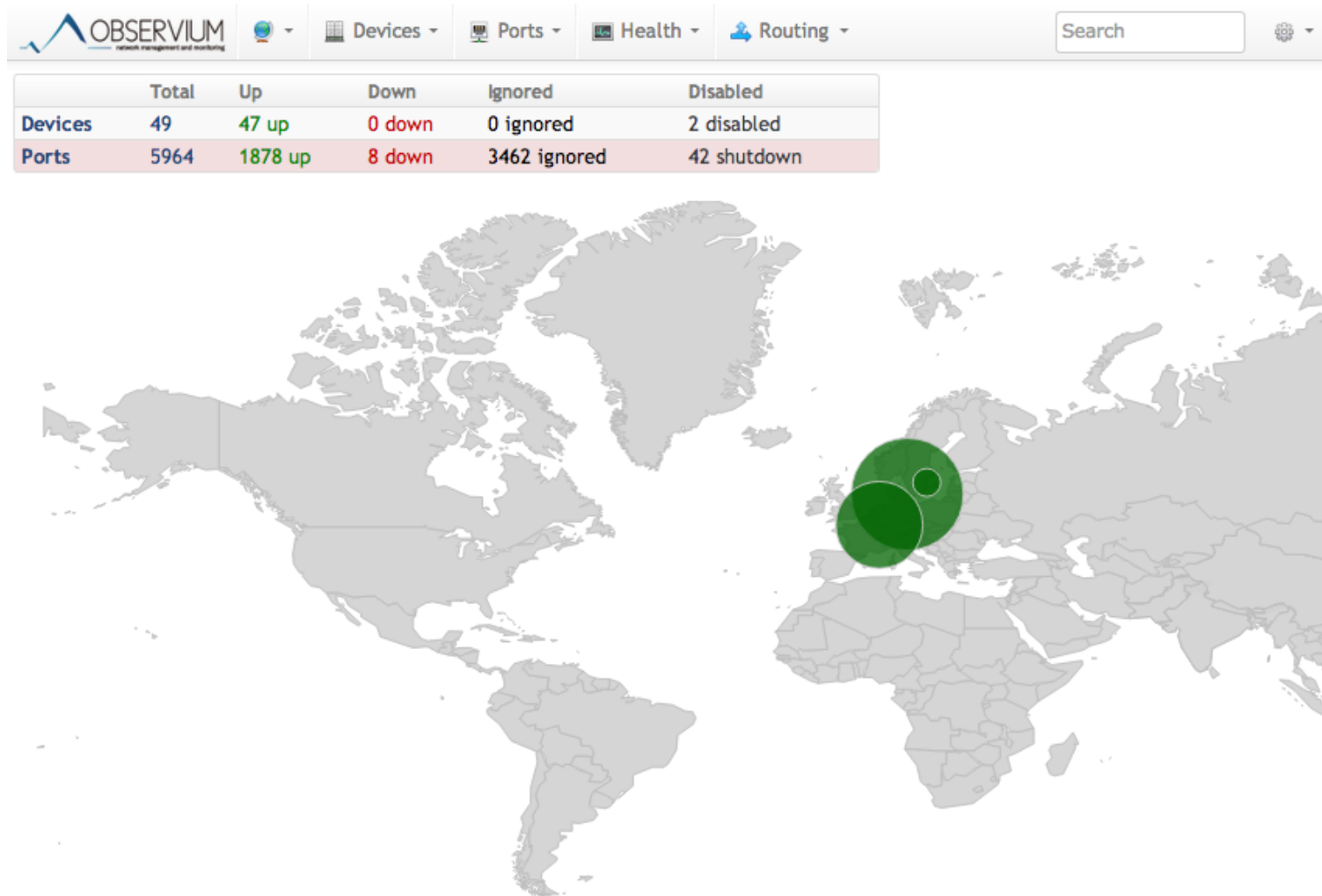


## Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	31,077,005
Attack on Netbios protocol	1,108,033
Attack on Port 5353	921,115
Attack on SSH protocol	919,145
Attack on Port 33434	687,446

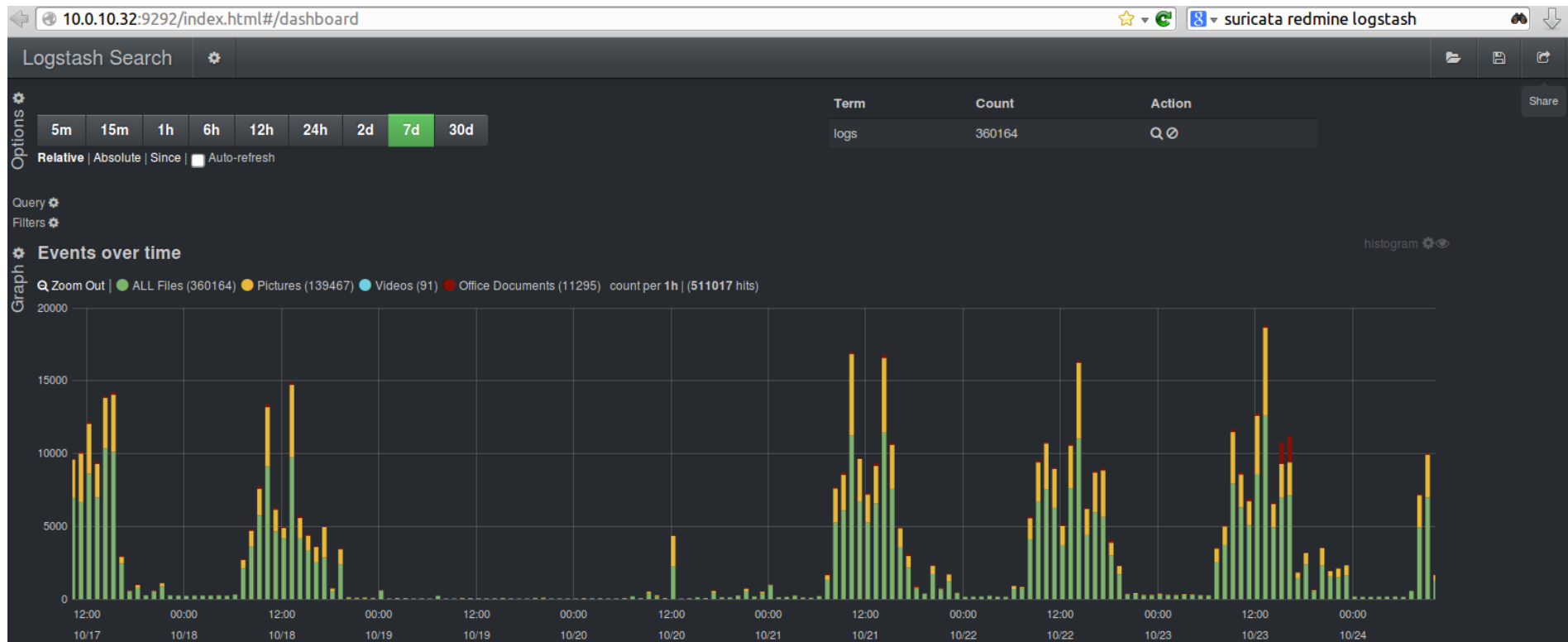
<http://www.sicherheitstacho.eu/?lang=en>

# Graphs and Dashboards!

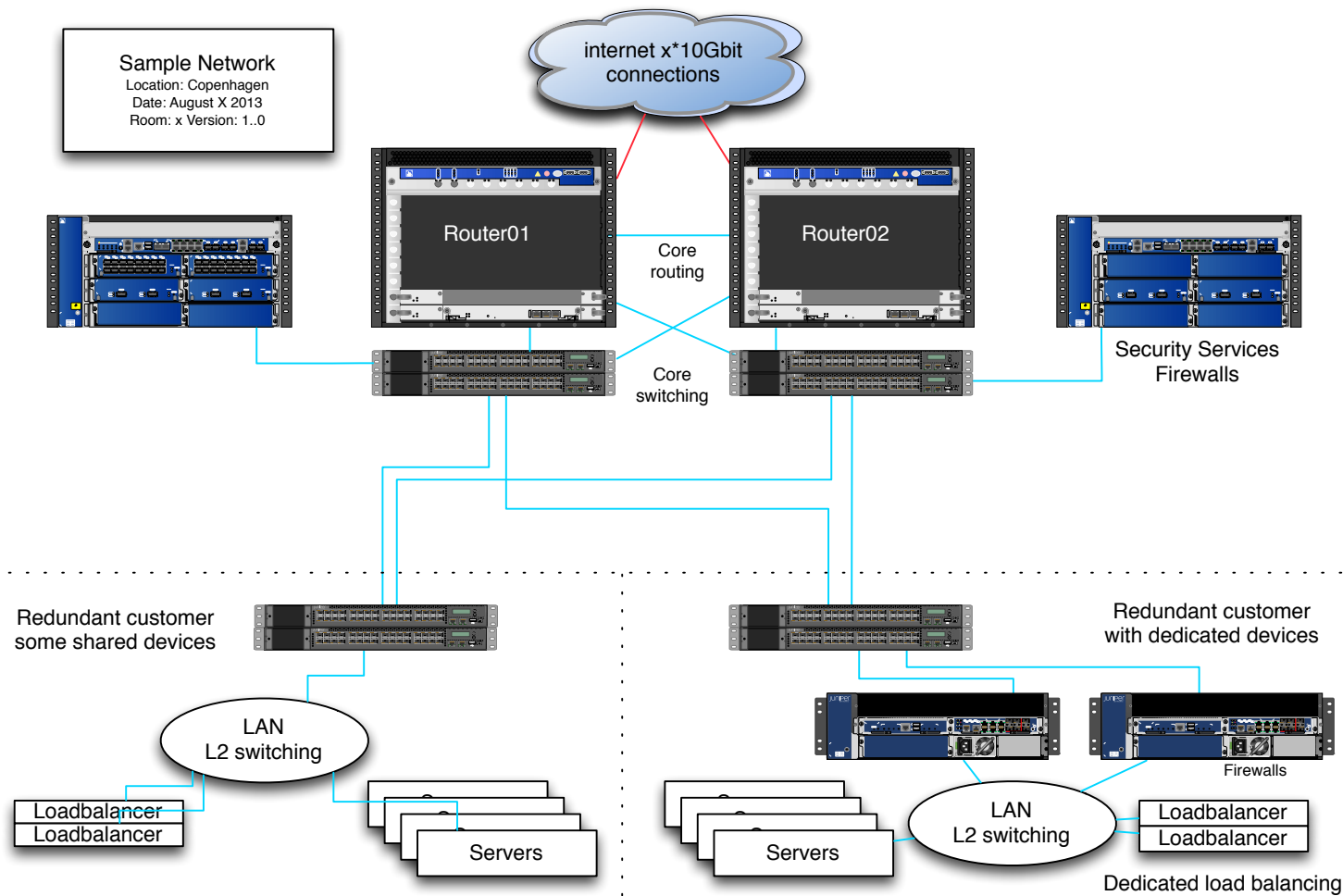


<https://observium.solido.net/>

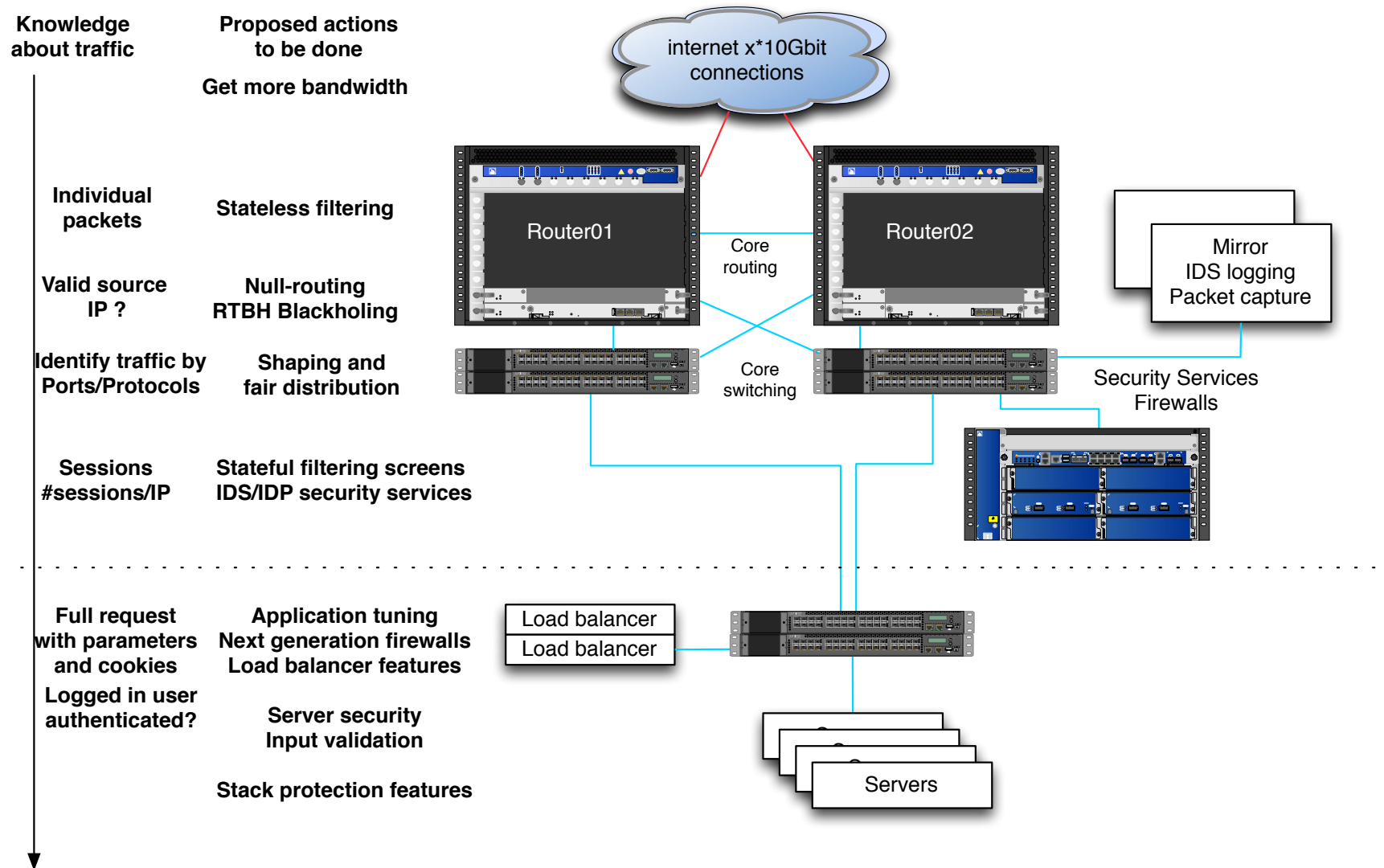
# Graphs and Dashboards!



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

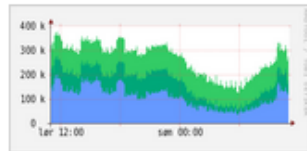


# Defense in depth - multiple layers of security

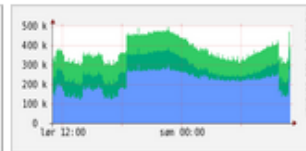


## Profile: live

### TCP



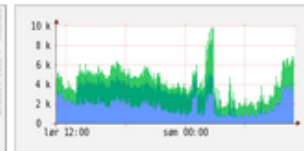
### any



### ICMP

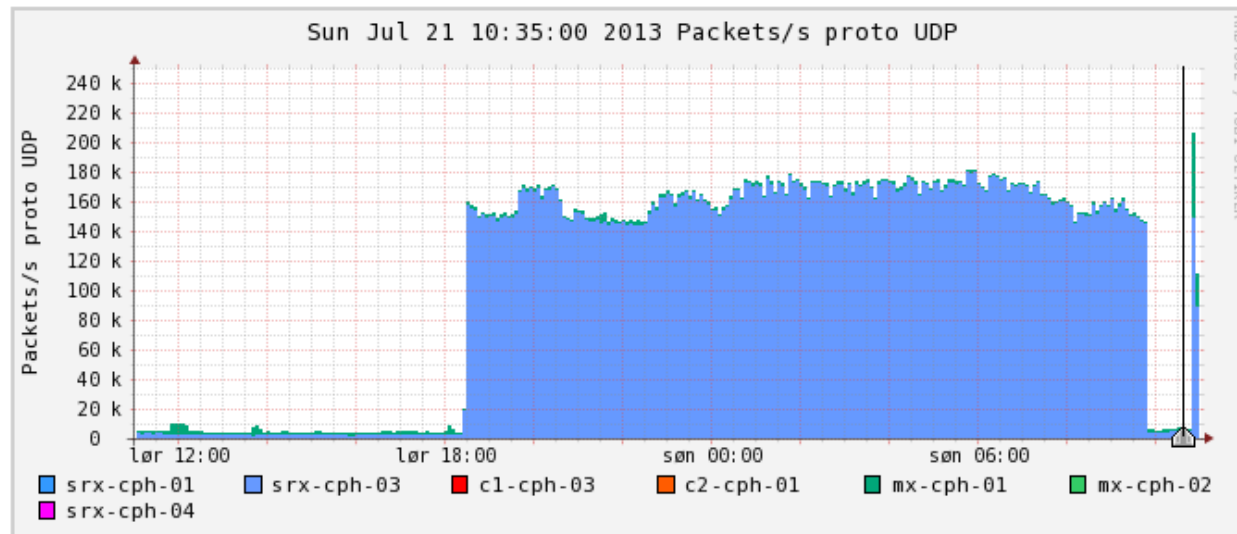


### other



### Profileinfo:

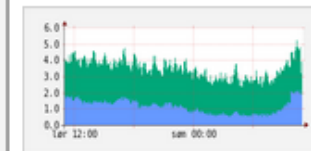
Type: live  
Max: unlimited  
Exp: never  
Start: Jun 23 2011 - 13:10 CEST  
End: Jul 21 2013 - 11:00 CEST



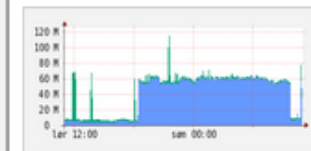
t<sub>start</sub> 2013-07-21-10-35

t<sub>end</sub> 2013-07-21-10-35

### Flows



### Traffic



Select

Display:



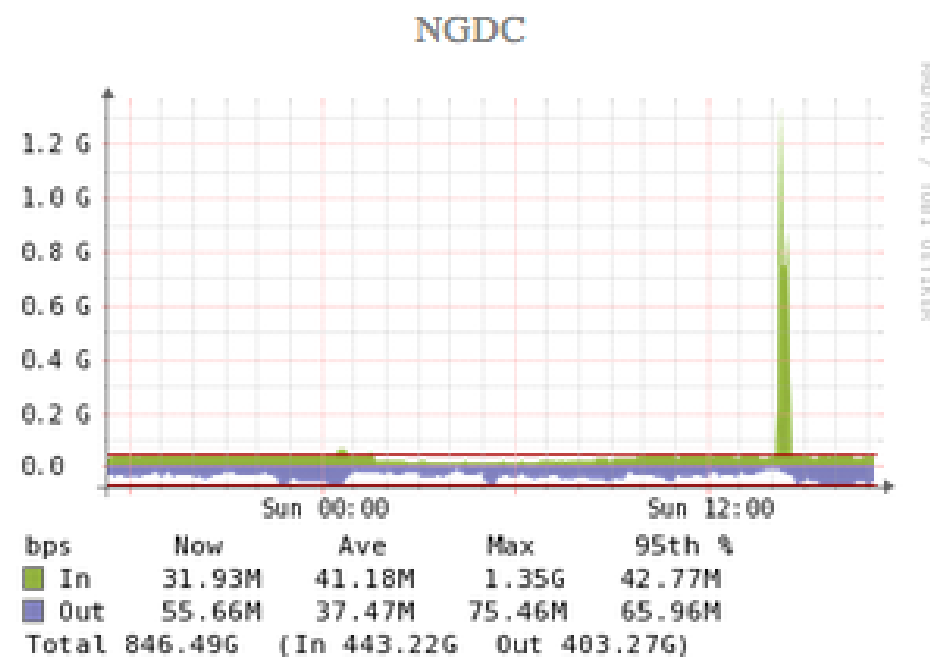
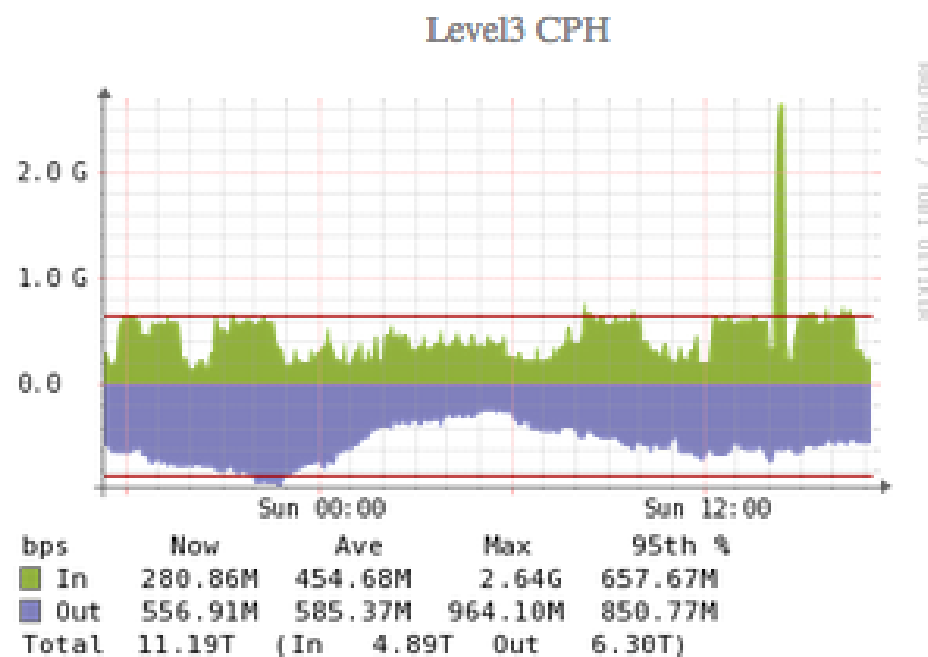
☒ Lin Scale ☒ Stacked Graph

☐ Log Scale ☐ Line Graph

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

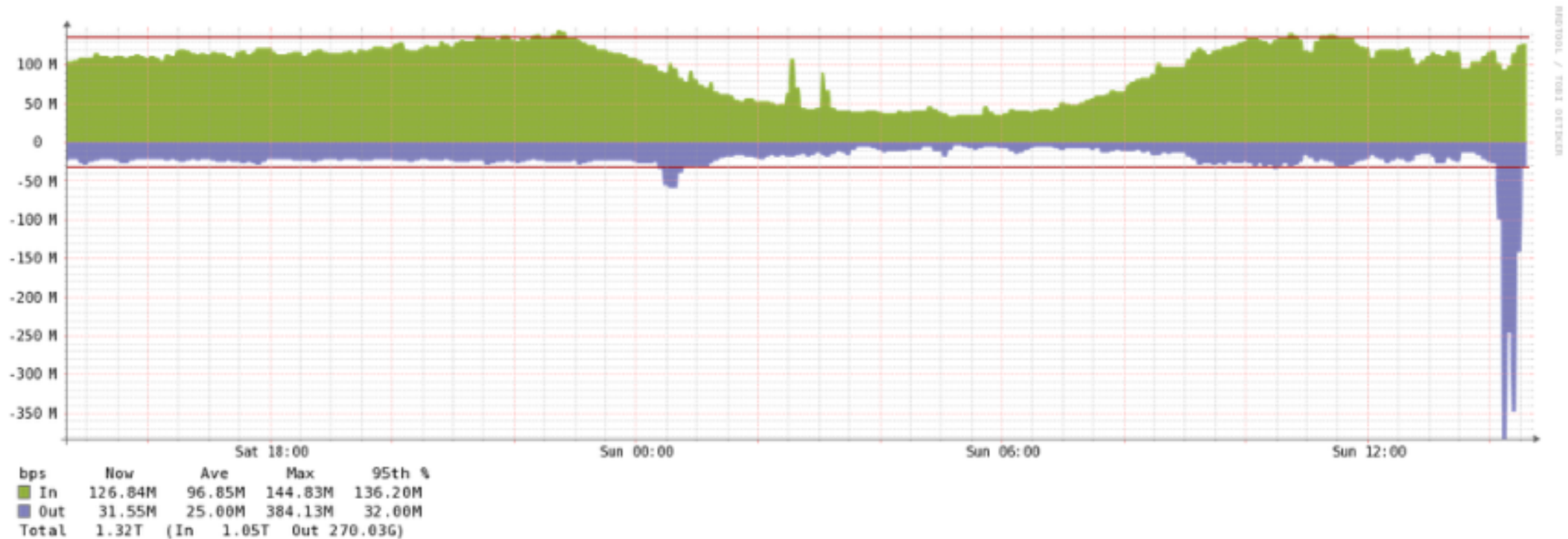


# DDoS traffic before filtering



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 searching for security events?

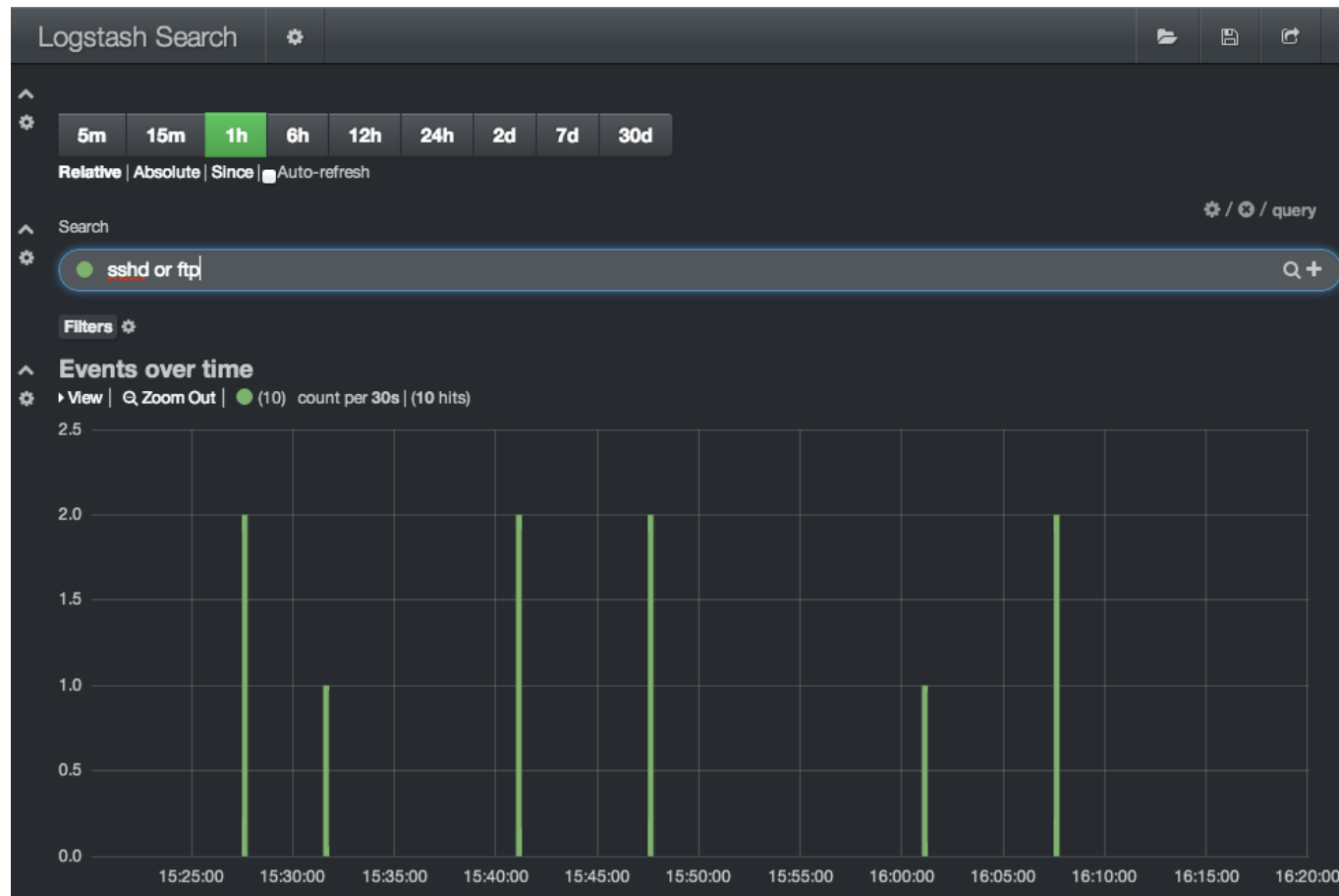
Collect basic data from your devices and networks

- 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 by digging into it easily - must be fast

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



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

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!

Henrik Lund Kramshøj, internet samurai  
hlk@solido.net

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email



- Henrik Lund Kramshøj, IT-security and internet samurai
- Email: [hlik@solido.net](mailto:hlik@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