SharkMon

Be precise!

Monitor YOUR data – with YOUR metrics !

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

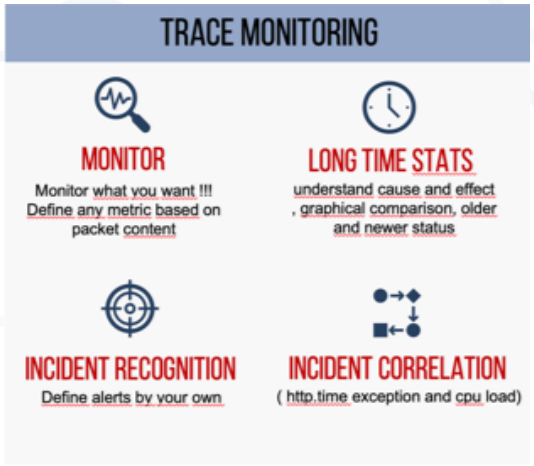
Run your deep packet analytics – as a constant monitoring process, send alerts, reduce MTTR.

interView
Network Solutions

Why SharkMon ?

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 SharkMon user

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

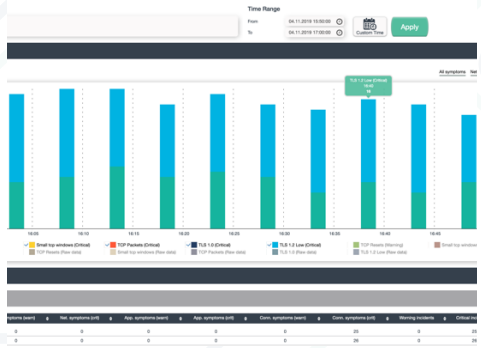
The Process

- **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 shorttime dashboards, covering seconds, hours, days, months
- **participate** - foward packealerts into event management systems

The Result

SharkMon 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.



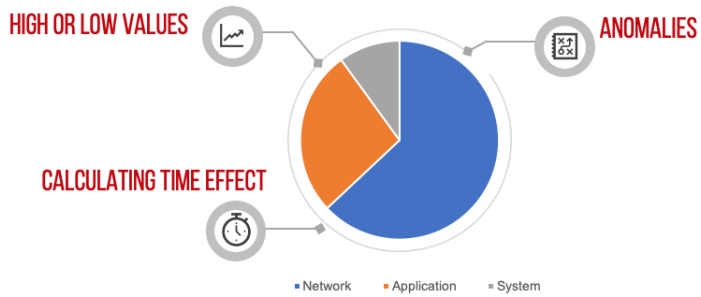
User can define the whole process of pcap monitoring in a single stack

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

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.



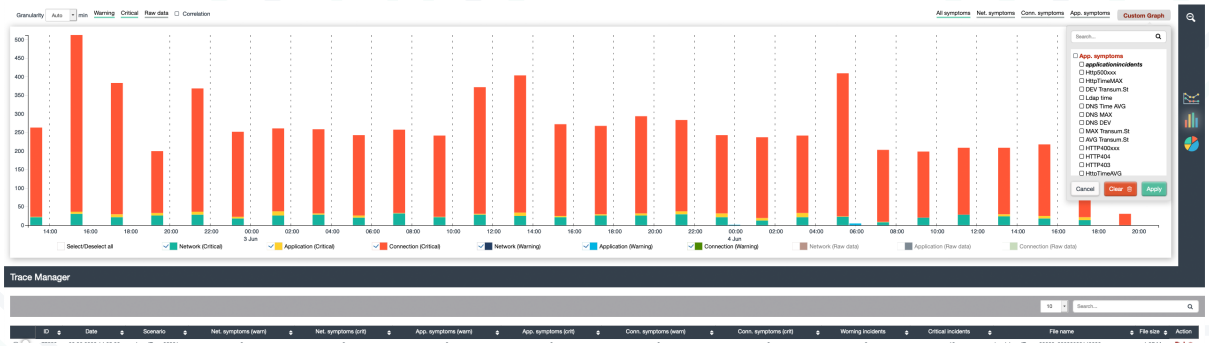
Scenario dashboards show the packet values from secunds
to months or years
User can decide to watch

- 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.



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.

SharkMon 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