Honeypot Anomaly Detection

Reflectie

Bachelor in de Electronica-ICT
keuzerichting Cloud & Cyber Security

Alex Coulon

Academiejaar 20xx-20xx

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

Inhoud

1 INLEIDING

In dit document reflecteer ik terug op mijn Internationale Stage bij de Thomas Bata University in Zlíně (Tsjechische Republiek). Ik reflecteer zowel op de inhoud van mijn stage als mijn persoonlijke reflectie op het hele gebeuren. Ik ga dieper in mijn realisaties, projectvorderingen en toekomst mogelijkheden van dit project. Daarnaast vertel ik meer over de betekenis van deze stage naar mijn mening, in welke competenties en technische items ik gegroeid ben en welke confrontaties ik ben tegen gekomen en hoe ik deze opgelost heb. Ik hoop hiermee de lezer een duidelijker inzicht over mijn stageperiode te kunnen aanbieden.

2 INHOUDELIJKE REFLECTIE

2.1 Realisatie

De realisatie van dit project is een volledige afwerking van het vooropgestelde plan van aanpak. Samen met 2 mede studenten (Bram Geudens & Yannick Vandevenne) hebben we een totaal honeypot anomaly detection project opgezet. Dit houdt in dat er werkende honeypots zijn voor Linux, Windows & MacOS. De gegevens die uit deze honeypots gehaald worden sturen we via een veilige datastream door naar onze ELK omgeving. Logstash bezorgt onze data vanop de honeypot aan onze Elasticsearch. Kibana zal hierna data uit Elasticsearch halen voor onze visualisaties te voorzien van filterbare data. Het ingebruikneming van dit project heeft serieuze voordelen voor de UTB, zo kunnen ze hackers direct weren uit andere delen en hebben ze een beter inzicht in wat hackers proberen te realiseren op het netwerk/servers. Naast het technische aspect heeft deze opdracht een serieuze onderzoeksfase voorafgegaan.

2.2 Project einde & ingebruikname

De vereiste van het project zijn voldaan tijdens onze stageperiode. Er is mogelijkheid tot het uitbreiden van het project met nog meer honeypots en honeynets, hiernaast kan het nog geoptimaliseerd worden. De term honeypot is meer dan enkel een honeypot, de mogelijkheden met dit project zijn enorm. Doordat het project volledig opensource gerealiseerd is kunnen zowel wij als de UTB als eender wie wanneer ze willen verder aan dit project werken zonder enige problemen. Onze oplossing zal in gebruik genomen worden door de UTB na bepaalde controles en optimalisaties door de IT/Cyber dienst terplekke.

2.3 Adviezen

Een advies aan de opdrachtgever/stagementor is het optimaliseren van opvolging en feedback. Het was ons op voorhand duidelijk gemaakt dat we veel vrijheden zouden krijgen in het project, maar opvolging was er bijna enkel als wij het vroegen. Een vast feedback moment om de x tijd zou stagairs hun project kunnen helpen. Dit zorgt voor een snellere en efficiëntere bijsturing van het project, de professionele houding en handeling van de student en een algemeen beter eindresultaat.

3 PERSOONLIJKE REFLECTIE

3.1 Persoonlijke betekenis

Voor mij betekent stage een tijd waarin je de eerste keer je technische kennis kan ontplooien in een professionele omgeving. Mijn internationale stage heeft volledig voldaan aan mijn verwachtingen. Dit was een unieke kans waarbij ik mijn kennis kon gebruiken aangevuld met eigen research en onderzoek over bepaalde technologieën, hiernaast kom je in een professionele werkomgeving terecht waar je toch een andere houding en gedachtegang creëert. Hiernaast in een stage een opportuniteit om je portfolio of CV aan te vullen met een noemenswaardige werkervaring.

3.2 Competenties & Persoonlijke groei

Doorheen de stage heb ik heel wat zaken geleerd, zowel technisch als soft skills. Graag vertel ik per onderdeel wat meer hierover.

3.2.1 Soft skills

3.2.1.1 Professioneel handelen

Deze stage heeft me een diepere inkijk en hands on ervaring gegeven in professioneel handelen op de werkvloer. Omgaan met collega's, infrastructuur zijn kernzaken die je in een verder leven zeker nog nodig hebt.

3.2.1.2 Communicatie

Zo is communicatie zowel schriftelijk als mondeling veel aan bod gekomen. Doordat mijn project in groep was is er enorm veel vergaderd, samengezeten en overlegd. Correcte, duidelijke en essentiële communicatie was vereist om dit project tot een goed einde te brengen.

3.2.1.3 Agile

Door een project van deze omvang met taken langs alle kanten die erbij kwamen hebben we besloten Agile te werken, zo werken we met sprints van telkens 1 week. Op maandag sprint review en elke morgen een kleine standup meeting.

3.2.1.4 Presentatie

Door ons eindresultaat te mogen presenteren aan zowel collega's van de UTB, onze docenten en CZ.NIC/Turris hebben we ook onze presentatie skills kunnen verbeteren. Op het kantoor van Turris konden we in een professionele omgeving met een heel gevarieerd publiek onze eindpresentatie bezorgen en vragen beantwoorden.

Zo denk ik dat deze stage me heeft voorbereid voor een professionele carrière.

3.2.2 Hard skills

3.2.2.1 Linux

Ervaring met het gebruik van Linux had ik al, door 3maanden in Linux omgevingen te werken is de hands-on ervaring en efficiëntie met dit OS serieus gestegen.

3.2.2.2 Honeypots

Wat een honeypot was vroeg ik me af toen ik de stageopdracht las, dit was voor mij een nieuwe wereld. Zo heeft langdurig onderzoek, en het zelf opzetten van onze oplossing een nieuwe wereld van mogelijkheden omtrent honeypots geopend.

3.2.2.3 ELK

Wat een ELK stack was wist ik al, wat de mogelijkheden waren was beperkte kennis voor me. Door dit project te maken heb ik een groot inzicht gekregen in ELK, de mogelijkheden en de opties.

3.2.2.4 Painless

Painless scripting was voor mij totaal nieuwe scripting taal, na heel wat proberen, fouten oplossen en documentatie lezen heb ik toch degelijke scripts kunnen schrijven.

3.3 Confrontaties

De grootste confrontatie was de werk cultuur en ethiek. Er waren geen verplichte werkuren, geen deadlines of harde vereisten van voortgang, het moest af zijn eens we naar België gingen. Verantwoordelijk kunnen omgaan met deze vrijheden was de grootste confrontatie of shock dat we hebben meegemaakt. Dit hebben we netjes kunnen oplossen door voor onszelf vaste werkuren op te leggen en ons hier ook echt aan te houden. Hiernaast zijn we technisch ook tegen heel wat problemen gelopen, zo was het veilig combineren van data vanop zowel Linux, Mac als Windows een serieuze uitdaging waar heel wat denk en oefen werk heeft ingestoken.