## Wer ist (und was tut) Synapse Networks GmbH ?

**Synapse Networks** entwickeln Experten-Systeme zur LAN-Analyse seit 1996. Kunden werden mit Hilfe unserer Software in die Lage versetzt, hoch automatisiert mittels Deep Packet Inspection sowohl technische Fehler sowie Sicherheitsgefahren und Anomalien zu erkennen.

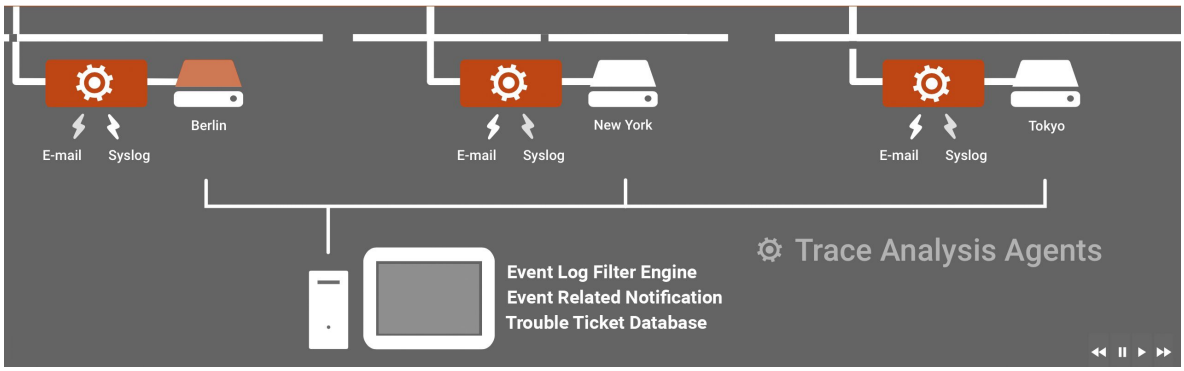
Die Technik ist non-invasiv (keine aktiven Komponenten im Kunden-Netzwerk) und entspricht daher allen Erfordernissen der Sicherheit (kann nicht selbst Teil des Problems werden); sie ist als Software-Lösung in kürzester Zeit einrüstbar, auch durch Fernwartung.

Analyse-Agenten überwachen den Datenverkehr und melden auffällige Ereignisse und Anomalien an eine oder mehrere Zentral-Konsolen, wo die Meldungen gefiltert, priorisiert und ggf automatisch weiter geleitet werden zwecks schnellster Reaktion.

## Qualitätssicherung per Fernwartung

**Synapse Networks** bieten den Managed Service an, per Fernwartung und mit Rufbereitschaft die permanente Datenverkehrsanalyse zu betreiben (proaktiv & reaktiv) und über eine gemeinsame Troubleticket-Datenbank die Techniker/Administratoren des Kunden mit Arbeitsaufträgen zu versorgen; weiterhin wird der Erfolg der fälligen Maßnahmen durch die Analyse selbst wiederum überwacht und verifiziert.

Synapse Networks betreiben Qualitätssicherung auf höchstem Niveau zwecks Aufrechterhaltung der Betriebsbereitschaft sowie zur täglichen Verminderung der Angriffsfläche bzw zur aktiven Gefahrenabwehr.



## Grundlagen der Analyse

**Synapse Networks** überwachen mit je einem Analyse-Agenten je ein LAN-Segment bzw den Datenverkehr eines **Switch/Router-Mirror-Port**s. Die sog. Trace-Daten verbleiben für eine beschränkte Dauer auf dem Datenträger des Analyse-Agenten; je nach Festplatten-Kapazität und Netzwerk-Datendurchsatz kann das mitwandernde Zeitfenster der vorgehaltenen LAN-Pakete bei Tagen oder Wochen liegen. Auf diese Weise kann bei Störfällen bzw Security Incidents auch auf länger zurück liegende Original-Daten zurück gegriffen werden. So kann vollständige **IT-Forensik** im Bereich der Datenkommunikation betrieben werden. Erhalten bleiben längerfristig die Reports:

Die Analyse-Software erzeugt Ereignis-Protokolle (Event Logs), Ergebnis-Listen und -Tabellen. Durch Filter kann bestimmt werden, welche Ereignisse sofort (im Moment des Erkennens) per Syslog an den zentralen Syslog-Sammler oder per E-Mail (verschlüsselt) an hinterlegte Administratoren/Techniker gesendet werden. Es werden Tagesberichte erzeugt und dauerhaft abgelegt. Die Identität der im Netzwerk kommunizierenden Rechner wird fortdauernd überwacht; Meldungen bzgl des Wechsels von ID-Merkmalen einzelner PCs werden mit Vorrang verarbeitet.

## Wartungsvertrag / Managed Service

**Synapse Networks** stellen für die Dauer eines Wartungsvertrages die Software der Analyse-Agenten leihweise zur Verfügung; führen regelmäßig Updates durch; überwachen die Ergebnisse; prüfen ständig die Aktualität der verwendeten Filter; pflegen die Trouble-Ticket-Datenbank des Kunden; überwachen den Fortschritt und Erfolg der kundenseitig vorgenommenen Arbeiten im Zusammenhang mit den aktuellen=offenen Trouble-Tickets.

Kern-Ziel des Wartungsvertrags ist es, **im höchsten Maße pro-aktiv** zu sein und Fehler bzw Sicherheitsgefahren zu erkennen bereits **vor** Erreichen der Wahrnehmungsschwelle der Anwender bzw bereits **vor** den Alarm-Meldungen etwa von Firewall und/oder IDS. Durch dauerhafte, tief gehende Analyse und Verbesserung der Konfigurationen soll ebenso dauerhaft die Angriffsfläche der IT möglichst gering und die Betriebsbereitschaft möglichst hoch gehalten werden.

## Referenz-Kunde

**Synapse Networks** erreichen bei einem weltweit tätigen Kunden folgende Leistungsdaten: 25-30 Analyse-Agenten auf 4 Kontinenten; über 100 GB Trace-Daten analysiert pro Tag; je nach aktueller Lage 10-30 Mio Ereignis-Meldungen per Syslog an die Zentrale; ca 600 Ereignis-Definitionen in der Filter-Engine, davon regelmäßig 300-400 aktiv (die restlichen beziehen sich auf frühere, bereits behobene Fehler, verbleiben aus Revisionsgründen aber in der Filter-Datenbank). Rufbereitschaft: telefonisch+sofort.

synalyst
SMART NETWORK ANALYSIS

(Stand: 2018-11-26)

www.synalyst.net