Automating incident response through xsoar

Reflectie

Bachelor in de Electronica-ict
keuzerichting cloud & cybersecurity

Academiejaar 2022-2023

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

Rune Mannaerts

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

Reflectie over mijn stage bij Cegeka

1.1 Inhoudelijke reflectie

Tijdens mijn stage bij Cegeka, had ik het voorracht om te werken aan een project dat zich richtte op het testen van verschillende artificiële intelligentie(ai) tools die beschikbaar zijn voor automatisering en integratie. Het belangrijkste doel was om de mogelijkheden van drie specifieke AI-technologieën te evalueren: ChatGPT, de ingebouwde ai van Palo Alto XSOAR, en python-scikit. Het project had als doel om de effectiviteit en geschiktheid van deze tools te beoordelen voor verschillende gebruiksscenario’s binnen de organisatie.

Deze taak heb ik tijdens mijn stage ook afgerond. Ik heb mijn bevindingen gepubliceerd in een document dat ik ook mocht gebruiken voor mijn bachelorproef. Om dit te doen, heb ik verschillende bewijzen gemaakt en ze gedocumenteerd als bevindingen in het document.

Naast het voltooien van dit grote project kreeg ik ook de kans om twee kleinere projecten binnen dit grote project af te ronden. Bij deze twee projecten heb ik verschillende AI-tools gebruikt om te beoordelen in welke scenario's ze van pas kwamen. Het automatiseren van phishing-incidentrespons was het belangrijkste project waarbij ik deze diverse AI-tools heb gebruikt en getest. Uiteindelijk heb ik drie werkende Python-scripts geschreven. Eén script kon worden geïntegreerd met Palo Alto's XSOAR en dit was ChatGPT. De andere twee Python-scripts waren gebaseerd op Python scikit en werden getraind op basis van historische incidentendata waar ik toegang toe had gekregen.

Voor het andere project heb ik ook gewerkt met een Python-script dat de link legde tussen de gegevens die beschikbaar waren in de objectindicator en het remediatieproces dat werd beschreven op de documentatiewebsite van Cegeka. Daarnaast heb ik ook een ander Python-script geschreven dat aan ChatGPT vroeg om een plan op te stellen voor het oplossen van een incident met deze specifieke indicator. Dit werd gedaan op basis van de beschrijving van de indicator.

1.2 Persoonlijke reflectie

Algemeen genomen heb ik enorm genoten van mijn stage en de samenwerking met mijn collega's. Tijdens deze periode heb ik veel geleerd over kunstmatige intelligentie, een vakgebied waar ik voorheen beperkte kennis van had. Bovendien heb ik ook mijn kennis op het gebied van mijn studierichting kunnen verdiepen. Met deze twee aspecten in acht genomen, ben ik verheugd te kunnen mededelen dat deze stage een succesvolle ervaring is geweest. Dit wordt tevens bevestigd door Cegeka, aangezien zij mij een baanaanbieding hebben gedaan.