



Leibniz Supercomputing Centre
of the Bavarian Academy of Sciences and Humanities



Improving higher education network security
by automating scan result evaluation
with Dr. Portscan

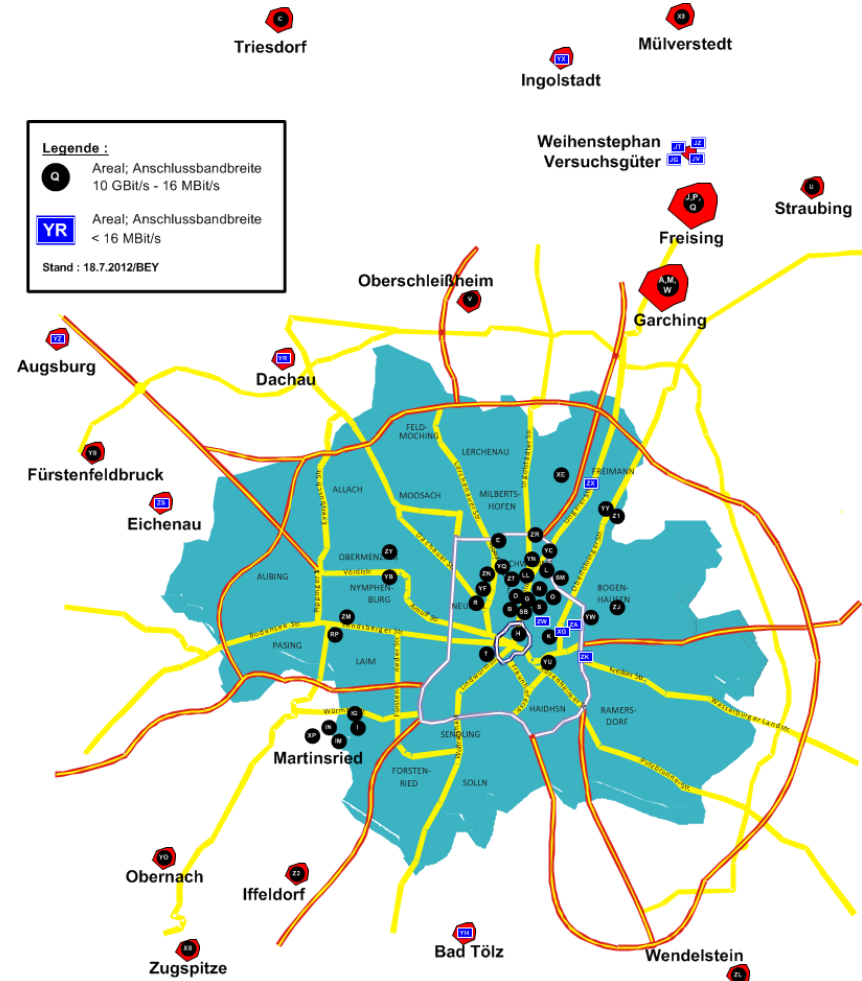
Daniela Pöhn, Felix von Eye, Wolfgang Hommel, and Stefan Metzger

- Motivation
- Current Situation
 - DFN-CERT Net Scanner
 - Internal and External Scanner
 - Experience with Port Scans
- Dr. Portscan
 - Requirements
 - Implementation
 - Operating Mode
- Experiences and Future Work

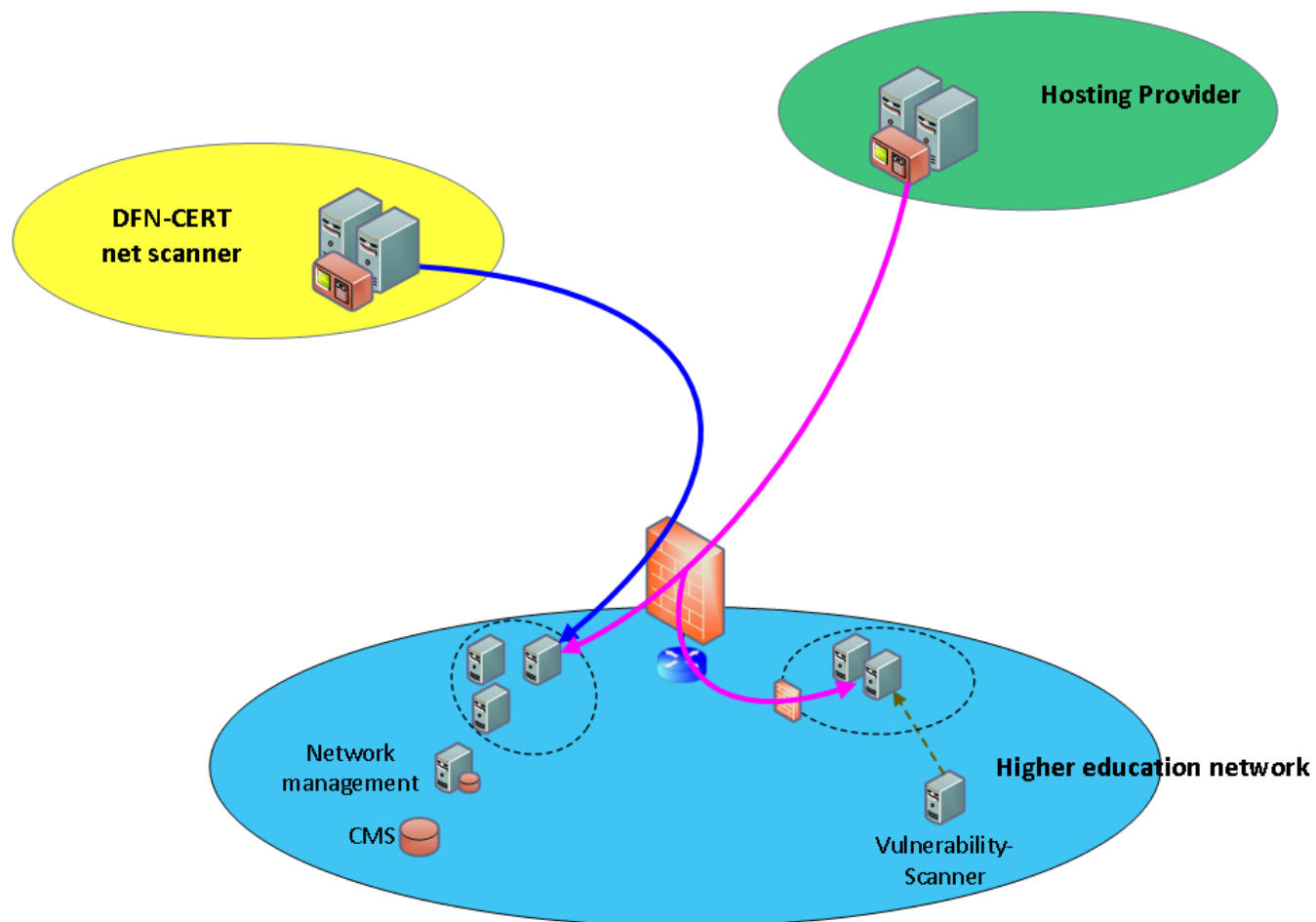
- Approx. 130,000 users
- Approx. 100,000 devices
- More than 500 buildings
- Expansion over Bavaria
- Decentral administration and system responsibility

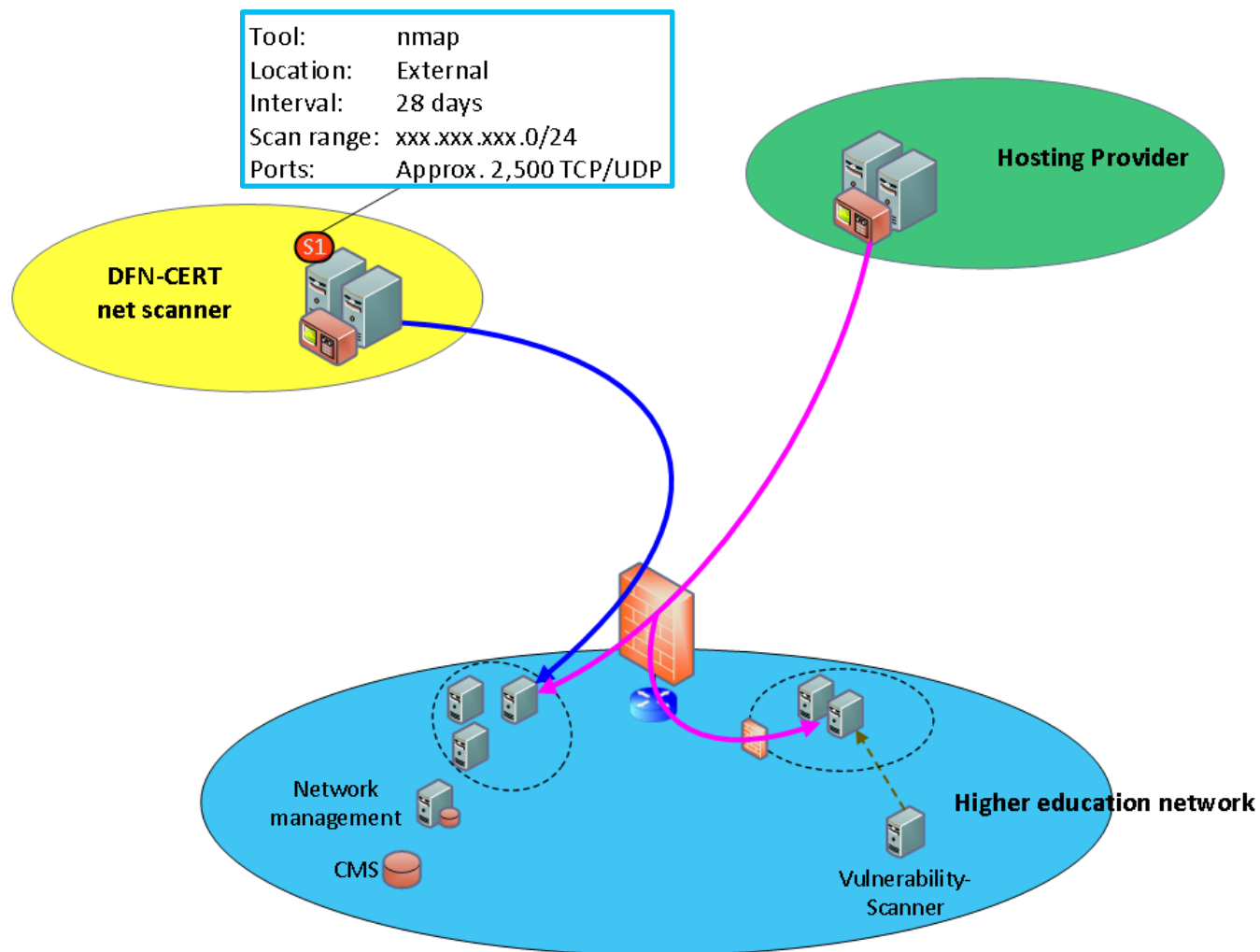
BUT:

LRZ is first contact
for external complaints.

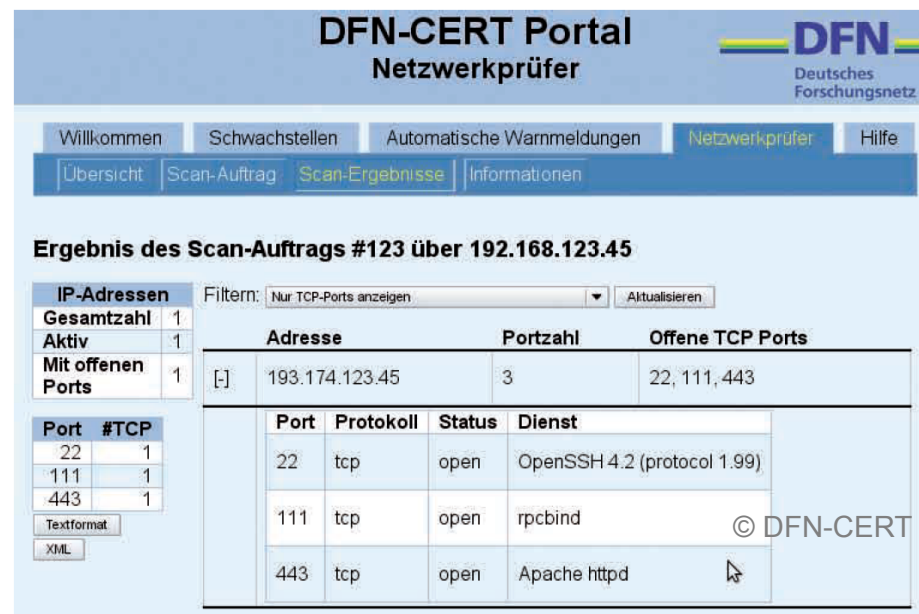


- Port scans as a proactive security measurement.
 - In our scenario we have approx. 1,400 own systems.
 - Simple port scans yield more than 10,000 open ports.
 - Geographical and temporal distribution of port scanners lead to varying results.
- No longer manageable manually!
- Therefore a “*Delta Reporting* port scanning tool” (Dr. Portscan) is required.





- External scan for own net
- Scan interval: 28 days
- Approx. 2,300 TCP and several UDP ports
- Results shown at DFN-CERT portal



DFN-CERT Portal
Netzwerkprüfer

Willkommen | Schwachstellen | Automatische Warnmeldungen | **Netzwerkprüfer** | Hilfe

Übersicht | Scan-Auftrag | **Scan-Ergebnisse** | Informationen

Ergebnis des Scan-Auftrags #123 über 192.168.123.45

IP-Adressen Filtern: Nur TCP-Ports anzeigen Aktualisieren

IP-Adressen	
Gesamtzahl	1
Aktiv	1
Mit offenen Ports	1

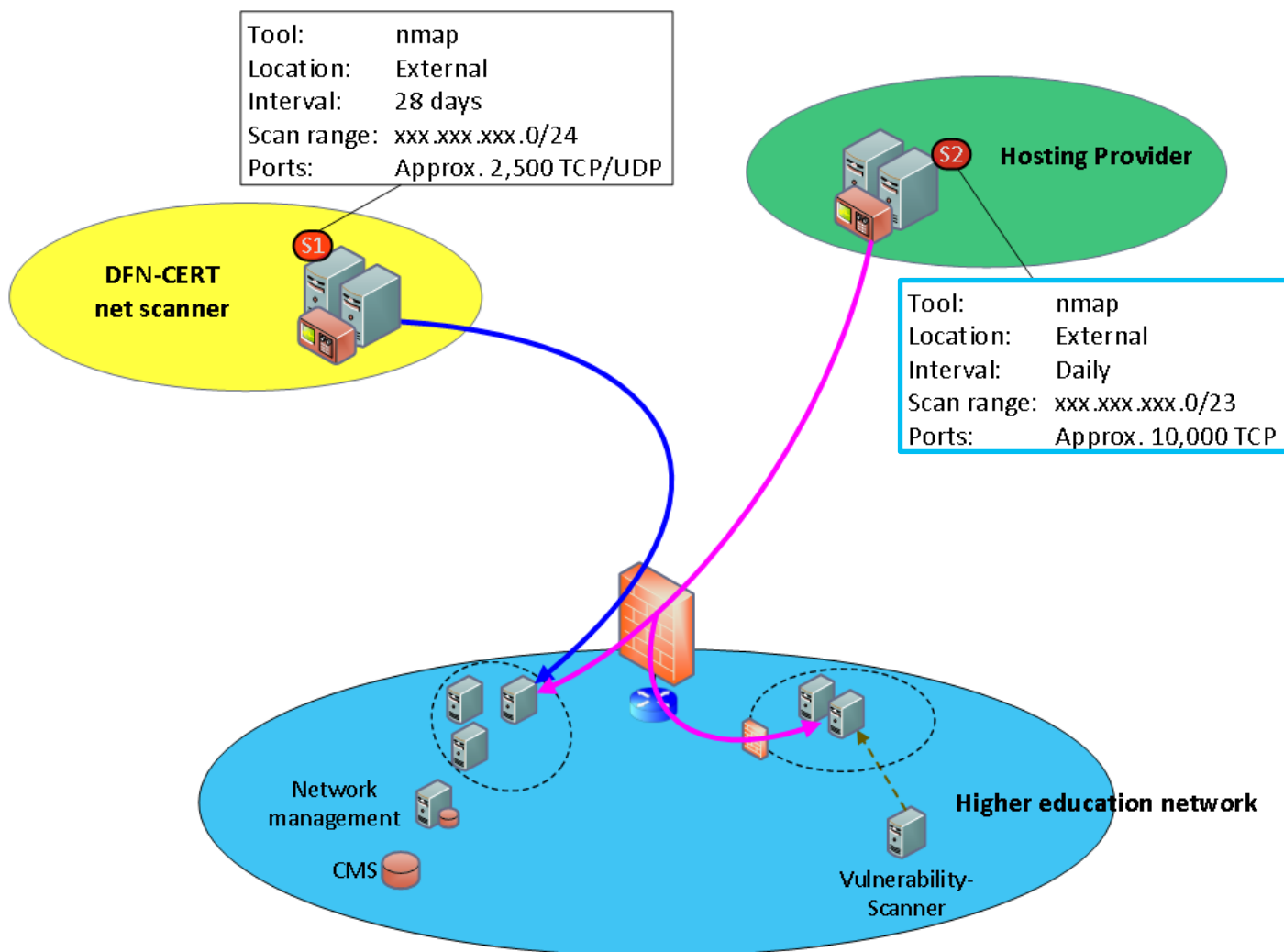
Adresse	Portzahl	Offene TCP Ports
[+] 193.174.123.45	3	22, 111, 443

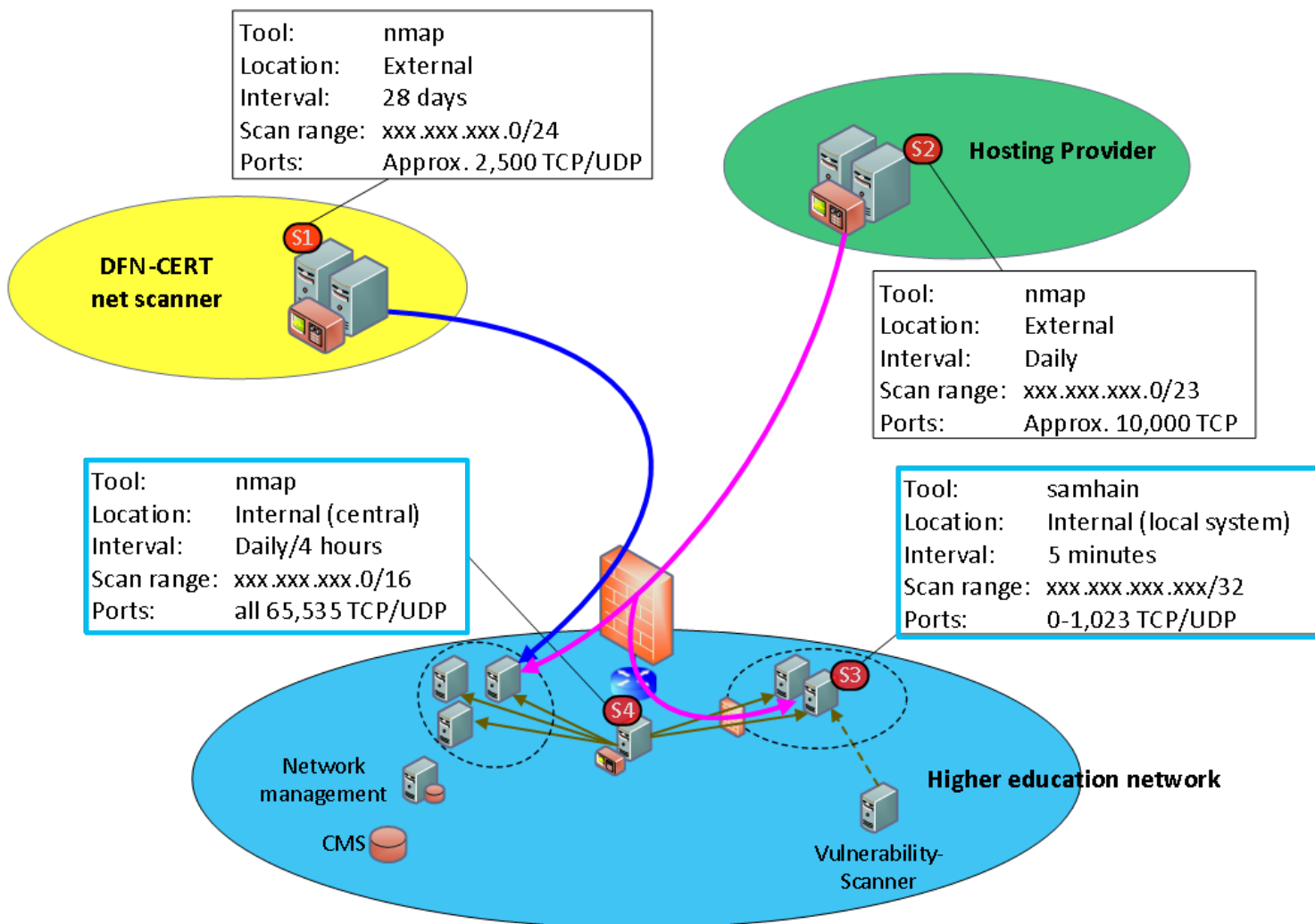
Port	#TCP
22	1
111	1
443	1

Textformat XML

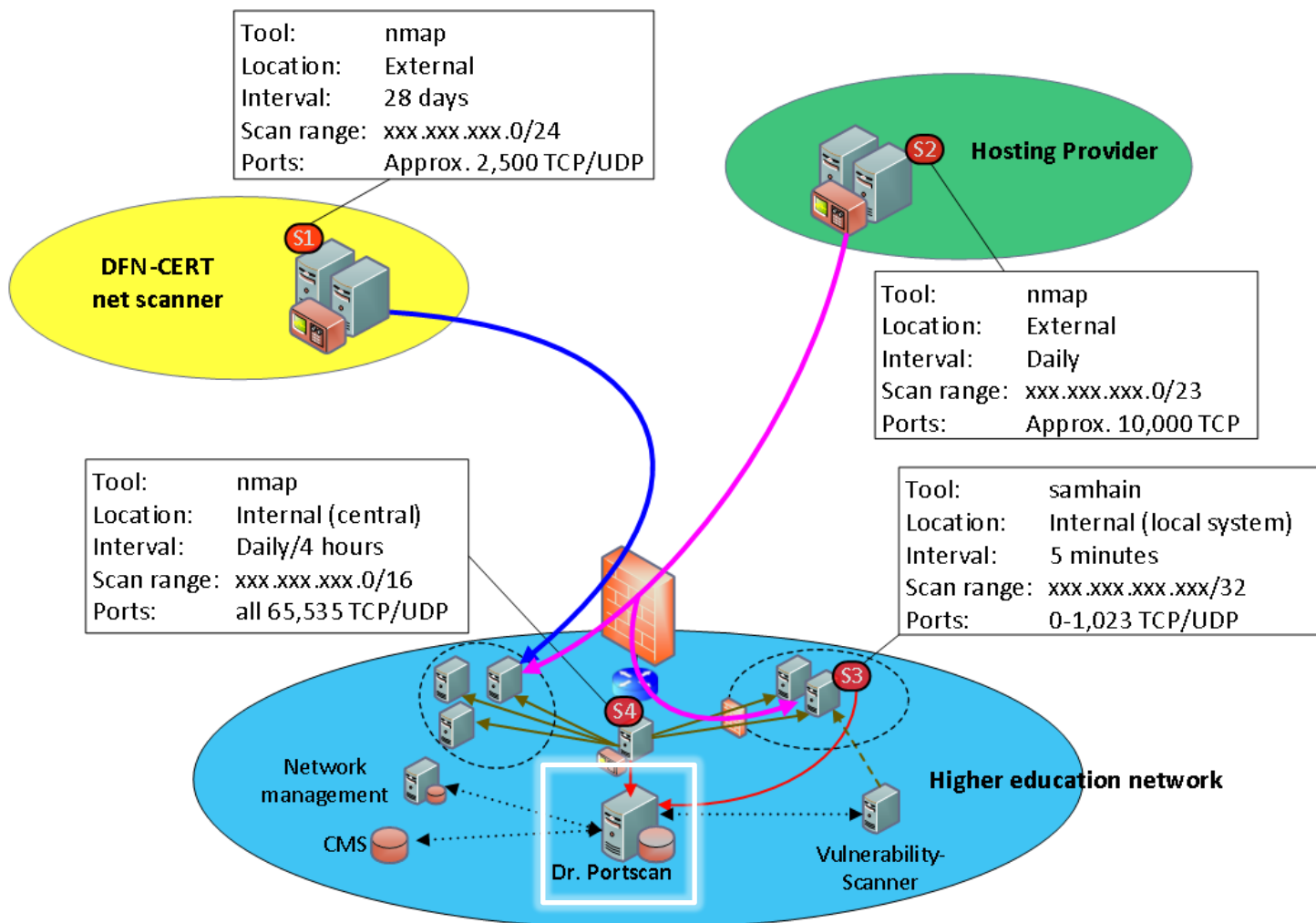
Port	Protokoll	Status	Dienst
22	tcp	open	OpenSSH 4.2 (protocol 1.99)
111	tcp	open	rpcbind
443	tcp	open	Apache httpd

© DFN-CERT





- Variations within results
 - Comparison scan too long ago
 - Different placement of scanner
 - Reliability of scanner
 - Determinism? (e.g., DSL connection)
 - Scanner running on virtual server?
 - Specific services open ports dynamically
 - e.g., CORBA-based services for server (only temporarily)
- Challenge: input with high quality

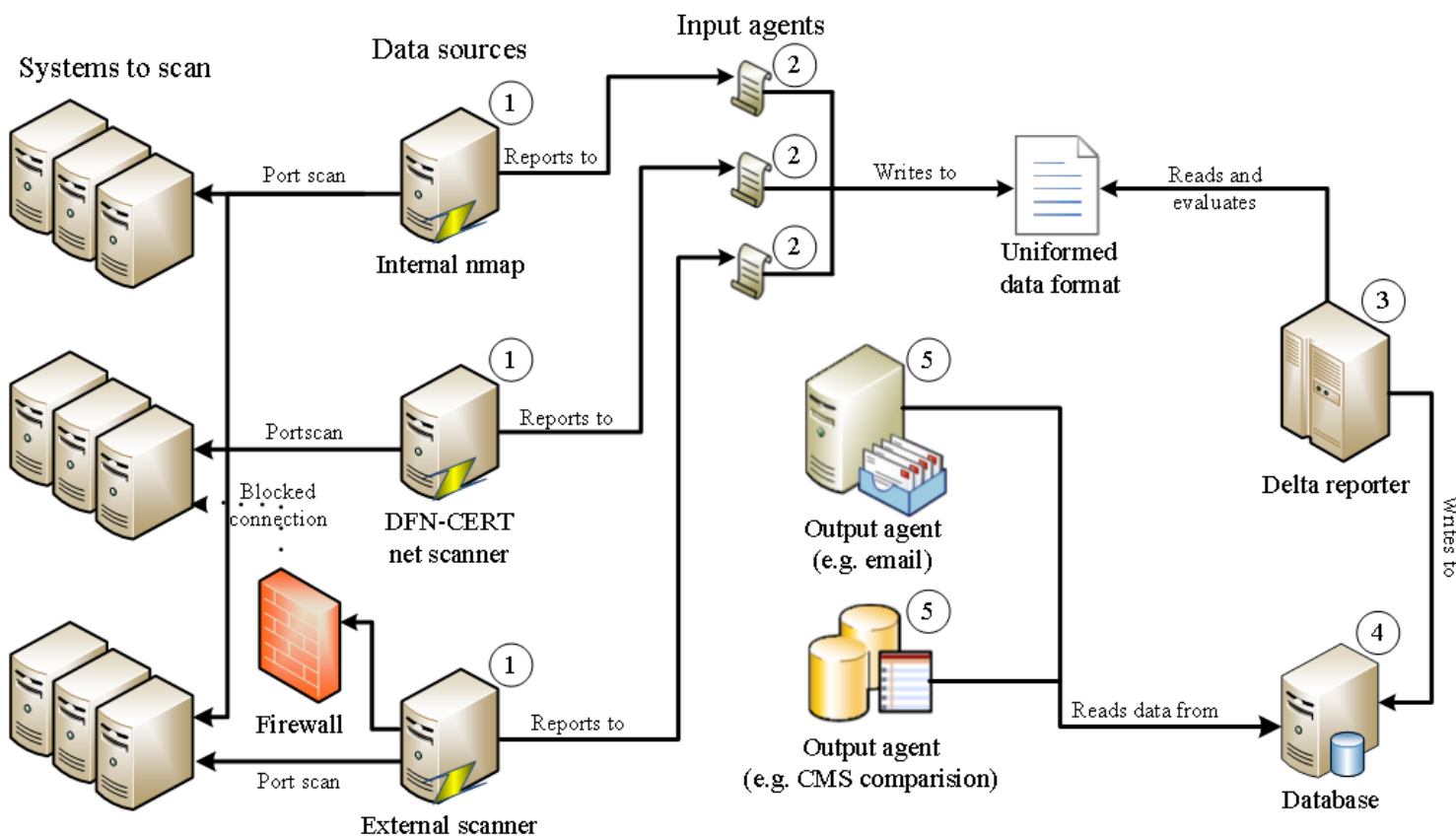


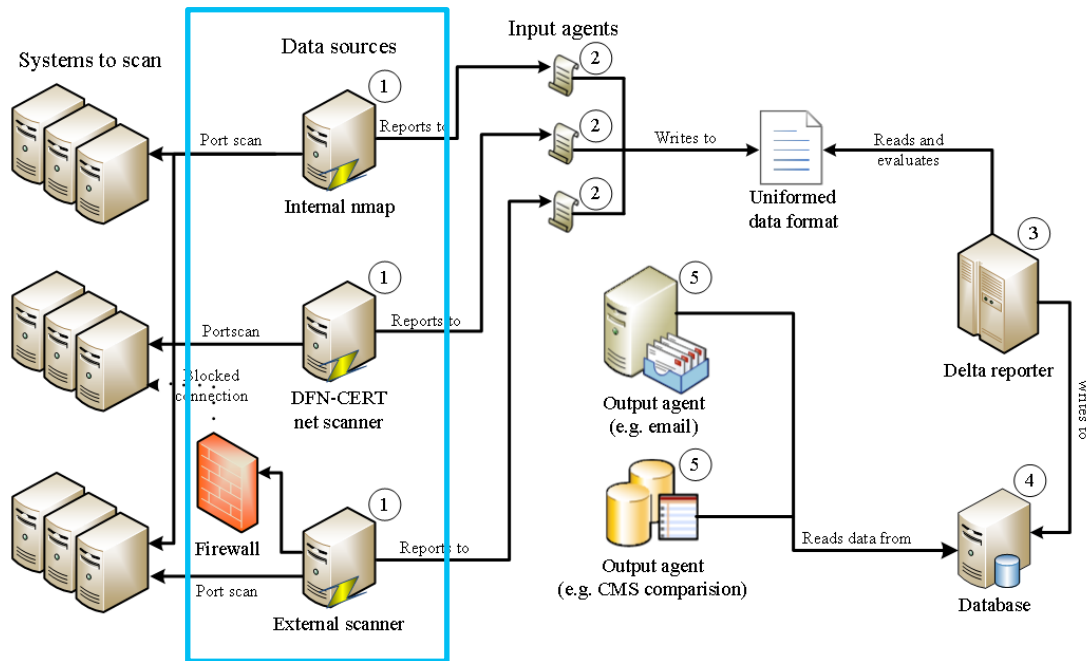
- Support for:
 - Arbitrary amount of port scanner in the net topology
 - Variable time-delayed scans
 - Arbitrary port scanner
 - Overview and *Delta-Reports*
- Focus on modifications:
 - Modifications since the last scan
 - Modifications regarding point of view (internal / external)
- Modular input and export functionality

- Perl-based implementation
- Independent of OS
 - Preconfigured for Linux
- Storage on database with Perl::DBI
 - Perl::DBI supports major database products
 - Preconfigured for SQLite

Newly added features:

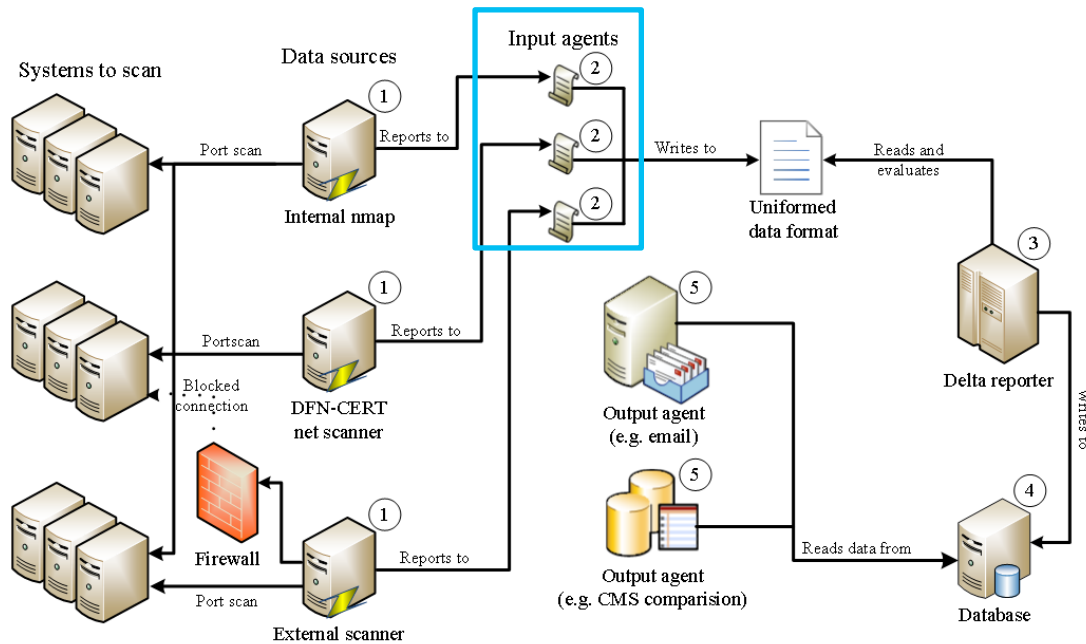
- Multi-client capability
 - Adjustable scan areas
 - Individual reporting
- Web-based and script-based control
- Git repository: <https://git.lrz.de/?p=DrPortScan.git>
- Please test and give us feedback!





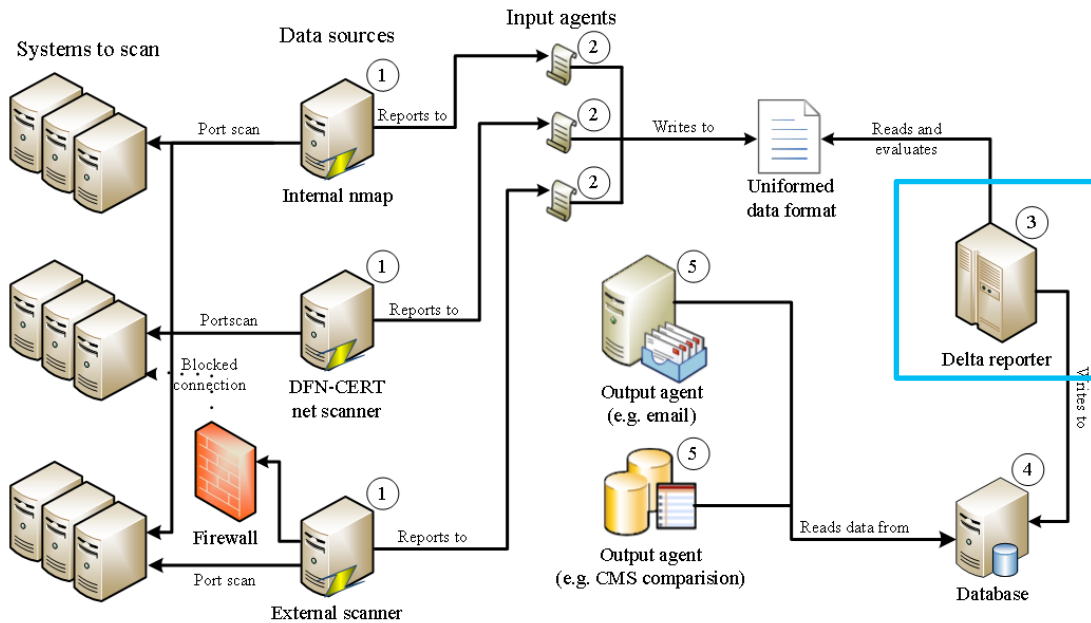
Data sources:

- External scanner
 - DFN-CERT net scanner
 - nmap
- Internal scanner
 - Samhain
 - nmap



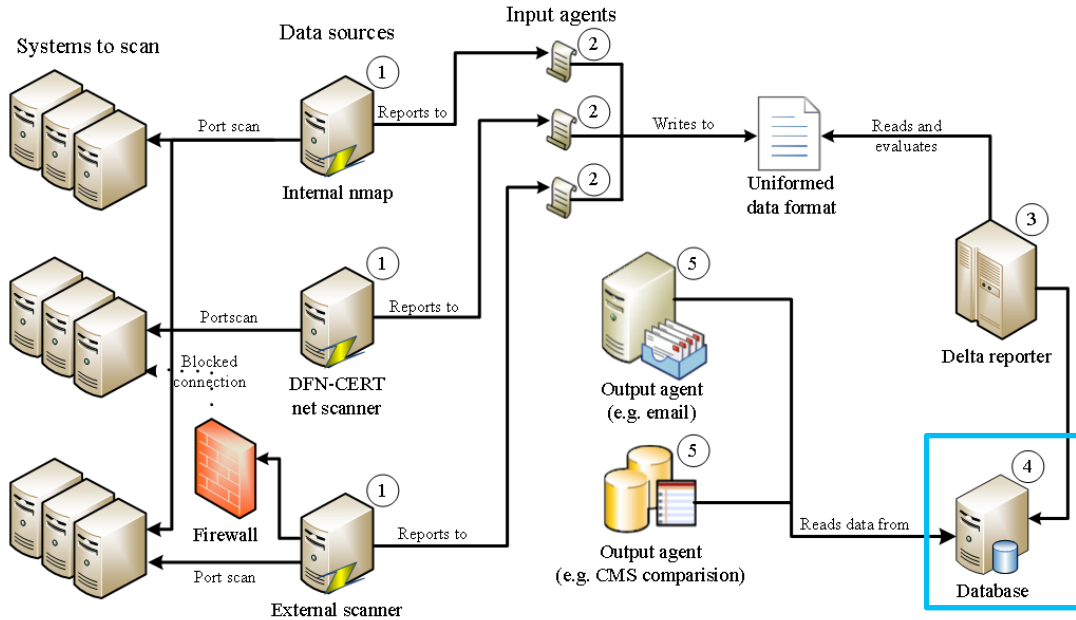
Input agents:

- Transfer results to the central Dr. Portscan instance
- Convert to a uniformed data format
 - IP address
 - Port and protocol
 - Timestamp



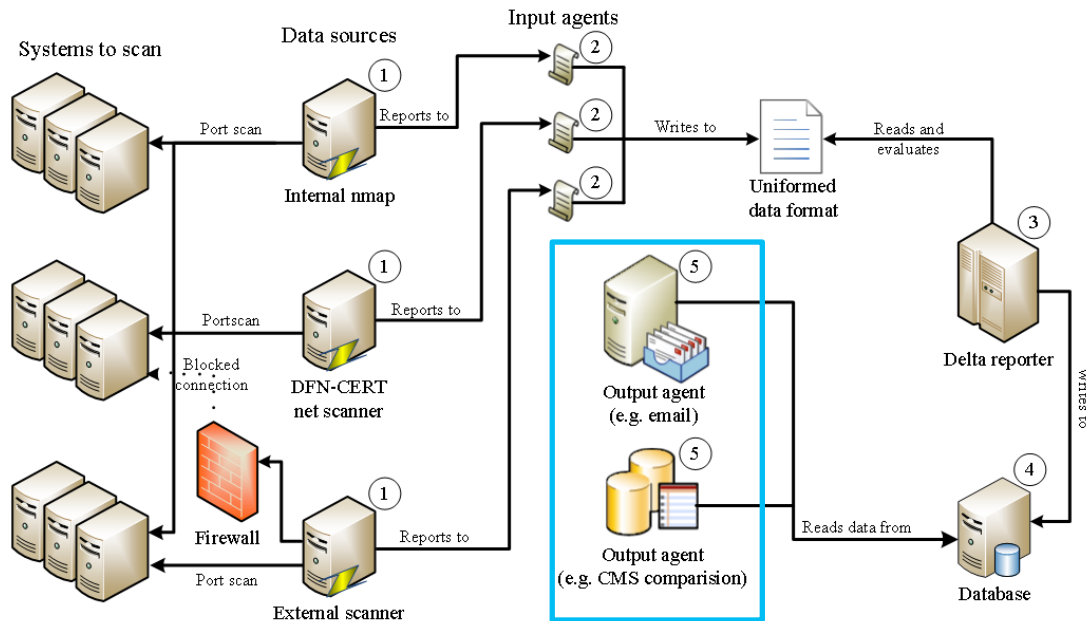
Results of the **Delta Reporter**:

- No change
- New system (IP address seen for the first time)
- System does not run anymore
- Change of DNS name
- Newly opened port
- Port closed
- Port re-opened



Central Database:

- Flexibility through the use of Perl :: DBI
- SQLite preconfigured
- „History“ available in part
- Only one entry per port
- Cleanup



Output agents:

Output is available via

- Text
- Mail
- Database access
- Scripts can be triggered (e.g., for detection of open resolvers for open DNS ports)

- Adjustable scan areas
- Individual reporting
- Web based control

The screenshot displays the Dr. Portscan web interface. On the left is a dark sidebar with the title 'Dr. Portscan' and a menu containing 'Configuration:' (with sub-items 'Scans' and 'Reporting'), 'Administration:' (with sub-item 'Network area'), 'Reporting:' (with sub-item 'Overview'), 'My account' (with a user icon), and 'Logout' (with an 'X' icon). The main content area is titled 'Configuration - Scans' with the subtitle 'Configuration internal and external port scans'. It features a section for 'Internal port scan' with the following options: 'Scan status' (radio buttons for 'active' and 'paused', with 'paused' selected), 'Network areas to scan' (a large text input field), 'TCP ports to scan (if empty 1-1024):' (a large text input field), 'UDP ports to scan (if empty no ports):' (a large text input field), 'Scan aggression::' (radio buttons for 'aggressive', 'normal', and 'slow', with 'normal' selected), 'Preferred scan time:' (a text input field containing '18:00'), and 'Scan days:' (checkboxes for 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Sun', all of which are checked). A 'Save' button is located at the bottom of the configuration area.

- Started operating ½ year ago
- DMZ and server nets scanned on daily bases
- Positive feedback
 - Detection of new systems
 - Detection of changed ports
- Minimal effort needed for configuration
 - Could be done by clients via web frontend

- Integration in SIEM solutions
- IPv6: Automatic detection of systems to be scanned
- More vulnerability scans

Sourcecode available:

<https://git.lrz.de/?p=DrPortScan.git>

or

```
git clone git://git.lrz.de/DrPortScan.git
```

Contact:

Daniela Pöhn

poehn@lrz.de

Felix von Eye

voneye@lrz.de