CREATE OR REPLACE STREAM AWS\_S3SERVERACCESS\_STREAM on TABLE DEV\_STAGING.PANTHER\_LOGS.AWS\_S3SERVERACCESS;

CREATE OR REPLACE STREAM AWS\_VPCFLOW\_STREAM on TABLE DEV\_STAGING.PANTHER\_LOGS.AWS\_VPCFLOW;

CREATE OR REPLACE STREAM OKTA\_SYSTEMLOG\_STREAM on TABLE DEV\_STAGING.PANTHER\_LOGS.OKTA\_SYSTEMLOG;

CREATE OR REPLACE STREAM OKTA\_SYSTEMLOG\_STREAM on TABLE DEV\_STAGING.PANTHER\_LOGS.OKTA\_SYSTEMLOG;

create or replace table DEV\_STAGING.PUBLIC.LOGTABLE(

TABLE\_NAME VARCHAR2,

SP\_NAME VARCHAR2,

START\_TIME TIMESTAMP,

END\_TIME TIMESTAMP,

STATUS VARCHAR2,

TRIGGERED\_BY VARCHAR2

);

---------Facts & Dimension Table-------

create or replace table DEV\_REFINED.PANTHER\_LOGS.AWS\_VPCFLOW\_EVENTS(

P\_ROW\_ID VARCHAR,

P\_SOURCE\_ID VARCHAR,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION NUMBER,

P\_ANY\_IP\_ADDRESSES VARCHAR

);

INSERT INTO DEV\_REFINED.PANTHER\_LOGS.AWS\_VPCFLOW\_EVENTS

SELECT P\_ROW\_ID,P\_SOURCE\_ID,P\_EVENT\_TIME,P\_PARSE\_TIME,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES

FROM DEV\_STAGING.PANTHER\_LOGS.AWS\_VPCFLOW

----

create or replace table DEV\_REFINED.PANTHER\_LOGS.AWS\_S3SERVERACCESS\_EVENTS(

P\_ROW\_ID VARCHAR,

P\_SOURCE\_ID VARCHAR,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION NUMBER,

P\_ANY\_IP\_ADDRESSES VARCHAR

);

INSERT INTO DEV\_REFINED.PANTHER\_LOGS.AWS\_S3SERVERACCESS\_EVENTS

SELECT P\_ROW\_ID,P\_SOURCE\_ID,P\_EVENT\_TIME,P\_PARSE\_TIME,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES

FROM DEV\_STAGING.PANTHER\_LOGS.AWS\_S3SERVERACCESS

-----------

create or replace table DEV\_REFINED.PANTHER\_LOGS.OKTA\_SYSTEMLOG\_EVENTS(

P\_ROW\_ID VARCHAR,

P\_SOURCE\_ID VARCHAR,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION NUMBER,

P\_ANY\_IP\_ADDRESSES VARCHAR

);

INSERT INTO DEV\_REFINED.PANTHER\_LOGS.OKTA\_SYSTEMLOG\_EVENTS

SELECT P\_ROW\_ID,P\_SOURCE\_ID,P\_EVENT\_TIME,P\_PARSE\_TIME,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES

FROM DEV\_STAGING.PANTHER\_LOGS.OKTA\_SYSTEMLOG

----------

create or replace table DEV\_REFINED.PANTHER\_LOGS.AWS\_CLOUDTRAIL\_EVENTS(

P\_ROW\_ID VARCHAR,

P\_SOURCE\_ID VARCHAR,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION NUMBER,

P\_ANY\_IP\_ADDRESSES VARCHAR

);

INSERT INTO DEV\_REFINED.PANTHER\_LOGS.AWS\_CLOUDTRAIL\_EVENTS

SELECT P\_ROW\_ID,P\_SOURCE\_ID,P\_EVENT\_TIME,P\_PARSE\_TIME,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES

FROM DEV\_STAGING.PANTHER\_LOGS.AWS\_CLOUDTRAIL

select \* FROM DEV\_STAGING.PANTHER\_LOGS.AWS\_CLOUDTRAIL limit 10;

--------------

create or replace table DEV\_REFINED.PANTHER\_RULE\_MATCH.AWS\_VPCFLOW\_ALERTS(

P\_ROW\_ID VARCHAR,

P\_SOURCE\_ID VARCHAR,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION NUMBER,

P\_ANY\_IP\_ADDRESSES VARCHAR,

SEVERITY VARCHAR,

ERROR\_CODE VARCHAR,

ERROR\_MESSAGE VARCHAR

);

INSERT INTO DEV\_REFINED.PANTHER\_RULE\_MATCH.AWS\_VPCFLOW\_ALERTS

SELECT P\_ROW\_ID,P\_SOURCE\_ID,P\_EVENT\_TIME,P\_PARSE\_TIME,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES,SEVERITY,ERROR\_CODE,ERROR\_MESSAGE

FROM DEV\_STAGING.PANTHER\_RULE\_MATCH.AWS\_VPCFLOW\_RULES\_MATCH

SELECT \* FROM DEV\_STAGING.PANTHER\_RULE\_MATCH.AWS\_VPCFLOW\_RULES\_MATCH

-----

create or replace table DEV\_REFINED.PANTHER\_RULE\_MATCH.AWS\_S3SERVERACCESS\_ALERTS(

P\_ROW\_ID NUMBER,

P\_SOURCE\_ID NUMBER,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION VARCHAR,

P\_ANY\_IP\_ADDRESSES VARCHAR,

SEVERITY VARCHAR,

ERROR\_CODE VARCHAR,

ERROR\_MESSAGE VARCHAR

);

INSERT INTO DEV\_REFINED.PANTHER\_RULE\_MATCH.AWS\_S3SERVERACCESS\_ALERTS

SELECT P\_ROW\_ID,P\_SOURCE\_ID,P\_EVENT\_TIME,P\_PARSE\_TIME,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES,SEVERITY,ERROR\_CODE,ERROR\_MESSAGE

FROM DEV\_STAGING.PANTHER\_RULE\_MATCH.AWS\_S3SERVERACCESS\_RULE\_MATCH

select \* FROM DEV\_STAGING.PANTHER\_RULE\_MATCH.AWS\_S3SERVERACCESS\_RULE\_MATCH

-----

create or replace table DEV\_REFINED.PANTHER\_RULE\_MATCH.AWS\_CLOUDTRAIL\_ALERTS(

P\_ROW\_ID VARCHAR,

P\_SOURCE\_ID VARCHAR,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION VARCHAR,

P\_ANY\_IP\_ADDRESSES VARCHAR,

P\_ANY\_ACTOR\_IDS VARCHAR,

P\_RULE\_ID VARCHAR,

P\_ALERT\_ID VARCHAR,

P\_ALERT\_CONTEXT VARCHAR,

P\_ALERT\_CREATION\_TIME TIMESTAMP\_NTZ,

P\_ALERT\_UPDATE\_TIME TIMESTAMP\_NTZ,

P\_ALERT\_SEVERITY VARCHAR,

ERRORCODE VARCHAR,

ERRORMESSAGE VARCHAR

);

INSERT INTO DEV\_REFINED.PANTHER\_RULE\_MATCH.AWS\_CLOUDTRAIL\_ALERTS

SELECT P\_ROW\_ID,P\_SOURCE\_ID,P\_EVENT\_TIME,P\_PARSE\_TIME,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES,P\_ANY\_ACTOR\_IDS,P\_RULE\_ID,P\_ALERT\_ID,P\_ALERT\_CONTEXT,P\_ALERT\_CREATION\_TIME,P\_ALERT\_UPDATE\_TIME,P\_ALERT\_SEVERITY,ERRORCODE,ERRORMESSAGE

FROM DEV\_STAGING.PANTHER\_RULE\_MATCH.AWS\_CLOUDTRAIL\_RULE\_MATCH

SELECT \* FROM DEV\_STAGING.PANTHER\_RULE\_MATCH.AWS\_CLOUDTRAIL\_RULE\_MATCH

DEV\_STAGING.PANTHER\_LOGS.AWS\_CLOUDTRAIL

--------

create or replace table DEV\_REFINED.PANTHER\_RULE\_MATCH.OKTA\_ALERTS(

P\_ROW\_ID VARCHAR,

P\_SOURCE\_ID VARCHAR,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION NUMBER,

P\_ANY\_IP\_ADDRESSES VARCHAR,

P\_ANY\_ACTOR\_IDS VARCHAR,

P\_RULE\_ID VARCHAR,

P\_ALERT\_ID VARCHAR,

P\_ALERT\_CONTEXT VARCHAR,

P\_ALERT\_CREATION\_TIME TIMESTAMP\_NTZ,

P\_ALERT\_UPDATE\_TIME TIMESTAMP\_NTZ,

SEVERITY VARCHAR,

ERROR\_CODE VARCHAR,

ERROR\_MESSAGE VARCHAR

);

INSERT INTO DEV\_REFINED.PANTHER\_RULE\_MATCH.OKTA\_ALERTS

SELECT P\_ROW\_ID,P\_SOURCE\_ID,P\_EVENT\_TIME,P\_PARSE\_TIME,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES,P\_ANY\_ACTOR\_IDS,P\_RULE\_ID,P\_ALERT\_ID,P\_ALERT\_CONTEXT,P\_ALERT\_CREATION\_TIME,P\_ALERT\_UPDATE\_TIME,SEVERITY,ERROR\_CODE,ERROR\_MESSAGE

FROM DEV\_STAGING.PANTHER\_RULE\_MATCH.OKTA

select \* FROM DEV\_STAGING.PANTHER\_RULE\_MATCH.OKTA

-------------

create or replace table DEV\_REFINED.PANTHER\_VIEWS.ALL\_LOGS(

--------------

create or replace table DEV\_REFINED.HR\_DATA.EMPLOYEE\_LOGIN\_INFO(

USERID NUMBER,

USERNAME VARCHAR2,

FULLNAME VARCHAR2,

DEPARTMENT VARCHAR2,

DATETIME DATE,

IPADDRESS VARCHAR2,

LOGINTYPE VARCHAR2,

STATUS VARCHAR2,

LOCATION VARCHAR2,

BROWSER VARCHAR2,

OPERATINGSYSTEM VARCHAR2,

DEVICENAME VARCHAR2,

APPLICATION VARCHAR2

);

INSERT INTO DEV\_REFINED.HR\_DATA.EMPLOYEE\_LOGIN\_INFO

select USERID,USERNAME,FULLNAME,DEPARTMENT,DATETIME,IPADDRESS,LOGINTYPE,STATUS,LOCATION,BROWSER,OPERATINGSYSTEM,DEVICENAME,APPLICATION

from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

select fullname from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

----------------

create or replace table DEV\_REFINED.HR\_DATA.EMPLOYEE\_INFO(

USERID NUMBER,

EMP\_FIRST\_NAME VARCHAR2,

EMP\_LAST\_NAME VARCHAR2,

EMP\_EMAIL VARCHAR2,

EMP\_DEPARTMENT\_ID INT,

LOCATION\_ID INT

);

INSERT INTO DEV\_REFINED.HR\_DATA.EMPLOYEE\_INFO

SELECT USERID,SPLIT\_PART(FULLNAME, ' ', 1) as EMP\_FIRST\_NAME, SPLIT\_PART(FULLNAME, ' ', -1) as EMP\_LAST\_NAME,CONCAT(USERNAME, '.', FULLNAME, '@gmail.com.com') AS EMP\_EMAIL,D.DEPARTMENT\_ID,L.LOCATION\_ID

FROM DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO as E

left join DEV\_REFINED.HR\_DATA.EMPLOYEE\_DEPARTMENT as D

on E.DEPARTMENT = D.DEPARTMENT\_NAME

left join DEV\_REFINED.HR\_DATA.EMPLOYEE\_LOCATION as L

on E.LOCATION = L.LOCATION\_NAME

select \* from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

-------------

create or replace table DEV\_REFINED.HR\_DATA.EMPLOYEE\_IPADDR(

USERID NUMBER,

EMP\_IPADDRESS VARCHAR2

);

INSERT INTO DEV\_REFINED.HR\_DATA.EMPLOYEE\_IPADDR

select USERID,IPADDRESS as EMP\_IPADDRESS

from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

select \* from DEV\_REFINED.HR\_DATA.EMPLOYEE\_IPADDR;

select DEPARTMENT,LOCATION from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

GROUP BY DEPARTMENT,LOCATION

------------

create or replace table DEV\_REFINED.HR\_DATA.EMPLOYEE\_DEPARTMENT(

department\_id INT IDENTITY(1,1),

DEPARTMENT\_NAME VARCHAR

);

INSERT INTO DEV\_REFINED.HR\_DATA.EMPLOYEE\_DEPARTMENT (DEPARTMENT\_NAME)

select distinct department as DEPARTMENT\_NAME from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

select \* from DEV\_REFINED.HR\_DATA.EMPLOYEE\_DEPARTMENT

INSERT INTO DEV\_REFINED.HR\_DATA.EMPLOYEE\_DEPARTMENT

select DISTINCT DEPARTMENT as DEPARTMENT\_NAME,LOCATION AS LOCATION\_NAME,LOCATION\_ID

from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

create or replace table DEV\_REFINED.HR\_DATA.EMPLOYEE\_LOCATION(

LOCATION\_ID INT IDENTITY(1,1),

LOCATION\_NAME varchar

);

INSERT INTO DEV\_REFINED.HR\_DATA.EMPLOYEE\_LOCATION (LOCATION\_NAME)

select distinct LOCATION as LOCATION\_NAME from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

select \* from DEV\_REFINED.HR\_DATA.EMPLOYEE\_LOCATION

select count(distinct location) from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO

-------------

create or replace table DEV\_REFINED.HR\_DATA.test(

USERID NUMBER,

department varchar2,

department\_id int

);

select userid,department,b.department\_id

from DEV\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO as a

left join DEV\_REFINED.HR\_DATA.EMPLOYEE\_DEPARTMENT as b on a.department = b.department\_name

drop table DEV\_REFINED.HR\_DATA.test

------------

create or replace table DEV\_REFINED.PANTHER\_LOGS.AWS\_VPCFLOW\_EVENTS(

P\_ROW\_ID VARCHAR,

P\_SOURCE\_ID VARCHAR,

P\_EVENT\_TIME TIMESTAMP\_NTZ,

P\_PARSE\_TIME TIMESTAMP\_NTZ,

P\_LOG\_TYPE VARCHAR,

P\_SOURCE\_LABEL VARCHAR,

P\_SCHEMA\_VERSION NUMBER,

P\_ANY\_IP\_ADDRESSES VARCHAR

);