Sitzungsprotokoll

Projekt:	Readiness for Tailored Attacks and Lateral Movement
Woche:	2
Datum / Zeit	27.09.2018 13:00 - 14:00

Sitzungsteilnehmer / E-Mail

Lukas Kellenberger	lukas.kellenberger@hsr.ch
Claudio Mattes	claudio.mattes@hsr.ch
Cyrill Brunschwiler	cyrill.brunschwiler@compass-security.com

Traktanden

- Stand des Projekts
- Unterstützungen
- Fragen
- Besprechung erste Version Projektplan (Meilensteine, Risikomanagement)
- Weiteres Vorgehen

Stand des Projekts

Arbeiten	Status
Dokumenten Templates erstellen	Abgeschlossen
Research und Übersicht schaffen	in Bearbeitung
Zeit- und Issuetracking-System aufsetzen	Abgeschlossen
Projektplan ausarbeiten (erste Version steht)	in Bearbeitung

Unterstützungen

Art der Unterstützung	Hilfsperson
Keine	-

Fragen

- Wie wird bei einer Analyse beim Kunden vorgegangen? Client/Server?
  - Manuelles durchspielen von Playbooks. Fokus auf Server.
- Logs mit Toolkits von allen Clients? ⇒ für anschliessende Analyse
  - Wäre schön, wenn von einer zentralen Stelle alle Clients überprüft werden könnten, da Clients aber meist identisch aufgesetzt und konfiguriert sind, ist dies nicht zwingend nötig.
- Cobalt Strike
  - Wahrscheinlich nicht zielführend
- Testumgebung (Tool sehen theoretisch gut aus, aber praktisch auch gut?)
  - Wird mit hoher Priorität versucht eine bereitzustellen
- Welche Dokumente werden alles erwartet? (Qualitätsmassnahmen, Anforderungsspezifikationen, Domain- und Architekturanalyse oder alles Zusammengefasst?)
  - Wie im Studium gelernt. Nach eigenem ermessen.
- Gibt es Co-Examiner für die Arbeit?
  - Möglicherweise - ist bis anhin noch nicht bekannt

Weiteres Vorgehen

Was	Verantwortlichkeit
Projektplan abschliessen	Team
Research und Tool Testing	Team

Nächster Termin

Datum:	02.10.2018
Zeit:	08:30 - 09:30
Ort:	Standort Alice

Kommende Abwesenheiten

Person	Von	Bis
Claudio Mattes	04.10.18	08.10.18
Cyrill Brunschwiler	08.10.18	14.10.18
Claudio Mattes	19.10.18	21.10.18
Lukas Kellenberger	26.10.18	29.10.18

Beschlüsse (Diskussion)

- Ende Oktober, Anfang November einen Zwischenbericht abliefern
- SonarQube für Coding-Guidelines verwenden
- Fokus auf MITRE und JPCert