

THREAT INTELLIGENCE (OCI)

1. What is OCI?

- OCI, or Oracle Cloud Infrastructure, is Oracle's cloud computing platform. It offers a range of services for deploying and scaling applications with high performance and security. OCI is known for its global presence, robust infrastructure, and support for diverse workloads, making it a preferred choice for enterprises.

2. What is OCI Security?

- OCI security involves protective measures in Oracle Cloud Infrastructure to safeguard data and resources from unauthorized access and cyber threats, using features like encryption and identity management.

3. What is Threat Intelligence?

- Threat intelligence in OCI refers to curated information about potential cybersecurity threats and vulnerabilities relevant to the Oracle Cloud Infrastructure environment. It includes data on malicious activities, attack patterns, emerging threats, and indicators of compromise (IOCs).

4. What is Threat Intelligence Data Base?

- A threat intelligence database is a repository of structured threat intelligence data, typically containing information such as known malware signatures, IP addresses of malicious servers, domain names associated with phishing campaigns, and other threat indicators.

5. Important of Threat Intelligence?

- Proactive Security

- Risk Assessment

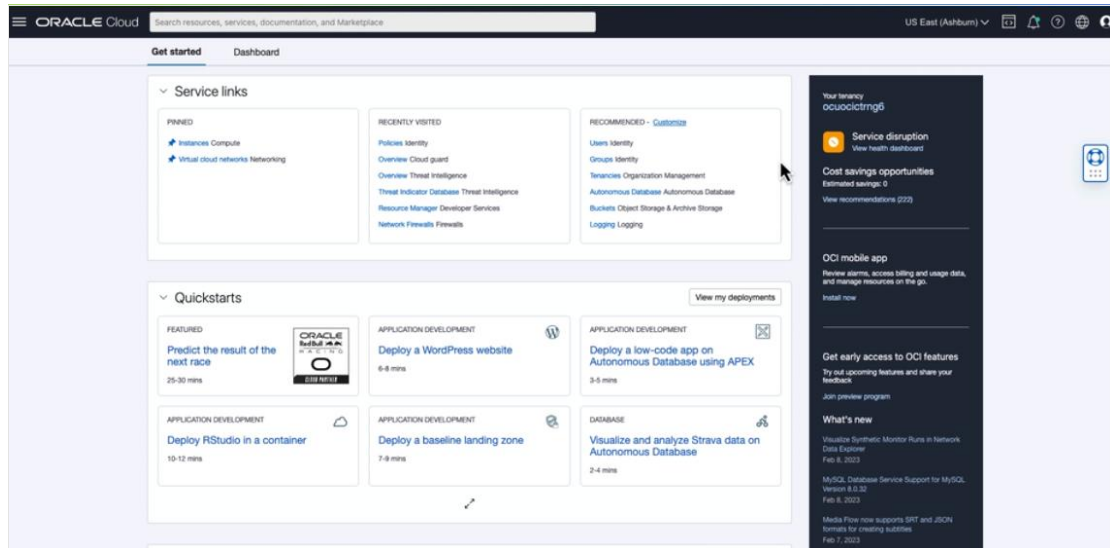
- Incident Response

- Adaptive Defense

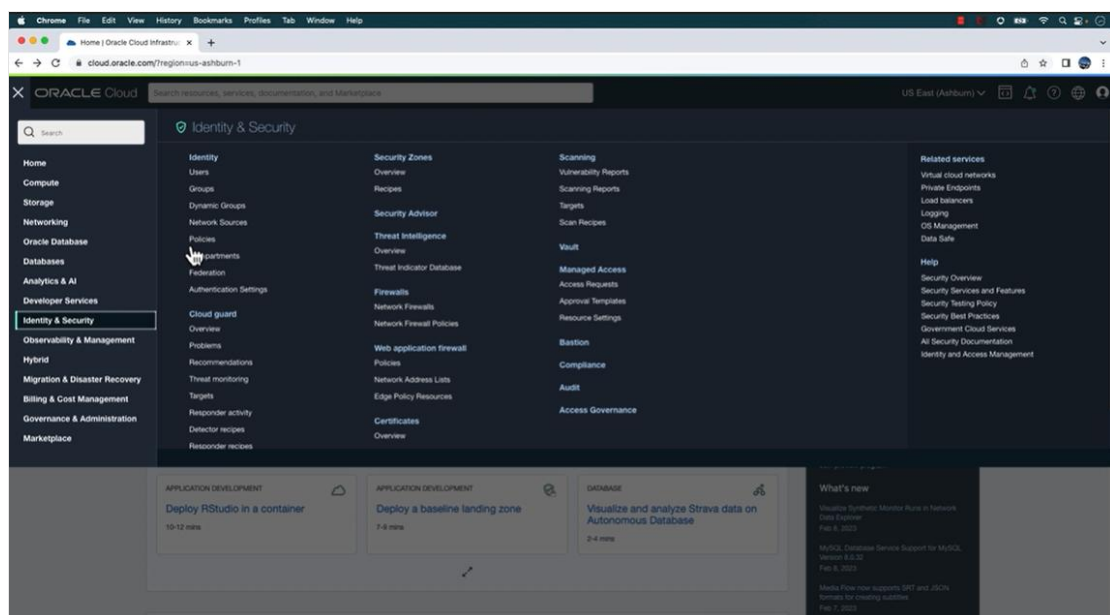
- Compliance Requirements

CONFIGURATION

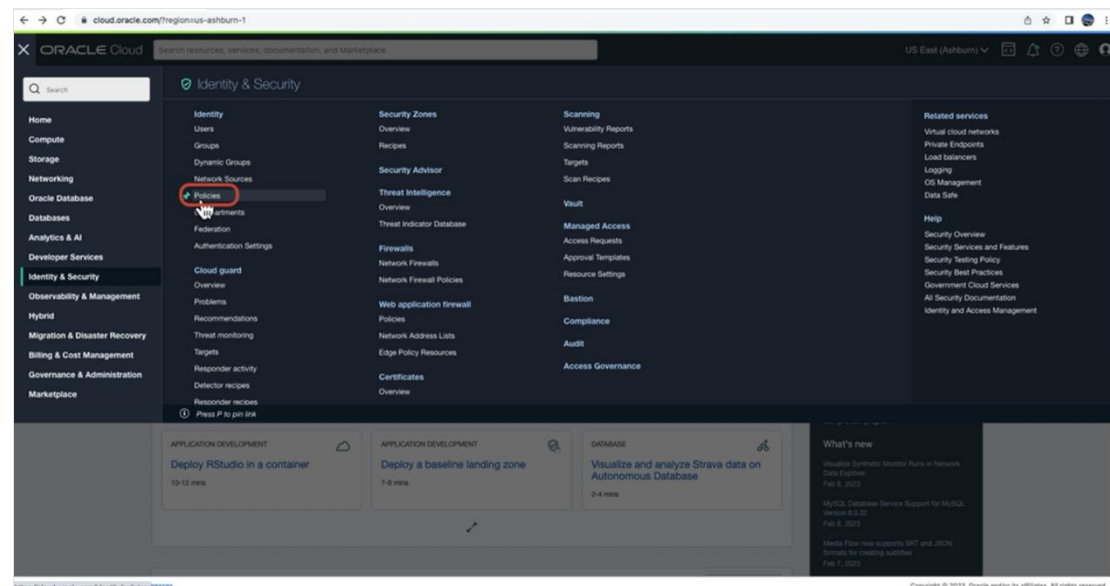
STEP 1 :- First login to the OCI



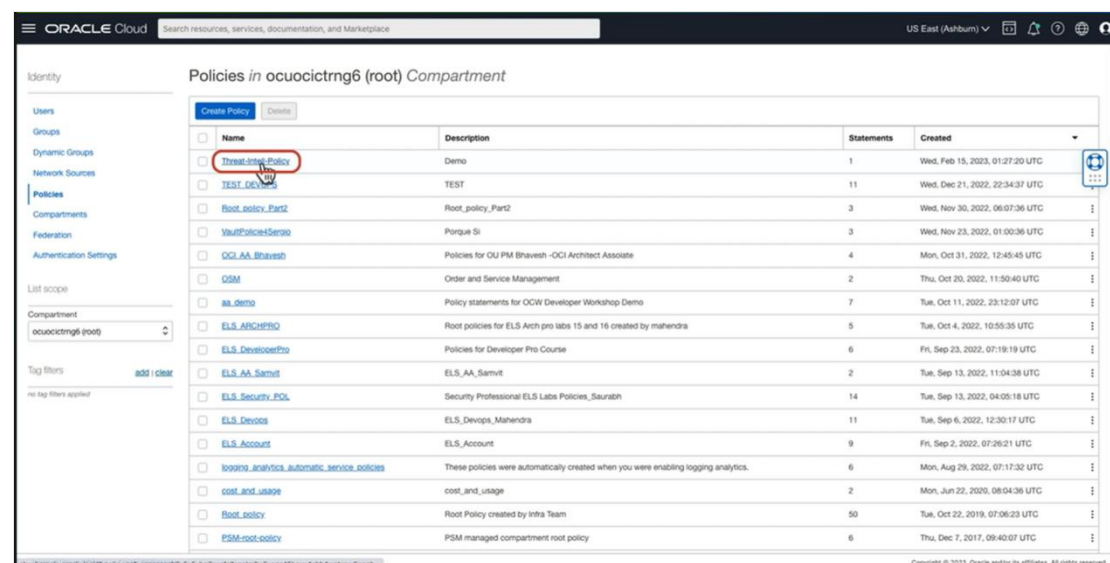
STEP 2 :- Click on the Identity & Security



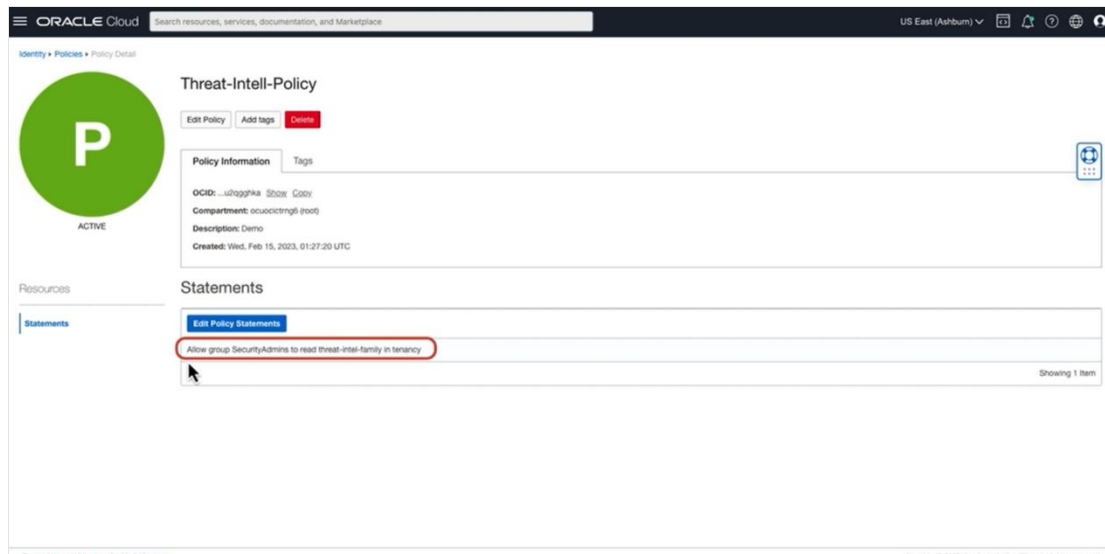
STEP 3 :- Click on the Policies



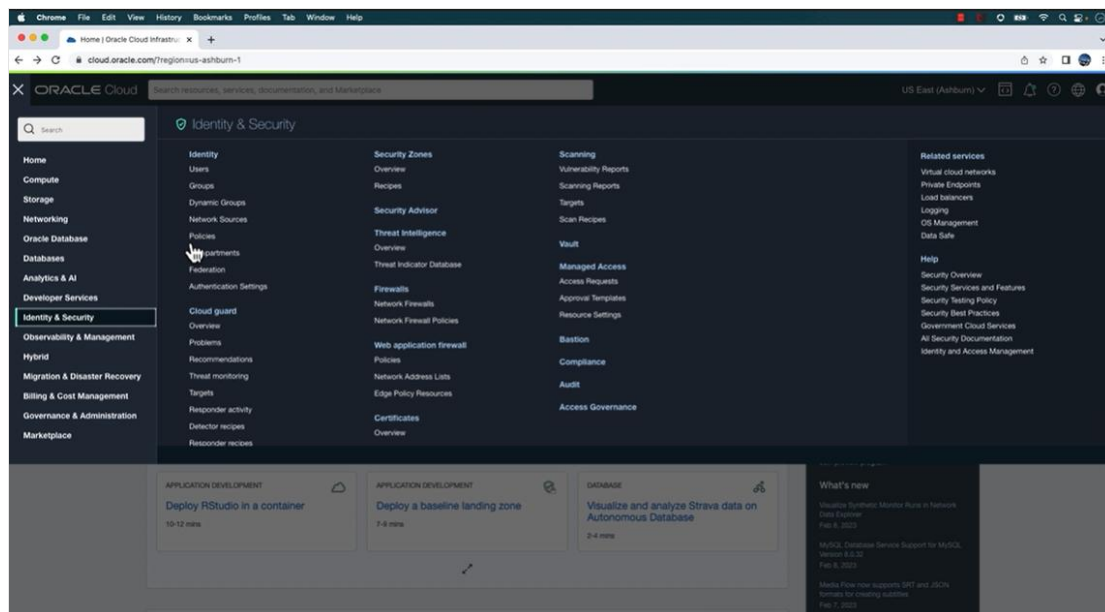
STEP 4 :- We need to check that we have the following policy to use the threat Intelligence database
Click on the “ Threat-intell-policy”



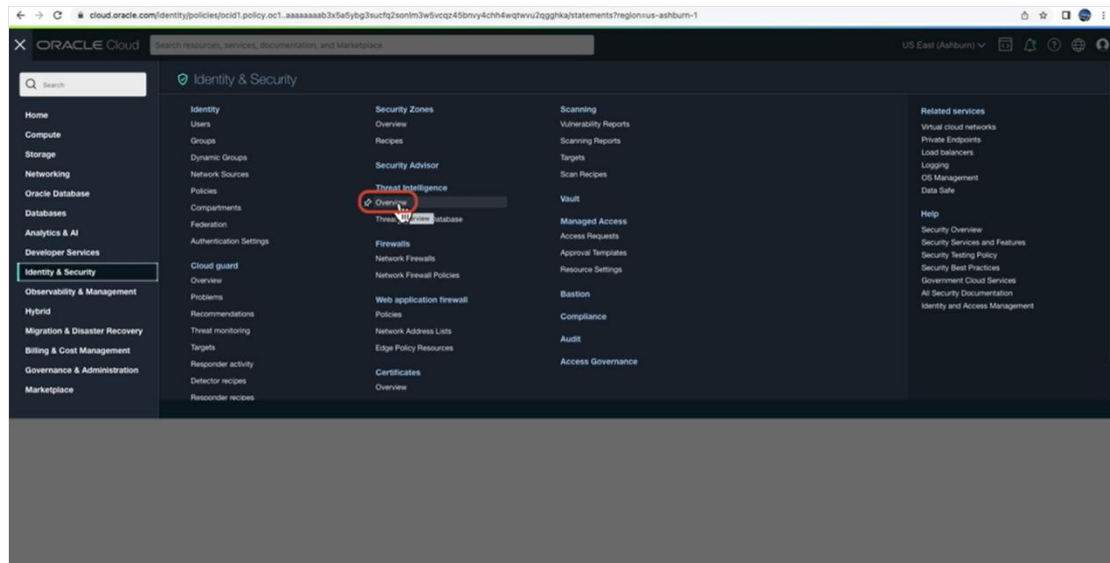
STEP 5 :- Allow group SecurityAdmins to read threat-intel-family in tenancy



STEP 6 :- Now we can move ahead to check the Threat Intelligence Database, go to the Identity & Security

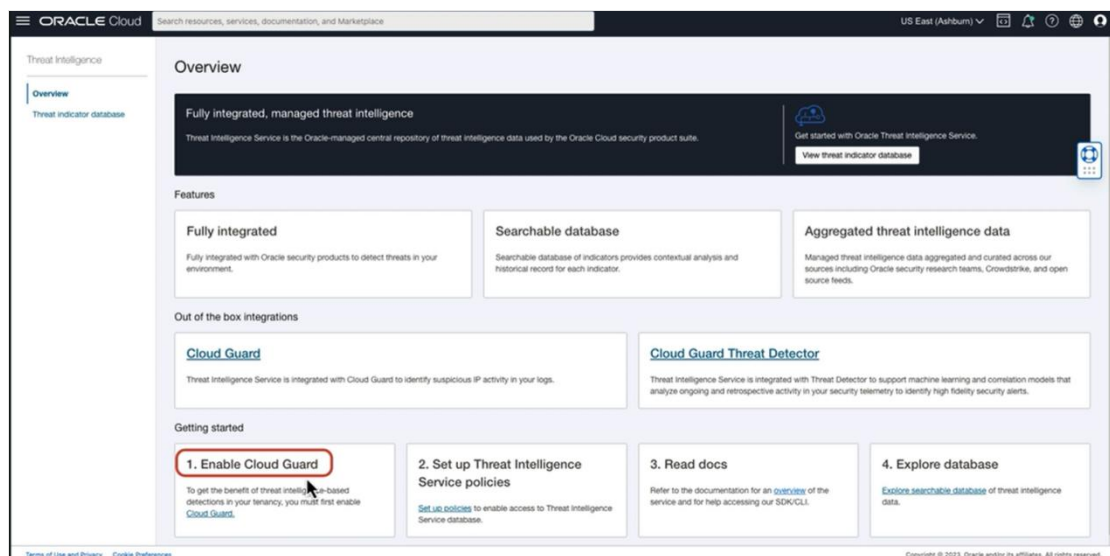


STEP 7 :- Under Threat Intelligence click on the Overview



STEP 8 :- Check the requirements

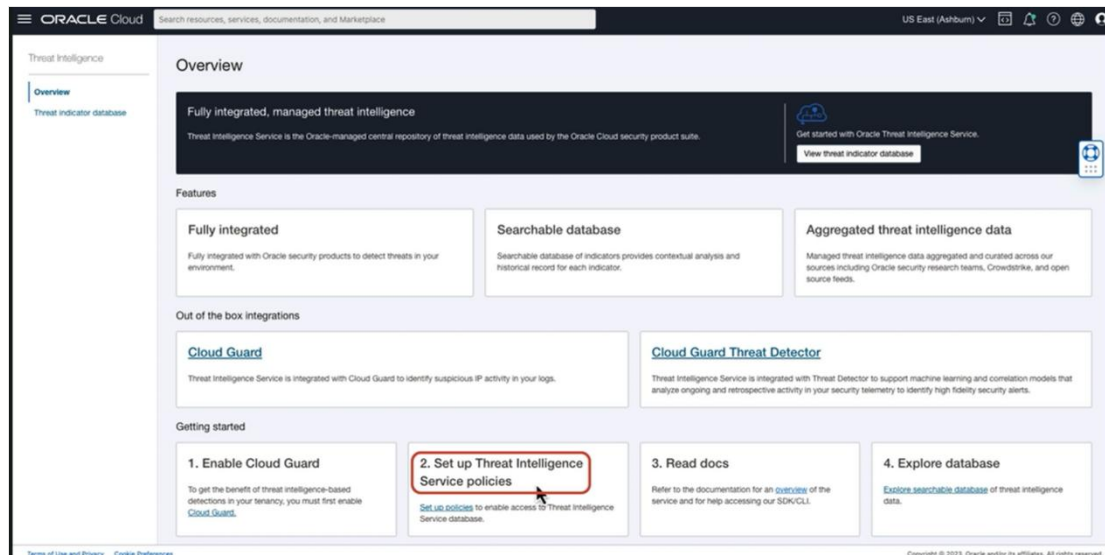
1. First we need to enable cloud guard for that please refer to the cloud guard documentation



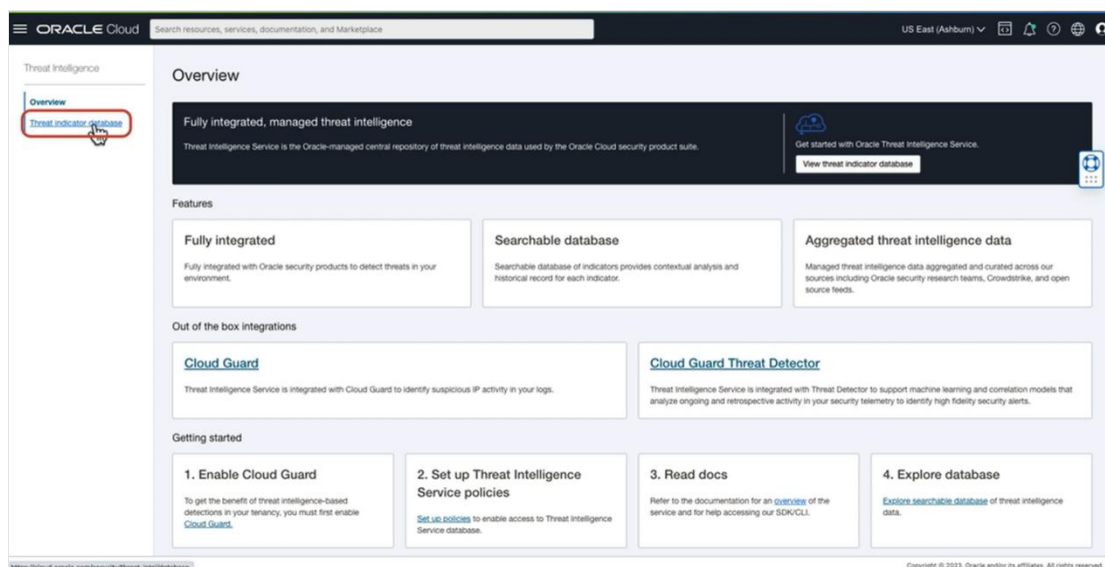
STEP 9:- 2. Set up Threat intelligence Service Policy which we already checked

3. Read docs

4. Explore Database



STEP 10 :- Now click on the threat intelligence database



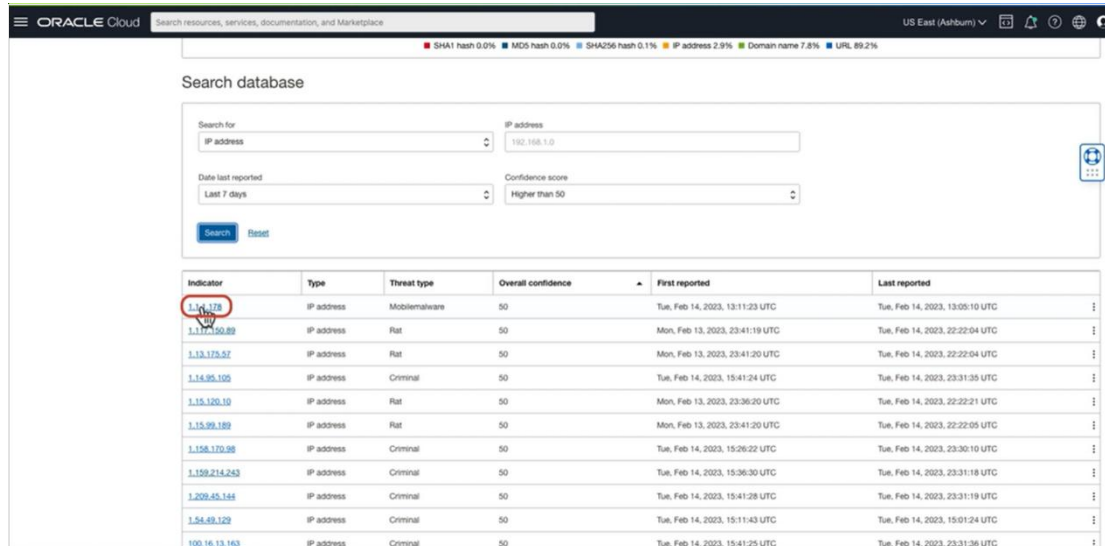
STEP 11 :- Now here we can search according to our requirements
Search for, Date last reported, Confidence score

The screenshot shows the Oracle Cloud Threat Intelligence Threat indicator database search interface. The top navigation bar includes the Oracle Cloud logo, a search bar, and the region 'US East (Ashburn)'. The left sidebar shows 'Threat Intelligence' with 'Overview' and 'Threat indicator database' options. The main content area is titled 'Threat indicator database' and includes a description of the database. Below this is a horizontal bar chart titled 'Indicator types across database' showing the distribution of indicator types: SHA1 hash (0.0%), MD5 hash (0.0%), SHA256 hash (0.1%), IP address (2.9%), Domain name (7.8%), and URL (89.2%). A red box highlights the 'Search database' button. Below the button is a search form with a 'Search for' dropdown menu (set to 'Please select an option'), a 'Date last reported' dropdown menu (set to 'Last 30 days'), and a 'Confidence score' dropdown menu (set to 'Higher than 50'). There are 'Search' and 'Reset' buttons at the bottom of the form.

STEP 12 :- Fill the details according to the requirement

The screenshot shows the Oracle Cloud Threat Intelligence Threat indicator database search interface with the search dropdown menu open. The dropdown menu lists the following options: Domain name, File name, IP address, Malware, MD5 hash, SHA1 hash, SHA256 hash, and Threat actor. The 'Domain name' option is highlighted with a red box. The search form also includes a 'Date last reported' dropdown menu (set to 'Last 30 days') and a 'Confidence score' dropdown menu (set to 'Higher than 50'). There are 'Search' and 'Reset' buttons at the bottom of the form.

STEP 13 :- Click on the Search, all the data will show up



Search database

Search for: IP address 192.168.1.0

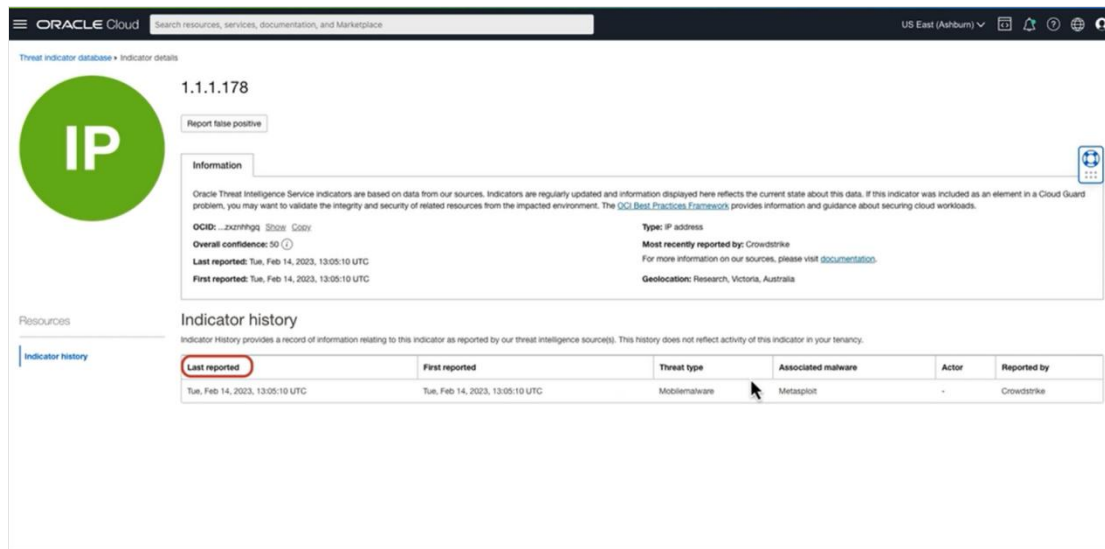
Data last reported: Last 7 days

Confidence score: Higher than 50

Search Reset

Indicator	Type	Threat type	Overall confidence	First reported	Last reported
1.1.1.178	IP address	Mobilemalware	50	Tue, Feb 14, 2023, 13:11:23 UTC	Tue, Feb 14, 2023, 13:05:10 UTC
1.1.1.150.89	IP address	Rat	50	Mon, Feb 13, 2023, 23:41:19 UTC	Tue, Feb 14, 2023, 22:22:04 UTC
1.13.175.57	IP address	Rat	50	Mon, Feb 13, 2023, 23:41:20 UTC	Tue, Feb 14, 2023, 22:22:04 UTC
1.14.95.105	IP address	Criminal	50	Tue, Feb 14, 2023, 15:41:24 UTC	Tue, Feb 14, 2023, 23:31:35 UTC
1.15.120.10	IP address	Rat	50	Mon, Feb 13, 2023, 23:36:20 UTC	Tue, Feb 14, 2023, 22:22:21 UTC
1.15.99.189	IP address	Rat	50	Mon, Feb 13, 2023, 23:41:20 UTC	Tue, Feb 14, 2023, 22:22:05 UTC
1.158.170.98	IP address	Criminal	50	Tue, Feb 14, 2023, 15:26:22 UTC	Tue, Feb 14, 2023, 23:30:10 UTC
1.159.214.243	IP address	Criminal	50	Tue, Feb 14, 2023, 15:36:30 UTC	Tue, Feb 14, 2023, 23:31:18 UTC
1.209.45.144	IP address	Criminal	50	Tue, Feb 14, 2023, 15:41:28 UTC	Tue, Feb 14, 2023, 23:31:19 UTC
1.54.49.129	IP address	Criminal	50	Tue, Feb 14, 2023, 15:11:43 UTC	Tue, Feb 14, 2023, 15:01:24 UTC
100.16.13.160	IP address	Criminal	50	Tue, Feb 14, 2023, 15:41:25 UTC	Tue, Feb 14, 2023, 23:31:36 UTC

STEP 14 :- click on the required data there you can see
Last reported date, First reported date, Threat type, Associated malware, reported by, overall Confidence score



Threat indicator database • Indicator details

1.1.1.178

Report false positive

Information

Oracle Threat Intelligence Service indicators are based on data from our sources. Indicators are regularly updated and information displayed here reflects the current state about this data. If this indicator was included as an element in a Cloud Guard problem, you may want to validate the integrity and security of related resources from the impacted environment. The [OCI Best Practices Framework](#) provides information and guidance about securing cloud workloads.

OCID: ...zcxrhngs Show Copy

Overall confidence: 50

Last reported: Tue, Feb 14, 2023, 13:05:10 UTC

First reported: Tue, Feb 14, 2023, 13:05:10 UTC

Type: IP address

Most recently reported by: CrowdStrike

For more information on our sources, please visit [documentation](#).

Geolocation: Research, Victoria, Australia

Resources

Indicator history

Indicator history provides a record of information relating to this indicator as reported by our threat intelligence source(s). This history does not reflect activity of this indicator in your tenancy.

Last reported	First reported	Threat type	Associated malware	Actor	Reported by
Tue, Feb 14, 2023, 13:05:10 UTC	Tue, Feb 14, 2023, 13:05:10 UTC	Mobilemalware	Metasploit	-	CrowdStrike

- **Last reported date:** The most recent date when information about a threat was provided.
- **First reported date:** The initial date when information about a threat was disclosed.
- **Threat type:** The category or classification of the threat (e.g., malware, phishing, DDoS).
- **Associated malware:** Any malicious software linked to the threat.
- **Reported by:** The entity or source that reported the threat information.
- **Overall Confidence score:** A measure indicating the reliability or certainty of the reported threat information.

