CESNET Monitoring & Security Infrastructure

Monitoring

- CESNET Monitoring & Security
- Data storage & analysis
- Alert processing
- Protection

**CESNET2 network**

**Monitoring probes**
- *Deployment on all perimeter links (complete visibility of internal traffic)*
- *Based on our in-house developed 10Gbps network cards with FPGA for hardware acceleration.*
- *L7-extended flow monitoring*
- *Full speed (up to 100Gbps)*
- *NetFlow collector and analyzer.
- *FTAS (Flow Traffic Analysis System)*
- *IPFIX output protocols*
- *SecurityCloud – Scalable flow data collector:* Fast queries thanks to distributed data storage. Allows data search via a modern GUI.
- *NOC (Network Operations Center)*
- *Service desk*  
- *CertS (Czech Computer Security Watchdog)*  
- *Antispam gateway*  
- *Protection*  
- *Alerts*  
- *Wardegn – Simple alert-sharing system:*  
- *NERD (Advanced IP reputation database):* A record for each known malicious IP address.
- *Sharing with other NRENs* (example: PROTECTIVE, see another poster)
- *Other alert sources* (examples for another network, Intelsat, Shadowserver, ..)

**Data storage & analysis**

- *NEMEA (IDS) – Modular IDS system for real-time analysis of flow data.*  
- *Passive DNS – Keeps history of DNS resolutions made by our main DNS server.*  
- *SecurityCloud – Stores and processes IDEA messages from Warden.*  

**Alert processing**

- *Wardegn – Simple alert-sharing system:*  
- *NERD (Advanced IP reputation database):* A record for each known malicious IP address.
- *Sharing with other NRENs* (example: PROTECTIVE, see another poster)
- *Other alert sources* (examples for another network, Intelsat, Shadowserver, ..)

**Protection**

- *Antispam gateway*  
- *Rate-limiting of some protocols*
- *DDoS Protector*  
- *RTBH (Remote Traffic Handling System):***Unwanted traffic can be routed to the backbone.*
- *Ad-hoc traffic filtering*  
- *Bots and Honeypots as a Service (HAAS):***Preconfigured VMs with various honeypots.*
- *CertS (Czech Computer Security Watchdog):***A record for each known malicious IP address.*  
- *Wardegn – Simple alert-sharing system:*  
- *NERD (Advanced IP reputation database):* A record for each known malicious IP address.