Überprüfung der Funktionsfähigkeit von Sensorik und Überwachung mittels «Splunk Attack Range»

Studiengang: MAS Cyber Security

Das Cyber Fusion Center der Führungsunterstützungsbasis FUB schützt dank dem Monitoring von Ereignissen den Cyberraum von Hacker-Angriffen. Mithilfe von Attack Range soll die Möglichkeit zur Überprüfung der Funktionsfähigkeit von Sensorik und Überwachung verbessert werden.

Ausgangslage

Das Cyber Fusion Center CFC stellt die Sicherheit der Systeme und Infrastruktur der Schweizer Armee in allen Lagen sicher. Cyberbedrohungen von opportunistischen bis hin zu komplexen zielgerichteten Angriffen müssen erkannt und abgewehrt werden können. Zu dieser Leistung gehört das Analysieren von Log Files, welche unter anderem mit der skalierbaren Plattform Splunk verarbeitet werden. Die Analyst*innen setzen selbst erstellte Suchmuster sowie Use Cases von Drittanbietern ein, um in den Logs Anomalien auf Netz- und Endpointebene feststellen zu können und reagieren anschliessend auf die erzeugten Alarme mit dem Eröffnen eines Incidents.

Motivation

Im Laufe der Zeit entdecken Angreifer*innen immer wieder neue Taktiken, Techniken und Vorgehensweisen (TTP), weshalb überprüft werden muss, ob essentielle Erkennungsregeln fehlen oder zu optimieren sind. Das CFC will unter anderem ein neues Werkzeug namens «Attack Range» einsetzen, mit dem neue Cyberangriff Szenarien erstellt und auf ausgewählten Testsystemen durchgeführt werden können. Bevor das neue Werkzeug produktiv eingesetzt werden kann, soll ein Proof of Concept durchgeführt und anhand von verschiedenen Anwendungsbeispielen Erfahrungen mit Attack Range gesammelt werden. Ein Grobkonzept soll zeigen, wie Attack Range im CFC produktiv eingesetzt werden kann.

Vorgehen

Alle notwendigen Bestandteile von Attack Range wurden innerhalb von mehreren isolierten Testumgebungen aufgesetzt und in Betrieb genommen. Um für den Proof of Concept die passenden Use Cases definieren zu können, wurden Informationen über aktuelle Cyberbedrohungen gesammelt sowie Recherchen über bereits vorgefallene Incidents getätigt. Dabei lag der Fokus bei Emotet und Turla, wobei sich das CFC mindestens mit einem der beiden Threat Actors in der Vergangenheit beschäftigt hatte. Anschliessend wurde ein Grobkonzept erstellt, welches ein produktives Einsetzen von Attack Range im CFC beschreibt.

Ergebnisse

Attack Range kann in zwei verschiedenen Methoden verwendet werden. Einerseits mit der Open-Source-Bibliothek «Atomic Red Team» zum Simulieren von hostbasierten Angriffen und andererseits mit der Plattform «Caldera», welche in der Lage ist, komplette TTPs basierend auf dem Mitre ATT&CK Framework zu simulieren. Attack Range soll in Zukunft dazu verwendet werden, neue Use Cases zu erstellen. Ein Use Case besteht aus dem Payload des Angreifenden, der neuen Erkennungsregel zum detektieren des Payloads sowie aus der notwendigen Dokumentation, dass zu einem späteren Zeitpunkt die Entwicklungsumgebung wieder mit der richtigen Konfiguration provisioniert werden kann.

Ausblick

Das Grobkonzept wird innerhalb des CFC in der Hauptverantwortung des Autors im Detail ausgearbeitet und auf einem intern zugänglichen Testsystem bereitgestellt, welches durch die Miliz getestet werden kann. Nach dem Verarbeiten von Feedbacks und Verbesserungsvorschlägen sollen die Angehörigen der Armee, die sich im Cyberlehrgang 2023 befinden, damit arbeiten dürfen.

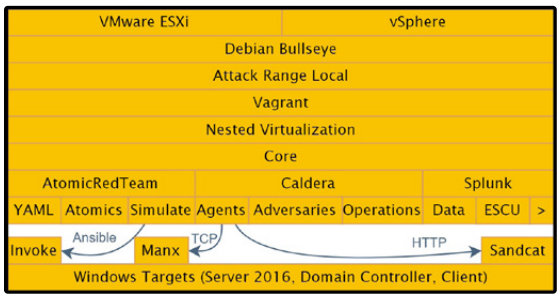
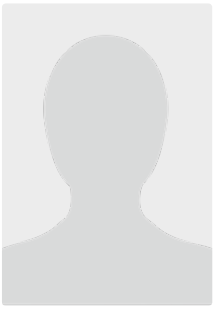


Abbildung 1: Architektur Attack Range Testsystem



Marius Friederich

marius.friederich@proton-mail.com