b
UNIVERSITÄT
BERN

Qradar @ University of Bern

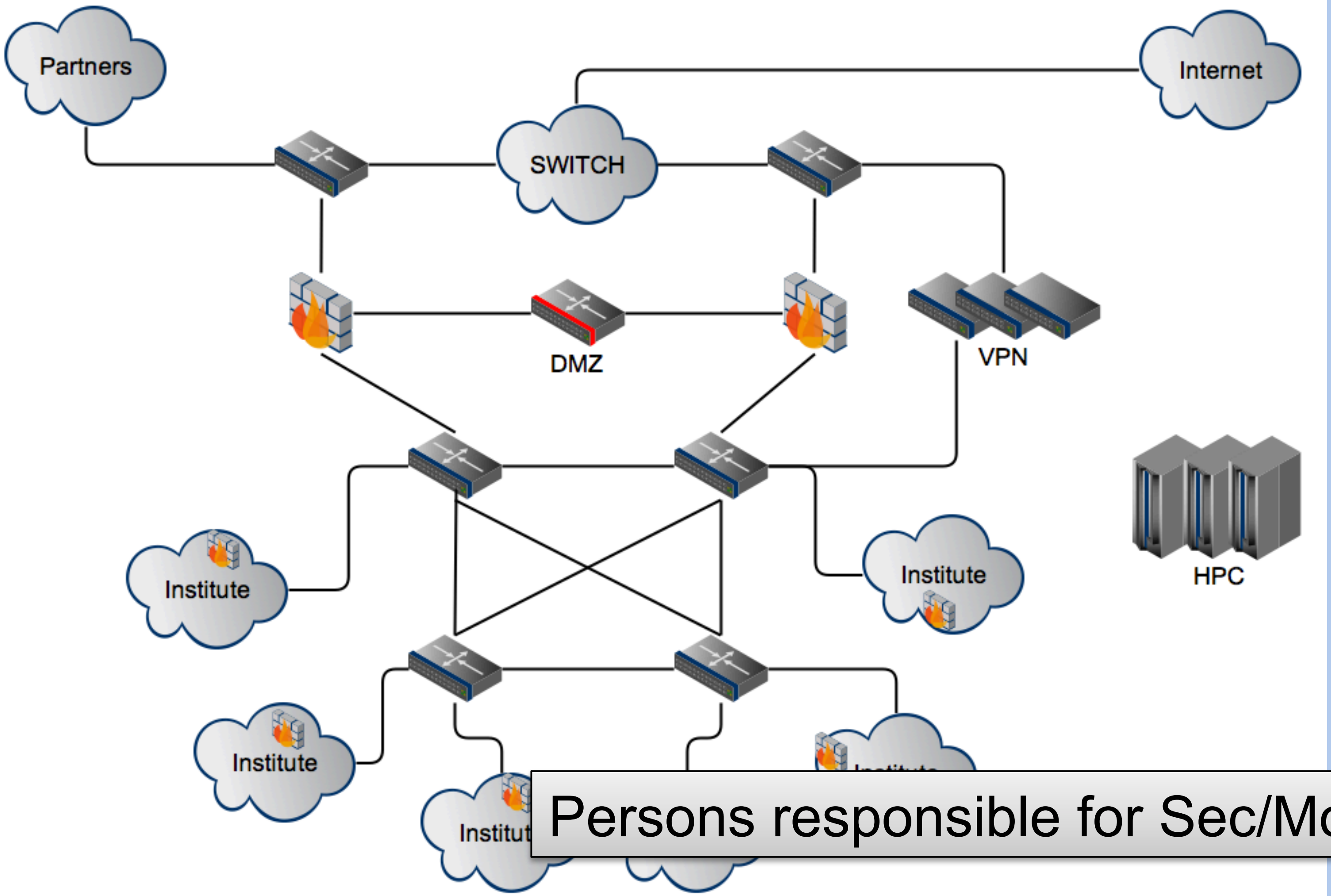
Stefan Zahnd

IT Services Department
Security, CSIRT
University of Bern

Agenda

- Network infrastructure
- Why using QRadar
- Integration
- Experiences and RFIs

Network overview



Institutes: 160

Students: 16‘257

Employees: ~5000

Router: 27

Switches: 600

WiFi AP: 870

Firewall/VPN: 50

Windows: 8200

Mac OS: 3500

Linux: 2000

Printer: 950

Ports: >34‘000

Persons responsible for Sec/Mon/Log: 2 ☺

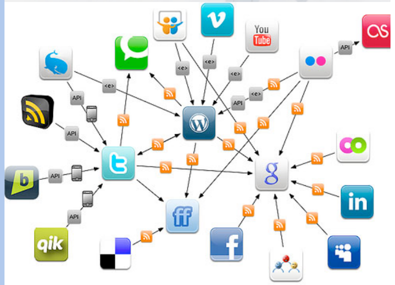
Why using Qradar?

- What happens within our network?
  - From decentralization to centralization

- Is it dangerous?
  - Malware infections
  - System breaches
  - Scanners

- Who did what yesterday or half a year ago?
  - Public networks
  - Forensics investigation

- Keep administrational overhead low



Integration

1. Security relevant information to track user within the network
   - Username, IP, MAC
   - NetFlow and Syslog
   - Firewalls, Routers, AD, RADIUS, VPN, MPP (Public Wireless)

2. Security relevant events from all systems
   - Login and configuration changes

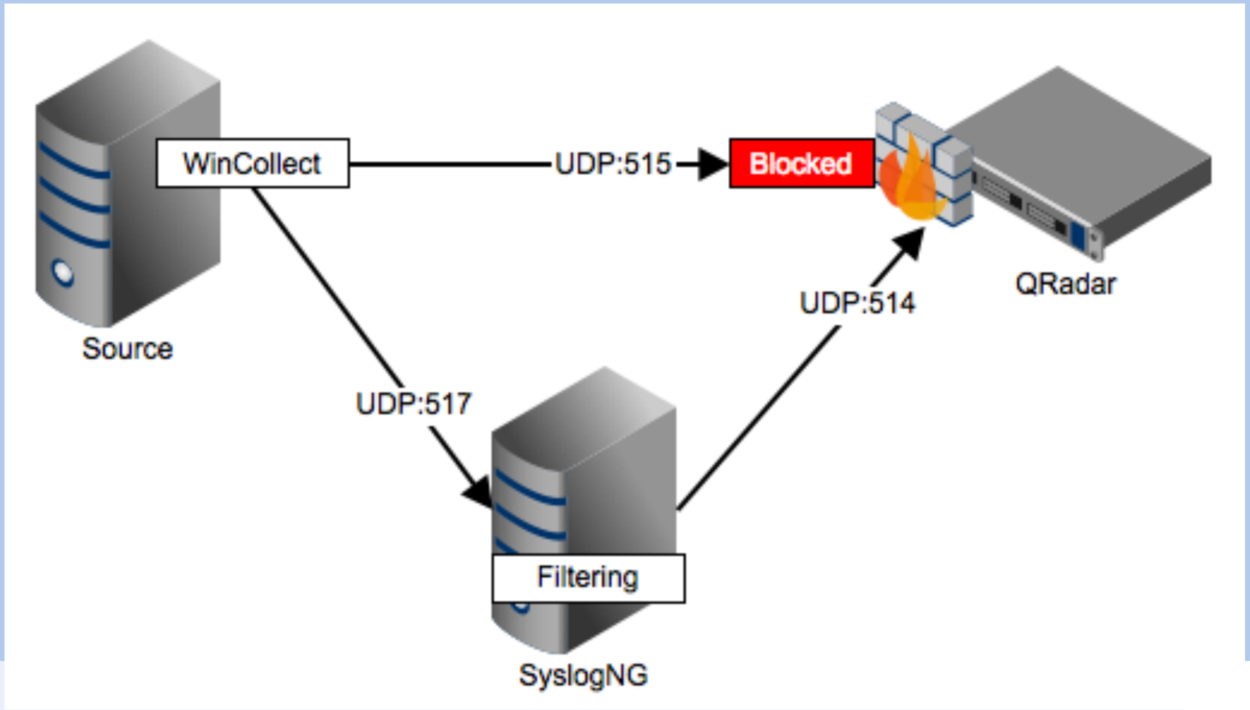
3. IDS, Honeypots and other cool stuff

Where are we now?

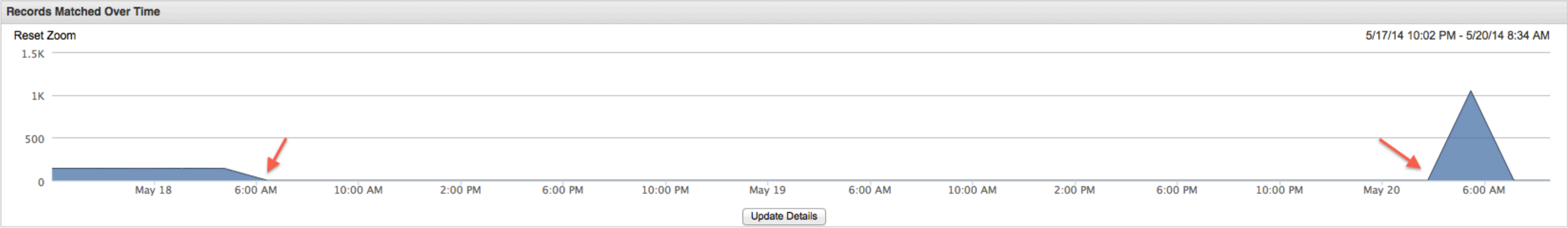
- At the beginning...
- All-in-One running since Nov 2013
- User tracking within network possible
- Tuning at 80%
  - Some tricky offenses that need identification
  - A heterogeneous and decentralized network doesn‘t make it easier

Problems / Workarounds

- Money matters and so do EPS
  - Tuning the source to only send what‘s needed is sometimes tricky
    - WinCollect and AD
- No DSM for FreeRADIUS

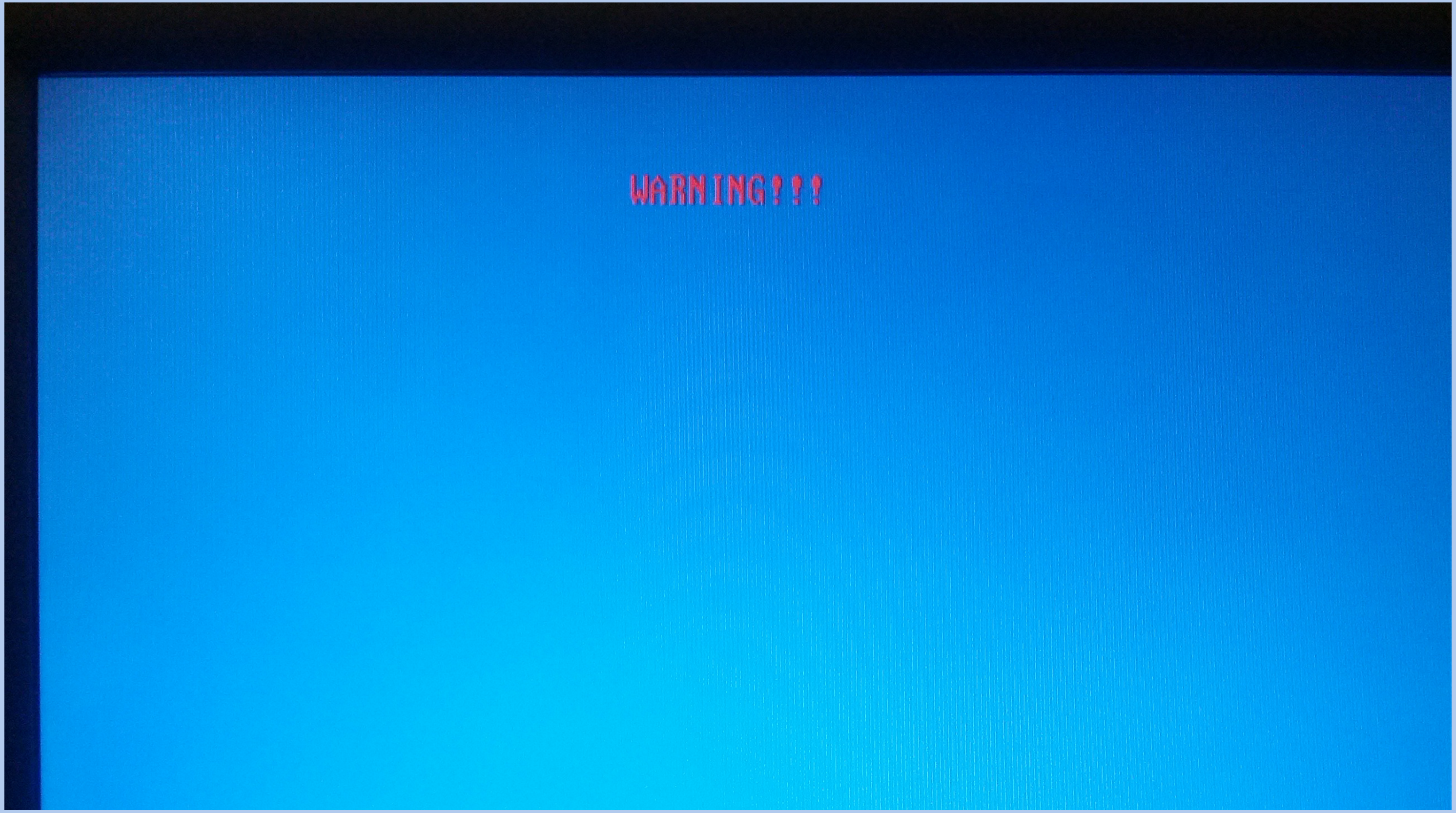


TLS-Syslog with SyslogNG



- Event collection suddenly stops
- After period of time all missed events are indexed at once
- Support case open

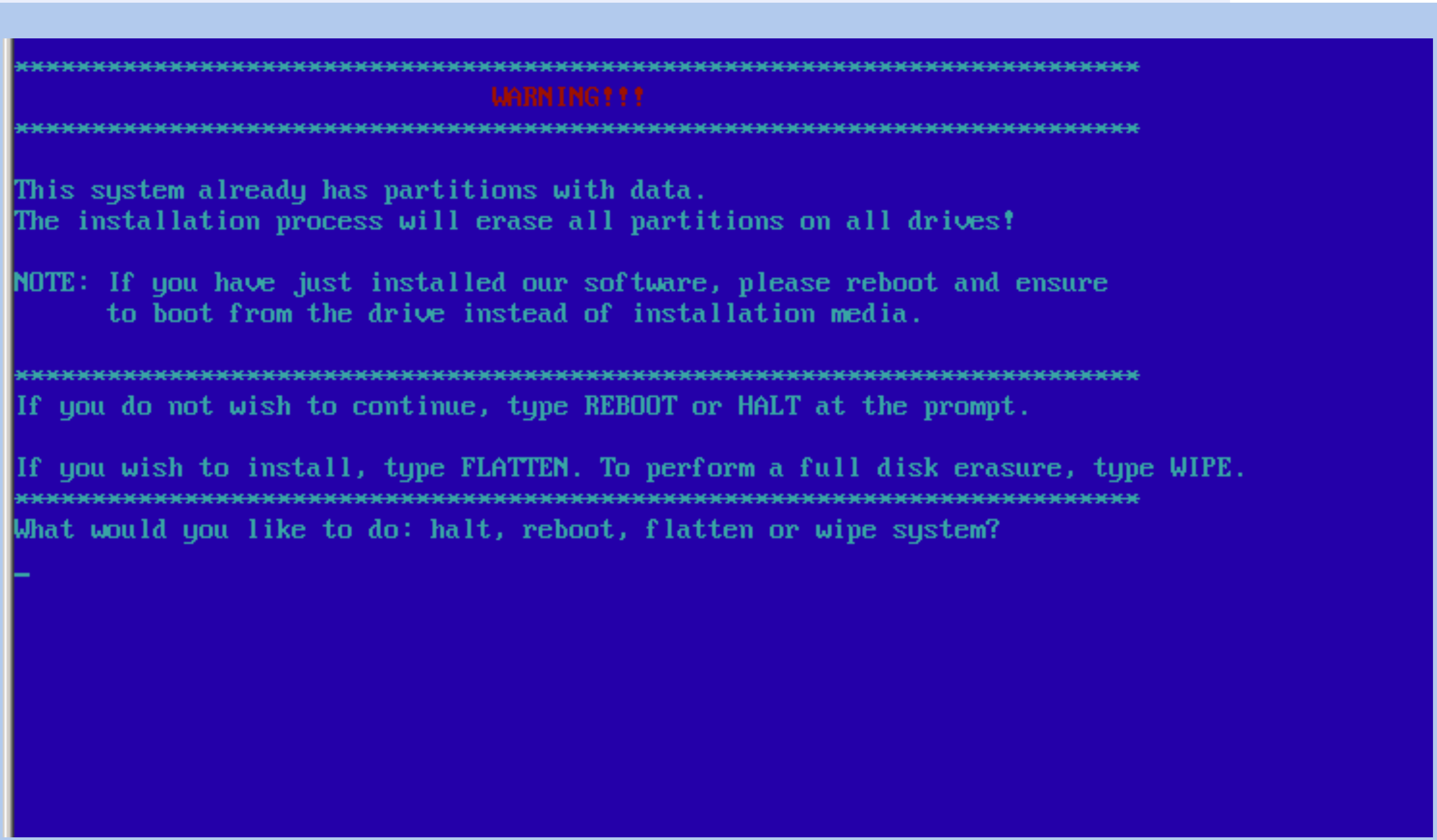
Screen Vs. Remote Session



WARNING!!!

Screen connected to VGA port

Screen Vs. Remote Session (2)



```
*************************************************************************
                               WARNING!!!
*************************************************************************

This system already has partitions with data.
The installation process will erase all partitions on all drives!

NOTE: If you have just installed our software, please reboot and ensure
      to boot from the drive instead of installation media.

*************************************************************************
If you do not wish to continue, type REBOOT or HALT at the prompt.

If you wish to install, type FLATTEN. To perform a full disk erasure, type WIPE.
*************************************************************************
What would you like to do: halt, reboot, flatten or wipe system?

_
```

Screen redirection through ILOM

Request For Improvement

- GUI
  - Printing (not working in all views)
  - Server Discovery (crash on E-Mail-Server discovery)
- Search
  - Should be more intuitive (like Splunk ☺)
- Edit already applied filters

Questions?