Anomalie Detection in Netzwerken

Statusbericht Nr.3

Ives Schneider

1. Projektarbeit

Aufgrund eines Hardwareausfalls musste leider von dem physischen PoC-Lans auf eine virtuelle Umgebung geswitcht werden.
Der Aufwand war nicht wirklich extrem hoch, da bereits eine kompatible Infrastruktur vorhanden war.
Clients und Server (Auch für die Testumgebung), werden nun via Terraform provisioniert und Ansible konfiguriert.

Die ersten tests, zeigten bereits, dass die Software innerhalb weniger Sekunden Host-detection erfolgreich durchführt. Anhand einer definierten Konfigurationsdatei kann definiert werden, welcher Port geöffnet oder geschlossen sein sollte.

Folgende Punkte stehen noch für die Applikation aus: - Web-UI - Support für mehrere Splunks - Mögliche deaktivierung von Services

Dokumentation: - Installation - Betrieb - Controlling

Allerdings sind das eher kleinere Änderungen welche durchgeführt werden müssen, daher rechne ich nicht mit extrem hoher Zeitinvestition.

Zusätzlich ist die Hauptstudie nun Fertiggestellt und bedarf nur noch eines kleinen Reviews, welche ich von einer Dritt-Person durchführen lasse. Allem in allem liege ich gut im Zeitplan und denke, dass ich zur geplanten Zeit mit allem fertig werde

2. Reflexion

Natürlich hat der Hardwareausfall für etwas aufwand gesorgt. Da ich glücklicherweise einen Plan-B hatte, lies sich der Vorfall schnell beheben.

Applikationsspezifisch habe ich die sub-Threads etwas unterschätzt.
Da das Scanning (ARP+Nmap) im Hintergrund in gewissen intervallen durchgeführt wird, heisst das natürlich, dass sie unabhängig der eigentlichen Applikation durchgeführt werden müssen. Nach einigen versuchen, habe ich es allerdings hinbekommen, das auch die Konfiguration Thread-Save übertragen wird.

Hauptstudien spezifisch gab es keine direkten Probleme.

3. Zukünftig

Bevor ich die restlichen Dokumente schreiben kann, benötigt die Applikation noch die implementation der oben genannten Punkte.
Sobald dies erledigt ist, wird es relativ leicht sein, die restlichen Dokumente zu schreiben.