Day - 4

14 January 2025 15:00

Rex ---- Regular expression

```
| makeresults
| eval t1 = "Mon Mar 19 20:16:27 2018 Info: Bounced: DCID 8413617 MID 19338947 From:
<MariaDubois@example.com> To: <zecora@buttercupgames.com> RID 0 - 5.4.7 - Delivery expired (message too old)
('000', ['timeout'])"
| rex field=t1 "From:\s+<(?P<from_id>.*)>\s+To:\s+<(?P<to_id>.*)>"
```

Assignment --- 1. credit_Card_number ---> 1234-5678-9101-1213 O/P ---- 1234 5678 9101 1213 2. Field1 = "bob;search;saved_search" Name = bob App_name = search Savedsearchname = saved_search	

2. Alert --->

Definition --- SPL, Schedule, Interval
Trigger Condition --- When you want the alert should fire. Ex --- No Data, certain condition / count is met
Trigger Action --- What you want to do after? Ex --- Email, Alert trigger, Script etc.

Report ---->

Definition ---- SPL, Schedule Interval
Trigger Action --- Email, Script, Notification

Index= _internal ----> 1. Pull Event 2. Extraction of fields -- All the extraction of fields

Data Model ---> 1. Tsidx File --- Timestamp File --- Index the data

2. Extract the field in advance.
3. Hierarchical Concept ---> Root -- Child1 --- Child2

Root
Child1 -- Root + Constraint1
Child2 -- Child1 + Constraint2

Tstats ---> Tsidx file