interView
Network Solutions

Sharkmon – feature & functions

Topic	**Description**
Plattform	• OS – Container
	• Cloud (3 versions depending on required functionality)
	• OnPremise
Access	• Web based Application • Multi User Platform • Per Web Browser (pref. GoogleChrome/Firefox)
Architecture	• Single instance (distributed agent in progress)
Data processing	• Network packets – PCAP Files • split files, trim packets, de-duplicate, merge, filter (shark-display filter)
Data sources / Import	• PCAP bulk upload (drag&drop) • PCAP FTP Stream • Capture Appliance (API access)
Data Volume	• Pcap File size up to 10GB • Up to 5.000 files • Data history – for 2 years • 1 secund data history on demand / byRequest
Data Org	• Scenarios (data sources) • Profiles (metrics and aggregations) • Pcap Files
Analysis Org	• **Categories** (alignment of metrics to **Network** / **Connection**/ **Application**)
Analysis sides	• **Single side** (single scenario)

	• **Multi side** (multiple scenario - correlation) – allowing overlay of multiple perspective / views on single analysis
Analysis functions	• **Symptoms (critical /warnings)** - Each metric for each aggregation (see below) can compared against 2 thresholds
Metrics	• Each wireshark protocol / field: up to 200.000 metrics • User can define or request from INS metric / profiles for any field
Metric Value aggregation	• COUNT • MAX, AVG, MIN, SUM • DEVIATION • %PERCENT
Metric features	• Web Response Analysis • Per metric - Timing analysis • More on demand / in progress
Data dashboards	• **Scenario overview** – top Dashboard, longtime chart (only symptoms, only categories min. 5 minute- data) • **Scenario view -** one / multiple scenario, longtime Chart – symptoms and/or raw data) • **Insight view** – single pcap file, max 4 hours duration, min. 1 secund granularity, all fields, categories, per-file analysis (timing)
Data Export	• **Symptoms (critical / warning)** – per metric - CSV Export • **Single file Metrics –** raw data metric CSV Export • **Data export to SLIC (symptoms / Raw Values)**
Reporting	• **In combination with SLIC –** KPI dashboard, history reporting – aggregation / correlation with other datasources like network/ System devices, cloud metrics etc.