1. LB2 - Beschreibung und Recherche der Software Sysmon (15%)

1.1 Lernziele

Jede/r Lernende:

- ...kann in eigenen Worten die Applikation Sysmon beschreiben
- ...kann Sysmon automatisiert installieren lassen
- ...kann Sysmon manuell installieren
- ...kann Sysmon nach Vorgaben konfigurieren

1.2 Aufträge und Bewertungskriterien

Recherche - Sysmon 0-4P:

- Was ist Sysmon? Wofür wird es verwendet
- Was ist die aktuellste Version von Sysmon?
- Was sind Beispiel-Anwendungen/Use-Cases bei welchen Sysmon helfen kann?

> **Wichtig**
>
> Auf Ihrem System wurde Sysmon bereits installiert und konfiguriert (Best-Practices) - **Tipp:** Betrachten Sie das Script "scripts/install-sysinternals.ps1"

Installation - Sysmon 0-4P:

- Recherchieren und dokumentieren Sie wie man Sysmon manuell auf einem Windows-Server/Client installieren würde
- Recherchieren und dokumentieren Sie wie Sysmon auf Ihren Systemen (automatisiert) installiert wurde

Konfiguration - Sysmon 0-4P:

- Lesen Sie bitte die folgenden Blog-Posts durch:
  - Teil 1
  - Teil 2
  - Teil 3

- Dokumentieren Sie das Config-File welches auf Ihrem System für Sysmon installiert ist
- Dokumentieren Sie die Struktur des Config-Files

> **Quellen**
>
> Sysmon ist extrem verbreitet, entsprechend gibt es sehr viele gute Quellen um sich mit diesem Werkzeug vertraut zu machen. Nutzen Sie sie! (youtube z.Bsp)