



Analyse und Überwachung verteilter Netzwerke weltweit

analysis and monitoring of distributed networks worldwide



Forensik: Speicherung der LAN-Daten zur forensische Analyse

long-term storage of LAN/WAN data allows forensic analysis



ermöglicht die Verifikation anderer Schutz-Elemente wie z.B. Firewalls

analysis/verification of other security devices (firewalls etc)



unterstützt Verifikation von DSGVO, ISO 27001, ISIS12, ITSM

supports verification of GDPR, ISO 27001, ITSM



Client/Server-Analyse: Zugriffe, Fehler, Ablehnungen, Abbrüche

analysis of peer-to-peer relations: access, error, rejection, abort



Analyse-Agenten in mögl. vielen Subnetzen (Client/Server,DMZ,etc)

analysis agents positioned in as many subnets as possible



Erfassen von Client-Identitäten Erkennen von Identitätswechseln

identity monitoring, detection of identity changes



zentrale Erfassung aller Meldungen Filterung, Priorisierung, Weitergabe

central collection of events plus filtering, prioritizing, forwarding



Erkennung unerwünschter Kommunikation in LAN & WAN

detection of suspicious communication (active/passive) (LAN/WAN)



automatisches Aggregieren der Ereignis-Logs und Analyse-Reports

automatic aggregation of event logs and analysis reports



Alarime bei Störungen und Sicherheitsverletzungen

alarm notifications in case of technical errors or security incidents



mehrere Hundert oder Tausend Filter mögl. zur Event-Verarbeitung

hundreds and thousands of filters possible for event processing

SEMINARE

Lernen Sie in praxisnahen **Workshops**:

- wie Sie Datenpakete aufzeichnen:
- Switch / Router Mirror Port
- libpcap Format der LAN-Pakete
- Wireshark für Stichproben-Sichtung
- manuelle Filter in Stichproben

Analyse mit Experten-System

- autom. Aufzeichnung & Auswertung
- autom. Berichts-Erstellung
- autom. Meldungen & Warnungen
- Analyse in verteilten Netzwerken
- Dokumentation der LAN-Teilnehmer
- White List: Fremd-Adressen erkennen
- Einbruchs-Erkennung: Intruder
- Ausbruchs-Erkennung: Jailbreak
- Verschlüsselungsprobleme
- Schwachstellen-Analyse
- Performance-Analyse

Sprechen Sie uns an:

06725 – 999 0710

analysis@synalyst.net

AUDITS

Bestandsaufnahme Ihrer LAN-Umgebung:

- Kurz-Audit mit 1-2 Tagen
- Langzeit-Überwachung
- Managed Service / Fernwartung
- Geringer Aufwand, reicher Ertrag
- Ausführliche Ergebnis-Daten

Analyse: non-invasiv = kein Risiko

- Schließen von Sicherheitslücken
- Beheben von Inkompatibilitäten
- Ausbessern von Konfig-Fehlern
- Daten bleiben in Ihrem Hause
- DSGVO-konformes Vorgehen
- Datenschutz-konforme Analyse
- Jederzeit kurzfristige Audits möglich
- Einzige Voraussetzung: Mirror Ports
- RZ, DMZ, Client/Server Subnetze
- Beratung zur künftigen Entwicklung

Sprechen Sie uns an:

06725 – 999 0710

analysis@synalyst.net