

## Sitzungsprotokoll

**Projekt:** Readiness for Tailored Attacks and Lateral Movement  
**Woche:** 5  
**Datum / Zeit** 16.10.2018 08:30 - 09:30

### Sitzungsteilnehmer / E-Mail

Lukas Kellenberger	lukas.kellenberger@hsr.ch
Claudio Mattes	claudio.mattes@hsr.ch
Cyrill Brunswiler	cyrill.brunswiler@hsr.ch

### Traktanden

- Stand des Projekts
- Unterstützungen
- Darlegen unseres Konzeptes
- Fragen
- Weiteres Vorgehen

## Stand des Projekts

Arbeiten	Status
Research und Übersicht schaffen	in Bearbeitung
Schreiben der Dokumentation	in Bearbeitung
Definition von Use Cases und NRFs	in Bearbeitung

## Unterstützungen

Art der Unterstützung	Hilfsperson
Keine	-

## Fragen

- Technologie-Entscheid mit Powershell
- Use-Cases
- NRFs

## Weiteres Vorgehen

Was	Verantwortlichkeit
Definition der Sprint Features	Team
Neuer Use Case "Save Result" mit Pfadangabe	Team
Ev. Domain Model	Team
Prototyping	Team (einzeln)

## Nächster Termin

Datum: 23.10.2018  
Zeit: 07:30 - 08:30  
Ort: Standort Alice

## Kommende Abwesenheiten

Person	Von	Bis
Lukas Kellenberger	26.10.18	29.10.18

## Beschlüsse (Diskussion)

- NRFs
  - NFR01: deliberately alter; Nebenbemerkung, dass das Tool Logs generieren wird
  - NFR02: any → significant
  - NFR04: minimal target version
  - Neues NFR: Tool läuft in One Go, aber kann auch in einzelnen Steps ausgeführt werden mit der Möglichkeit einzelne Steps zu Überspringen (Pausieren/Abbruch bei Performanceproblemen)
- Welche Events wird das Tool werfen?
- Storage Angaben für temporäre Files und den Export des Ergebnisses
- "Save Result" Use Case
- Ablauf Scripts/Use Cases: Zuerst Audit Policy auslesen & analysieren und dann Event Log auslesen & analysieren
- rsop.msc