



*North American Technology Division
Solution Engineering Team*

300 Oracle Public Cloud Workshop

Oracle Management Cloud – Security Monitoring & Analytics

Update: January 04, 2018

Introduction

The purpose of this lab is to give the participant hands on experience of Security Monitoring and Analytics Cloud Service and how they can leverage this service to enable rapid detection and investigation of security threats.

To log issues, click here to go to the [github oracle](https://github.com/oracle/SecurityCloudDay/issues/new) (<https://github.com/oracle/SecurityCloudDay/issues/new>) repository issue submission form.

Objectives

In this lab, we will cover –

- How to access your SMA environment
- Enabling SMA service
- Reviewing pre-configured correlation rules
- Creating alert rules
- Uploading sample data
- How to evaluate threats

Pre-requisites

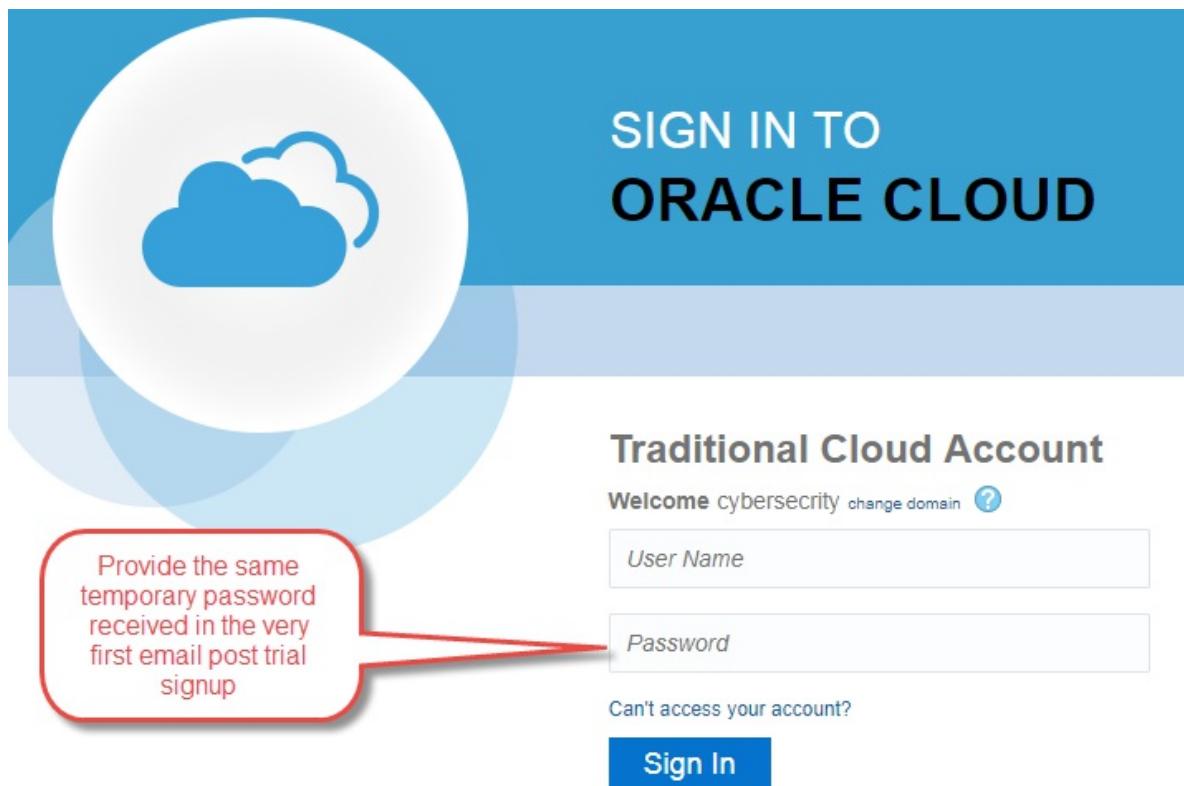
The following are minimum requirements for this lab

- Oracle Cloud Trial account with OMC instance provisioned. Refer to [How to request your free trial account](https://csdoracle.github.io/Cloud-Security-Day/CSD-SETUP.html) (<https://csdoracle.github.io/Cloud-Security-Day/CSD-SETUP.html>) if you haven't already done so.
- Sample data: Staged on the linux host provided
- A computer with an internet connection and an SSH client

STEP 1 – Accessing your Environment & Initial Configuration

Accessing your OMC Instance

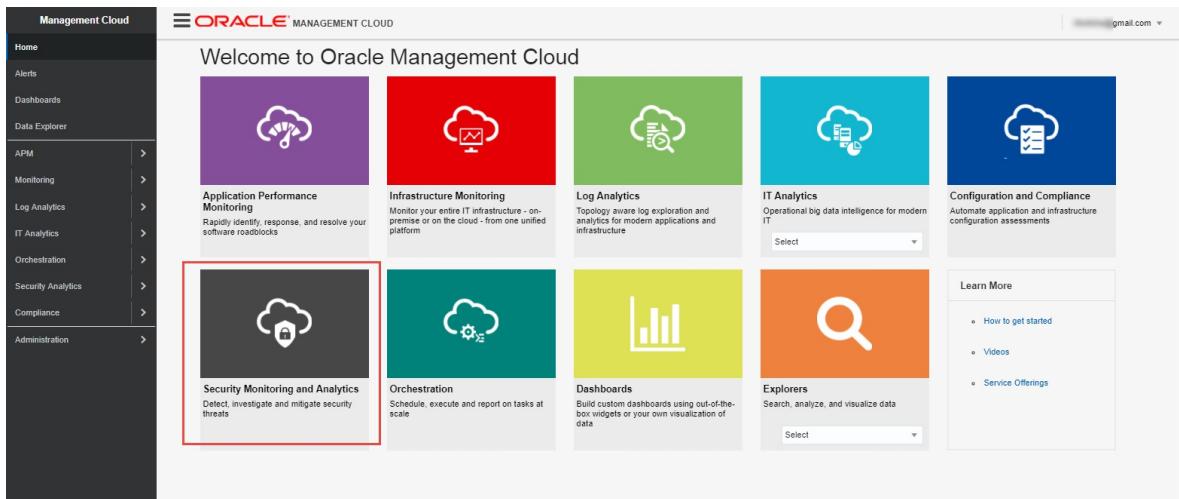
1. Navigate to one of the URLs in your Service Activation email to access the service. You will be prompted to change the password on first login.



2. Create a new password and provide challenge Q&A for resetting should you ever need to.

The image shows the 'Password Management' page. At the top, there's a header with a user icon and the text 'Password Management'. On the right, there are 'Submit' and 'Required field' buttons. The main form area contains three password input fields: 'Old Password', 'New Password', and 'Re-Type New Password', all marked with an asterisk to indicate they are required. Below these, there's a section for 'Register challenge questions for your account' with three rows. Each row has a question (e.g., 'What is the name of your pet?'), a dropdown menu, an answer field (e.g., 'Answer 1'), and another dropdown menu. The entire form is enclosed in a light gray border.

3. You're now ready to start using any of the services shown below. Our focus will be narrowed to "Security Monitoring and Analytics"



Instance Configuration

Prior to using the new service the following minimum configuration should be completed:

1. Enable Security Monitoring & Analytics
2. SMA alert rules

Enabling Security Monitoring Analytics

1. Navigate to Menu Icon -> Home -> Administration -> Entities Configuration -> Licensing

Key	Value	Assigned Entities
There are no tags defined		

2. Click on "DISABLED" under "SMA Enrichment"

The screenshot shows the Oracle Management Cloud Administration interface. On the left, there's a sidebar with various administration options like Alert Rules, Notification Channels, Agents, etc. The main panel is titled 'Administration' and specifically focuses on 'Licensing'. It displays the date 'As of Fri, Dec 15, 2017, 1:48:11 PM'. Under 'New License Auto-Assignment', it says 'None'. The 'Log Collection' status is 'ENABLED'. In the top right corner, the 'SMA Enrichment' status is shown as 'DISABLED' with a red box around it. Below this, there's a section for 'Entities' with counts for Unlicensed (0), Standard Edition (0), Enterprise Edition (0), and Configuration & Compliance (0). A modal window at the bottom allows selecting entities to change licensing editions.

- Push selector for “Enable Security Monitoring and Analytics” to the right and click “Apply” to enable

This screenshot shows the same Oracle Management Cloud interface as above, but with a modal window open over the 'Entities' section. The modal has a 'Settings' header and contains two options: 'Enable Log Collection' (which is selected, indicated by a blue toggle switch) and 'Enable Security Monitoring and Analytics' (which is unselected, indicated by a grey toggle switch). A red arrow points to the 'Enable Security Monitoring and Analytics' option. At the bottom of the modal are 'Apply' and 'Cancel' buttons.

- Enable New License Auto-Assigment by Clicking on "None"

This screenshot shows the Oracle Management Cloud interface again. The 'New License Auto-Assignment' status has been changed from 'None' to 'Enterprise' (highlighted with a red box). The other settings remain the same: 'Log Collection' is 'ENABLED' and 'SMA Enrichment' is 'ENABLED'. The rest of the interface looks identical to the previous screenshots.

- Toggle selector as shown below and click “Apply”

This screenshot shows the Oracle Management Cloud interface with a modal window titled 'New License Auto-Assignment'. Inside the modal, there are two dropdown menus: 'License Edition' (set to 'Enterprise') and 'Config & Compliance' (set to 'Configuration & Compliance'). Both of these dropdowns are highlighted with a red box. At the bottom of the modal are 'Apply' and 'Cancel' buttons.

Create Security Monitoring & Analytics-based Alert(s)

1. Navigate Menu Icon -> Home -> Administration -> Alert Rules and Select “Security Analytics” from the Drop-Down Menu

The screenshot shows the Oracle Management Cloud interface. On the left, a sidebar titled 'Administration' lists various management options like Alert Rules, Notification Channels, Agents, etc. A red box highlights the 'Alert Rules' option. The main content area is titled 'Alert Rules' and shows a table with columns: Rule, Entities, Channels, Last Modified By, and Enabled. At the top of the table, there is a search bar and a dropdown menu labeled 'Service' with 'Security Analytics' selected. A red box highlights this dropdown. There are also buttons for '+ Create Alert Rule' and 'Disable Notifications'.

2. Click on “Create Alert Rule”

This screenshot shows the same Oracle Management Cloud interface as above, but the table in the main content area displays the message 'You have no matching alert rules defined.' A red box highlights the '+ Create Alert Rule' button at the top right of the table area.

3. Follow the steps provided below to create the “Warning” alert rule. Fill in the form as shown below and click “+ Email Channel”

This screenshot shows the 'Create Alert Rule' dialog box. The left sidebar of the main interface is visible, showing various monitoring and analytics services. The dialog box has fields for 'Rule Name' (set to 'Warning Security Threat Risk Level Alert Rule'), 'Rule Description' (set to 'Warning Security Threat Risk Level Alert Rule'), and 'Generate Alerts' (set to 'For All Threats'). A red box highlights the 'Warning Alert' radio button under 'Generate Alerts'. Below this, there are sections for 'Notifications' and 'Integrations'. Under 'Notifications', there is a 'Email' section with a dropdown menu and a red box highlighting the '+ Email Channel' button. Under 'Integrations', there is a 'Select integrations' dropdown menu. Buttons for 'Save' and 'Cancel' are at the bottom right of the dialog box.

4. Fill in the form as shown below, click “Create” to add your first “Email Channel”, then click “Save” to create the “Warning” alert rule

The screenshot shows the Oracle Management Cloud interface. On the left, a sidebar lists various services: Home, Alerts, Dashboards, Data Explorer, APM, Monitoring, Log Analytics, IT Analytics, Orchestration, Security Analytics, Compliance, and Administration. The main area is titled "Create Alert Rule". It has fields for "Rule Name" (Warning Security Threat Risk Level Alert Rule), "Rule Description" (Warning Security Threat Risk Level Alert Rule), "Generate Alerts" (radio buttons for "For All Threats", "Warning Alert", and "Critical Alert"), "Based on Risk Level" (radio buttons for "Operator" and "Risk Level"), and "Notifications" (Email, Mobile, Integrations). A modal window titled "Create Email Channel" is open, showing a "Channel Name" field with "My App Security Support Mail-Group" and an "Email Addresses" field with "app-sec@mycompany.com". Buttons for "Create" and "Cancel" are at the bottom of the modal.

5. Optionally repeat step above and create the “critical” rule by switching from warning to critical

The screenshot shows the Oracle Management Cloud interface under the "Administration" section. The left sidebar includes "Alert Rules", "Notification Channels", "Agents", "Add Entity", "Cloud Discovery Profiles", "Entities Configuration", "APM Admin", "Monitoring Admin", "Log Admin", "Security Admin", and "Compliance Admin". The main area is titled "Alert Rules" and displays a table with two rows of data. The columns are "Rule", "Entities", "Channels", and "Last Modified By". The first row contains "Critical Security Threat Risk Level Alert Rule" and "Threat" under Entities, with channels "@gmail.com" and last modified by "@gmail.com, 1 hour ago". The second row contains "Warning Security Threat Risk Level Alert Rule" and "Threat" under Entities, with channels "@gmail.com" and last modified by "@gmail.com, 1 hour ago". Navigation buttons for "Previous" and "Next" are at the bottom of the table.

Review Correlation Rules for Evaluating Threats

1. Login to your OMC instance and select the SMA service

The screenshot shows the Oracle Management Cloud homepage. The top banner says "Welcome to Oracle Management Cloud". Below are six service tiles arranged in a grid:

- Application Performance Monitoring**: Rapidly identify, response, and resolve your software roadblocks.
- Infrastructure Monitoring**: Monitor your entire IT infrastructure - on-premise or on the cloud - from one unified platform.
- Log Analytics**: Topology aware log exploration and analytics for modern applications and infrastructure.
- IT Analytics**: Operational big data intelligence for modern IT.
- Configuration and Compliance**: Automate application and infrastructure configuration assessments.
- Security Monitoring and Analytics**: Detect, investigate and mitigate security threats.

The "Security Monitoring and Analytics" tile is highlighted with a red border.

2. Click the ‘Menu Icon’ to the left of Oracle logo in the top left of your window to access the menu
3. Click on Security Admin

The screenshot shows the Oracle Security Analytics interface. On the left, a dark sidebar lists several options: Alerts, Users (which is selected and highlighted with a blue bar at the top), Threats, Activity, Assets, Services, Domains, Log Explorer, and Security Admin. The 'Security Admin' option is highlighted with a red box. The main content area has a header 'MANAGEMENT CLOUD | Security Monitoring and Analytics'. Below the header, there's a 'Threats' section with a threat icon and counts: All 0, Critical 0, High 0, Medium 0, Low 0. To the right, there's a 'Risk Trend' section with three categories: 'Risky Users', 'Threats', and 'Risky Assets'. A message 'No data to display' is visible in the center.

4. Click on Correlation Rules

The screenshot shows the 'Security Admin' screen. The left sidebar has 'Correlation Rules' highlighted with a red box. Other options in the sidebar include Machine Learning Models, Storage Usage, Log Configuration, Alert Rules, and Watch Lists. The main content area includes a 'Threats' summary with counts: All 0, Critical 0, High 0, Medium 0, Low 0. A 'Risk Trend' section for 'Risky Users' is also present.

5. On the Correlation Rules screen, take a moment to explore some of the built-in correlation rules available within SMA for the purposes of threat detection. In today’s lab we will exercise three threats under the Host category
 - o Host <-- Targeted Account Attack
 - o Host <-- Multiple Failed Logins
 - o Host <-- Brute Force Attack
6. Click on each one in turn and review the Definition as well as the Parameters available

Correlation Rules

The screenshot shows the 'Correlation Rules' section of a security tool. On the left, there's a sidebar with a search bar and filters for 'Enabled Only' and 'Disabled Only'. Below that are 'Expand All' and 'Collapse All' buttons. The main area is a tree view of correlation rules:

- Database**: Rules detecting potential attacks on databases.
- Firewall**: Rules detecting potential attacks originating outside the firewall.
- Host**: Rules detecting potential attacks on hosts.
 - BruteForceAttack** (3)
 - DirectRootLogin**
 - LocalAccountCreation**
 - MultipleFailedLogin** (2)
 - MultipleFailedSu**
 - MultipleFailedSudo**
 - SuspiciousSuLogin**
 - TargetedAccountAttack** (1)
- Watch List**: Rules detecting potential attacks involving entities.

7. Access the sidebar menu again, and click on the back arrow in the sidebar menu, then select Log Explorer
8. Access the sidebar menu, select Log Admin -> Uploads

The screenshot shows the 'Log Admin' interface. The sidebar on the left lists various management options:

- Alert Rules
- Collection Warnings
- Entities
- Log Parsers
- Log Sources
- Lookups
- Saved Searches
- Storage
- Uploads** (highlighted with a red box)

The main pane has several sections:

- Visualize**: A dropdown menu currently set to 'Records with Histogram'.
- Fields**: A list of fields being analyzed:
 - Entity
 - Entity Type
 - Log Source
 - Host Name (Server)
 - Severity
- Field Summary**: A histogram showing the count of records for different entity types. The y-axis is labeled 'Count' and ranges from 0.4K to 2.4K. The x-axis categories are Entity Type, Entity, Log Source, Host Name (Server), and Severity.
- Records with Histogram**: A checkbox with the text 'Use the Show Log' next to it.

9. For the moment, this page should be empty. In the next section, we will upload all relevant files and then return to this screen to review our uploads and check associated log data and then Activity in SMA

STEP 2 – On-Demand Security Logs Data Upload

There are multiple methods for getting data into your environment, the most common methods are installing Cloud Agents directly on the source machines in question or using the ODU method. For this lab, we will be using the ODU method.

Connecting to the Linux Host to Upload Test Data

On the shared Linux Server, you will find the sample data and upload scripts for the lab under /u01/stage. The host IP address and credentials will be provided by the instructor before the lab.

1. Obtain the Linux server IP address and password from the instructor
2. Using your preferred SSH utility from your laptop, login with OS username "cdsma"

Adding User Context to OMC

In addition to log data, sample user context data will be added to OMC as well to provide a richer experience by mapping users identified in security logs to detailed corporate directory sourced from the company's Identity Service. In real production setting, this data will come from an Identity Service such as IDCS and by means of integration.

1. In your SSH session, navigate to /u01/stage
2. From [My Cloud Services Dashboard](https://myservices.us2.oraclecloud.com/mycloud/cloudportal/dashboard) (<https://myservices.us2.oraclecloud.com/mycloud/cloudportal/dashboard>), toggle "Identity Domain" selector to your "Traditional" domain, then click on Management Cloud as shown below

The screenshot shows the Oracle My Cloud Services Dashboard. At the top, there is a navigation bar with 'Dashboard', 'Users', and a search icon. A red box highlights the 'Identity Domain' dropdown menu, which is set to 'davidree - North America (traditional)'. Below the navigation bar, there is a 'Cloud Services' summary section with 'Important Notifications' (0) and a '\$300' promotion banner. A red box highlights the 'Management Cloud' section title. This section contains a chart titled 'Management Cloud' with a Subscription ID of 1747520. The chart displays four data series: 'Standard entities (100...)' with values [60, 30, 0], 'Enterprise entities (100...)' with values [1.2, 0.6, 0.0], 'Log data (300 GB...)' with values [1.2, 0.6, 0.0], and 'Config and Entities...' with values [1.2, 0.6, 0.0]. The x-axis for all charts ranges from 28 to 6. At the bottom of the Management Cloud section, there are three icons: a checkmark, a gear, and a grid.

3. Get the Tenant ID, OMC Service Instance Name, and OMC Username as shown below

Identity Domain Name: **davidrlee**

TenantID: **davidrlee**

Service Instances:

Service Instance	instanceName	username	Administrator	Requested By	Service Instance URL
davidrleeomc1	davidrleeomc1	@davidrlee.com	@davidrlee.com	@davidrlee.com	https://davidrleeomc1-davidrlee.itom.management.cloud.us.oracle.com

- Using the items gathered above, update environment variables accordingly as shown in this example

```
export tenantID=acmeinc          #Tenant ID
export instanceName=ops          #OMC Service Instance Name
export username=John.Doe@gmail.com #OMC Username
```

- Execute the Unix shell script `omc_upload_usr_context.sh` and type in your OMC account password when prompted to upload User context file

```
[cdsma@myhost]$ ./omc_upload_usr_context.sh
```

Uploading Linux Secure Logs to OMC

For the benefit of this lab, you will be uploading sample Linux Secure logs files to OMC covering the following 3 security threats types:

- Target Account Attack
- Multiple Failed Login
- Brute Force Attack

In real production setting, this data will be continuously streamed to OMC by OMC cloud agents and API integration. SMA supports uploading user data available in SCIM or LDIF format. The former will be used.

- From the same Linux host as indicated earlier and still with the environment variables set, run the Unix shell script `omc_upload_security_events.sh` to upload Linux secure logs.

```
[cdsma@myhost]$ ./omc_upload_security_events.sh
```

STEP 3 – Visualization – Review Log Data and Threat Activities

Once you have successfully uploaded the three log files, navigate back to the Uploads page. Refresh the page to see your uploaded log files.

File Name	Created By	Last Updated
csd_brute_force_attack	gian.sartor@oracle.com	12/19/2017, 8:47:34 PM
csd_mult_failed_login	gian.sartor@oracle.com	12/19/2017, 8:43:01 PM
csd_target_attack	gian.sartor@oracle.com	12/19/2017, 8:42:46 PM
... (other log files)	... (other log files)	... (other log files)

Review Log Data and Threat Activities in OMC

The data uploaded provides insights into key steps that make up what is known as a Kill Chain: Anomaly Detection ==> Reconnaissance ==> Infiltration ==> Lateral Movement.

Assess Linux Targeted Account Attack Data

You may recall that the definition of a Targeted Account Attack is *5 or more failed login events associated with the same user account are detected within an interval of 60 seconds across single or multiple endpoints* from the Correlation Rules page we review earlier.

1. Switch to your SSH session and open the linux_ta_attack.log file

- o [gsartor@lux sample-logs]\$ less linux_ta_attack.log
- o Note the hostnames for hr1 and finance1 as well as the value for rhost and user
- o Note how many records are in this file (12)

```
Dec 19 08:08:01 hr1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=mbaker2
Dec 19 08:08:02 hr1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=mbaker2
Dec 19 08:08:03 hr1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=mbaker2
Dec 19 08:08:04 hr1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=mbaker2
Dec 19 08:08:05 hr1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=mbaker2
Dec 19 08:08:06 hr1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=mbaker2
Dec 19 08:08:07 hr1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=mbaker2
Dec 19 08:13:07 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sklm_us
Dec 19 08:13:08 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sklm_us
Dec 19 08:13:09 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sklm_us
Dec 19 08:13:10 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sklm_us
Dec 19 08:13:11 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sklm_us
Dec 19 08:13:12 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sklm_us
```

2. Switch back to your browser and to the Uploads page. Click the 'Menu Icon' in the csd_target_attack row and select View in Log Explorer

3. You are now viewing the log data in OMC Log Analytics. Security relevant data flowing to SMA goes through LA where it is enriched with security relevant tags. Note the filter being applied in the page as well as the number of relevant events (12).

4. In the sidebar menu, click the back button in the top left-hand corner and select Security Analytics from the service list.
5. Toggle the timeframe selector in the upper right-hand corner, set it to "12/18/2017 – 12/20/2017", then return to the sidebar menu and click on Activity to get a high-level overview of relevant security activities detected in your environment during that timeframe

6. Scroll further down the same page to view a list of the activities

Security Analytics

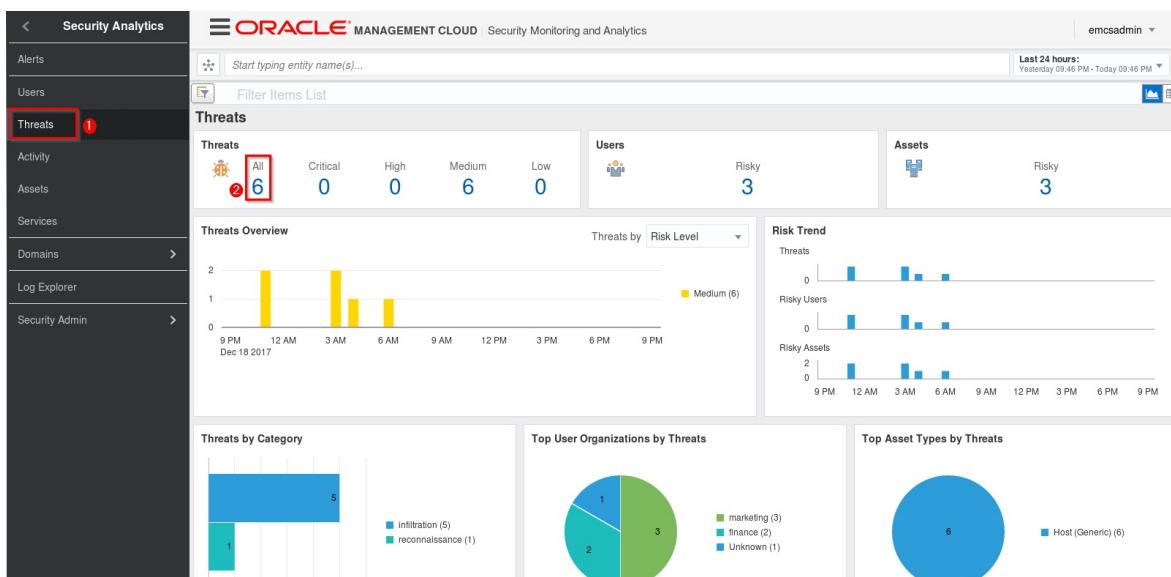
- Alerts
- Users
- Threats
- Activity**
- Assets
- Services
- Domains >
- Log Explorer
- Security Admin >

Activity List

Log

ID	User	Activity	Result	Category	Original Action	Resource	Source	Destination	Time
9ef...	User_Internal_sagrawal	authentication.login	success	authentication	sshd	sagrawal	10.260.213.60	finance1.host.oracle.com	Dec 19, 2017 6:55:06 AM
6f36...	User_Internal_sagrawal	authentication.login	denied	authentication	sshd	sagrawal		finance1.host.oracle.com	Dec 19, 2017 6:55:05 AM
462f...	User_Internal_sagrawal	authentication.login	denied	authentication	sshd	sagrawal		finance1.host.oracle.com	Dec 19, 2017 6:55:04 AM
c2c...	User_Internal_sagrawal	authentication.login	denied	authentication	sshd	sagrawal		finance1.host.oracle.com	Dec 19, 2017 6:55:03 AM
c18...	User_Internal_sagrawal	authentication.login	denied	authentication	sshd	sagrawal		finance1.host.oracle.com	Dec 19, 2017 6:55:02 AM
8ee...	User_Internal_sagrawal	authentication.login	denied	authentication	sshd	sagrawal		finance1.host.oracle.com	Dec 19, 2017 6:55:01 AM
4f16...	User_Internal_sagrawal	authentication.login	denied	authentication	sshd	sagrawal		finance1.host.oracle.com	Dec 19, 2017 6:55:00 AM
60e...	User_Internal_harry_ramab	authentication.login	denied	authentication	sshd	harry_ramab		finance1.us.oracle.com	Dec 19, 2017 4:03:03 AM
62c...	User_Internal_shirley_kimab	authentication.login	denied	authentication	sshd	shirley_kimab		finance1.us.oracle.com	Dec 19, 2017 4:01:07 AM
f96e...	mary.baker@acmeloric.com	authentication.login	denied	authentication	sshd	mbaker_us		hr1.us.oracle.com	Dec 19, 2017 4:01:06 AM
767f...	mary.baker@acmeloric.com	authentication.login	denied	authentication	sshd	mbaker_db		hr1.us.oracle.com	Dec 19, 2017 4:01:05 AM
067...	mary.baker@acmeloric.com	authentication.login	denied	authentication	sshd	mbaker_qa		hr1.us.oracle.com	Dec 19, 2017 4:01:04 AM
089...	mary.baker@acmeloric.com	authentication.login	denied	authentication	sshd	mbaker_dev		hr1.us.oracle.com	Dec 19, 2017 4:01:03 AM
bac...	mary.baker@acmeloric.com	authentication.login	denied	authentication	sshd	mbaker_us		hr1.us.oracle.com	Dec 19, 2017 4:01:02 AM
4ee...	mary.baker@acmeloric.com	authentication.login	denied	authentication	sshd	mbaker2		hr1.us.oracle.com	Dec 19, 2017 4:01:01 AM

7. Click Threats in the sidebar menu, then click the number under All in the Threats section



8. Scroll down to the bottom of the page and review the threat details. Note the Correlation Rule value as well as the Category type of ‘infiltration’ and the accounts being targeted.

Security Analytics

- Alerts
- Users
- Threats**
- Activity
- Assets
- Services
- Domains >
- Log Explorer
- Security Admin >

Threats

Threat Timeline

Details

Log

Activity Explorer

ID	Risk	Correlation Rule	Category	Activity	User	Account	Destination	Destination Type	Start Time
941...	Medium	TargetedAccountAttack	Infiltration	authentication.login	User_Internal_sagrawal	skim_us	finance1.host.oracle.com	Host (Generic)	Dec 19, 2017 3:13:07 AM
1bfa...	Medium	TargetedAccountAttack	Infiltration	authentication.login	mary.baker@acmeloric.com	mbaker2	hr1.host.oracle.com	Host (Generic)	Dec 19, 2017 3:08:01 AM
ef5e...	Medium	TargetedAccountAttack	Infiltration	authentication.login	skim3@acmeloric.com	skim_us	finance1.host.oracle.com	Host (Generic)	Dec 18, 2017 11:13:07 PM
c5a...	Medium	TargetedAccountAttack	Infiltration	authentication.login	mary.baker@acmeloric.com	mbaker2	hr1.host.oracle.com	Host (Generic)	Dec 18, 2017 11:04:01 PM

9. Now let's repeat this process for the Multiple Failed Login and Brute Force Attack log files

Assess Multiple Failed Logins Data

Before reviewing the files, lets remind ourselves of the definition for Multiple Failed Login Correlation Rule, *5 or more failed login events are detected on multiple accounts on the same endpoint, within a time interval of 60 seconds*

1. Switch to your SSH session and open the linux_mfl_attack.log file
 - o [gsartor@lux sample-logs]\$ less linux_mfl_attack.log
 - o On this occasion, each failed login is for a different username. This is different from the Targeted User Attack we covered in the previous section.
 - o Note how many records are in this file (8)

```
Dec 19 09:01:01 hrl.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=mbaker2
Dec 19 09:01:02 hrl.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=mbaker_us
Dec 19 09:01:03 hrl.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=mbaker_dev
Dec 19 09:01:04 hrl.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=mbaker_qa
Dec 19 09:01:05 hrl.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=mbaker_db
Dec 19 09:01:06 hrl.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=mbaker_us
Dec 19 09:01:07 finance1.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=shirley_kimab
Dec 19 09:03:03 finance1.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=harry_ramab
```

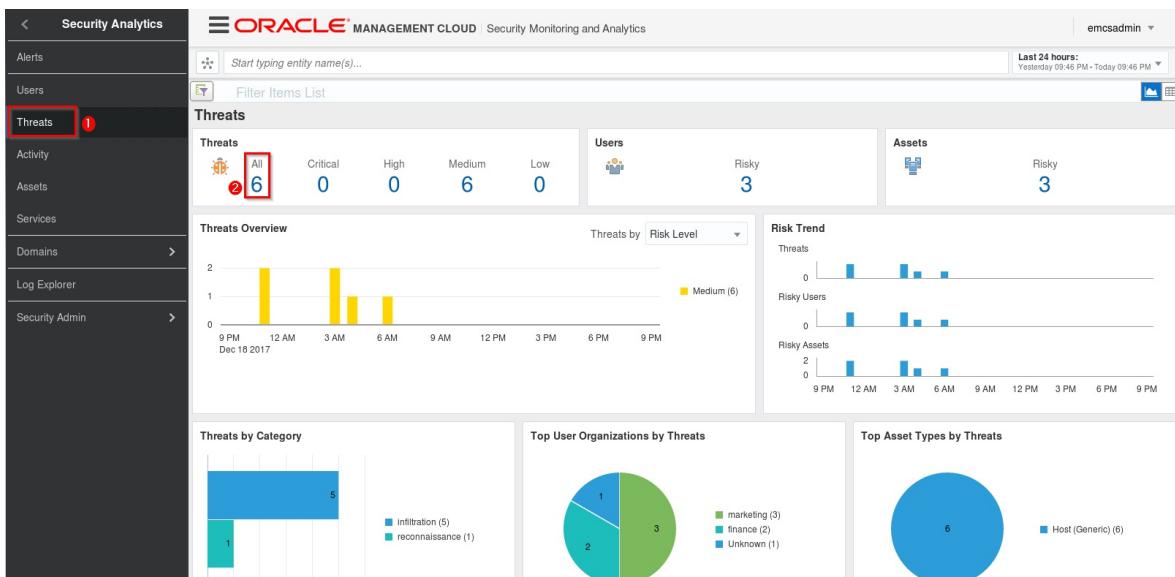
2. Switch back to your browser and to the Uploads page. Click the 'Menu Icon' in the csd_multi_failed_login row and select View in Log Explorer

		Created By	Last Updated	
csd_brute_force_attack	gian.sartor@oracle.com	12/19/2017, 8:47:34 PM		
csd_mult_failed_login	gian.sartor@oracle.com	12/19/2017, 8:43:01 PM		
csd_target_attack	gian.sartor@oracle.com	12/19/2017, 8:42:46 PM		
[redacted]	[redacted]	12/18/2017, 10:31:56 PM		

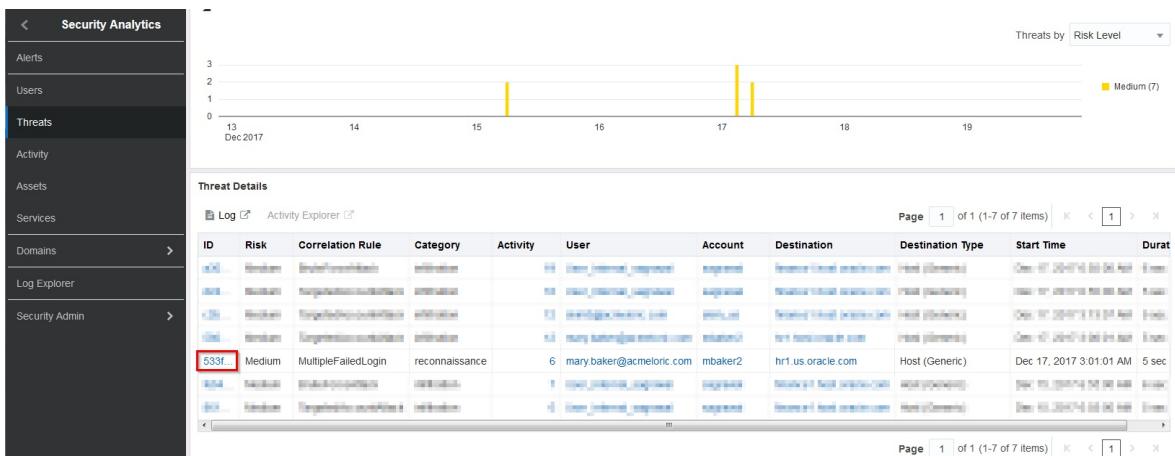
3. We are now back in Log Analytics and again take note of the filter being applied to the data we are viewing as well as the number of records being displayed. This matches the number of logs in our source file

Time (UTC-5:00)	Original Log Content
Dec 19, 2017, 4:03:03 AM	Dec 19 09:03:03 finance1.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=harry_ramab Entity = LinuxSyslog1 Entity Type = Host (Linux) Log Source = Linux Secure Logs Host Name (Server) = finance1.us.oracle.com
Dec 19, 2017, 4:01:07 AM	Dec 19 09:01:07 finance1.us.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abby.road.com user=harry_ramab Entity = LinuxSyslog1 Entity Type = Host (Linux) Log Source = Linux Secure Logs Host Name (Server) = finance1.us.oracle.com

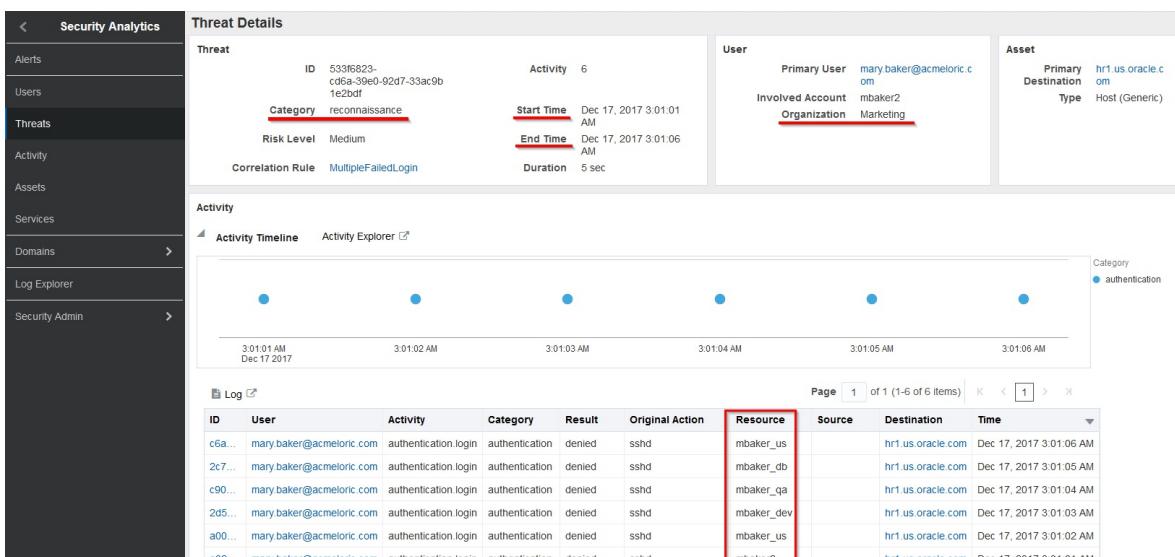
4. This time lets go straight to the Threats page in SMA. Once you are at the Threats page, click on the number below All in the Threats section.



5. In the Threat Details section, locate the MultipleFailedLogin and click the ID



6. On the new Threat Details page, you now have access to a lot of detailed information for this specific threat. You can see the Category, Start and End time of this activity, the account being used for the attack as well as which Department that account belongs to, in this case Marketing. This departmental information came from our User Context Upload. Lastly, note the various usernames in the Resource column; the same as the ones in the upload file.



Assess Brute Force Attack Data

Finally, in this last section, we will assess the activity for a Brute Force Attack. Described as *5 or more failed login events are followed by a successful login on the same endpoint, associated with the same user account, within an interval of 60 seconds.*

1. Let's return for the last time the SSH session and review the upload file for the Brute Force Attack. Switch to your SSH session and open the linux_bfa_attack.log file
 - o [gsartor@lux sample-logs]\$ less linux_bfa_attack.log
 - o Note the timing of the events, note that only one user is being targeted and lastly, note that we have a successful login on the last line
 - o Note how many records are in this file (7)

```
Dec 19 11:55:00 finance1.host.oracle.com sshd[23558]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sagravwal
Dec 19 11:55:01 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sagravwal
Dec 19 11:55:02 finance1.host.oracle.com sshd[23550]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sagravwal
Dec 19 11:55:03 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sagravwal
Dec 19 11:55:04 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sagravwal
Dec 19 11:55:05 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sagravwal
Dec 19 11:55:06 finance1.host.oracle.com sshd[23586]: Accepted password for sagravwal from 10.260.213.60 port 28783 ssh2
```

2. Switch back to your browser and to the Uploads page. Click the 'Menu Icon' in the csd_brute_force_attack row and select View in Log Explorer

Upload Name	Created By	Last Updated
csd_brute_force_attack	gian.sartor@oracle.com	12/19/2017, 8:47:34 PM
csd_mult_failed_login	gian.sartor@oracle.com	12/19/2017, 8:43:01 PM
csd_target_attack	gian.sartor@oracle.com	12/19/2017, 8:42:46 PM
rfrontcha.cloud_days_upload_2c	Rene.fontha@oracle.com	12/18/2017, 10:31:56 PM

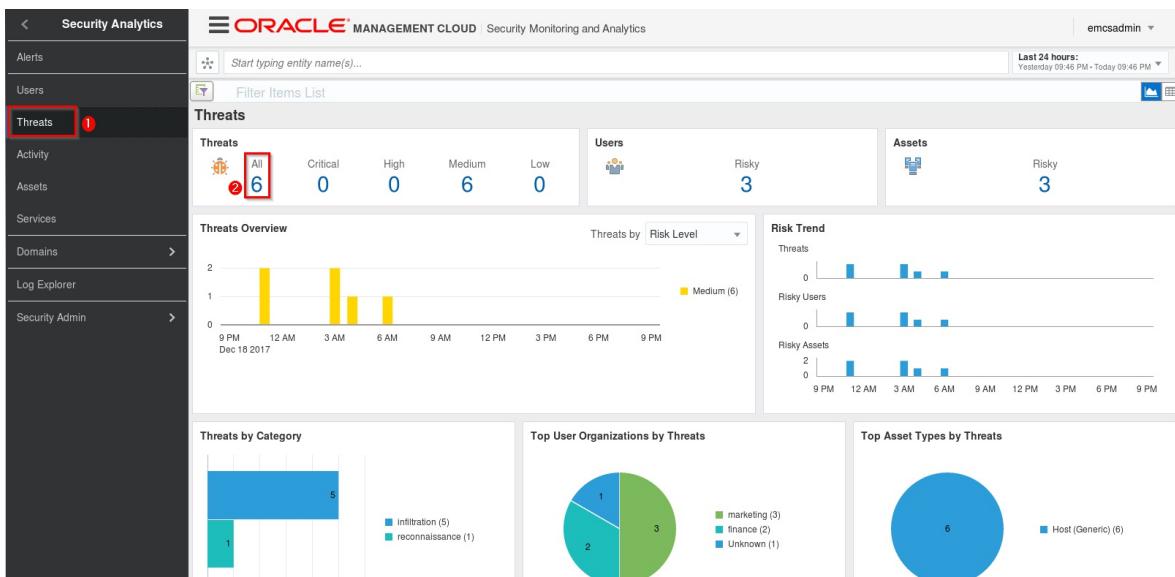
3. Back in Log Analytics and again take note of the filter being applied to the data we are viewing as well as the number of records being displayed. This matches the number of logs in our source file

Log Explorer: Untitled

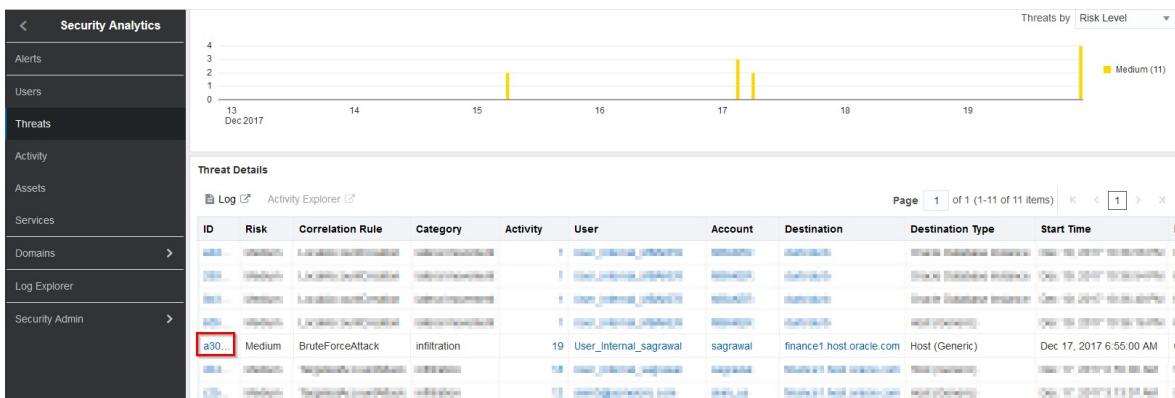
Upload Name: 'gian.sartor@oracle.com.csd_brute_force_attack' ①

Time (UTC-5:00)	Original Log Content
Dec 19, 2017, 6:55:05 AM	Dec 19 11:55:06 finance1.host.oracle.com sshd[23586]: Accepted password for sagravwal from 10.260.213.60 port 28783 ssh2
Dec 19, 2017, 6:55:05 AM	Ent1 = LinuxSyslog1 Entity Type = Host (Linux) Log Source = Linux Secure Logs Host Name (Server) = finance1.host.oracle.com
Dec 19, 2017, 6:55:05 AM	Dec 19 11:55:05 finance1.host.oracle.com sshd[23559]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=submarine.abbey.road.com user=sagravwal
Dec 19, 2017, 6:55:05 AM	Ent1 = LinuxSyslog1 Entity Type = Host (Linux) Log Source = Linux Secure Logs Host Name (Server) = finance1.host.oracle.com

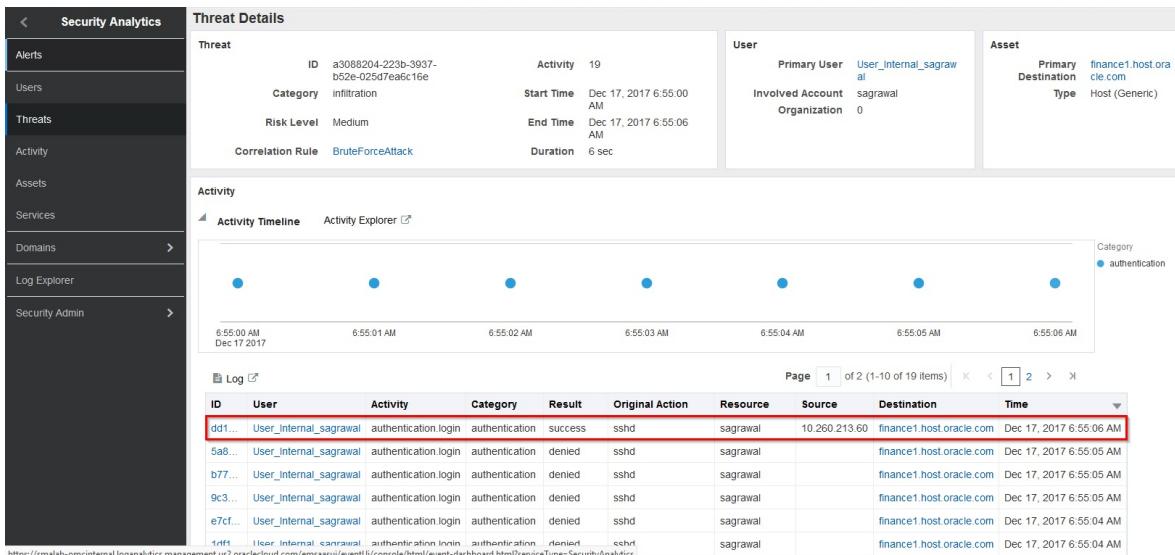
4. Once again, we'll go straight to the Threats page in SMA. Once you are at the Threats page, click on the number below All in the Threats section.



5. In the Threat Details section, locate the BruteForceAttack and click the ID



6. Take a few moments to review the details on the page, noting most importantly that we have many failed logins followed by a successful login.



This concludes the threat assessment portion of this lab.

Review alert emails

In case you haven't already noticed, you should have received some alert emails based on the activity we have been generating over the course of this lab.

The screenshot shows an email from Oracle Management Cloud. The subject line is "Critical Alert: Comprehensive Risk level for Threat with ID 02321ab9-da02-3459-900e-d7d920592681 and name MultipleUserCreation in category lateral movement is 3; it is greater than expected critical value of 1 (1 - Low; 2 - Medium; 3 - High; 4 - Critical)". The email body contains the following information:

Hello,

Oracle Management Cloud has reported an alert. Here are the details:

Alert Message	Comprehensive Risk level for Threat with ID 02321ab9-da02-3459-900e-d7d920592681 and name MultipleUserCreation in category lateral movement is 3; it is greater than expected critical value of 1 (1 - Low; 2 - Medium; 3 - High; 4 - Critical)
Severity	Critical
Raised On	Wed, December 20, 2017 03:36:58 AM UTC
Alert Rule	Security Threat Risk Level Alert Rule Critical

Thank You,
Oracle Management Cloud - Empowering Modern Business in the Cloud

Copyright 2017, Oracle and/or its affiliates. All rights reserved. [About Oracle](#) | [Legal Notices and Terms of Use](#) | [Privacy Statement](#)

This is a system generated message. Do not reply to this message. You are receiving this email as a result of your current relationship with Oracle Cloud. General marketing opt-out preferences have been over-ridden to ensure that you receive this email.

Summary

In this lab, we:

- Setup alerts
- Reviewed Correlation Rules in SMA
- Uploaded data to your environment
- Assessed the threats associated with the data uploads
- Navigated through the user interface of both the Log Analytics Cloud Service as well as the Security Monitoring & Analytics Cloud Service
- We saw how SMA categorizes threats and how we can enrich the log data with user context
- Understood what comprises a kill chain and why that is important
- Reviewed alert emails