

Firewall management in Tatra banka, a.s.



Why?

Essential purposes

Network system complexity (more than 18 000 devices in network).

Number of rules between firewalls (in hundred thousands).

Lot of changes (tenths per months).

Missing security threads monitoring on existing FW settings.

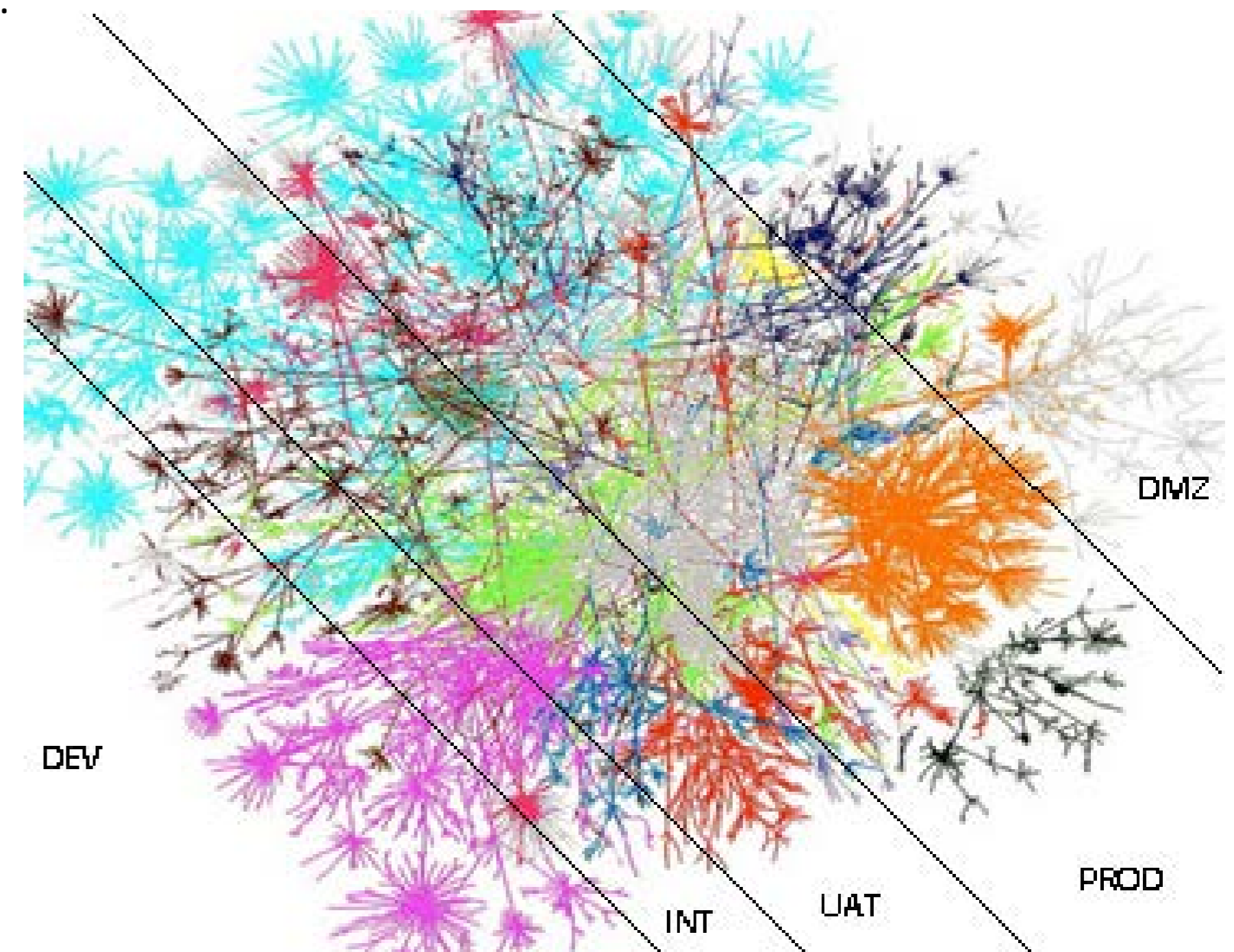
Security standard requirements (PCI DSS and GNSP).

IN TB, We have 10 important FW + 1 between RPC a TB.

Aproximatelly half a milion important rules.

Everything is managed only in excel files.

Regular vulnerability scan producing a lot of information



What we are looked for?

- Network model
- Firewall analysis
- Rule Lifecycle
- Vulnerability analysis
- Analysis of attack surface
- Prioritize response
- Tracking remediation

- Monitor compliance

What We have?

Firewall management

- Skybox on all main firewalls

- Firewall change management

 - It is only one possible way, how to change Firewall settings in TB

- Ability to immediately analyze possible network access

- Firewall configuration optimization

 - automatic identification of shadowed, redundant rules, unsupported changes

- Risk based process for documented firewall changes

- Automatic detection of devices accessible from internet (custom)

- Automatic detection of new services on devices accessible from internet (custom)

Vulnerability management

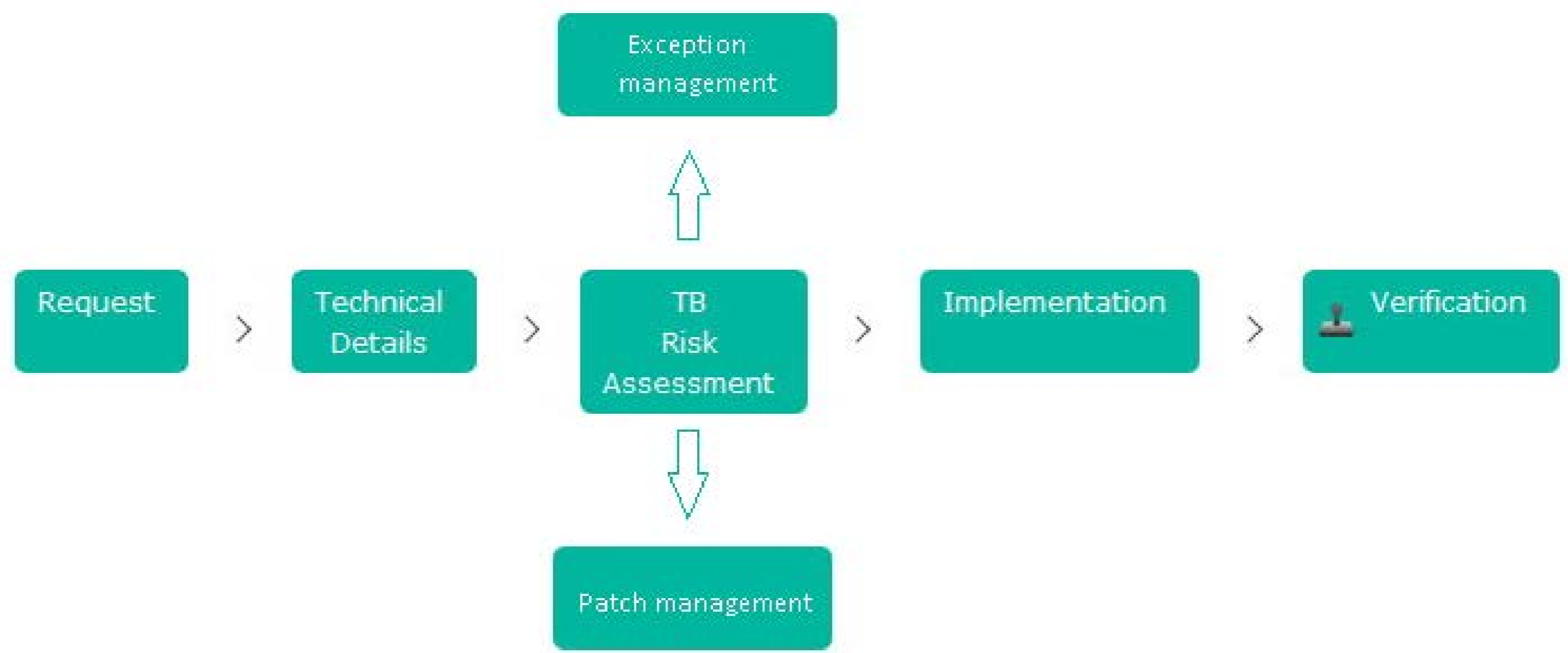
- All vulnerability data in one view

- Identification of vulnerabilities

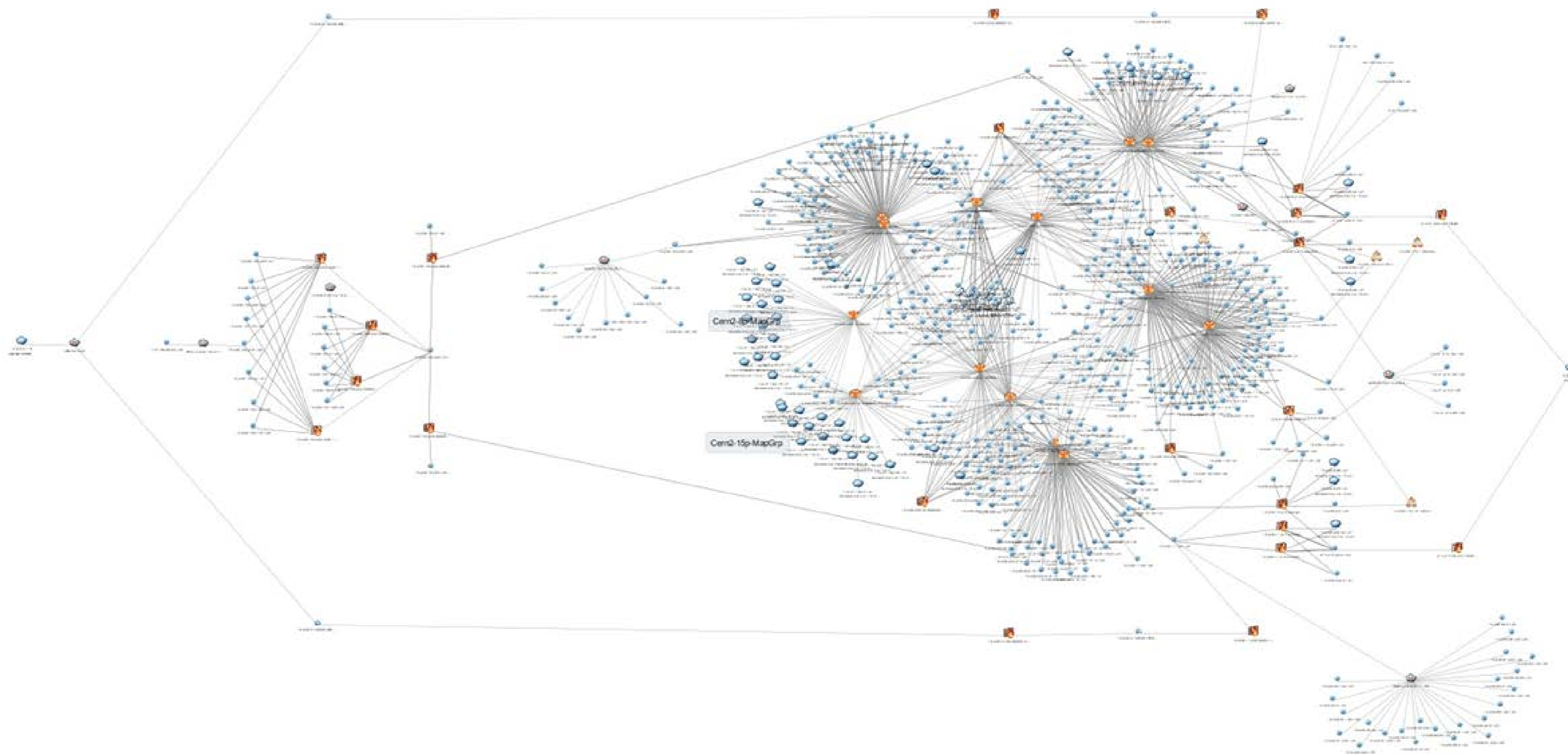
- Prioritization of vulnerabilities

- Notification of new exposed vulnerability to attacker/internet

Processes for FW rule change - TB



Online network topology



Example of access path analysis from internet

The screenshot displays the Skybox - Access Analyzer interface. On the left, the 'Access Query' panel is configured with Source: 0.0.0.0/0 - Internet and Destination: Any. The 'Analysis Results' panel shows a tree view of accessible destinations, including Europe, Paris, developmentWindowsWS, developmentUnixWS, developmentServers, and US. The 'Routes' panel shows a path from Internet (cloud) to developmentServers (192.170.19.0/24) through several steps: Internet (cloud), main_FW (16.0.0.1), Main Router (192.169.1.2), Internal Router (192.170.8.2), dev FW (192.170.1.1), and Dev_L3 Switch (192.170.1.18). The 'Network Map' panel on the right shows a detailed network topology with nodes for Lab, Los Angeles, US, Paris, AWS, New York, Europe, London, and Branches. Red arrows point to specific elements in the interface: the Source field, the Analysis Results tree, the 'Show Routing Rules' checkbox, and the 'Access Route' section.

#	Step	Inbound Access Rules	Outbound Access Rules
	Source:		
	Internet (cloud)		
	source IP range(s) 16.0.0.0-16.0.0.0, 16.0.0.2-16.255.255.255		
	Sending To IP Range(s): 192.170.19.0-192.170.19.255		
	sending to Service(s): 21/TCP		
1.	main_FW (16.0.0.1)	8 (ACCESS) - Allow	
2.	Main Router (192.169.1.2)		
3.	Internal Router (192.170.8.2)		
4.	dev FW (192.170.1.1)	4 (ACCESS) - Allow	
5.	Dev_L3 Switch (192.170.1.18)		
	Destination:		
	developmentServers (192.170.19.0/24)		
	destination IP range(s): 192.170.19.0-192.170.19.255		
	destination service(s): 21/TCP		

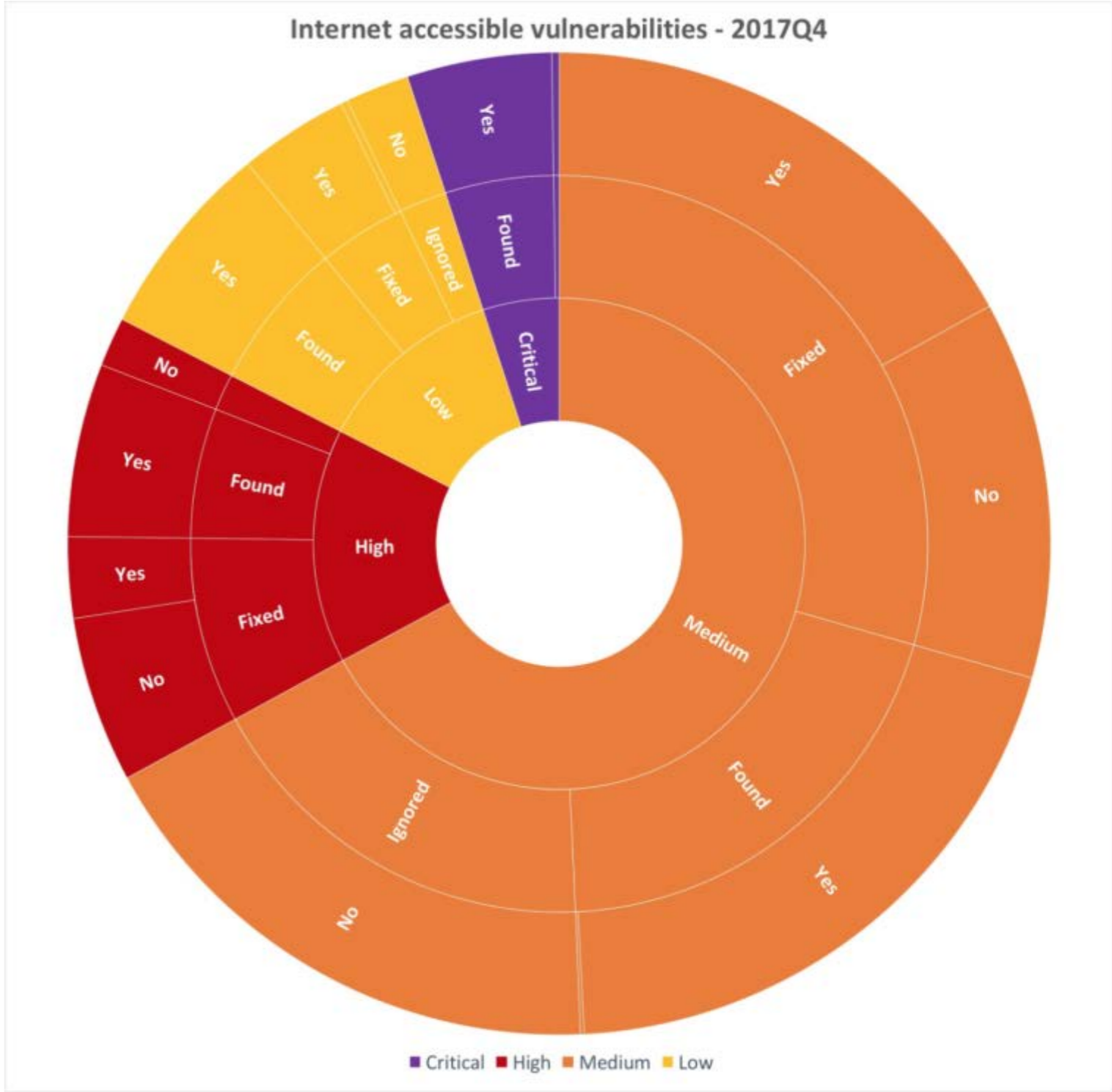
Main Advantages

- Network administrator & IT Security has possibility to **analyze real network paths**.
- IT admins, ITPM, PM requests network change by workflow with **standard approval process**.
- All **exceptions are registered** in standard manner.
- IT Security can monitor **actual setup** and implementation of new requests.
- It is possible to **find** most dangerous **vulnerabilities** and linked them with all TB environments.
- Vulnerabilities are **prioritized** in seconds.

Main KPI

Status of implementation
servers accessible from internet are fully covered.
Plan Q1/2018
CNI (RI network)

Graph
Inner circle – severity of vulnerability
Middle circle – status of implementation
Outer circle – vulnerability handling by SD ticket







Ďakujem za pozornosť

Ing. Ján Václavík

Tatra banka, a.s.

