synalyst
SMART NETWORK ANALYSIS

Synapse Networks GmbH

Audit – Analysis – Troubleshooting

Preisliste Herbst 2018

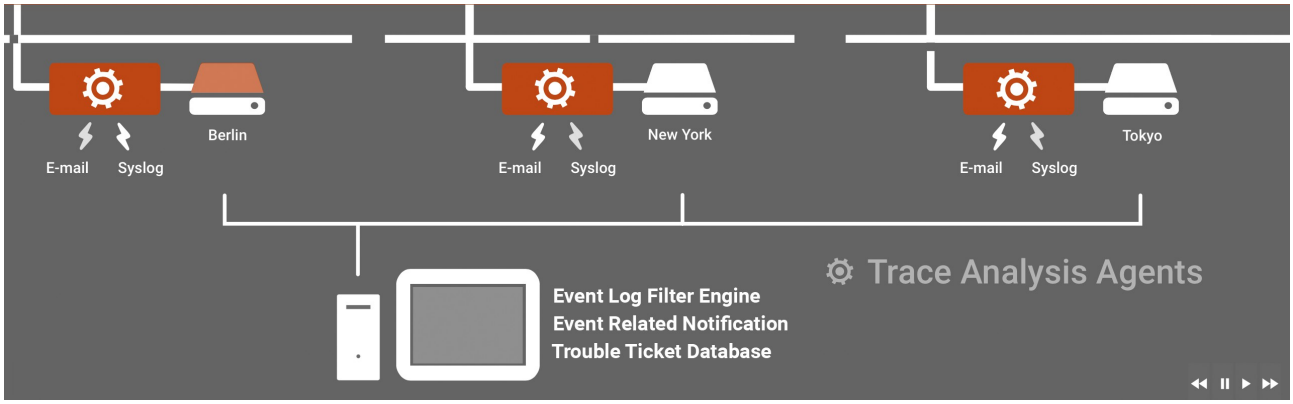
Synapse Networks führen LAN/WAN-Analyse durch mit dem Mittel der Deep Packet Inspection: Ethernet-TCP/IP-Pakete des Netzwerks werden aufgezeichet und ausgewertet. Diese Leistung wird angeboten als Workshop bzw Entstörung sowie als Wartungsdienst im Dauerauftrag (Managed Service). Im Regelfall verbleiben die Daten im Hause des Kunden, eine Übergabe an uns findet nicht statt. Wir sind ein sicherheitsgeprüftes Unternehmen und daher befugt, auch in hohen Sicherheitsklassen zu arbeiten.

Einzel-Auftrag	**z.B. Notfall-Analyse**	**(zzgl MWSt)**	**Preis pro Tag**
Analyse vor Ort	*Preis variiert je HW-Aufwand*	Basis-Preis:	00 €
Analyse per Fernzugriff			1.200 €

Dauer-Auftrag	**z.B. Wartungsvertrag**	**(zzgl MWSt)**	**Preis pro Tag**
Analyse vor Ort	*sicherheitsgeprüftes Personal*		1.200 €
Analyse per Fernzugriff			600 €

Analyse-Agenten	**Synapse MintMagic**	**(zzgl MWSt)**	**Preis / Agent**
Einzel-Lizenz / Kauf	Update-Service: ohne		7.200 €
Einzel-Lizenz / Kauf	Update-Service: mit		7.920 €
im Wartungsvertag	Rufbereitschaft: ohne	Pro Monat:	600 €
im Wartungsvertag	Rufbereitschaft: mit	Pro Monat:	660 €

Synapse Networks überwachen im Zuge von Wartungsverträgen (Managed Service) die Analyse-Agenten, sichtet die Ergebnisse, überträgt die wichtigsten Befunde in die Trouble-Ticket-Datenbank des Kunden (i.d.R. MS-SharePoint), führt Software-Updates der Analyse-Agenten durch. Im Rahmen der Wartungsverträge stellt Synapse Networks GmbH die Software, der Kunde die PC-Hardware (Windows). Im Preis der Analyse-Agenten enthalten sind der zentrale Syslog-Sammler & die zentrale Filter-Engine.



synalyst
SMART NETWORK ANALYSIS

Synapse Networks GmbH

Audit – Analysis – Troubleshooting

Preisliste Herbst 2018

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 Rechner 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 Angriffsflächer der Kunden-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.

** Die genannten Preise sind unverbindlich und frei bleibend. Es gilt nur das im Einzelfall heraus gegebene Angebot. **