# Kick-off Lateral Movement SA

## Anforderungen

* Meetingprotokoll (Traktanden, Beschlüsse, Stand, Unterstützung, weiteres Vorgehen) und versenden
* Projektplan spätestens in 2 Wochen (3.10.18)
* Zeiterfassung (Toggle) – Soll/Haben (empfehlenswert 1 Woche Puffer am Schluss)
* Testumgebung beschreiben

## Sonstige Anmerkungen

* Am Schluss gedruckte Version, sonst elektronisch
* Anforderungsdokument durchlesen und auf nächstes Mal unterschreiben.
* Quellenangabe nicht vernachlässigen – lieber viel als zu wenig
* Viel in Anhang – kurz und knackig
* Gelesener Stoff bewerten (Relevanz für SA) und dementsprechend dokumentieren
* Kapiteleinleitungen und Kapitelsummary
* Wenn Abbildungen, dann mit Bezug darauf
* Research, Evaluation Tools, Testing/Implementation, Dokumentation
* BloodhoundAD (Privilegien in Domainen - Github) – in dieser Art und Weise
* Persona Endbenutzer: IT Experte
* PowerBI
* JPCert Tools
* MITRE
* MS Defender Advanced Hunting nur Clientseitig
* Plaso / Timescetch (Google RapidResponse) eventuell erweitern
* Eher nicht auf der grünen Wiese anfangen, sondern bestehendes Erweitern (Design/Analyse davon)
* Erster Schritt Analyzer (Beschreibung was zu machen ist und direkt auch GPOs anpasst)
* Standalone Applkation, welche nicht vorab installiert werden muss

## Fragen

* Benötigen wir einen Server von der HSR für die SA?
  + Eventuell – vielleicht kann auch auf der Azure Cloud von Compass gearbeitet werden
* Tool bereits bestehend?
  + Nein

## Termine

* 27.09.18 13:00 – 14:00 nächste Sitzung

## Abwesenheiten

* Claudio: Do. 4.10.18 – Mo. 8.10.18
* Lukas: 26.10.18 – 29.10.18