With **InterTrace** user can define precise what to search and monitor in network packets.

Run your deep packet analytics – as a constant monitoring process, send alerts, reduce MTTR.

Interview
Network Solutions

InterTrace

Be precise!
Monitor YOUR data – with YOUR metrics !

CONTACT US
INFO@INTERVIEWNS.DE
WWW.INTERVIEWNS.DE

WHY INTERTRACE ?

Tcpdump and wireshark are widely used and even part of operating systems to create highly valuable PCAP files used for incident analysis.

- Setup of such capture tasks is done in seconds - but the analysis of single files can take hours or days -
- **how to view content data of many files** - covering hours, days or weeks - with your required deep data ?

With **InterTrace** user

- can run deep content analytics
- do longtime monitoring
- send alerts

THE PROCESS

- **continous -** Import PCAP files for hours, days, months - or direct stream
- **precise** - Define and apply custom metrics and thresholds in scenario-related profiles
- **comprehensive -** evaluate scenario-data in long-and short-time dashboards, covering seconds, hours, days, months
- **participate -** forward packe-alerts into event management systems

TRACE MONITORING

MONITOR

Monitor what you want !!!
efine any metric based on packet content

LONG TIME STATS

understand cause and effect , graphical comparison, older and newer status

ICIDENT RECOGNITION

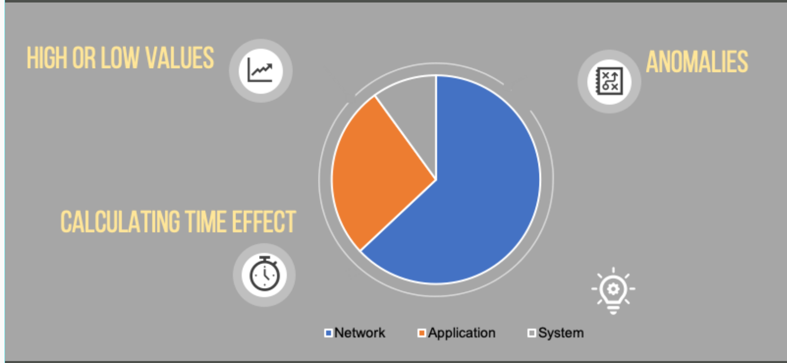
Define alerts by your own

INCIDENT CORRELATIOI

(http.time exception and cpu lo

THE RESULT

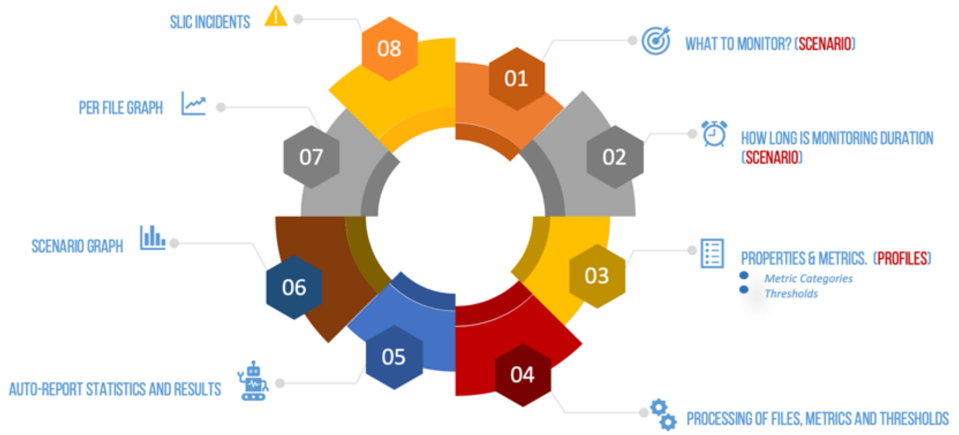
InterTrace can contain up to 100.000s of metrics, organised in categories.
Values are compared against thresholds, to measure deviations of timing, absolute values



Usually just a few metrics are used to validate a service - a web-service needs web metrics, LDAP or SMB use their own metrics.
In InterTrace you can define the analysis scenarios precisely - the objects, the services, the protcols and metrics and its values, for hours, days, weeks, months.

User can define the whole process of pcap monitoring in a single stack

- the "what", the object, a service
- the duration (hours, days, weeks)
- the metrics and conditions and
- the alerting



SLIC INCIDENTS

08

01

WHAT TO MONITOR? (SCENARIO)

PER FILE GRAPH

07

02

HOW LONG IS MONITORING DURATION (SCENARIO)

SCENARIO GRAPH

06

03

PROPERTIES & METRICS. (PROFILES)

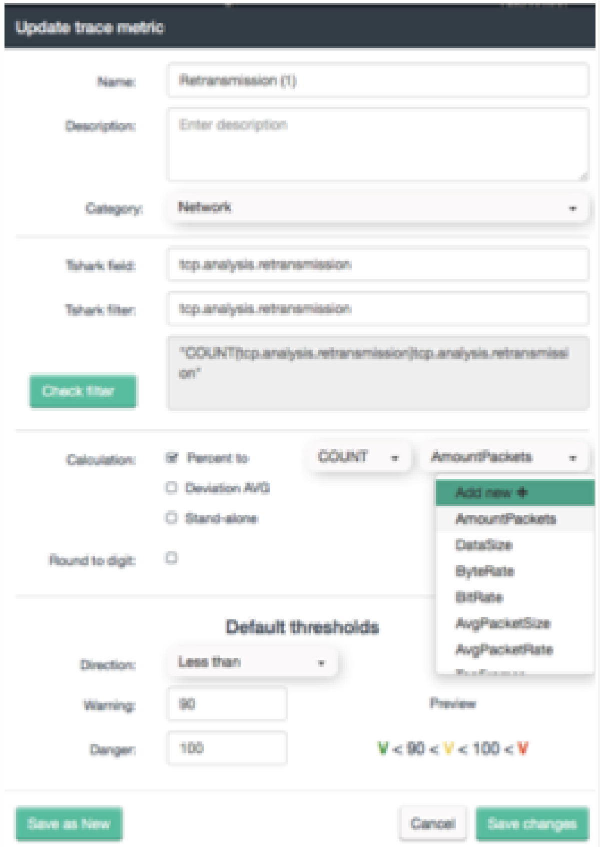
- *Metric Categories*
- *Thresholds*

05

04

AUTO-REPORT STATISTICS AND RESULTS

PROCESSING OF FILES, METRICS AND THRESHOLDS



Update trace metric

Name:	Retransmission (1)
Description:	Enter description
Category:	Network
Tshark field:	tcp.analysis.retransmission
Tshark filter:	tcp.analysis.retransmission
	"COUNT(tcp.analysis.retransmission)tcp.analysis.retransmission"

Check filter

Calculation: ☑ Percent to COUNT AmountPackets

○ Deviation AVG

○ Stand-alone

Round to digit: □

Default thresholds

Direction:	Less than
Warning:	90
Danger:	100

Preview

V < 90 < V < 100 < V

InterTrace user can use Wireshark display filter, same syntax, same counter types. InterTrace does import raw values of defined metrics and compares them against

- a fixed threshold or
- a percent (can be any packet type , eg. retransmissions can be percent of generic packets, or IP Packets, or TCP packets, or HTTP packets or "http.returncode=500"-Packets) packets or
- infile-average - calculating the standard deviation in a single pcap file

Based on results **alerts** are defined in 2 levels - **critical** or **warning**. Intertrace allows defintion of such alert conditions for each single service separate.

Dynamic Alert

Response thresholds time of 2 seconds can be for "service A" a good value – but for another "service B" a disaster. Alerts should be configurable for each individual service !Inter/trace does support such individual thresholds. All scenarios can share same profiles - or each can use a different with same metrics and other thresholds. Additional you can define a metric linked to a certain ID like an IP address or host and set thresholds there. Thresholds can be defined in 2 levels – critical – or warning.

Scenario dashboards show the packet values from secunds to months or years

User can decide to watch

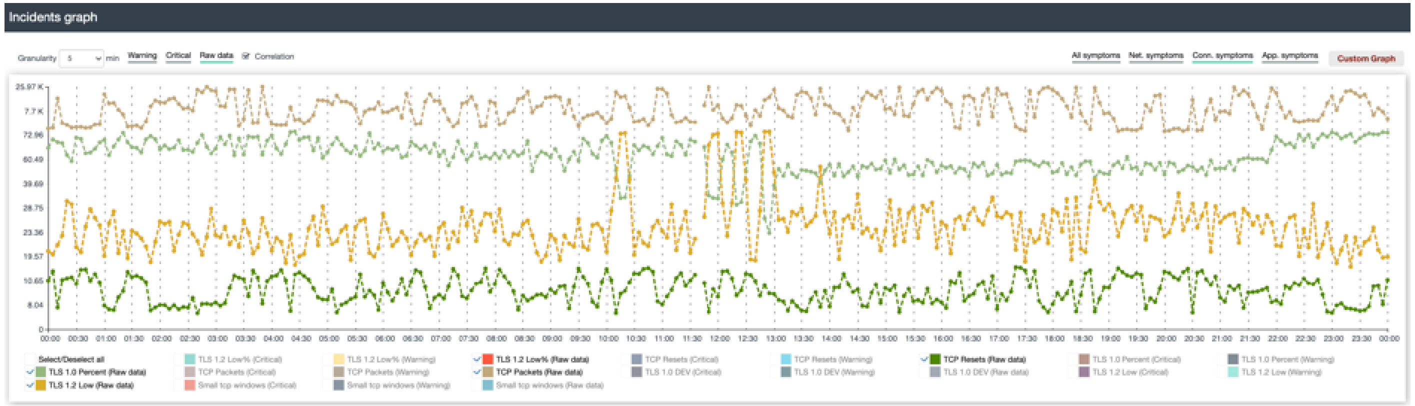
- symptoms or
- alerts or
- RAW values or
- altogether

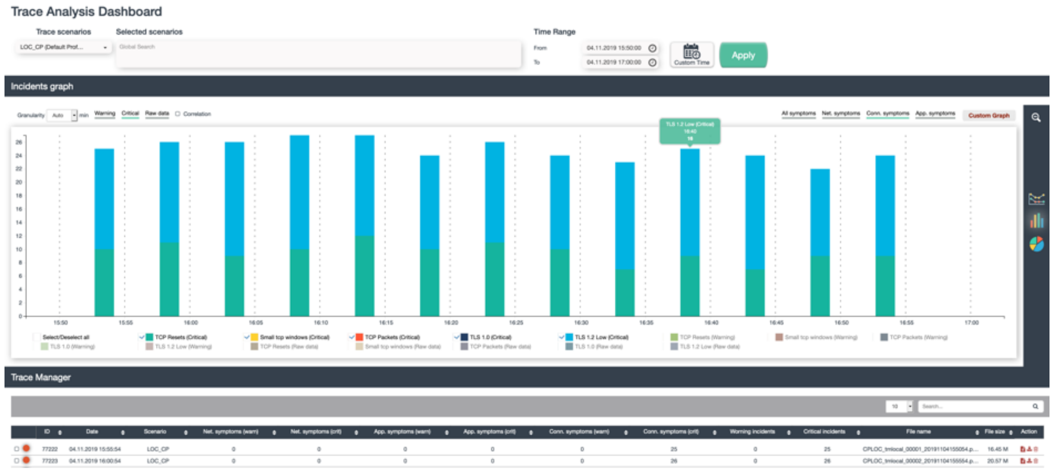
Metrics are organised in categories

- Network , connection - or application metrics - so user can easy address the responsible people.

User can easy identify which metrics do correlate, even if totally different metrics, like TLS packets and TCP Reset rate.

A logarithmic graph allows the usefull graphical comparison of larger counters like packets in millions and tiny like response times in milliseconds





	ID	Date	Scenario	Net. symptoms (warn)	Net. symptoms (crit)	App. symptoms (warn)	App. symptoms (crit)	Conn. symptoms (warn)	Conn. symptoms (crit)	Warning incidents	Critical incidents	File name	File size	Action
□ ●	77222	04.11.2019 15:55:54	LOC_CP	0	0	0	0	0	25	0	25	CPLOC_tmlocal_00001_20191104155054.p...	16.45 M	
□ ●	77223	04.11.2019 16:00:54	LOC_CP	0	0	0	0	0	26	0	26	CPLOC_tmlocal_00002_20191104155554.p...	20.57 M	

The scenario overview represents just incidents or alerts -- it is the longtime dashboard for multiple services consisting of toally different counters, metrics, defintion - but all share same methods of evaluation - the incident.

This dashboard allows to compare critical states of the load of a network, high RTO, DNS time, http responsetime or the number of TLS1.0 sessions, or data from industrial Ethernet, custom application etc.- what ever found in a packet can be a metric and defined as normal, warning or critical.

InterTrace is part of **InterView** Service Incident Monitoring

We are working on data integration - capture appliances, PCAP Files, Application Monitoring, NAPM, Netflow, Support tickets - from many different vendors - to display the state of a IT services and its elements.

visit us at   www.interviewns.de