

1. LB2 - Fleet Osquery Testing (15%)

1.1 Lernziele

Jede/r Lernende:

- ...kann in eigenen Worten die Applikation Fleet beschreiben
- ...kann Fleet für eigene Ziele verwenden

Auf dem Logger wurde Fleet bereits installiert : <https://192.168.56.105:8412>

1.2 Aufträge und Bewertungskriterien

Recherche - Fleet 0-4P:

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

Dokumentation / Testing (1) - Fleet 0-4P:

Über <https://192.168.56.105:8412/queries/manage> sind bereits einige Querys vordefiniert

- Suchen Sie sich eine Query aus die für Ihre Windows-Umgebung sinnvoll erscheint
- Beschreiben Sie die Query ausführlich (Sinn / Zweck / Umsetzung der Abfrage)
- Testen Sie die Abfrage und dokumentieren Sie die Resultate (mit Screenshots)

Dokumentation / Testing (2) - Fleet 0-4P:

Über <https://192.168.56.105:8412/queries/manage> sind bereits einige Querys vordefiniert

- Suchen Sie sich eine Query aus die für Ihre Windows-Umgebung sinnvoll erscheint
- Beschreiben Sie die Query ausführlich (Sinn / Zweck / Umsetzung der Abfrage)
- Testen Sie die Abfrage und dokumentieren Sie die Resultate (mit Screenshots)

