PROD\_ANALYTICS.PANTHER\_LOGS--------DATABASES

USE ROLE SYSADMIN;

CREATE DATABASE DEV\_STAGING;

CREATE DATABASE DEV\_REFINED;

CREATE DATABASE DEV\_ANALYTICS;

CREATE DATABASE QA\_STAGING;

CREATE DATABASE QA\_REFINED;

CREATE DATABASE QA\_ANALYTICS;

CREATE DATABASE PROD\_STAGING;

CREATE DATABASE PROD\_REFINED;

CREATE DATABASE PROD\_ANALYTICS;

---------Schemas

USE ROLE SYSADMIN;

create or replace schema DEV\_STAGING.panther\_rule\_match;

create or replace schema DEV\_STAGING.panther\_logs;

create or replace schema DEV\_STAGING.panther\_views;

create or replace schema DEV\_STAGING.HR\_DATA;

create or replace schema DEV\_REFINED.panther\_rule\_match;

create or replace schema DEV\_REFINED.panther\_logs;

create or replace schema DEV\_REFINED.HR\_DATA;

---------Tables

create or replace table dev\_staging.panther\_rule\_match.okta(

uuid VARCHAR2,

published VARCHAR2,

eventType VARCHAR2,

version VARCHAR2,

severity VARCHAR2,

legacyEventType VARCHAR2,

displayMessage VARCHAR2,

actor VARCHAR2,

client VARCHAR2,

request VARCHAR2,

outcome VARCHAR2,

target VARCHAR2,

transaction VARCHAR2,

debugContext VARCHAR2,

authenticationContext VARCHAR2,

securityContext VARCHAR2,

device VARCHAR2,

p\_event\_time VARCHAR2,

p\_parse\_time VARCHAR2,

p\_log\_type VARCHAR2,

p\_row\_id VARCHAR2,

p\_source\_id VARCHAR2,

p\_source\_label VARCHAR2,

p\_schema\_version VARCHAR2,

p\_any\_ip\_addresses VARCHAR2,

p\_any\_domain\_names VARCHAR2,

p\_any\_emails VARCHAR2,

p\_any\_actor\_ids VARCHAR2,

p\_rule\_id VARCHAR2,

p\_alert\_id VARCHAR2,

p\_alert\_context VARCHAR2,

p\_alert\_creation\_time VARCHAR2,

p\_alert\_update\_time VARCHAR2,

p\_enrichment VARCHAR2,

p\_rule\_tags VARCHAR2,

p\_rule\_reports VARCHAR2,

p\_alert\_severity VARCHAR2,

p\_rule\_severity VARCHAR2

);

create or replace table dev\_staging.panther\_logs.okta\_systemlog(

uuid VARCHAR2,

published VARCHAR2,

eventType VARCHAR2,

version VARCHAR2,

severity VARCHAR2,

legacyEventType VARCHAR2,

displayMessage VARCHAR2,

actor VARCHAR2,

client VARCHAR2,

request VARCHAR2,

outcome VARCHAR2,

target VARCHAR2,

transaction VARCHAR2,

debugContext VARCHAR2,

authenticationContext VARCHAR2,

securityContext VARCHAR2,

device VARCHAR2,

p\_event\_time VARCHAR2,

p\_parse\_time VARCHAR2,

p\_log\_type VARCHAR2,

p\_row\_id VARCHAR2,

p\_source\_id VARCHAR2,

p\_source\_label VARCHAR2,

p\_schema\_version VARCHAR2,

p\_any\_ip\_addresses VARCHAR2,

p\_any\_domain\_names VARCHAR2,

p\_any\_emails VARCHAR2,

p\_any\_actor\_ids VARCHAR2

);

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

p\_db\_name VARCHAR2,

p\_table\_name VARCHAR2,

p\_any\_actor\_ids VARCHAR2,

p\_any\_aws\_account\_ids VARCHAR2,

p\_any\_aws\_arns VARCHAR2,

p\_any\_aws\_instance\_ids VARCHAR2,

p\_any\_aws\_tags VARCHAR2,

p\_any\_domain\_names VARCHAR2,

p\_any\_emails VARCHAR2,

p\_any\_ip\_addresses VARCHAR2,

p\_any\_mac\_addresses VARCHAR2,

p\_any\_md5\_hashes VARCHAR2,

p\_any\_sha1\_hashes VARCHAR2,

p\_any\_sha256\_hashes VARCHAR2,

p\_any\_trace\_ids VARCHAR2,

p\_any\_usernames VARCHAR2,

p\_event\_time VARCHAR2,

p\_log\_type VARCHAR2,

p\_parse\_time VARCHAR2,

p\_row\_id VARCHAR2,

p\_schema\_version VARCHAR2,

p\_source\_id VARCHAR2,

p\_source\_label VARCHAR2

);

create or replace table dev\_staging.panther\_logs.aws\_s3serveraccess(

bucketowner VARCHAR2,

bucket VARCHAR2,

time VARCHAR2,

remoteip VARCHAR2,

requester VARCHAR2,

requestid VARCHAR2,

operation VARCHAR2,

key VARCHAR2,

requesturi VARCHAR2,

httpstatus VARCHAR2,

errorcode VARCHAR2,

bytessent VARCHAR2,

objectsize VARCHAR2,

totaltime VARCHAR2,

turnaroundtime VARCHAR2,

referrer VARCHAR2,

useragent VARCHAR2,

versionid VARCHAR2,

hostid VARCHAR2,

signatureversion VARCHAR2,

ciphersuite VARCHAR2,

authenticationtype VARCHAR2,

hostheader VARCHAR2,

tlsVersion VARCHAR2,

accesspointarn VARCHAR2,

aclrequired VARCHAR2,

additionalFields VARCHAR2,

p\_event\_time VARCHAR2,

p\_parse\_time VARCHAR2,

p\_log\_type VARCHAR2,

p\_row\_id VARCHAR2,

p\_source\_id VARCHAR2,

p\_source\_label VARCHAR2,

p\_schema\_version VARCHAR2,

p\_any\_ip\_addresses VARCHAR2,

p\_any\_domain\_names VARCHAR2,

p\_any\_aws\_account\_ids VARCHAR2,

p\_any\_aws\_instance\_ids VARCHAR2,

p\_any\_aws\_arns VARCHAR2

);

create or replace table dev\_staging.panther\_logs.aws\_vpcflow(

version VARCHAR2,

account VARCHAR2,

interfaceId VARCHAR2,

srcAddr VARCHAR2,

dstAddr VARCHAR2,

srcPort VARCHAR2,

dstPort VARCHAR2,

protocol VARCHAR2,

packets VARCHAR2,

bytes VARCHAR2,

starts VARCHAR2,

end VARCHAR2,

action VARCHAR2,

status VARCHAR2,

vpcId VARCHAR2,

subNetId VARCHAR2,

instanceId VARCHAR2,

tcpFlags VARCHAR2,

trafficType VARCHAR2,

pktSrcAddr VARCHAR2,

pktDstAddr VARCHAR2,

pktSrcAwsService VARCHAR2,

pktDstAwsService VARCHAR2,

flowDirection VARCHAR2,

trafficPath VARCHAR2,

region VARCHAR2,

azId VARCHAR2,

sublocationType VARCHAR2,

sublocationId VARCHAR2,

p\_event\_time VARCHAR2,

p\_parse\_time VARCHAR2,

p\_log\_type VARCHAR2,

p\_row\_id VARCHAR2,

p\_source\_id VARCHAR2,

p\_source\_label VARCHAR2,

p\_schema\_version VARCHAR2,

p\_any\_ip\_addresses VARCHAR2,

p\_any\_aws\_account\_ids VARCHAR2,

p\_any\_aws\_instance\_ids VARCHAR2

);

create or replace table dev\_staging.panther\_logs.aws\_cloudtrail(

additionalEventData VARCHAR2,

apiVersion VARCHAR2,

awsRegion VARCHAR2,

errorCode VARCHAR2,

errorMessage VARCHAR2,

eventID VARCHAR2,

eventName VARCHAR2,

eventSource VARCHAR2,

eventTime VARCHAR2,

eventType VARCHAR2,

eventVersion VARCHAR2,

managementEvent VARCHAR2,

readOnly VARCHAR2,

recipientAccountId VARCHAR2,

requestID VARCHAR2,

requestParameters VARCHAR2,

resources VARCHAR2,

responseElements VARCHAR2,

serviceEventDetails VARCHAR2,

sharedEventID VARCHAR2,

sourceIPAddress VARCHAR2,

userAgent VARCHAR2,

userIdentity VARCHAR2,

vpcEndpointId VARCHAR2,

eventCategory VARCHAR2,

sessionCredentialFromConsole VARCHAR2,

edgeDeviceDetails VARCHAR2,

tlsDetails VARCHAR2,

p\_event\_time VARCHAR2,

p\_parse\_time VARCHAR2,

p\_log\_type VARCHAR2,

p\_row\_id VARCHAR2,

p\_source\_id VARCHAR2,

p\_source\_label VARCHAR2,

p\_schema\_version VARCHAR2,

p\_any\_ip\_addresses VARCHAR2,

p\_any\_domain\_names VARCHAR2,

p\_any\_md5\_hashes VARCHAR2,

p\_any\_sha1\_hashes VARCHAR2,

p\_any\_sha256\_hashes VARCHAR2,

p\_any\_trace\_ids VARCHAR2,

p\_any\_aws\_account\_ids VARCHAR2,

p\_any\_aws\_instance\_ids VARCHAR2,

p\_any\_aws\_arns VARCHAR2,

p\_any\_aws\_tags VARCHAR2,

p\_any\_emails VARCHAR2,

p\_any\_usernames VARCHAR2,

p\_any\_mac\_addresses VARCHAR2,

p\_any\_actor\_ids VARCHAR2

);

create or replace table dev\_staging.panther\_logs.aws\_cloudtrail\_test(

additionalEventData VARCHAR2,

apiVersion VARCHAR2,

awsRegion VARCHAR2,

errorCode VARCHAR2,

errorMessage VARCHAR2,

eventID VARCHAR2,

eventName VARCHAR2,

eventSource VARCHAR2,

eventTime VARCHAR2,

eventType VARCHAR2,

eventVersion VARCHAR2,

managementEvent VARCHAR2,

readOnly VARCHAR2,

recipientAccountId VARCHAR2,

requestID VARCHAR2,

requestParameters VARCHAR2,

resources VARCHAR2,

responseElements VARCHAR2,

serviceEventDetails VARCHAR2,

sharedEventID VARCHAR2,

sourceIPAddress VARCHAR2,

userAgent VARCHAR2,

userIdentity VARCHAR2,

vpcEndpointId VARCHAR2,

eventCategory VARCHAR2,

sessionCredentialFromConsole VARCHAR2,

edgeDeviceDetails VARCHAR2,

tlsDetails VARCHAR2,

p\_event\_time VARCHAR2,

p\_parse\_time VARCHAR2,

p\_log\_type VARCHAR2,

p\_row\_id VARCHAR2,

p\_source\_id VARCHAR2,

p\_source\_label VARCHAR2,

p\_schema\_version VARCHAR2,

p\_any\_ip\_addresses VARCHAR2,

p\_any\_domain\_names VARCHAR2,

p\_any\_md5\_hashes VARCHAR2,

p\_any\_sha1\_hashes VARCHAR2,

p\_any\_sha256\_hashes VARCHAR2,

p\_any\_trace\_ids VARCHAR2,

p\_any\_aws\_account\_ids VARCHAR2,

p\_any\_aws\_instance\_ids VARCHAR2,

p\_any\_aws\_arns VARCHAR2,

p\_any\_aws\_tags VARCHAR2,

p\_any\_emails VARCHAR2,

p\_any\_usernames VARCHAR2,

p\_any\_mac\_addresses VARCHAR2,

p\_any\_actor\_ids VARCHAR2

);

create or replace TABLE DEV\_STAGING.PANTHER\_RULE\_MATCH.AWS\_CLOUDTRAIL\_RULE\_MATCH (

additionalEventData varchar2,

apiVersion varchar2,

awsRegion varchar2,

errorCode varchar2,

errorMessage varchar2,

eventID varchar2,

eventName varchar2,

eventSource varchar2,

eventTime varchar2,

eventType varchar2,

eventVersion varchar2,

managementEvent varchar2,

readOnly varchar2,

recipientAccountId varchar2,

requestID varchar2,

requestParameters varchar2,

resources varchar2,

responseElements varchar2,

serviceEventDetails varchar2,

sharedEventID varchar2,

sourceIPAddress varchar2,

userAgent varchar2,

userIdentity varchar2,

vpcEndpointId varchar2,

eventCategory varchar2,

sessionCredentialFromConsole varchar2,

edgeDeviceDetails varchar2,

tlsDetails varchar2,

p\_event\_time varchar2,

p\_parse\_time varchar2,

p\_log\_type varchar2,

p\_row\_id varchar2,

p\_source\_id varchar2,

p\_source\_label varchar2,

p\_schema\_version varchar2,

p\_any\_ip\_addresses varchar2,

p\_any\_domain\_names varchar2,

p\_any\_md5\_hashes varchar2,

p\_any\_sha1\_hashes varchar2,

p\_any\_sha256\_hashes varchar2,

p\_any\_trace\_ids varchar2,

p\_any\_aws\_account\_ids varchar2,

p\_any\_aws\_instance\_ids varchar2,

p\_any\_aws\_arns varchar2,

p\_any\_aws\_tags varchar2,

p\_any\_emails varchar2,

p\_any\_usernames varchar2,

p\_any\_mac\_addresses varchar2,

p\_any\_actor\_ids varchar2,

p\_rule\_id varchar2,

p\_alert\_id varchar2,

p\_alert\_context varchar2,

p\_alert\_creation\_time varchar2,

p\_alert\_update\_time varchar2,

p\_enrichment varchar2,

p\_rule\_tags varchar2,

p\_rule\_reports varchar2,

p\_alert\_severity varchar2,

p\_rule\_severity varchar2

);

create or replace table All\_Logs\_Panther(

P\_ROW\_ID VARCHAR(200),

P\_SOURCE\_ID VARCHAR(200),

P\_EVENT\_TIME VARCHAR(200),

P\_PARSE\_TIME VARCHAR(200),

P\_LOG\_TYPE VARCHAR(200),

P\_SOURCE\_LABEL VARCHAR(200),

P\_SCHEMA\_VERSION VARCHAR(200),

P\_ANY\_IP\_ADDRESSES VARCHAR(200)

);

create or replace table All\_Logs\_Panther\_Rule\_match(

P\_ROW\_ID VARCHAR(200),

P\_SOURCE\_ID VARCHAR(200),

P\_EVENT\_TIME VARCHAR(200),

P\_PARSE\_TIME VARCHAR(200),

P\_LOG\_TYPE VARCHAR(200),

P\_SOURCE\_LABEL VARCHAR(200),

P\_SCHEMA\_VERSION VARCHAR(200),

P\_ANY\_IP\_ADDRESSES VARCHAR(200)

);