create or Replace database QA\_STAGING CLONE DEV\_STAGING ;

create or Replace database PROD\_STAGING CLONE DEV\_STAGING ;

SELECT GET\_DDL('DATABASE', 'DEV\_REFINED');

USE database DEV\_REFINED;

"""

create or replace schema HR\_DATA;

create or replace TABLE EMPLOYEE\_DEPARTMENT ( DEPARTMENT\_ID NUMBER(38,0), DEPARTMENT\_NAME VARCHAR(16777216), DEPARTMENT\_MANAGER\_ID VARCHAR(16777216), LOCATION\_ID NUMBER(38,0), PK\_HASH VARCHAR(16777216) );

create or replace TABLE EMPLOYEE\_INFO ( USERID NUMBER(38,0), EMP\_FIRST\_NAME VARCHAR(16777216), EMP\_LAST\_NAME VARCHAR(16777216), EMP\_EMAIL VARCHAR(16777216), EMP\_DEPARTMENT\_ID NUMBER(38,0), PK\_HASH VARCHAR(16777216) );

create or replace TABLE EMPLOYEE\_IPADDR ( USERID NUMBER(38,0), IPADDRESS VARCHAR(16777216) );

create or replace TABLE EMPLOYEE\_LOGIN\_INFO ( USERID NUMBER(38,0), USERNAME VARCHAR(16777216), FULLNAME VARCHAR(16777216), DEPARTMENT VARCHAR(16777216), DATETIME DATE, IPADDRESS VARCHAR(16777216), LOGINTYPE VARCHAR(16777216), STATUS VARCHAR(16777216), LOCATION VARCHAR(16777216), BROWSER VARCHAR(16777216), OPERATINGSYSTEM VARCHAR(16777216), DEVICENAME VARCHAR(16777216), APPLICATION VARCHAR(16777216), PK\_HASH VARCHAR(16777216) );

create or replace schema PANTHER\_LOGS;

create or replace TABLE AWS\_CLOUDTRAIL\_EVENTS ( P\_ROW\_ID VARCHAR(16777216), P\_SOURCE\_ID VARCHAR(16777216), P\_LOG\_TYPE VARCHAR(16777216), P\_SOURCE\_LABEL VARCHAR(16777216), P\_SCHEMA\_VERSION NUMBER(38,0), P\_ANY\_IP\_ADDRESSES VARCHAR(16777216), P\_EVENT\_TIME VARCHAR(16777216), P\_PARSE\_TIME VARCHAR(16777216), PK\_HASH VARCHAR(16777216) );

create or replace TABLE AWS\_S3SERVERACCESS\_EVENTS ( P\_ROW\_ID VARCHAR(16777216), P\_SOURCE\_ID VARCHAR(16777216), P\_EVENT\_TIME TIMESTAMP\_NTZ(9), P\_PARSE\_TIME TIMESTAMP\_NTZ(9), P\_LOG\_TYPE VARCHAR(16777216), P\_SOURCE\_LABEL VARCHAR(16777216), P\_SCHEMA\_VERSION NUMBER(38,0), P\_ANY\_IP\_ADDRESSES VARCHAR(16777216), PK\_HASH VARCHAR(16777216) );

create or replace TABLE AWS\_VPCFLOW\_EVENTS ( P\_ROW\_ID VARCHAR(16777216), P\_SOURCE\_ID VARCHAR(16777216), P\_EVENT\_TIME TIMESTAMP\_NTZ(9), P\_PARSE\_TIME TIMESTAMP\_NTZ(9), P\_LOG\_TYPE VARCHAR(16777216), P\_SOURCE\_LABEL VARCHAR(16777216), P\_SCHEMA\_VERSION NUMBER(38,0), P\_ANY\_IP\_ADDRESSES VARCHAR(16777216), PK\_HASH VARCHAR(16777216) );

create or replace TABLE OKTA\_SYSTEMLOG\_EVENTS ( P\_ROW\_ID VARCHAR(16777216), P\_SOURCE\_ID VARCHAR(16777216), P\_EVENT\_TIME TIMESTAMP\_NTZ(9), P\_PARSE\_TIME TIMESTAMP\_NTZ(9), P\_LOG\_TYPE VARCHAR(16777216), P\_SOURCE\_LABEL VARCHAR(16777216), P\_SCHEMA\_VERSION NUMBER(38,0), P\_ANY\_IP\_ADDRESSES VARCHAR(16777216), PK\_HASH VARCHAR(16777216) );

create or replace schema PANTHER\_RULE\_MATCH;

create or replace TABLE AWS\_CLOUDTRAIL\_ALERTS ( P\_ROW\_ID VARCHAR(16777216), P\_SOURCE\_ID VARCHAR(16777216), P\_EVENT\_TIME TIMESTAMP\_NTZ(9), P\_PARSE\_TIME TIMESTAMP\_NTZ(9), P\_LOG\_TYPE VARCHAR(16777216), P\_SOURCE\_LABEL VARCHAR(16777216), P\_SCHEMA\_VERSION VARCHAR(16777216), P\_ANY\_IP\_ADDRESSES VARCHAR(16777216), P\_ANY\_ACTOR\_IDS VARCHAR(16777216), P\_RULE\_ID VARCHAR(16777216), P\_ALERT\_ID VARCHAR(16777216), P\_ALERT\_CONTEXT VARCHAR(16777216), P\_ALERT\_CREATION\_TIME TIMESTAMP\_NTZ(9), P\_ALERT\_UPDATE\_TIME TIMESTAMP\_NTZ(9), P\_ALERT\_SEVERITY VARCHAR(16777216), ERRORCODE VARCHAR(16777216), ERRORMESSAGE VARCHAR(16777216), PK\_HASH VARCHAR(16777216) );

create or replace TABLE AWS\_S3SERVERACCESS\_ALERTS ( P\_EVENT\_TIME TIMESTAMP\_NTZ(9), P\_PARSE\_TIME TIMESTAMP\_NTZ(9), P\_LOG\_TYPE VARCHAR(16777216), P\_SOURCE\_LABEL VARCHAR(16777216), P\_SCHEMA\_VERSION VARCHAR(16777216), P\_ANY\_IP\_ADDRESSES VARCHAR(16777216), SEVERITY VARCHAR(16777216), ERROR\_CODE VARCHAR(16777216), ERROR\_MESSAGE VARCHAR(16777216), PK\_HASH VARCHAR(16777216), P\_ROW\_ID VARCHAR(16777216), P\_SOURCE\_ID VARCHAR(16777216) );

create or replace TABLE AWS\_VPCFLOW\_ALERTS ( P\_ROW\_ID VARCHAR(16777216), P\_SOURCE\_ID VARCHAR(16777216), P\_EVENT\_TIME TIMESTAMP\_NTZ(9), P\_PARSE\_TIME TIMESTAMP\_NTZ(9), P\_LOG\_TYPE VARCHAR(16777216), P\_SOURCE\_LABEL VARCHAR(16777216), P\_SCHEMA\_VERSION NUMBER(38,0), P\_ANY\_IP\_ADDRESSES VARCHAR(16777216), SEVERITY VARCHAR(16777216), ERROR\_CODE VARCHAR(16777216), ERROR\_MESSAGE VARCHAR(16777216), PK\_HASH VARCHAR(16777216) );

create or replace TABLE OKTA\_ALERTS ( P\_ROW\_ID VARCHAR(16777216), P\_SOURCE\_ID VARCHAR(16777216), P\_EVENT\_TIME TIMESTAMP\_NTZ(9), P\_PARSE\_TIME TIMESTAMP\_NTZ(9), P\_LOG\_TYPE VARCHAR(16777216), P\_SOURCE\_LABEL VARCHAR(16777216), P\_SCHEMA\_VERSION NUMBER(38,0), P\_ANY\_IP\_ADDRESSES VARCHAR(16777216), P\_ANY\_ACTOR\_IDS VARCHAR(16777216), P\_RULE\_ID VARCHAR(16777216), P\_ALERT\_ID VARCHAR(16777216), P\_ALERT\_CONTEXT VARCHAR(16777216), P\_ALERT\_CREATION\_TIME TIMESTAMP\_NTZ(9), P\_ALERT\_UPDATE\_TIME TIMESTAMP\_NTZ(9), SEVERITY VARCHAR(16777216), ERROR\_CODE VARCHAR(16777216), ERROR\_MESSAGE VARCHAR(16777216), PK\_HASH VARCHAR(16777216) );

create or replace schema PANTHER\_VIEWS;

"""

;

create or replace procedure DEV\_REF\_SP()

returns VARCHAR LANGUAGE SQL execute as caller as

BEGIN

insert into DEV\_REFINED.HR\_DATA.EMPLOYEE\_IPADDR select USERID , IPADDRESS from QA\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO;

insert into DEV\_REFINED.HR\_DATA.EMPLOYEE\_LOGIN\_INFO select

USERID , USERNAME , FULLNAME , DEPARTMENT , DATETIME DATE, IPADDRESS , LOGINTYPE , STATUS , LOCATION , BROWSER , OPERATINGSYSTEM , DEVICENAME ,APPLICATION, null from QA\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO;

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,

SRCADDR,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,SRCADDR))

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

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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

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

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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

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

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

SELECT

P\_ROW\_ID,

P\_SOURCE\_ID,

P\_LOG\_TYPE,

P\_SOURCE\_LABEL,

P\_SCHEMA\_VERSION,

P\_ANY\_IP\_ADDRESSES,

TO\_VARCHAR( P\_EVENT\_TIME),

TO\_VARCHAR( P\_PARSE\_TIME),

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

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

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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

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

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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

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

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

SELECT

P\_EVENT\_TIME,

P\_PARSE\_TIME,

P\_LOG\_TYPE,

P\_SOURCE\_LABEL,

P\_SCHEMA\_VERSION,

REMOTEIP,

SEVERITY,

ERROR\_CODE,

ERROR\_MESSAGE,

SHA1(CONCAT(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,REMOTEIP)),

P\_ROW\_ID,

P\_SOURCE\_ID

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

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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,SRCADDR))

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

END;

create or replace task ROLES\_INFO\_TB\_TASK

warehouse = COMPUTE\_WH

schedule = 'USING CRON 0 3 \* \* \* UTC'

As

call DEV\_REF\_SP();

create or replace procedure QA\_REF\_SP()

returns VARCHAR LANGUAGE SQL execute as caller as

BEGIN

insert into QA\_REFINED.HR\_DATA.EMPLOYEE\_IPADDR select USERID , IPADDRESS from QA\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO;

insert into QA\_REFINED.HR\_DATA.EMPLOYEE\_LOGIN\_INFO select

USERID , USERNAME , FULLNAME , DEPARTMENT , DATETIME DATE, IPADDRESS , LOGINTYPE , STATUS , LOCATION , BROWSER , OPERATINGSYSTEM , DEVICENAME ,APPLICATION, null from QA\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO;

INSERT INTO QA\_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,

SRCADDR,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,SRCADDR))

FROM QA\_STAGING.PANTHER\_LOGS.AWS\_VPCFLOW;

INSERT INTO QA\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM QA\_STAGING.PANTHER\_LOGS.AWS\_S3SERVERACCESS;

INSERT INTO QA\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM QA\_STAGING.PANTHER\_LOGS.OKTA\_SYSTEMLOG;

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

SELECT

P\_ROW\_ID,

P\_SOURCE\_ID,

P\_LOG\_TYPE,

P\_SOURCE\_LABEL,

P\_SCHEMA\_VERSION,

P\_ANY\_IP\_ADDRESSES,

TO\_VARCHAR( P\_EVENT\_TIME),

TO\_VARCHAR( P\_PARSE\_TIME),

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM QA\_STAGING.PANTHER\_LOGS.AWS\_CLOUDTRAIL;

INSERT INTO QA\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM QA\_STAGING.PANTHER\_RULE\_MATCH.AWS\_CLOUDTRAIL\_RULE\_MATCH;

INSERT INTO QA\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM QA\_STAGING.PANTHER\_RULE\_MATCH.OKTA;

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

SELECT

P\_EVENT\_TIME,

P\_PARSE\_TIME,

P\_LOG\_TYPE,

P\_SOURCE\_LABEL,

P\_SCHEMA\_VERSION,

REMOTEIP,

SEVERITY,

ERROR\_CODE,

ERROR\_MESSAGE,

SHA1(CONCAT(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,REMOTEIP)),

P\_ROW\_ID,

P\_SOURCE\_ID

FROM QA\_STAGING.PANTHER\_RULE\_MATCH.AWS\_S3SERVERACCESS\_RULE\_MATCH;

INSERT INTO QA\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,SRCADDR))

FROM QA\_STAGING.PANTHER\_RULE\_MATCH.AWS\_VPCFLOW\_RULES\_MATCH;

END;

call QA\_REF\_SP();

create or replace task ROLES\_INFO\_TB\_TASK

warehouse = COMPUTE\_WH

schedule = 'USING CRON 0 3 \* \* \* UTC'

As

call QA\_REF\_SP();

use role prod\_refined\_rw;

use database PROD\_REFINED;

create or replace procedure PROD\_REF\_SP()

returns VARCHAR LANGUAGE SQL execute as caller as

BEGIN

insert into PROD\_REFINED.HR\_DATA.EMPLOYEE\_IPADDR select USERID , IPADDRESS from PROD\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO;

insert into PROD\_REFINED.HR\_DATA.EMPLOYEE\_LOGIN\_INFO select

USERID , USERNAME , FULLNAME , DEPARTMENT , DATETIME DATE, IPADDRESS , LOGINTYPE , STATUS , LOCATION , BROWSER , OPERATINGSYSTEM , DEVICENAME ,APPLICATION, null from PROD\_STAGING.HR\_DATA.EMPLOYEE\_LOGGING\_INFO;

INSERT INTO PROD\_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,

SRCADDR,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,SRCADDR))

FROM PROD\_STAGING.PANTHER\_LOGS.AWS\_VPCFLOW;

INSERT INTO PROD\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM PROD\_STAGING.PANTHER\_LOGS.AWS\_S3SERVERACCESS;

INSERT INTO PROD\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM PROD\_STAGING.PANTHER\_LOGS.OKTA\_SYSTEMLOG;

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

SELECT

P\_ROW\_ID,

P\_SOURCE\_ID,

P\_LOG\_TYPE,

P\_SOURCE\_LABEL,

P\_SCHEMA\_VERSION,

P\_ANY\_IP\_ADDRESSES,

TO\_VARCHAR( P\_EVENT\_TIME),

TO\_VARCHAR( P\_PARSE\_TIME),

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM PROD\_STAGING.PANTHER\_LOGS.AWS\_CLOUDTRAIL;

INSERT INTO PROD\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM PROD\_STAGING.PANTHER\_RULE\_MATCH.AWS\_CLOUDTRAIL\_RULE\_MATCH;

INSERT INTO PROD\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,P\_ANY\_IP\_ADDRESSES))

FROM PROD\_STAGING.PANTHER\_RULE\_MATCH.OKTA;

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

SELECT

P\_EVENT\_TIME,

P\_PARSE\_TIME,

P\_LOG\_TYPE,

P\_SOURCE\_LABEL,

P\_SCHEMA\_VERSION,

REMOTEIP,

SEVERITY,

ERROR\_CODE,

ERROR\_MESSAGE,

SHA1(CONCAT(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,REMOTEIP)),

P\_ROW\_ID,

P\_SOURCE\_ID

FROM PROD\_STAGING.PANTHER\_RULE\_MATCH.AWS\_S3SERVERACCESS\_RULE\_MATCH;

INSERT INTO PROD\_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,

SHA1(concat(P\_ROW\_ID,P\_SOURCE\_ID,P\_LOG\_TYPE,P\_SOURCE\_LABEL,P\_SCHEMA\_VERSION,SRCADDR))

FROM PROD\_STAGING.PANTHER\_RULE\_MATCH.AWS\_VPCFLOW\_RULES\_MATCH;

END;

create or replace task ROLES\_INFO\_TB\_TASK

warehouse = COMPUTE\_WH

schedule = 'USING CRON 0 3 \* \* \* UTC'

As

call PROD\_REF\_SP();