Anomāliju noteikšana ELK stack

Autore: Inga Kauliņa

Studenta apliecības numurs: ik18075

Darba vadītājs: Dr. sc. ing. Edžus Žeiris

Darba mērķis:

Izpētīt un salīdzināt Elastic SIEM un Humio produktu piedāvāto anomāliju noteikšanu, kā arī uzbūvi kopumā un izveidot ideju kāds risinājums anomāliju noteikšanai varētu labāk derēt ZZDats un pievienošanai jau esošam ELK stack risinājumam ZZDats.

Uzdevumi:

1.Aplūkot ELK stack, Humio un Elastic SIEM produktu uzbūvi un komponentes.

2.Veikt salīdzinājumu starp Elastic SIEM un Humio anomāliju noteikšanas pieejām.

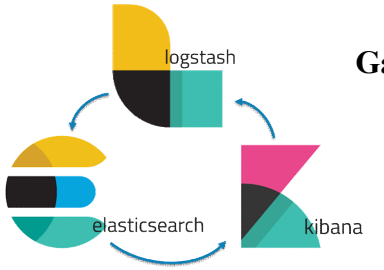
3.Veikt secinājumus par potenciāli labāko anomāliju risinājumu

Turpmākie plāni:

1.Turpināt izpēti izvēlētajiem produktiem vēl padziļinātāk, konkrētāk fokusējoties uz anomāliju noteikšanas aspektu.

2. Praktiski salīdzināt vairākus mašīnmācīšanās algoritmus un modeļus, lai noskaidrotu piemērotāko ZZDats vajadzībām.

3.Izstrādāt strādājošu risinājumu izmantojot labāko algoritmu un modeli.



ELK stack

Elastic SIEM

Galvenie secinājumi:

- Salīdzinot Humio un Elastic SIEM komponentes, konkrētāk anomāliju noteikšanas risinājumu, var secināt, ka korelāciju pieeja (definēti nosacījumi, kuru atbilstības gadījumā žurnālieraksts (*log*) tiek atzīts par anomāliju) anomāliju noteikšanai izmaksā konstatu darbinieku iesaisti, ko var mazināt pielietojot mašīnmācīšanos (veido modeli, kuru apmāca un žurnālieraksti, kuri neiekļaujas modelī, tiek uzskatīti par anomāliju) anomāliju noteikšanai.

- Pielietojot Elasticsearch žurnālierakstu uzglabāšanai un vaicājumu izpildei, populārākais veids datu iegūšanai no avotiem ir Logstash, kas datus vienlaicīgi arī normalizē, lai tie būtu gatavi Elastic darbībām.

- Monitorēšanai visatzītākā ir paziņojumu sūtīšana caur e-pastu uz uzturētājuzņēmuma darba vidē pielietoto e-pasta sistēmu. Kā arī lietotājiem ērti lietojama un pārskatāma saskarne par datu stāvokli Elasticsearch.