

Supporting Digital Forensics: A Latvian Police Perspective

Nils Kristians Cers, State Police of Latvia — Cybercrime Department





Cybercrime Department, State Police of Latvia

Digital forensics: analyzing evidence data from seized devices

Hundreds of terabytes of evidence per year

Volume grows every year

The problem

More data every year

Dozens of machines, many analysis tools

Manual monitoring becomes impossible

Downtime = delayed investigations

Evidence integrity is crucial

Limited budget – every hardware purchase must be justified

Our infrastructure

50+ Servers

Both hardware and virtualized

30+ Network devices

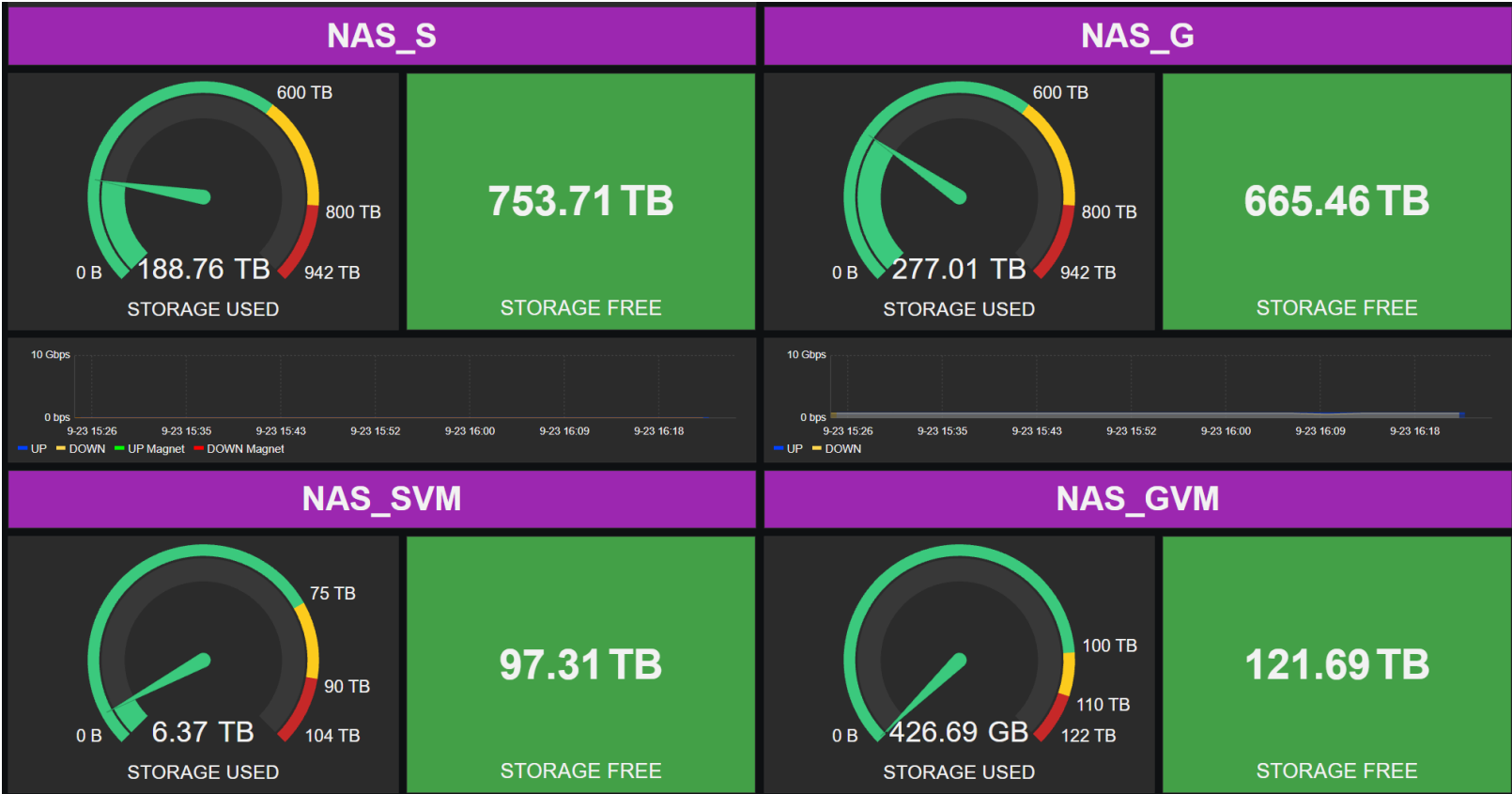
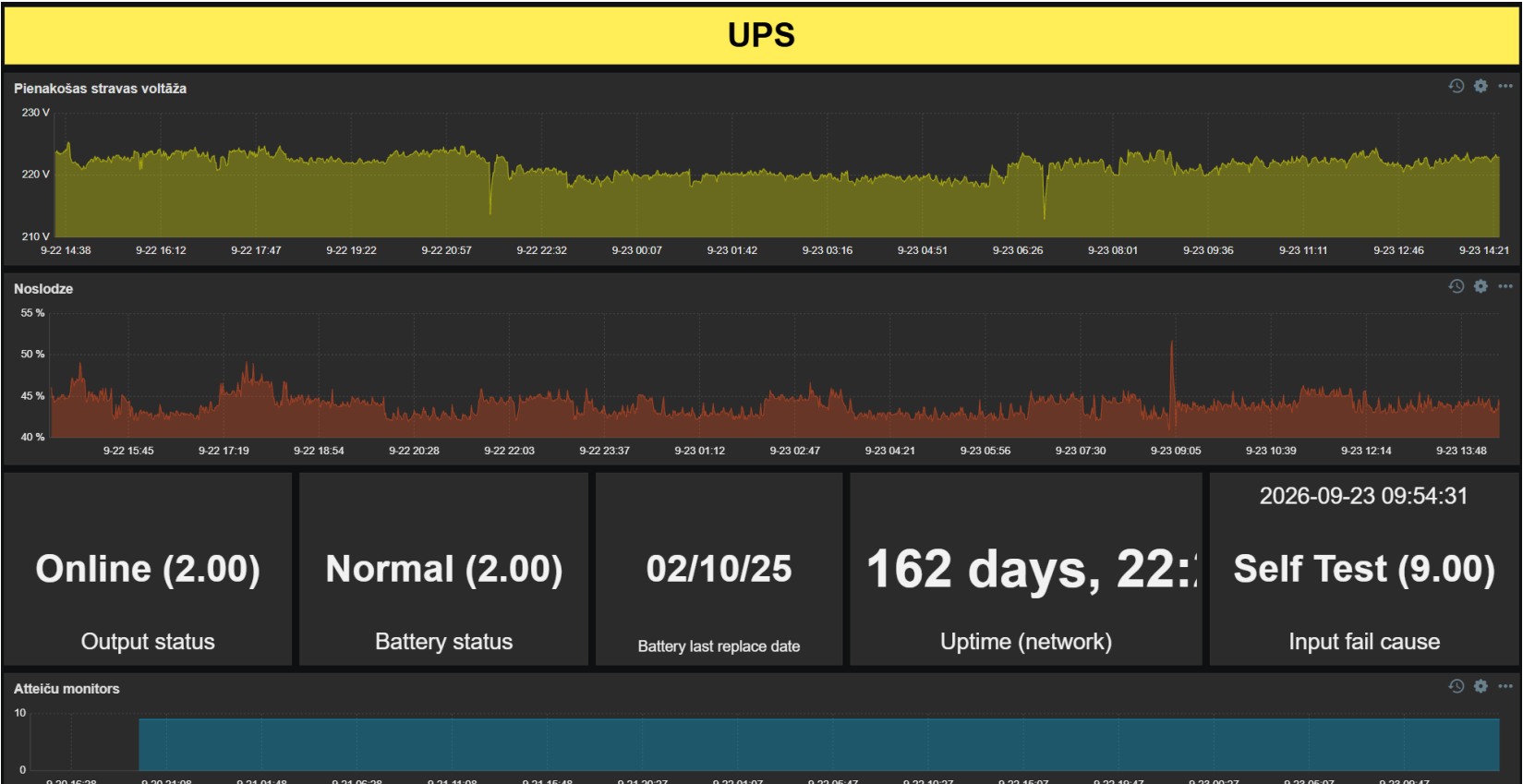
Routers, switches and other devices

20+ Power and environment monitoring devices

UPS, thermometers and humidity
monitors

Distributed infrastructure

Multiple locations across the country



Example dashboards

Why forensics is different

Data integrity

Evidence data must stay intact – no excuses

Reliability needs

Hardware failure = potential evidence loss

Non-stop work

Processing hardware must run uninterrupted

Slow hardware = slow law enforcement

Bottlenecks directly slow down investigations

Zabbix: one place to see everything

Central monitoring of the whole environment

Ability to instantly spot bottlenecks

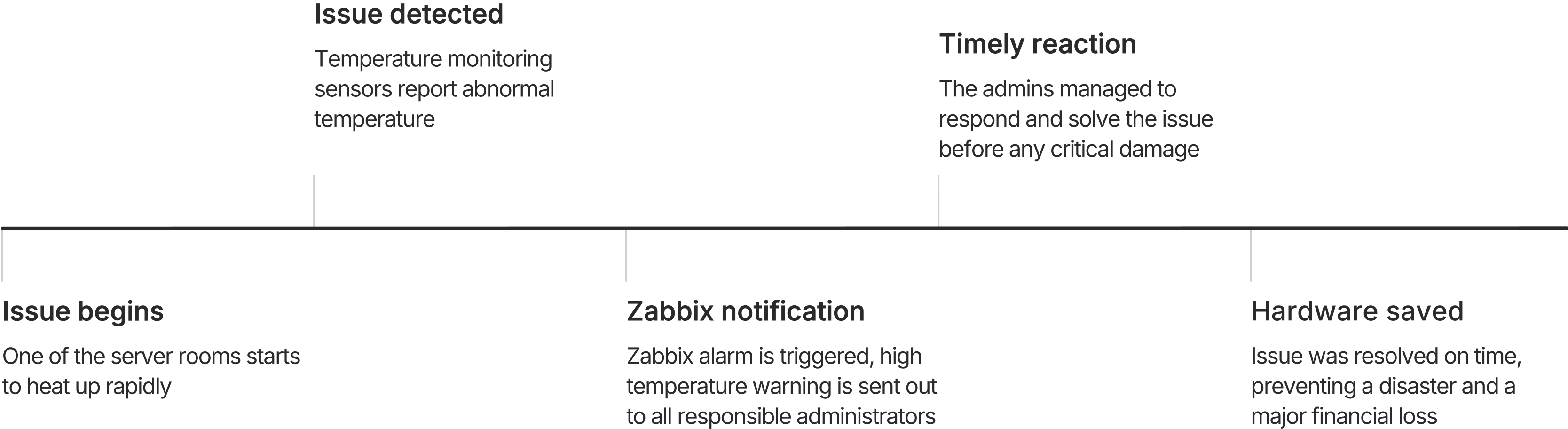
Redistribute workload to other machines

**Plan hardware purchases based on
historical trends**

**Immediate alerts – ability to pinpoint hardware and
software issues**

**Self-hosting provides security and cuts
expenses**

Case study: cooling issues





Temperature problem graph

Deployment specifics

Zabbix templates

We use both default and community-built templates to onboard different types of hardware

Automatic host discovery

Used to quickly attach hardware to Zabbix monitoring

Integrations for notifications

We use integrations for email notifications, as well as webhooks

Planned: automatic remediation

We plan soon to integrate automatic remediation scripts that would respond to common issues

Results & what's next

Significantly reduced downtime

Problems are noticed and solved much faster, often before they escalate

Forecasting

Hardware needs can be accurately forecasted

Forensic processes optimised

Necessary recourses can be assigned dynamically based on the demand

What's next?

Automatic remediation, complete infrastructure device coverage

Thank you! Questions?

Nils Kristians Cers

nils.krististians.cers@vp.gov.lv

