Sitzungsprotokoll

Projekt:	Readiness for Tailored Attacks and Lateral Movement
Woche:	6
Datum / Zeit	23.10.2018 07:30 - 08:30

Sitzungsteilnehmer / E-Mail

Claudio Mattes	claudio.mattes@hsr.ch
Cyrill Brunschwiler	cyrill.brunschwiler@hsr.ch

Traktanden

- Stand des Projekts
- Fragen
- Weiteres Vorgehen

Stand des Projekts

Arbeiten	Status
Research und Übersicht schaffen	Abgeschlossen
Definition von Use Cases und NFRs	Abgeschlossen
Schreiben der Dokumentation	in Bearbeitung
Einarbeitung Powershell, einzelne Funktionen schreiben/testen	in Bearbeitung
PoC Sysmon-Detektion	Erreicht

Unterstützungen

Art der Unterstützung	Hilfsperson
Keine	-

Fragen

- Cobalt Strike
- Domain Model (unserer Meinung nach lohnt es sich nicht ein objektorientierte Lösung anzustreben, da es mehr Boilerplate wäre)

Weiteres Vorgehen

Was	Verantwortlichkeit
Domain Model Ausarbeitung (Ist-Zustand)	Team
PoC Audit Policy	Claudio
PoC Event Log	Lukas
Dokumentation: Analyse fertigstellen	Team
Dokumentation: Technologie fertigstellen	Team
Ausarbeitung und Dokumentation Design des Tools	Team
Beginn Implementation	Team

Nächster Termin

Datum:	31.10.2018
Zeit:	08:30 - 09:30
Ort:	Standort Alice

Kommende Abwesenheiten

Person	Von	Bis
Lukas Kellenberger	26.10.18	29.10.18

Beschlüsse (Diskussion)

- Design des Tools
- Neue Risikobeurteilung (Krankheit, Verzug)
- Cobalt Strike wird keine Option sein
- Sysmon-Tools (olafhartong/sysmon-modular, nshalabi/SysmonTools) zur Prävention und korrekter Konfiguration von Sysmon in Analyse aufnehmen
- Transaction-Safety (was geschieht mit den Files, wenn das Tool abstürzt)
- Domain Model zur Zeit im Soll-Zustand → Ist-Zustand mit Client/Server und Verify/Analyse-Prozess aufnehmen
  - Für zukünftige Weiterentwicklung und richtige Herangehensweise
- Gibt es ein Pattern für das Domain Model?
- Objektorientierter Ansatz wird nicht verfolgt, da zu viel Boilerplate Code für das Tool entstehen sowie die Performanz darunter leiden würde